Федеральное государственное бюджетное образовательное учреждение
высшего образования "МИРЭА – Российский технологический университет"

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

Диссертация на соискание учёной степени
доктора технических наук

Научный консультант:
доктор технических наук, профессор
Никульчев Евгений Витальевич

Москва — 2024

Оглавление

Стр.

Стр.

Стр.

Стр.

Введение

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.

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 (ОВС) 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 сервисов ОВС, так как помимо классической задачи управления доступом необходимо учитывать особенности реализации учебного процесса на основе распределенных информационных систем. Частично это можно учесть за счет использования ролевых и атрибутивных моделей, но комплексно проблему можно решать на базе риск-ориентированного атрибутивного управления доступом. Это позволяет рассматривать задачу управления доступом в ОВС как задачу, требующую проведения специализированных теоретических и практических исследований с целью создания моделей и методов управления доступом, направленных на решение задач обеспечения безопасности доступа при максимальной доступности услуг.

Для гранулярного управления доступом и организации противодействия деятельности злоумышленников в гетерогенных, распределенных системах возникла необходимость найти 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 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.

Анализ международных стандартов позволяет выделить специализированные задачи, связанные с организацией управления доступом и анализа рисков. В разделе A.9 ISO/IEC 27001:2022 ("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. COBIT 2019 ("Control Objectives for Information and Related Technologies") – комплексный набор рекомендаций и практик по управлению информационными технологиями. В разделе APO12 "Managed Security

Services" отражены руководства по управлению доступом, включая установление политик и процедур, идентификацию и аутентификацию, авторизацию и аудит. 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. В ANSI INCITS 359-2004 ("Role-Based Access Control (RBAC)") определена модель управления доступом, использующая для определения прав доступа роли. В этой модели представлены спецификации и указания для ее реализации, методы для разработки и ее внедрения. 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 рекомендации по управлению рисками информационной безопасности, связанными с предоставлением доступа. В документе ISO/IEC 31000:2018 ("Risk management – Guidelines") сформулированы основные положения, руководства и рекомендации по управлению рисками, предоставляет методологию для систематической оценки рисков и принятия решений, связанных с управлением доступом. NIST SP 800-30 Rev. 1 ("Guide for Conducting Risk Assessments") включает описание методов и способов идентификации и оценки рисков, связанных с управлением доступом. В стандарте ISO/IEC 27001:2022 ("Information technology – Security techniques – Information security management systems – Requirements") представлены требования к системам управления информационной безопасностью, положения о риске и риск-ориентированном подходе, связанны с управлением доступом. 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 анализа рисков в отечественных стандартах и документах. ГОСТ Р ИСО/МЭК 27005-2018 "Информационная технология. Методы управления рисками информационной безопасности" является аналогом стандарта ISO/IEC 27005:2018. В нем установлены основные положения управления рисками информационной безопасности, в т.ч. управление рисками, связанными с управлением доступом. ГОСТ Р 54818-2011 "Система стандартов по информационной безопасности. Риск-ориентированный подход" устанавливает основные положения, принципы и требования к риск-ориентированному подходу в области информационной безопасности. ГОСТ Р ИСО/МЭК 27001-2013 "Информационная технология. Методы управления информационной безопасностью" – это принятый в Российской Федерации аналог стандарта ISO/IEC 27001:2022, который определяет основные требования к системам, управляющим информационной безопасностью, "Методические рекомендации по принципам информационной безопасности государственных информационных систем" ФСТЭК России включают рекомендации по управлению рисками для государственных информационных систем. В документе "Управление рисками информационной безопасности" (Росстандарт) представлены рекомендации по управлению рисками, связанными с управлением доступом к информационным системам. Руководство "О мерах по управлению рисками информационной безопасности" (ФСБ России) включает в себя еще и вопросы управления рисками, связанные с управлением доступом к информационным ресурсам. Методики и указания для измерения управляемости системы управления информационной безопасностью содержатся В ГОСТ Р 53235-2008 "Система менеджмента информационной безопасности. Измерения управляемости". ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Технологии информационной безопасности. Управление информационной безопасностью" (является аналогом ISO/IEC 13335-1:2004) включает рекомендации по оценке и управлению рисками информационной безопасности, в том числе связанными с управлением доступом. Инструктивное письмо ФСТЭК России № 17/15 от 31.05.2021 г. "Методические рекомендации по реализации системы информационной безопасности Федерального органа исполнительной власти" содержит методические рекомендации по реализации системы ин-

формационной безопасности в Федеральном органе исполнительной власти, в т. ч. вопросы управления доступом и рисками. Приказ ФСТЭК России от 18.03.2019 № 32 "Об утверждении Порядка формирования и ведения отчетности о состоянии защищенности информационных систем персональных данных" определяет порядок формирования и ведения отчетности о состоянии названных систем, включая отчетность о риске и управлении доступом. 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 управления доступом. ГОСТ Р ИСО/МЭК 27004-2019 "Информационная технология. Методы оценки и измерения эффективности управления информационной безопасностью" определяет методы оценки и измерения эффективности управления информационной безопасностью. Методические рекомендации ФСТЭК России "Требования к анализу угроз безопасности информации и определению рисков" предоставляют инструкции и рекомендации по проведению анализа угроз безопасности информации и определению рисков. Включает аспекты управления рисками и управления доступом. Описывает основные шаги процесса оценки эффективности, включая определение целей и контекста оценки, выбор методов оценки, сбор и анализ данных, оценку результатов и разработку плана улучшения. Оценка эффективности управления рисками и управления доступом помогает организации определить, насколько успешно реализованы принятые меры в области информационной безопасности, а также выявить области, требующие улучшений или дополнительных мер безопасности. Практические рекомендации для обеспечения безопасности информации содержатся в ГОСТ Р ИСО/МЭК 27002-2017 "Информационная технология. Методы контроля безопасности. Практическое руководство", который является аналогом ISO/IEC 27002:2013. Включает рекомендации по управлению рисками, связанными с управлением доступом. Руководство ФСБ России "Методологические указания к проведению оценки угроз безопасности информации" предоставляет методологические указания по проведению оценки угроз безопасности информации. Включает аспекты управления рисками, связанными с управлением доступом и анализом угроз. ГОСТ Р 56089-2014 "Информационные технологии. Моделирование процессов управления рисками в информационных технологиях" определяет требования и правила для моделирования процессов управления

рисками информационных технологий. Методические рекомендации ФСТЭК России "О реализации требований Федерального закона "О персональных данных" в сфере информационной безопасности" предоставляют рекомендации по реализации требований Федерального закона "О персональных данных" с учетом аспектов управления рисками и управления доступом к персональным данным.

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.

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.).

Также ведутся активные исследования по разработке моделей и методов количественной оценки риска реализации угроз информационной безопасности. Среди наиболее значимых работ следует отметить работы 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.

Исходя из анализа представленных нормативно-правовых актов и документов возможно сделать вывод о необходимости доработки существующих механизмов управления доступом, поскольку большинство из них использует устаревшие мандатные и ролевые модели. 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.

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

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 до-

ступом 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.

Основные 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.

Реализация результатов. 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 исследования 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 были также 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 49 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.

Глава 1. Исследования в области управления доступом в распределенных информационных системах

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

1.1 Анализ состояния защищенности распределенных информационных систем

В современном цифровом мире, где технологии проникают во все сферы информационного взаимодействия, вопросы информационной безопасности становятся более актуальными и сложными. Современные киберугрозы несравненно более сложны и хитры, чем когда-либо прежде, и эволюционируют с высокой скоростью. Примером могут служить фишинговые атаки, при которых злоумышленники маскируются под доверенные источники, чтобы обмануть пользователей и получить доступ к их учетным данным. Недавние случаи компьютерных атак типа Ransomware, такие как WannaCry, демонстрируют разрушительные последствия вследствие того, что подвергшиеся атаке организации не обеспечили соответствующую адекватную защиту информационных ресурсов.

Специалистами компании Positive Technologies во втором квартале 2023 отмечается рост на 10% целенаправленных атак по сравнению с первым кварталом, их доля составила 78% от общего числа зафиксированных атак. По словам специалистов, количество атак с использованием вирусов-шифровальщиков во втором квартале 2023 года в целом увеличилось на 13%. При этом на технологические компании пришлось 11% от общего количества жертв вымогателей, что на 5 процентных пунктов выше показателя предыдущего квартала. Также отмечается, что помимо свежих уязвимостей злоумышленники активно используют старые. Некоторые инциденты, по словам аналитиков, показывают,

что уязвимости могут подвергнуться атаке даже спустя несколько лет существования. Например, одними из самых эксплуатируемых уязвимостей стали CVE-2018-9995 в DVR-устройствах (Digital Video Recorder) компании TBK и CVE-2016-20016 (Common Vulnerabilities and Exposures) цифровых видеорегистраторов MVPower, обнаруженные в 2016 и 2018 годах соответственно. Таким образом старые и уязвимые устройства легко могут подвергнуться атакам даже спустя несколько лет после создания эксплойтов. Данный факт свидетельствует о необходимости комплексного подхода к осуществлению защитных мер в области информационной безопасности [1].

Кибератаки не только угрожают безопасности данных, но и могут привести к серьезным экономическим убыткам. Например, атака на банковскую систему может вызвать финансовый кризис, а компрометация данных компании может привести к потере клиентов и репутации. Крупные корпорации, такие как Target и Equifax, стали жертвами атак, которые обошлись им миллиардами долларов. Успешно проведенные атаки на образовательные учреждения могут полностью парализовать их работу, привести к срыву учебного процесса и привести в итоге к значительным финансовым убыткам [2].

Также следует отметить, что с ростом сложности информационных систем повышается уязвимость перед различными видами атак. Системы дистанционного образования, базирующиеся на распределенных информационных системах, эволюционировали на протяжении длительного времени, однако с точки зрения информационной безопасности следует отметить ряд важных рубежей. Этап становления условно можно отнести к 2000-м годам, когда появились платформы Blackboard и Moodle, предоставляющие базовые инструменты для удаленного обучения. Переход к виртуальным классам: разработка и внедрение веб-конференций, например, Zoom и Microsoft Teams, позволил проводить онлайн-обучение в режиме реального времени. Массовое распространение мобильных технологий: платформы Coursera и edX, позволило разработать мобильные приложения, которые предоставляют возможность удаленного доступа с мобильных устройств, обеспечивая гибкость функционирования системы дистанционного обучения.

Развитие угроз в области управления доступом в распределенных информационных системах дистанционного обучения обуславливается ростом объема данных: происходит увеличение числа студентов, курсов, устройств, с которых осуществляется доступ, что в свою очередь порождает новые

требования к защите как самих устройств доступа, так и распределенных информационных систем в целом. 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. Образовательные вычислительные сервисы (ОВС) характеризуются наличием требования к осуществлению требуемого уровня разнокатегорийного доступа (преподаватели, студенты, администраторы, административный персонал образовательных учреждений) к защищаемым ресурсам.

При организации доступа к таким системам необходимо осуществлять идентификацию и аутентификацию пользователей, управление доступом к ресурсам, контроль передачи и приема данных, а также обеспечивать целостность всей распределенной информационной системы [3; 4]. Не последнюю роль играют существующие уязвимости в программном обеспечении (ПО), обусловленные использованием устаревшего ПО или распределенных систем с отсутствующими критическими обновлениями безопасности, что, в свою очередь, может стать точкой входа для проведения кибератак и деструктивных действий злоумышленников. Несмотря на предпринимаемые меры по информированию и повышению компьютерной грамотности, методы социальной инженерии до сих пор успешно применяются. Так фишинговые атаки, осуществляемые посредством электронной почты, социальных сетей или средств мгновенного обмена сообщениями представляют угрозу как для студентов, так и преподавателей.

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 защиты является не только обеспечение безопасности доступа, но и повышение доступности ресурсов, что представляет собой 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 [5].

Лазовски и др. представили подход к управлению доступом, используемый в компьютерных средах, которые являются открытыми, распределенными, гетерогенными и сетевыми. Он охватывает и совершенствует традиционные модели управления доступом, доверием и цифровыми правами (DRM, Digital Rights Management), а его основными преимуществами являются изменчивость атрибутов и непрерывность оценки решений о доступе. Создание представленного подхода позволило перейти к разработке вычислительных систем с учетом новых требований безопасности [6].

Дитер и Наньянг в своих исследованиях представили режимы аутентификации пользователей и способы их развертывания, протоколы веб-аутентификации и методы перехода от аутентификации к протоколам авторизации и формализации свойств аутентификации для систем управления доступом. Акцент осуществлялся на ведении и сохранении аудиторских отчетов и логировании событий безопасности. Указанные особенности обусловлены тем, что правила конфиденциальности могут налагать ограничения на документирование событий, а существование зарегистрированных событий может свести к минимуму нарушения конфиденциальности [7].

Н. Мехра и др. описали основные проблемы безопасности распределенных информационных систем, построенных по принципу облачных архитектур. Авторы указали на необходимость многочисленных изменений в существующих технологиях обеспечения безопасности для достижения защищенности при использовании преимуществ облачных вычислений [8]. Поскольку построение современных инфраструктур ОВС вуза основано на облачных технологиях, данное исследование наиболее полно отражает существующие проблемы в системах и методах управления доступом. Основные проблемы представлены в таблице 1.

С.Сингх и П.Верма представили общие принципы распределенных брандмауэров, их параметры, принципы действия, описали адаптируемость к распространенным интернет-угрозам, также разъяснив, как распределенный брандмауэр обеспечивает полную защиту сети [9].

Чжэнтао Лю и другие представили обзор системных требований, позволяющих осуществлять управление доступом: традиционные модели, модели управления доступом для сервисов и систем в сети Интернет и модели управления доступом в среде облачных вычислений, которые возможно адаптировать

для применения в ОВС вуза. Для адаптирования к разнообразным приложениям и сервисам, применяемым в современных ОВС, традиционная модель требует все большей модернизации, для чего предлагается интегрировать технологию шифрования управления доступом и семантическую технологию для обеспечения более надежной и защищенной информационной поддержки [10].

Таблица 1 — Существующие проблемные аспекты в системах и методах управления доступом распределенных информационных систем

Угроза	Влияние	Решение
Утечка данных	Данные компрометируются автоматически, если пользователь утерял/ разгласил свой ключ шифрования	Разработка политики безопасности и обеспечение шифрования данных. Возможно проведение оценки уязвимости
Потеря данных	Из-за несовершенства политики безопасности пользователь может утратить личные данные	Применение сквозного шифрования для защиты данных
Захват учетной записи или сервиса	Один из пользователей получает доступ к данным другого пользователя, паролю или учетной информации	Реализация методов управления доступом, применения политик безопасности и аутентификации
Небезопасные интерфейсы и API (Application Programming Interface)	Используемые API и программные интерфейсы для защиты данных между пользователями и поставщиками	Мониторинг и защита программных интерфейсов посредством аутентификации и шифрование
Отказ в обслуживании	Замедление работы системных ресурсов для увеличения времени отклика	Реализация системы контроля и мониторинга используемых сервисов
Внутренний нарушитель (инсайдер)	Функционирует при условии наличия ошибок в политике безопасности	Применение методов управления доступом и политиками безопасности
Злоупотребление облачными сервисами	Совместное использование сервисов позволяет злоумышленникам получать информацию	Использование более сложных механизмов регистрации и аутентификации
Нарушение установленных правил использования	Наличие уязвимостей в используемых облачных сервисах и ПО	Применение средств и технологий анализа уязвимостей
Уязвимости технологий виртуализации	Совместное использование облачной платформы не обеспечивает изолированность между экземплярами ПО	Методы анализа защищенности технологий виртуализации, повышение изолированности экземпляров приложений

K. Kaур и A. Kaур представили подробное исследование виртуальных частных сетей (VPN, Virtual Private Network). VPN защищает частную сеть, используя шифрование и некоторые другие методы аутентификации, чтобы гарантировать доступ к устройству только легитимным пользователям [11]. Альхвайти и др. представили метамодель, которая является достаточно универсальной, чтобы включить все текущие модели управления доступом, а также

предоставляет организациям механизмы переключения с одной модели управления доступом на другую [12]. Традиционные модели управления доступом основаны на нескольких элементах управления доступом в форме именованных сущностей (субъекта, объекта и процесса), определенных правилами. Определены ресурсы (объект), которые могут быть достигнуты каждым субъектом доступа, и действия (процесс), которые ему разрешено выполнять [13].

Политика дискреционного управления доступом (DAC, Discretionary access control) означает, что в этой форме управления доступом у каждого объекта есть владелец. Владелец предоставляет доступ к ресурсам другим пользователям и/или группам (объектам). Способ использования прав доступа в данном контексте представлен следующим образом: матрица определяет всю политику устройства, относящуюся к интересам отдельных пользователей. Существует два способа применения матрицы [14]:

1. Система предоставляет права объектам или субъектам: либо объект хранит столбец матрицы, либо субъект хранит строку матрицы. В строке матрицы содержатся права использования определенного объекта.
2. Матрицы возможностей используются для хранения прав наряду с субъектами, они обрабатывают биометрические данные, так что доступ может быть реализован в любой операционной системе. Контрольные списки используются для управления произвольным доступом. Модель (DAC) позволяет пользователям вносить изменения в стратегию доступа.

Политика мандатного управления доступом (MAC, Mandatory access control) означает, что решения о политике управления доступом принимает центральный орган, а не единоличный владелец объекта, и владелец не может изменить право доступа. Этот механизм предназначен для безопасного многоуровневого управления доступом. Он определяет иерархию уровней безопасности. Политика безопасности описывает правила, которые управляют предоставлением доступа. Модель успешно решает проблемы защиты от вредоносного программного обеспечения типа "троянский конь" (троянская программа) в модели DAC [15].

Управление доступом на основе ролей требует контроля над пользователями, четкого выбора ролей для пользователей, набора ресурсов и системы разрешений на доступ. Суть этого управления – инкапсуляция всех возможных прав доступа в соответствии с ролями. Задание конкретной роли для

пользователя определяет наличие у него доступа к ресурсам, которые у него есть, и они находятся в пределах этой роли [16]. Ролевое управление доступом (RBAC, Role-Based Access Control) дает возможность установить полностью автоматизированное управление доступом путем разделения прав доступа субъектов. Модель RBAC многоступенчата: сначала выполняется авторизация на подключение к ролям, а затем устанавливается пользовательская функция. Авторизация пользователя для доступа к сервисам (объектам) осуществляется на основе роли пользователя [17].

В модели доступа на основе атрибутов (ABAC, Attribute-Based Access Control) осуществляется шифрование данных с помощью набора атрибутов, а каждому клиенту присваивается ключ, сгенерированный из заданных клиентом атрибутов. Клиент может использовать контент, если он способен использовать его атрибуты для расшифровки правил доступа к информации, найденных либо в ключе расшифровки, либо в зашифрованном тексте [18]. Модель ABAC решает проблемы традиционной модели управления с крупномасштабным динамическим увеличением числа пользователей и ненужной грубой детализацией концепции управления доступом. Она адаптируется к открытым и разнообразным технологиям Интернета и демонстрирует замечательную расширяемость и универсальность. Работа над моделью ABAC сосредоточена в основном на надежных атрибутах ABAC, определении и семантической совместимости методов ABAC, анализе и устранении конфликтов методов, которые формализовали модель ABAC при взаимодействии между атрибутами и стратегической защитой [19].

Модель управления доступом в среде облачных вычислений. Облачные вычисления представляют собой централизованную общедоступную инфраструктуру, управляемую поставщиком облачных услуг (CSP, Cloud Services Provider), где пользователям доступны объединенные ресурсы, обычно с оплатой по мере поступления. Облачные вычисления могут быть разделены на типы: платформа, предоставляемая как услуга (PaaS, Platform as a Service), ПО как услуга (SaaS, Software as a Service); инфраструктура как услуга (IaaS, Infrastructure as a Service) [20]. Системы управления доступом должны быть достаточно универсальными, чтобы фиксировать критерии для сложного доступа, основанного на атрибутах или учетных данных: ключевые соглашения об уровне обслуживания также должны быть способны фиксировать конкретные аспекты моделей управления. Поставщики облачных услуг, как правило, зара-

нее не знают своих пользователей, поэтому роли вряд ли могут быть назначены непосредственно пользователям. Соответственно, для повышения гибкости могут использоваться политики, основанные на квалификации или атрибутах. Утверждение безопасности языка разметки (SAML, Security Assertion Markup Language), расширяемого языка разметки для управления доступом (XACML, eXtensible Access Control Markup Language) и спецификации для веб-служб могут использоваться для определения правил безопасного доступа. Доступ на основе ролей является одним из нескольких предложенных методов.

Проведенный анализ существующих политик и систем управления доступом позволил сделать вывод о том, что система управления доступом на основе аттрибутов (ABAC) является наиболее приоритетной в силу универсальности в выявлении сложных критериев и реализации принципов минимальных привилегий и эффективного управления привилегиями [21]. Следует отметить, что также ABAC дает возможность управлять доступом для мобильных приложений, которые содержат динамические данные. Такие типы данных могут передаваться в мобильном приложении на сервер/базу данных с использованием интерфейса прикладного программирования API. Механизмы управления доступом используются для управления доступом (предоставление или отказ) к системных ресурсам или приложениям. Управление доступом на основе ролей (ABAC) является одним из наиболее распространенных механизмов; в ABAC пользователям назначаются роли, и каждое задание содержит различные утверждения, включающие правила, по которым операции и объекты могут быть доступны одному пользователю. Каждый отдельный пользователь ограничен одним списком, выделяемым за сеанс. Использование принципов RBAC на уровне мобильных устройств заключается в идентификации ресурсов по функциям. Пользователи будут вызывать API, в зависимости от времени и условий определяется комбинация пользователь/роль и принимается решение об осуществлении доступа [22].

Существующие подходы к управлению доступом не в полной мере адаптируются к решаемым задачам сервисов ОВС, базирующихся на распределенных информационных системах, так как в таких системах помимо классической задачи управления доступом необходимо учитывать особенности реализации учебного процесса на базе распределенных информационных систем. Частично это можно учесть за счет использования ролевых и атрибутивных моделей, но комплексно проблему можно решать на основе риск-ориентированного атрибу-

тивного управления доступом. Это позволяет рассматривать задачу управления доступом в ОВС, базирующихся на распределенных информационных системах, как задачу, требующую проведения специализированных теоретических и практических исследований в области управления доступом в распределенных информационных системах.

1.2 Анализ методов и моделей управления доступом в распределенных информационных системах

Методы управления доступом определяют набор политик, определяемых условиями, согласно которым пользователи получают доступ к ресурсам системы (всем или отдельным). Методы управления доступом используются на всех уровнях построения информационных систем и информационно-телекоммуникационной инфраструктуры, главным образом в операционных системах, базах данных, информационных системах и вычислительных сетях для защиты файлов, каталогов, посредством управления доступом к объектам, содержимому баз данных и информации, обрабатываемой в пользовательских приложениях. При этом первоочередной целью внедрения механизмов управления доступом остается выполнение разработанных политик доступа [23; 24].

В общем случае [25—27] модели и механизмы управления доступом определяются в терминах субъектов, объектов и прав доступа. Понятие субъекта обычно относится к пользователю или программе; понятие объекта соответствует тому объекту, к которому хочет получить доступ пользователь: к файлу, классу и т.д. При этом у субъекта может присутствовать или отсутствовать право доступа к этому объекту. Само наличие права доступа означает, что возможность субъекта выполнять операции над объектом (чтение, внесение изменений, выполнение и т.д.). Для управления выполнением операции следует определить права доступа или привилегии, создать модель и политику доступа.

Под моделью доступа понимается проекция области действия политики и необходимого поведения между субъектами и объектами. Политика доступа представляет собой набор рекомендаций, которые обобщаются, абстрагируются, формально или полуформально описываются [25]. Ресурсы данных защищаются в соответствии с различными политиками доступа. Для

обоснования используемой модели управления доступом необходимо провести сравнительный анализ существующих исследований в области разграничения и управления доступом.

Модель дискреционного управления доступом

Модель дискреционного управления доступом (DAC) была представлена Лэмпсоном в 60-х гг. прошлого века. Понятие "защита системы" в этой модели состоит из 3 основных составляющих – это набор объектов, набор доменов и матрица. Позднее модель, предложенную Лэмпсоном, дополнили Грэм и Деннинго, включив понятие предмета вместо домена. Далее модель была дополнена Харрисоном, Руццо и Ульманом (HRU, Harrison Ruzzo Ullman) с целью нахождения формального доказательства неразрешимости в общем случае задачи отслеживания распространения привилегий [25].

Модель DAC ориентирована на пользователя: владелец файла устанавливает разрешения на доступ к файлу для других пользователей [26]. Пользователи могут управлять правами доступа к своим файлам по умолчанию. Матрица управления доступом (ACM, Access Control Matrix), в которой указываются права субъектов на объекты, задает права доступа. Иначе реализовать управление доступом можно с помощью списков возможностей (CL, Control List) и списков управления доступом (ACL, Access Control List). При использовании списков возможностей права доступа пользователей хранятся в строках, а в списках управления доступам – в столбцах. Модели Lampson и Harrison Ruzzo Ullman (HRU) – это основные представители моделей дискреционного управления доступом [25].

Модель дискреционного управления доступом достаточно удобна для назначения прав доступа субъектов к объектам, однако, существуют ограничения, усложняющие обслуживание системы и контроль соблюдения принципов безопасности, поскольку пользователи управляют правами доступа к принадлежащим им объектам. Кроме того, возможны компьютерные атаки посредством использования троянских программ (троянов) [25; 27].

Совершенствованием подходов дискреционного доступа является разработка моделей мандатного управления доступом (MAC).

Модель мандатного управления доступом

В 1970-х годах была представлена защита с обязательным управлением доступом, включающая использование ядра безопасности. В 1987 году в IEEE Symposium of Security and Privacy была опубликована статья, в которой Кларк и

Уилсон представили принципиальные различия между коммерческими и военными требованиями безопасности, которые легли в основу разработки моделей мандатного управления доступом (MAC) [25]. В MAC пользователи не могут самостоятельно определять права доступа. Управление политикой доступа осуществляется централизованно.

В модели реализована концепция уровней безопасности для всех субъектов и объектов. В этой концепции определены доступы и возможные действия. Классы безопасности делятся на компоненты двух видов: иерархические и неиерархические. Для классификации субъектов и объектов по уровням доверия и чувствительности в иерархических компонентах выделяют типы: несекретный (U), конфиденциальный (C), секретный (S) и совершенно секретный (TS), где$TS \geqslant S \geqslant C \geqslant U$. Уровень безопасности объектов называют уровнем классификации, уровень безопасности субъектов – уровнем допуска. Неиерархический компонент определяется набором категорий. Метки безопасности соответствуют уровням безопасности при классификации объектов и допуска субъектов, применяют простое свойство безопасности и *-свойство безопасности. Наибольшее распространение получили модели: многоуровневой безопасности Bell и LaPadula (BLP) и модель BIBA, представляющие собой два класса модель мандатного управления доступом. Так в модели BLP субъекту разрешено читать объект, если его допуск "больше или равен" классификации объекта, и писать, если он "меньше или равен" [25—27].

Модель Белла-Лападулы (Bell-Lapadula Model, B-L) Модель Белла-Лападулы была предложена для обеспечения управления доступом в правительственных и военных структурах. Субъекты и объекты разделены на различные уровни безопасности (рис. 1.1). Субъект может получить доступ к объектам только на определенных уровнях, определяемых его уровнем безопасности. Следуют правилам запись/чтение [28]. Модель поддерживает обязательное управление доступом, определяя права доступа на основе уровней безопасности, связанных с субъектами и объектами. Каждый объект имеет различные права доступа, которые группируются по имени роли, а использование ресурсов ограничивается

В модели управления доступом на основе решетки (Lattice-based access control, LBAC) [29] для доступа субъекта к объекту используется специальная решетка доступа, которая включает в себя информацию об уровнях безопасности объектов и субъектов. Модель LBAC также известна как модель управления

доступом на основе меток (управления доступом на основе правил). В качестве решетки доступа выступает частично упорядоченное множество, в котором каждый объект и субъект имеют наибольшую нижнюю границу (соответствие) и наименьшую верхнюю границу (объединение) прав доступа. Для реализации доступа субъекта к объекту его уровень безопасности должен быть не ниже уровня безопасности объекта.

Модели MAC отличаются простотой и признаны лучшими для использования в коммерческих системах, функционирующих во враждебной среде, где достаточно велик риск атак [30]. Имеющиеся ограничения, например, зависимость от доверенных компонентов и необходимость перерабатывать программные средства для того, чтобы они соответствовали меткам и свойствам MAC, не позволяют использовать ее для сложных распределительных информационных систем. Кроме того, назначение системой уровней безопасности накладывает ограничения на действия пользователей, что препятствует динамическому изменению исходных политик, что не может быть применимо в ОВС вуза.

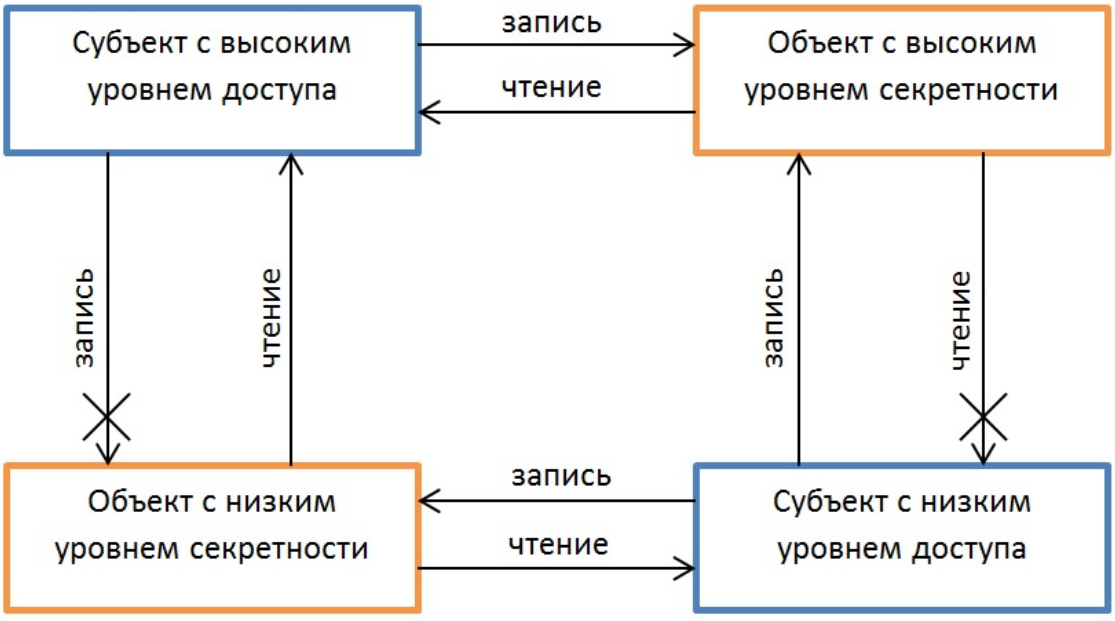


Рисунок 1.1 — Модель Белла-Лападулы

Дальнейшее развитие моделей управления доступа характеризуется появлением моделей управления доступом на основе идентичности пользователя (IBAC, Identity Based Access Control).

Модель управления доступом на основе идентичности пользователя

Модель IBAC – одна из первых моделей, предложенных в литературе для управления доступом и является наиболее простой [31]. Она вводит фундаментальные понятия субъекта, объекта и действия:

- субъект – это активный объект, который чаще всего относится к пользователю или приложению, выполняющемуся в интересах пользователя;
- объект – это пассивная сущность, которая относится к информации или ресурсу, к которому субъект может доступ к которой субъект может получить для выполнения действия;
- действие означает желаемый эффект при доступе субъекта к объекту (чтение, запись, изменение и т. д.).

Цель модели IBAC заключается в осуществлении управления любого прямого доступа субъектов к объектам посредством использования действий. Реализация управления основана на идентификации субъекта и объекта доступа. При этом в данной модели есть ограничения, поскольку при создании нового субъекта или нового объекта необходимо обновить политику авторизации, чтобы определить новые права, связанные с этим субъектом или объектом, что может быть громоздким, если количество субъектов велико. В то время как модель IBAC может предоставлять права только пользователям, представленным ее аппликативной учетной записью, она в первую очередь фокусируется на группировке субъектов на основе общих ролей.

С учетом преимуществ и недостатков моделей дискреционного, мандатного разграничения доступа, моделей управления доступом на основе идентичности пользователя разработана модель ролевого управления доступом или модель управления доступом на основе ролей (RBAC).

Модель управления доступом на основе ролей

Исходя из исторической практики, управление доступом на основе ролей (RBAC) определялось работой, выполняемой пользователем, которому назначается одна или более ролей для того, чтобы приписать ему определенные права доступа [25].

Модель RBAC является альтернативой моделям DAC и MAC. В модели RBAC каждому пользователю можно назначить более одной роли, а одна и та же роль может быть связана с разными пользователями [26]. Под ролью понимается набор разрешений на использование определенных объектов для

реализации рабочей функции, которая включает в себя ответственность и полномочия, возложенные на субъекта, например, роль директора, руководителя подразделения, инженера и т. д. Все роли ассоциированы с определенными привилегиями и разрешениями [25]. Целью модели RBAC является упрощение администрирования политики управления доступом. В основе модель RBAC лежат определенные сущности: пользователи, роли, разрешения, действия, операции и объекты. Каждой роли могут соответствовать несколько разрешений, в то же время одно разрешение может соответствовать нескольким ролям. Субъект может исполнять несколько ролей, а одна роль может быть связана с несколькими субъектами [27]. Существуют различные модели RBAC: плоская – $RBAC_0$, иерархическая $RBAC_1$, ограниченная $RBAC_2$, симметричная $RBAC_3$ [27; 32].

К достоинствам модели следует отнести возможность централизованно управлять соответствием субъектов и объектов ролям и правилам доступа, возможность использования в распределенных системах (т. к. основой служит система ограничений и согласованности) [27; 30]. Иерархия ролей в модели RBAC задает роли и разрешения для субъектов, основываясь на механизмах наследования прав. Иерархии ролей и механизмы наследования в моделях представлены в [33; 34]. Кроме того, в распределенных системах, где различные ресурсы распределены между пользователями, RBAC обладает мощными средствами спецификации решений управления доступом [35]. К недостаткам RBAC относятся: сложность настройки первоначальной ролевой структуры и отсутствие гибкости в современной ситуации стремительно изменяющихся инфраструктурных решений для информационных систем. Модель недостаточно хорошо поддерживает динамические атрибуты (например, время), которые часто могут быть обязательными при назначении прав пользователя [36]. В больших системах, где необходимы наследование ролей и настраиваемые привилегии, использование RBAC затруднительно из-за сложной процедуры администрирования [30].

Помимо RBAC альтернативными моделями для DAC и MAC являются модели управление доступом на основе представления (VBAC), управление доступом на основе задач (TBAC), модель безопасности взаимного сотрудничества (CBAC).

Одним из направлений дальнейшего развития RBAC является разработка модели управления доступом на основе представления (VBAC).

Модель управления доступом на основе представления

Управление доступом на основе представления (VBAC, View-Based Access Control) [37] расширяет RBAC, вводя представление статической, типизированной языковой конструкции для описания тонких прав доступа, которые являются правами по совершению операций над распределенными объектами. По сути, VBAC основан на классической модели матрицы доступа с ролями в качестве субъектов, а представления (view) – элементами матрицы. Представления на объекты назначаются принципалам, то есть отдельным субъектам или ролям, и принципал имеет доступ совершать операции с объектом, если у него есть представление на объект с правом на эту операцию. Принципал не имеет доступа, если операция явно запрещена в другом представлении на этот объект, доступном для роли, или если необходимых прав не найдено.

Помимо RBAC и VBAC альтернативными моделями для DAC и MAC являются модели управление доступом на основе задач (TBAC), безопасности взаимного сотрудничества (CBAC), командного управление доступом (TMAC), управления доступом на основе организации (OrBAC) и модель управления доступом на основе поведения (BBAC).

Модель управления доступом на основе задач

Управление доступом на основе задач (TBAC, Task-Based Access Control) – модель управления доступом, в которой реализация механизмов безопасности строится с точки зрения задач (действий) и обеспечения динамического управления доступом в реальном времени во время обработки задач [38; 39]. В данной модели управление доступом к объектам не статично, а меняется в зависимости от контекста выполнения задач, из чего можно сделать следующие выводы:

- данная модель рассматривается в среде рабочих процессов, в которых каждый шаг обработки данных связан с предыдущим, как и соответствующие решения о предоставлении доступа;
- различные политики управления доступом могут применяться в рамках одного рабочего процесса в зависимости от конкретной задачи;
- у каждой задачи присутствует конкретный срок исполнения, что говорит о том, что предоставленные права также имеют определенный срок действия, обусловленный задачей.

В рамках данной модели следует обозначить следующий набор терминов:

1. Набор прав – это права доступа, которые имеют члены набора доверенных лиц, когда им предоставляется шаг авторизации. Когда

инициализируется шаг авторизации, члену из набора доверенных лиц предоставляется шаг авторизации.

2. Задача – это логическая единица в рабочем процессе. Она представляет собой различимое действие, может быть связана с несколькими пользователями, а также может включать несколько подзадач. Например, процесс обработки заявки состоит из трех задач: подготовка, утверждение и согласование заявки. Задача имеет следующие характеристики:
   - она сохраняется в течение длительного периода времени;
   - она может включать несколько подзадач;
   - для выполнения подзадачи могут потребоваться разные люди.

TBAC следует двум принципам управления доступом:

- принцип наименьших привилегий. Во время выполнения задачи пользователю назначаются только необходимые права, а после того, как задача не выполняется или завершается, они снимаются с пользователя;
- принцип разделения обязанностей. Некоторые конфиденциальные задачи должны выполняться разными пользователями, например, процесс обработки заявок, когда сотрудники, занимающиеся подготовкой заявки и ее согласованием, должны быть разными.

Кроме того, TBAC поддерживает принцип абстракции данных. Например, набор прав не ограничивается типичными "чтение/запись/исполнение", а основывается на реальном рабочем процессе.

Модель безопасности взаимного сотрудничества

Модель безопасности взаимного сотрудничества (CBAC, Coalition Based Access Control) [40] основана на ассоциированном мультидомене, позволяет реализовать безопасный обмен информацией в распределенной среде с характеристикой динамического домена. В этой модели динамический домен обычно включает более двух организаций, которые составляют кооперационный альянс, и каждый член альянса может обмениваться информацией с другими членами альянса. Существенным недостатком модели является то, что она не может реализовать управление и обслуживание стратегии управления доступом в распределенных системах аутентификации и авторизации ввиду того, что в ней не определены связи между ролью и правами.

Очередным развитием модели мандатного управления доступа является модель командного управления доступом (TMAC).

Модель командного управления доступом

Командное управление доступом (TMAC, Team Based Access Control) было разработано в 1997 году как подход к применению ролевого управления доступом в средах с множеством рабочих пространств [41; 42]. Является вариацией модели RBAC. Совместная деятельность подразумевает работу в команде. Таким образом, центральное место в подходе TMAC занимает понятие "команда" как абстракция, которая включает в себя совокупность пользователей, выполняющих определенные роли с целью выполнения конкретной задачи или достижения цели. Это подразумевает под собой два ключевых требования к управлению доступом:

- масштабируемое назначение прав на основе ролей (как в RBAC) (R1);
- потребность в выдаче прав на уровне отдельных пользователей и объектов (R2).

RBAC [43], в свою очередь, не может быть использована для одновременного выполнения этих требований. Это связано с тем, что если обеспечить выполнение R1, то будет утеряна гибкость, необходимая для выполнения R2. Обеспечение выполнения R2 в отдельности не требует подхода RBAC, однако, в таком случае будут утеряны масштабируемость и удобство администрирования, которые дает RBAC. Таким образом, необходим такой подход к управлению доступом, при котором (R1) и (R2) могут выполняться одновременно.

В моделях RBAC единственной группой пользователей, распознаваемой моделью, является группа, принадлежащая к одной и той же роли. Именно это ограничение изначально привело к концепции команды как модели набора пользователей в различных ролях. Команда неявно несет в себе контекст сотрудничества, который содержит информацию об общей миссии и задаче, которую необходимо выполнить. С точки зрения управления доступом контекст совместной работы команды должен содержать две категории данных:

- пользовательский контекст (UC, User Context) – это пользователи, входящие в команду в разное время;
- объектный контекст (OC, Object Context) – это набор экземпляров объектов, которые необходимы команде пользователей для выполнения задачи.

Таким образом, при условии, что известна базовая структура команды с точки зрения ее ролей, то выполняется требование R1. Если известен контекст

сотрудничества, выполняется требование R2. Команда состоит из следующих элементов:

- название команды;
- набор пользователей (членов команды);
- набор ролей команды, определяющий роли, которые могут соответствовать набору пользователей;
- особенная роль (глава команды), глава команды может быть только один в каждый момент времени;
- набор типов объектов;
- набор экземпляров объектов;
- набор прав команды.

Основная идея TMAC заключается в использовании RBAC для определения набора прав для команд на основе ролей. Отдельные команды одной структуры (типа/класса) будут включать одно и то же подмножество ролей, и, следовательно, унаследуют одно и то же подмножество. Однако TMAC требует привязки прав для каждой команды к наборам членов команды и объектам во время выполнения, что позволит выдать права на уровне отдельных пользователей и объектов. Для сохранения управления доступом к отдельным объектам в разных командах, контекст объекта может передаваться от одной команды к другой (рис. 1.2).

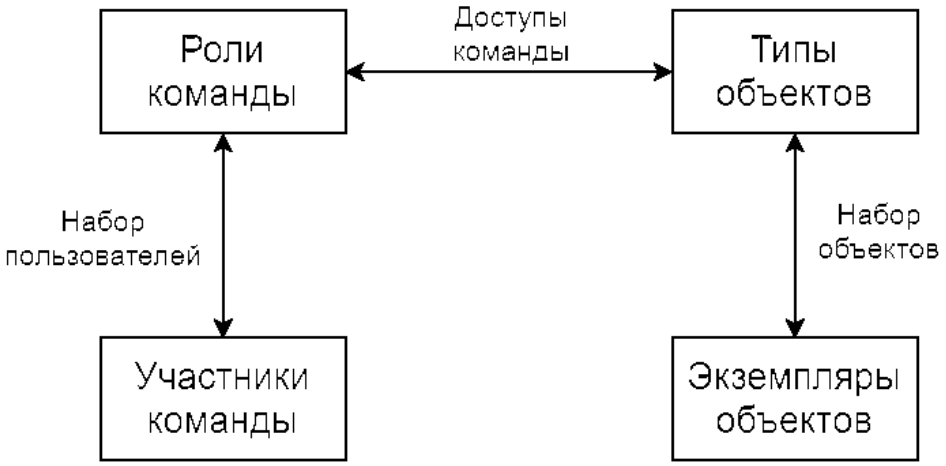


Рисунок 1.2 — Концепция TMAC

TMAC представляет собой модель управления доступом, которая сочетает в себе реализацию командного принципа управления доступом и обеспечение

выполнения задач в режиме одновременного множественного доступа. Достоинством TMAC является то, что она сочетает административные и модельные преимущества RBAC и при этом позволяет обеспечить дополнительный контроль предоставления доступа отдельным пользователям и объектам.

Для устранения недостатков приведенных ранее моделей управления доступом разработана модель управления доступом на основе организации (OrBAC).

Модель управления доступом на основе организации

Модель управления доступом на основе организации (OrBAC, Organization Based Access Control) была представлена в 2003 году. Целью модели управления доступом OrBAC является преодоление отдельных проблем предыдущих моделей (DAC, MAC и RBAC) для того, чтобы создать более абстрактную политику управления доступом. Модель OrBAC была создана для того, чтобы политика управления доступом определяла, какие субъекты имеют разрешение для определенного доступа к объектам. Любая организация (банк, больница, учебное заведение) можно представить в виде структурированной группы субъектов, которые обладают заданными ролями (сущностями). Модель OrBAC шире концепции только предоставления разрешений субъектам. Помимо этого в модели предусмотрена концепция запретов, обязательств и разрешений [27]. Каждая роль может иметь разрешение, запрет или обязательство осуществлять конкретную деятельность в заданном представлении при соответствующем контексте. Модель OrBAC предусматривает наличие 7 сущностей:

- на абстрактном (организационном) уровне – 3 сущности (роль, действие, вид);
- на конкретном уровне – 3 сущности (субъект, действие, объект);
- контекст – седьмая сущность, расположен между предыдущими уровнями. Служит для соответствия между элементами уровней. В модели управления доступом на основе организации выражает динамические правила связей между сущностями [27; 44].

Достоинство OrBAC заключается в устранении конфликтов между правилами безопасности, при этом данная модель управления доступом характеризуется наличием уязвимостей для проведения атак вида "применение скрытых каналов" [27]. Развитием OrBAC выступает модель управления доступом на основе поведения (BBAC).

Модель управления на основе поведения

Модель управления доступом на основе поведения (BBAC, Behavior Based Access Control) – модель безопасности, предоставляющая или запрещающая доступ к ресурсам на основе наблюдаемого поведения пользователей или субъектов. Она динамически адаптирует права в соответствии с действиями в реальном времени, повышая безопасность за счет оценки текущей деятельности и не полагаясь на статические политики [45].

Основные компоненты модели BBAC:

- субъекты (Subjects): пользователи, которые запрашивают доступ к ресурсам в системе;
- объекты (Objects): данные и/или ресурсы, нуждающиеся в защите. К ним запрашивается доступ;
- анализаторы поведения (Behavioral analyzers): компоненты программного обеспечения, фиксируют активность,исследуют с помощью собранных данных поведение субъектов;
- правила и политики доступа (Access rules and policies): правила, регламентирующие действия, которые могут выполнять субъекты и ресурсы, доступ к которым могут получить. На это влияет их поведение и прочие факторы;
- решение о доступе (Access decision): процесс принятия решения о предоставлении или отказе в доступе на основе результатов поведенческого анализа, правил и политик доступа.

Ключевые особенности BBAC:

- BBAC отслеживает поведение пользователей в режиме реального времени, что позволяет немедленно корректировать права доступа;
- система учитывает контекстную информацию, такую как время, местоположение и роли пользователей, чтобы принимать обоснованные решения о доступе;
- права доступа динамически изменяются в зависимости от меняющегося профиля риска, снижая вероятность несанкционированного доступа.

Варианты применения BBAC:

- BBAC может выявить аномальное поведение пользователя, например, несколько попыток входа в систему из разных мест в течение короткого времени. В этом случае доступ блокируется;

– в ситуации, когда пользователь запрашивает доступ к конфиденциальным данным из необычного места и/ или в нерабочее время, модель BBAC может применить дополнительные меры его аутентификации.

Модель BBAC – представляет собой гибкий и адаптивный подход к управлению доступом для обеспечения безопасности субъектов и объектов. Следующая модель предусматривает тематическое разграничение доступа.

Модель тематического разграничения доступа

Модель основана на применении решетки подмножеств тематических категорий и принципе иерархической классификации [46—49]. Схема модели – это структура в виде дерева, которая базируется на принципах таксономии. Тематика задается узлами классификатора, причем на объекты в подчиненных тематических узлах свойства распространяются автоматически.

Принципы модели:

– схема предметной области модели – это иерархический тематический рубрикатор, в который входит конечное множество рубрик. На этом множестве задан частичный порядок, соответствующий корневому дереву;
– сущности модели отображаются на мультирубрики, заданные на корневом дереве иерархического рубрикатора. Это реализуется с помощью функции тематического окрашивания, определяющей для каждой сущности в заданный момент времени мультирубрику, которая ей соответствует;
– работу системы сопровождает смена состояний. При этом появляются новые отношения доступа между субъектами и объектами доступа, субъекты и объекты появляются и удаляются. Смены состояний, при которых создаются новые объектов/субъектов, могут быть описаны также, как и смены состояний, которые вызываются доступами имеющихся субъектов к имеющимся объектам, и потоками (на чтение и на запись);
– смены состояний системы, вызванные запросами и осуществлением доступов субъектов к объектам, регламентирует монитор безопасности, действующий на основе свода правил;
– кроме потоков, вызываемых доступами типа "один субъект к одному объекту", в системе коллективного доступа могут также появляться потоки, соответствующие множественным доступам: "разные субъекты

одновременно к одному объекту", или "один субъект одновременно к разным объектам".

Информационная система, построенная на основе спецификаций модели тематико-иерархического разграничения доступа, функционирует в рамках требований безопасности тематической политики. Стоит отметить, что применение тематико-иерархической модели требует формирования решетки доступа и обновления в режиме реального времени спецификаций доступа, что не позволяет своевременно изменять правила доступа в зависимости от динамически изменяющихся во времени условий функционирования компонентов и средств защиты информационных систем. Следующий вид моделей – мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками уже не содержит ограничения и недостатки, присущие предыдущим моделям.

Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками

Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Линукс (далее МРОСЛ-ДП) [50] используется большинством отечественных разработчиков защищенных операционных систем (ОС). Данная модель применяется формально для реализации механизма управления доступом ввиду того, что модели устаревшего формата (например, модели RBAC и BBAC) не позволяет обеспечить требуемый уровень доверия к реализации механизма управления доступом. Актуальным является создание формальной модели, сочетающей мандатное и ролевое управления доступом. Примитивное соединение двух этих видов управления без учета их особенностей скорее всего отрицательно скажется на безопасности этого решения.

Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux (МРОСЛДП-модель) представляет собой комбинацию мандатного и ролевого управления доступом, а также контроля целостности Это обеспечивает через представление ролей в качестве сущностей-контейнеров возможность противостояния созданию нарушителем запрещенных информационных потоков по времени от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности.

При построении модели формируются следующие уровни:

– 1-й уровень – ролевое управление доступом;

– 2-й уровень – ролевое управление доступом и контроль целостности;
– 3-й уровень – ролевое управление доступом, контроль целостности и мандатное управление доступом с информационными потоками по памяти;
– 4-й уровень – ролевое управление доступом, контроль целостности, мандатное управление доступом с информационными потоками по памяти и по времени.

Нижние уровни представления модели соотносятся с абстрактной системой, элементы которой не зависят от новых элементов более высокого уровня. Более высокий уровень наследует, иногда вносит изменения или дополняет элементы более низкого уровня. Это дает возможность, включая новые элементы, соответствующие следующему рассматриваемому уровню, переходить к более сложным определениям и утверждениям модели.

Отличительной особенностью мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками является ее применение для обеспечения управления доступом в операционных системах, что не позволяет масштабировать данную модель до уровня распределенных информационных систем. Для устранения указанного недостатка могут применяться модели управления доступом на основе атрибутов (ABAC)

Модель управления доступом на основе атрибутов

Концепция управления доступом на основе атрибутов (ABAC, Attribute Based Access Control) схожа с моделью RBAC, при этом обладает преимуществами за счет возможности управлении авторизацией и поддержки динамических атрибутов. Главная идея ABAC – это разрешение/запрет на запросы субъектов, которое происходит, основываясь на определенных атрибутах субъектов и объектов [25; 36]. Указанная особенность позволяет осуществлять управление доступом, который допускает большее количество дискретных входов в решение о предоставлении доступа. Это, в свою очередь, обеспечивает более широкий набор возможных комбинаций переменных для отражения большего набора возможных правил политики управления доступом [33]. Модель ABAC нашла широкое применение в области коммерции, научных исследований, а также организаций, функционирующих на базе распределенных информационных систем в связи с наличием ограничений моделей RBAC, DAC, MAC и др. Два стандарта, в которых широко используется система ABAC, это: Extensible AC

Markup Language (XACML) и Next Generation AC (NGAC) с возможностями управления доступа для приложений [25].

Концепция ABAC подразумевает доступ субъектов к большему кругу объектов. При этом не важны отношения между субъектом и объектом. В модели предусмотрены атрибуты 3 типов: субъекта, объекта и окружающей среды. Атрибуты субъекта и объекта – общие для всех моделей ABAC. Атрибут окружающей среды существует в моделях, зависящих от наличия системных датчиков, обнаруживающих и сообщающих значения (например, актуальное точное время или дату). При всех своих достоинствах концепция ABAC имеет определенные ограничения [24]:

1. Сложность определения актуального набора разрешений, доступных всем субъектам.
2. Для реализации этой модели необходимо значительное время.
3. Отсутствие возможности вычислить набор субъектов, имеющих доступ к конкретному объекту.
4. Сложность эффективного вычисления итогового набора разрешений для конкретного пользователя, т. к. все объекты должны быть проверены на соответствие всем соответствующим политикам.

Проведенный анализ методов и моделей управления доступом позволил выявить существующие достоинства и недостатки рассмотренных моделей управления доступом и обосновать возможность применения моделей управления доступом на основе атрибутов, а также моделей управления доступом с использованием ролей при обеспечении информационной безопасности распределенных информационных систем. Перед разработкой модели управления доступа для ОВС вуза, которые строятся на распределенных информационных системах, следует проанализировать исследования количественной оценки риска.

1.3 Анализ исследований в области количественной оценки риска

В процессе анализа исследований, посвященных количественной оценке риска, рассмотрены научные исследования в области оценки риска безопасности для динамических моделей управления доступом. Джейсон предложил

рассматривать следующие элементы модели управления доступом на основе риска [51]: количественная оценка уровня риска, соответствующего каждому запросу на доступ; вычисление допустимой величины риска в конкретной области; управление обменом информацией, основываясь на известной величине риска и политике управления доступом. Другая идея заключалась в том, чтобы каждая система фокусировалась бы на рисках и придерживалась этого ориентира. Для этого предлагается придерживаться следующих положений:

1. Измерение риска. "Если неизвестен размер риска, то им невозможно управлять". В случае, когда факторы риска невозможно измерить, возможно, что их можно достоверно оценить и полученный опыт применять для вычисления оценок, все более и более точных. Этот процесс можно формализовать, например, с помощью обновляемой байесовской сети доверия.
2. Определение приемлемого уровня риска. Страна/организация/предприятие может позволить терять X секретных и Y совершенно секретных документов в год. Кроме того того может позволить себе вероятность Z, что определенный технический потенциал или источник будет скомпрометирован. Если установить значения $X, Y, Z, \ldots$ в точности равные нулю, то все операции прекратятся, потому что все операции связаны с ненулевым риском. Каковы же приемлемые диапазоны значений для X, Y, Z и длинного списка аналогичных параметров? Еще лучше сказать, какие примерно значения будут оптимизировать операционную эффективность в долгосрочной перспективе, когда сегодняшние нарушения безопасности покажутся не просто абстрактно вредными, а реально угрожающими будущей операционной эффективности?
3. Убедитесь, что информация распространяется вплоть до приемлемого уровня риска. Это очень важный момент. В организациях применяются системы, которые пытаются минимизировать риск. Это неправильная метрика! На самом деле необходимо максимизировать поток информации при условии, что общее ограничение не превышает допустимый уровень риска, установленный в соответствии с принципом 2, описанным выше. Это означает, что вместо минимизации риска необходимо обеспечить его увеличение до допустимого максимума (но не выше).

Модель Risk Adaptable Access Control (RAdAC) принадлежит авторству Макгроу [52]. Основой этой модели является оценка риска безопасности и потребностей для предоставления/отказа в доступе. Модель RAdAC сначала оценивает риск, который соответствует запросу на доступ, потом сопоставляет его с требованиями политики управления доступом. Далее проверяются операционные потребности. Если все требования удовлетворяются, то предоставляется доступ. Автор модели не предложил детальной процедуры количественной оценки риска и операционных потребностей. Другие авторы, например, в [53] разработали подход, определяющий компоненты риска в модели RAdAC, используя подход управления доступом на основе атрибутов.

Динамическая и гибкая модель управления доступом на основе рисков была предложена Диепом и другими [54]. Эта модель использует оценку риска для определения величины риска в соответствии с результатом действий с учетом принципов доступности, целостности и конфиденциальности. Представить модель ценности можно через отношение между элементами. Иначе сделать это можно, поставив в соответствие всем элементам числовые значения. Для учета и контекста, и величины риска применяется еще один метод. Существует множество факторов, которые влияют на процесс оценки риска. Для каждого действия значение риска зависит от результатов. Если стоимость результата (из-за действия) высока, то и риск высок. Риск также зависит от текущих параметров контекста. Например, в условиях низкой скорости интернет-соединения легко потерять сессию FTP-соединения, что, в свою очередь, чревато потерей доступности. Кроме того, наличие незащищенного беспроводного соединения позволяет повысить риск взлома системы, использующей такое соединение. Свойство ресурсов в действии также имеет важную роль в оценке риска. Однако в этой модели не было однозначного стандарта того, а были приведены абстрактные примеры, как оценивать величину риска для каждого состояния среды и для каждого результата действия, не использовался пользовательский контекст и отсутствовали функции адаптации к риску.

Модель, предложенная Хамхамметту и другими [55], основана на оценке чувствительности объекта, достоверности субъекта и разницы между чувствительностью объекта и достоверностью субъекта с помощью оценки риска. Также приведена серия примеров в качестве основы для разработки и определения свойств подходов к оценке угроз, которые обеспечивают поддержку качественной оценки угроз доступа субъекта к объекту. Однако в модели не

было указано, как оценить значение риска для каждой ситуации в среде. Кроме того, модель требует от системного администратора задавать разумное значение для каждого входного признака на ранней стадии процесса оценки риска, и в ней отсутствуют функции адаптации к риску.

В работе [56] предложена нечеткая модель управления доступом с многоуровневой безопасностью (MLS, Multilevel security) для управления рискованными информационными потоками на основе оценки их операционных потребностей, возможности риска и особенностей среды. Модель оценивает риск на основе разницы между уровнем безопасности субъекта и уровнем безопасности объекта. Аналогичным образом Ни, Бертино и Лобо [57] предложили модель управления доступом на основе риска, основанную на нечетких умозаключениях. Они показали, что нечеткие умозаключения являются хорошим подходом для оценки рисков безопасности доступа. Однако обе модели игнорировали прошлое поведение пользователей в процессе оценки рисков, не имели функций адаптации к рискам. Также применение указанных моделей для управления доступом порождает новые проблемы, влияние которых еще до конца не исследовано:

- во-первых, поскольку существует множество различных нечетких операций, необходимо выбрать те нечеткие операции, которые лучше всего соответствуют требованиям безопасности;
- во-вторых, управление доступом на основе рисков, хотя и улучшает поток информации и лучше удовлетворяет требованиям критически важных организаций, может привести к нанесению ущерба злоумышленниками до того, как будут приняты меры по смягчению последствий;
- в-третьих, масштабируемость системы управления доступом на основе нечеткого вывода сомнительна. Время, необходимое машине нечеткого вывода для оценки рисков, может быть довольно большим, особенно при наличии десятков параметров и сотен нечетких правил.

Нечеткая модель управления доступом на основе риска была предложена Ли, Баем и Заманом [58] для оценки риска доступа к медицинской информации. Метрика риска связана с чувствительностью данных, серьезностью действий и историей риска в виде нечеткого значения для определения соответствующего управления доступом к медицинской информации в облачных вычислениях. Однако данная модель не дает представления о том, как количественно оценить риск. Кроме того, не определены четкие границы риска и отсутствуют

функции адаптации к риску. Также использование данной модели может быть осложнено разностью типов информации в медицинской сфере и в сервисах высшего образования.

Шайх и др. [59] предложили динамический метод принятия решений на основе риска. Этот метод основан на использовании прошлого поведения для определения хороших и плохих авторизованных пользователей. Он основан на начислении пользователям поощрительных и штрафных баллов после завершения транзакций. Однако для принятия решения о доступе недостаточно данных о прошлом поведении пользователя (награда/штраф). Кроме того, не используется техника прогнозирования рисков и отсутствуют функции адаптации к рискам. Раджбхандари и Снеккенес [60] предложили подход, основанный на анализе рисков, для динамического принятия решений о предоставлении доступа. Указанный подход основан на предпочтениях или значениях выгоды, которые могут предоставить субъекты, а не на субъективной вероятности, использующей теорию игр. Простой сценарий конфиденциальности между пользователем и онлайновым книжным магазином представлен для того, чтобы дать первоначальное представление о концепции. Однако использование только выгод субъекта для определения решения о доступе недостаточно для разработки гибкой и масштабируемой модели управления доступом. Кроме того, в ней отсутствуют функции адаптации к риску.

Шарма и др. [61] предложили модель управления доступом на основе задач для оценки величины риска с помощью функций, основанных на действиях, которые пользователь хочет выполнить. Значение риска вычисляется в терминах различных действий и соответствующих результатов. Исходы и вероятность риска определяются вместе с уровнем чувствительности данных. Для оценки общей величины риска используются модели поведения предыдущих пользователей. Оцененное значение риска сравнивается с пороговым значением риска для принятия решения о доступе. Однако в ней отсутствуют функции адаптации к риску. Модель управления доступом на основе контекстного риска была предложена Ли и др [62]. Модель собирает всю полезную информацию из окружающей среды и оценивает ее с точки зрения безопасности. Для оценки риска применяется метод многофакторного процесса оценки (MFEP, Multi Factor Evaluation Process). Значение риска основано на результатах действий с точки зрения доступности, конфиденциальности и целостности. Эта модель

была оценена для управления доступом в больнице. Однако в этой модели не учитывается поведение пользователей в прошлом, а также адаптация к риску.

Дос Сантос и др. [63] предложили модель управления доступом на основе риска. В этой модели используется понятие количественной оценки рисков и их агрегирования. Она основана на идее политик риска, которые позволяют поставщикам услуг и владельцам ресурсов определять свои собственные метрики, обеспечивая большую гибкость системы управления доступом. Однако эта модель требует наличия системного администратора для обеспечения минимального уровня безопасности. Чун и Атлури [64] предложили модель, основанную на риске, которая использует концепцию "сначала доступ, а потом проверка", подразумевающая собой то, что к требуемой информации/данным можно получить доступ немедленно, не откладывая его на потом. В работе также использована семантика для построения иерархий ситуационных ролей, которые используются для оценки риска безопасности при принятии решений о доступе.

Моллой и др. [65] рассматривают открытые проблемы в системах управления доступом на основе риска и предлагают использовать рыночные подходы для определения распределения и допустимости риска для каждой организации. В работе использовано моделирование, чтобы показать преимущества управления доступом на основе риска, которые способствуют безопасности и обмену информацией. Кроме того в работе Моллой [66] представил новую обучаемую и основанную на рисках архитектуру для распределенного применения политик в условиях неопределенности. В работе использовались обучаемые классификаторы решений по управлению доступом для повышения точности принятия решений о доступе. Помимо этого Моллой и др. в работе [67] использовали модель управления доступом на основе риска для принятия решений о доступе с использованием преимуществ доступа в качестве фактора риска. В работе также предложена усовершенствованная модель, использующая обучаемые классификаторы для принятия эффективных и точных решений о доступе.

Кларк и др. [68] представили модель управления доступом на основе риска и показали, как она может преодолеть проблемы, связанные с неопределенностью и изменяющимися во времени спецификациями безопасности. Для оценки риска с помощью системы нечеткой логики в различных реальных ситуациях использовались чувствительность к ресурсам в виде распределения вероятности, метки безопасности и уровень допуска. Хелил и др. [69] представили модель

управления доступом на основе доверия и риска, которая объединяет доверие и риск в качестве факторов риска для повышения уровня защиты данных и доступности информации. Доверие каждого пользователя и связанные с ним значения риска используются для принятия решения о доступе.

Ванг и Джин [70] предложили модель, основанную на количественной оценке риска. Величина риска оценивается в зависимости от целей доступа к различным уровням чувствительности данных. Для оценки риска использовалась концепция энтропии Шеннона из теории информации. Для иллюстрации эффективности предложенной модели был использован прототип на основе истории болезни. Ариас-Кабаркос и др. [71] в своей статье используют модель управления доступом на основе риска в процессе управления федеративными идентификационными данными в облачных вычислениях. Модель использует риск безопасности для принятия решения о доступе и уменьшения слабых мест и рисков при принятии решений о совместном доступе. В статье также предложена иерархическая система агрегирования рисков для облачной федерации.

Чен и Крэмптон [72] в своей работе объединили риск безопасности с RBAC для построения модели управления доступом на основе ролей с учетом риска. Кроме того, в статье обсуждаются проблемы предложенной модели с учетом риска и процедуры ее реализации. Баракальдо и Джоши [73] предложили расширение модели RBAC, которое включало также доверие и риск при принятии решения о предоставлении доступа. Создатели модели заявляли о возможности адаптации их системы к изменениям поведения пользователей, для чего использовалось пороговое значение, вычисляемое в процессе оценки риска.

В [74] авторами было предложено применять классификацию для оценки риска в каждой ситуации, когда запрашивается доступ. В этой работе предложены два подхода: 1) использование матрицы управления доступом для оценки риска разрешения пользователю доступа в зависимости от его прав; 2) выявление лучшей контекстной роли для обеспечения минимальной величины риска и максимальной доступности с помощью интеграции риска безопасности с ролевой моделью. В [75] Бижон и соавторы представили структуру, которая сочетает ролевую модель и учет риска безопасности для определения решений о доступе. В работе представлена концепция осознания рисков на основе RBAC, а также дано формальное описание адаптивной модели RBAC с учетом рисков.

Бернетт и другие [76] предложили модель управления доступом с учетом доверия и рисков, которая обеспечивает охват политики и динамическое приня-

тие решений о доступе. В работе определена модель зонной политики, которая позволяет владельцу данных полностью контролировать свои данные. Доверие используется для проверки того, соблюдает ли запросчик возложенные на него обязательства или нет. В работе также использовалась вероятностная вычислительная модель доверия, называемая субъективной логикой, для формулировки оценки доверия. Для оценки риска использовался классический метод определения ожидаемых потерь от нежелательного раскрытия информации. Бабу и Бхану [77] предлагают построить модель управления доступом на основе доверия и риска для принятия решений о доступе в облачных вычислениях. В работе представлена процедура управления привилегиями, которая сочетает риск безопасности и доверие для создания эффективной и масштабируемой системы управления доступом.

Намита и др. [78] реализовали модель управления доступом на основе риска, которая основана на характеристиках пользователей, включая стаж работы, назначение, уровень дефектов, данные о местоположении, времени и др. и вычисляет значение риска посредством математической функции. В [79] была представлена модель, объединяющая значения риска и доверия при принятии решения о предоставлении доступа. Согласно этой модели доступ будет разрешен, если значение уровня доверия больше, чем значение уровня риска. Кроме того, в том же источнике представлены способы смягчения негативных последствий для повышения уровня доверия и снижения уровня риска. Диас-Лопес и соавторы в [80] представили модель управления доступом, основанную на риске. Эта модель динамически адаптируется к возможным изменениям уровня риска для системных ресурсов. Для разработки оптимального набора действий в каждой конкретной ситуации были использованы генетические алгоритмы.

В [81] была предложена модель, сочетающая риск конфиденциальности и доверие субъекта при определении угроз, соответствующих запросам на доступ. Если уровень доверия субъекта выше уровня риска конфиденциальности, то доступ разрешается. Эта модель позднее была дополнена [82] для оценивания риска с помощью риска конфиденциальности и доверии субъекта. Также были разработаны возможные сценарии доступа для демонстрации эффективность этого подхода. Кроме того были созданы стратегии настройки для увеличения доверия и уменьшения риска конфиденциальности.

Атлам и др. [83] предложили динамическую и адаптивную модель управления доступом на основе риска, используя контекст пользователя, чув-

ствительность ресурса, уровень серьезности действий, предысторию рисков для вычисления величины риска, соответствующего конкретному запросу на доступ. При отслеживании поведения субъекта во время сеансов доступа предложено использование смарт-контракта для обнаружения и предотвращения действий, которые могут нанести ущерб. В [84] модель была дополнена демонстрацией ее проверки экспертами по безопасности. Далее, работа была дополнена [85] – для оценки рисков предлагались методы нечеткой логики с экспертными оценками. В [85] детально представлено применение нечеткой логики при оценке величины риска безопасности, связанного с каждым запросом на доступ, а также сценарии управления доступом к сетевому маршрутизатору.

Данкар и др. [86] предложили концептуальную модель с учетом риска, которая использует информацию реального времени и контекст в окружающей среде для принятия решения о доступе. В работе также реализованы некоторые меры по смягчению последствий для обеспечения принятия решения о доступе при наличии значений с высоким уровнем риска в запросе на доступ. В [87] представлена риск-ориентированная модель для разработки системы Tyche, контролирующей риск в физических устройствах. Tyche – это концепция принятия решений о доступе на основе информации о уровне риска. Все приложения делятся на группы риска. Для каждой группы задается набор разрешений на основании величины риска.

Проведенный анализ исследований в области количественной оценки рисков показал, что существующие модели управления доступом на основе анализа риска сосредоточены только на предоставлении решений о доступе, не предоставляя никаких способов предотвращения аномального и нетипичного доступа к данным со стороны авторизованных пользователей. Указанная особенность позволяет сделать вывод, что разработка модели управления доступа, основанная на динамически меняющихся атрибутах, учитывающих поведенческие особенности авторизованных пользователей в ОВС, построенных на базе распределенных информационных систем, является актуальным направлением исследований. Для разработки указанной модели необходимо разработать модель угроз и модель нарушителя для ОВС, построенных на базе распределенных информационных систем.

1.4 Модель угроз и модель нарушителя

Разработка модели угроз и модели нарушителя является одним из основных этапов процесса разработки или совершенствования как теоретических положений и предложений, так и практических решений в области кибербезопасности. Разработка моделей угроз и нарушителей предназначена для обнаружения недостатков разработки анализируемых распределенных информационных систем на наличие уязвимостей, влияющих на обеспечение конфиденциальной информации и персональных данных, передаваемых посредством анализируемых систем [88].

Для обоснования используемого подхода к разработке модели угроз и нарушителя проведен анализ существующих подходов к разработке моделей, а также требований нормативно-правовых актов в области, регулирующей аспекты разработки моделей безопасности в контексте предъявляемых требований к обеспечению безопасности распределенных информационных систем.

Основным подходом к разработке моделей угроз является экспертный подход, осуществляемый специалистами в области обеспечения безопасности в ручном режиме. Указанный факт характеризуется высокой трудоемкостью и требует наличия как значительного временного ресурса, так и достаточного количества обученных экспертов. Стоит отметить, что подходы данной группы отличаются наличием ошибок ввиду проведения субъективной оценки [89]. Кроме того, отмечается довольно быстрое устаревание разработанного подхода, основанного на экспертных оценках, к концу первого десятилетия XXI века [90].

Автоматизация моделирования угроз решает подобные недостатки за счет использования онтологий и концептуального моделирования ОВС, базирующихся на распределенных информационных системах [91]. К основным направлениям реализации автоматизированных средств моделирования распределенных информационных систем относятся: системы обнаружения вторжений, специально адаптированные для мониторинга электроэнергетических систем [92], а также инструменты на основе глубокого обучения для обнаружения входящих угроз [93]. Были предприняты попытки автоматизировать моделирование угроз [94; 95]. Однако представленные методы недостаточно точны, поскольку при моделировании используются общие знания в предметной области. Например, если информация получается из нескольких источников (например, активно-

го каталога и сканера уязвимостей), небольшие различия в представлении имен программного обеспечения могут привести к дублированию информации в модели. Еще одной проблемой автоматизации моделирования является несоответствие гранулярности данных, которое возникает, когда уровень абстракции данных источника отличается от уровня создаваемой модели [96].

Для решения указанных проблем разработан метод на основе онтологии [97]. Эффект достигается путем поддержки вычислений с структурированными данными для обеспечения согласованности и корректности вывода. Методы на основе онтологии могут использоваться для решения различных проблем качества данных во время выполнения путем использования контролируемых концепций словаря и машинопонятных семантик [98]. Для улучшения качества онтологий разработано предположение о том, что проектирование должно осуществляться на концептуальных шаблонах [99; 100]. Так в работе авторов [99] сообщалось, что небольшие онтологии с явными мотивациями могут использоваться как базовые элементы для автоматического моделирования. Более того, такой подход облегчает согласование, слияние и повторное использование онтологий, что повышает степень автоматизации.

Улучшение автоматизированного моделирования угроз было предложено в работе [88]. Авторы разработали фреймворк, использующий онтологии для моделирования угроз. Фреймворк улучшил автоматизированное моделирование угроз путем решения двух упомянутых ранее проблем: отсутствия знаний в области и несоответствия гранулярности. Онтологии создаются на основе концептуального моделирования, построенного на общих знаниях. Полезность созданных моделей оценивается путем реализации и использования моделированной рамки [99—101].

Помимо методов на основе онтологии, в работе [102] описана концепция поверхности атаки на распределенные информационные системы на уровне аппаратных и программных ресурсов. Рассматривается класс сервиса как промежуточный уровень между пользователями (либо конечными пользователями, либо арендаторами облака) и поставщиком облака (или операторами облака) в том смысле, что, если пользователь хочет атаковать поставщика облака или другого пользователя, то он должен осуществлять атаку на сервисы. Кроме того, осуществляется фокусировка на точках входа и выхода [103], которые указывают средства, с помощью которых начинается атака, и те, через которые происходит утечка данных, соответственно.

Проведенный анализ исследований в области разработки и автоматизации модели угроз и нарушителя позволил сделать вывод о наличии существенных недостатков в существующих решениях и необходимости использования федерального законодательства [104—106], нормативно-правовой документации ФСТЭК России [107—109] и ФСБ России [110; 111] при разработке модели угроз и модели нарушителя для ОВС на основе распределительной информационной системы.

Модель угроз безопасности информации ОВС, базирующейся на на распределительной информационной системе (далее – модель угроз) содержит описание объекта информатизации и его структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей объекта информатизации, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Анализ угроз безопасности информации проводится с учетом угроз, содержащихся в банке данных угроз безопасности информации, сформированном ФСТЭК России и размещенном на официальном сайте в информационно-телекоммуникационной сети "Интернет" (bdu.fstec.ru) (далее – банк данных угроз безопасности информации, сформированный ФСТЭК России).

Угрозы безопасности могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности информации. Модель угроз может быть пересмотрена по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности с учетом особенностей и (или) изменений информационных систем, а также по результатам мероприятий по контролю выполнения требований к обеспечению безопасности информации при ее обработке в информационной системе (ИС).

ОВС представляет собой комплекс физических серверов в инфраструктуре центра обработки данных РТУ МИРЭА Ядро ОВС расположено по адресу: 119454, г. Москва, проспект Вернадского, дом 78, строение 4, 2 этаж, помещение № 8 на поэтажном плане. Обобщенная схема ОВС, представленная на рисунке 1.3.

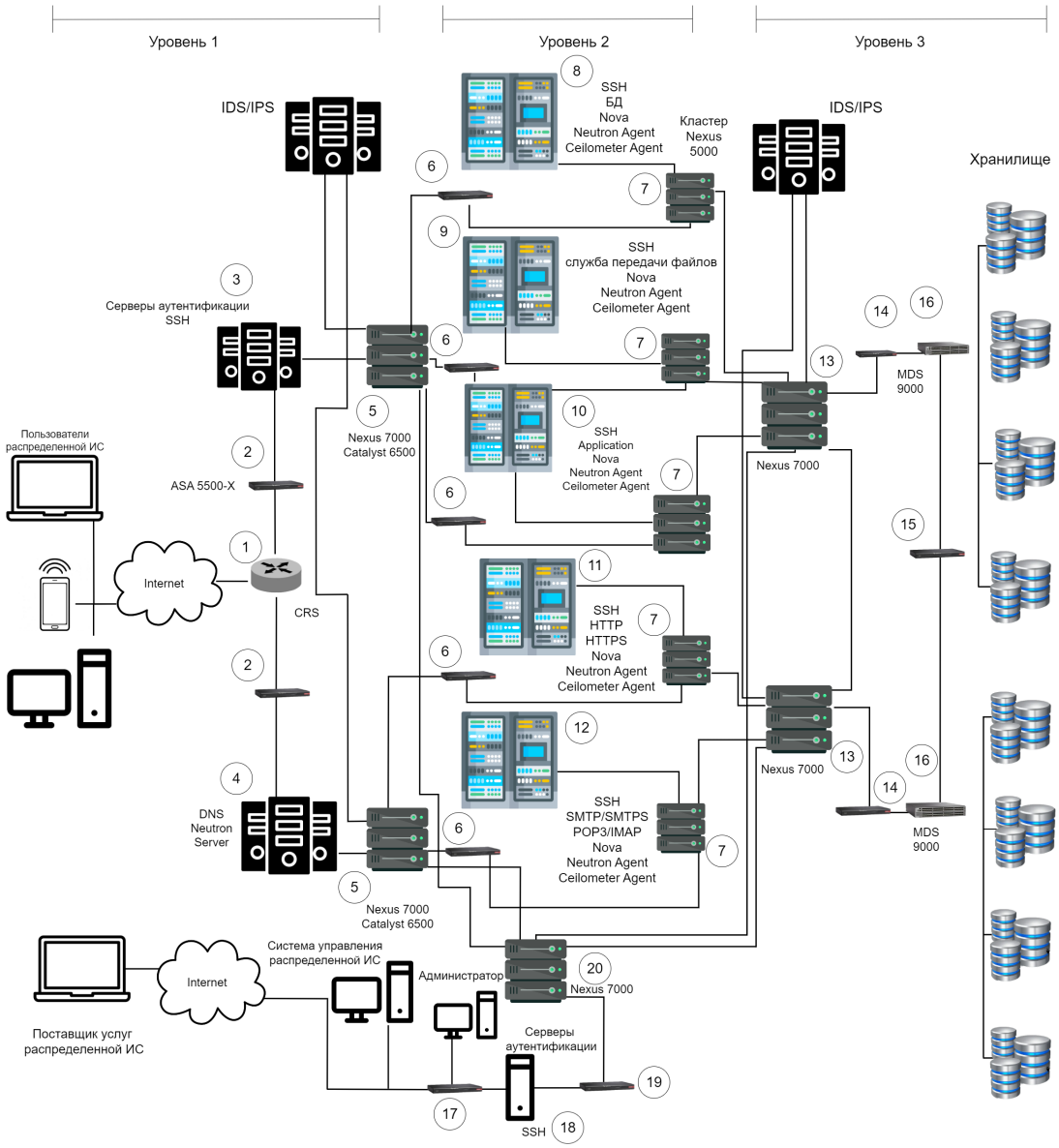


Рисунок 1.3 — Обобщенная схема образовательных вычислительных сервисов

ОВС состоит из следующих основных компонент:

1. Вычислительные серверы – комплекс электронно-вычислительных машин и программного обеспечения высокой надежности и производительности, производящий обработку данных и обеспечивающий функционирование информационных систем.
2. Система хранения данных – комплексное программно-аппаратное решение по организации надежного оперативного хранения информационных ресурсов и предоставления гарантированного доступа к ним вычислительных серверов через специализированную высокоскоростную сеть хранения данных по оптическим каналам связи.

3. Система резервного копирования – это специализированные сетевые накопители, подключенные к локальной вычислительной сети для обеспечения возможности выполнять резервные копии данных.
4. Оборудование локальной вычислительной сети – это комплексное программно-аппаратное решение, обеспечивающее высокоскоростную передачу данных внутри ИС и предоставляющее защищенный доступ пользователям сети к ресурсам информационных систем.
5. Виртуальная сеть – это комплексное программно-аппаратное решение, позволяющее организовывать сеансы видеосвязи и обмена информацией для ведения образовательного процесса с использованием публичных и выделенных каналов связи.
6. Автоматизированное рабочее место – это программно-аппаратный комплекс, обеспечивающий работу пользователя информационной системы.

Центральный узел обработки данных ОВС имеет одноточечное подключение к сетям общего пользования. ОВС изолирована от сети общего пользования сертифицированными межсетевыми экранами. В здании по адресу 119454, г. Москва, проспект Вернадского, дом 78, строение 4 действует контрольно-пропускной режим. Прием посетителей осуществляется в соответствии с инструкциями по режиму. Серверное помещение, где размещается серверные технические средства центрального узла обработки данных, оборудовано замком, СКУД, и охранной сигнализацией. Доступ в серверное помещение строго ограничен списком лиц, утвержденным приказом РТУ МИРЭА. Доступ в серверное помещение ведется в соответствии с утвержденной организационно-распорядительной документацией и списками допущенных лиц. Электропитание основных технических средств и систем ИС осуществляется от распределительного щита, расположенного на первом этаже охраняемого здания.

Структура информационного взаимодействия в информационной системе реализована на основе защищенной виртуальной сети и локальной вычислительной сети. Локальная вычислительная сеть (ЛВС) – коммуникационная система распределенной обработки данных, представляющая собой совокупность абонентских узлов, серверов и коммутационного оборудования, объеденных в доменную структуру с реализацией принципа дискреционного управления доступом. Все элементы ЛВС расположены в пределах границ контролируе-

мой зоны, оснащены сертифицированными средствами антивирусной защиты, также применяются сертифицированные средства защиты информации. Взаимодействие с внешними информационными ресурсами и подключение к сетям международного обмена осуществляется через единую точку входа-выхода с применением сертифицированных средств межсетевого экранирования.

Доступ пользователей ЛВС к ресурсам сети международного обмена ограничен утвержденным списком запрещенных к использованию Интернет-ресурсов и программного обеспечения. Ограничение доступа пользователей к запрещенным Интернет-ресурсам и программному обеспечению осуществляется при помощи сертифицированных средств антивирусной защиты и сертифицированного межсетевого экрана. В целях обеспечения защиты безопасности информации в ЛВС проводится круглосуточный мониторинг вирусной активности с использованием сертифицированного антивирусного программного обеспечения только российского производства. Все пользователи ЛВС работают под учетными записями с правами «обычный доступ», исключающими возможность самовольной установки программного обеспечения и изменения настроек системы защиты. Учетные записи с правами «администратор» имеют только сотрудники технических служб, эксплуатирующих ЛВС. Сервера вынесены в отдельный домен и подключены к сетям международного обмена с применением системы обнаружения и предотвращения вторжений. На всех серверах проводится круглосуточный мониторинг вирусной активности сертифицированными средствами антивирусной защиты российского производства. При организации технических систем защиты информации используются только сертифицированные средства российского производства.

Вся обрабатываемая в информационной системе информация хранится на центральном узле обработки данных в специально предназначенных для этого системах управления базами данных. Для подключения АРМ администраторов ИС используется пользовательский интерфейса с более широкими привилегиями и средства управления серверами ИС.

1.4.1 Характеристики информационной безопасности объектов защиты

Для защиты информации и других объектов, которые могут стать объектами угроз, должны быть соблюдены следующие компоненты безопасности:

- конфиденциальность,
- целостность,
- доступность.

Возможными последствиями нарушения безопасности информации могут быть:

- разглашение и несанкционированное изменение защищаемой информации. Это может нанести материальный и/или моральный ущерб субъекту, которого касается данная информация;
- причинение материального ущерба оператору;
- репутационные потери.

В контексте рассматриваемой ИС объектами защиты, включаемыми в модель угроз безопасности информации, являются:

- защищаемая информация, хранящаяся в ИС (информационные ресурсы ИС, информационные ресурсы, ориентированные на внешнего пользователя, файлы, базы данных и т. п.);
- технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео и речевой информации);
- общесистемное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, специальное программное обеспечение;
- средства защиты информации (в том числе средства криптографической защиты информации (СКЗИ));
- среда функционирования СКЗИ;
- информация, относящаяся к системе криптографической защиты, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- носители защищаемой информации, используемые в информационной системе, в том числе в процессе криптографической защиты

информации, носители ключевой, парольной и аутентифицирующей информации СКЗИ;

– используемые ИС каналы (линии) связи, включая кабельные системы.

Согласно классификации, используемой в банке данных угроз безопасности информации, созданном ФСТЭК России, актуальные для ИС типы объектов воздействия, с учетом структурных особенностей ИС и применяемых технологий, представлены в таблице 1.4.1.

Таблица 2 — Актуальные типы объектов воздействия для информационной системы

№ п/п	Применяемость к информационной системе	Тип объекта воздействия
1	Да	Аппаратное обеспечение
2	Да	Аппаратное и микропрограммное обеспечение BIOS/UEFI
3	Да	Аутентификационные данные пользователя
4	Да	База данных
5	Да	Виртуальная машина
6	Да	Виртуальные устройства хранения, обработки и передачи данных
7	Да	Виртуальные диски
8	Нет	Вычислительные узлы суперкомпьютера
9	Да	Гипервизор
10	Нет	Грид-система
11	Нет	Данные пользователя мобильного устройства
12	Да	Защищаемые данные
13	Да	Информация, хранящаяся на компьютере во временных файлах
14	Да	Информационная система
15	Нет	Информационная система, перенесенная в облако
16	Да	Информационные ресурсы
17	Да	Инфраструктура информационных систем
18	Да	Каналы связи
19	Нет	Каналы передачи данных суперкомпьютера
20	Нет	Консоль управления облачной инфраструктурой
21	Да	Консоль управления гипервизором
22	Нет	Ключевая система информационной инфраструктуры
23	Да	Машинный носитель информации
24	Да	Метаданные
25	Нет	Микропрограммное обеспечение
26	Нет	Мобильное устройство
27	Да	Носитель информации

28	Нет	Облачная инфраструктура
29	Нет	Облачная инфраструктура, созданная с использованием технологий виртуализации
30	Нет	Облачная система
31	Нет	Облачный сервер
32	Да	Образ виртуальной машины
33	Да	Объект файловой системы
34	Да	Прикладное программное обеспечение
35	Да	Программно-аппаратные средства со встроенными функциями защиты
36	Нет	Программное обеспечение автоматизированной системы управления технологическими процессами
37	Да	Рабочая станция
38	Нет	Ресурсные центры грид-системы
39	Да	Реестр
40	Да	Сервер
41	Да	Сетевое оборудование
42	Да	Сетевое программное обеспечение
43	Да	Сетевой трафик
44	Да	Сетевой узел
45	Да	Система управления доступом, встроенная в операционную систему компьютера
46	Нет	Система хранения данных суперкомпьютера
47	Да	Системное программное обеспечение
48	Да	Системное программное обеспечение, использующее реестр
49	Нет	Система разграничения доступа хранилища больших данных
50	Да	Средство вычислительной техники
51	Да	Средство защиты информации
52	Да	Стационарные и мобильные устройства (компьютеры и ноутбуки)
53	Да	Техническое средство
54	Нет	Точка беспроводного доступа
55	Нет	Узлы грид-системы
56	Нет	Узлы хранилища больших данных
57	Да	Учетные данные пользователя
58	Нет	Хранилище больших данных

1.4.2 Характеристики уязвимостей образовательных вычислительных сервисов

Уязвимость информационной системы – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности информации. В соответствии с методическим документом ФСТЭК России "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" причинами возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
- неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

С учетом состава ОВС и источников угроз безопасности информации, ниже представлена общая характеристика основных групп уязвимостей системы, включающих:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

– уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

Данные об уязвимостях разрабатываемого и распространяемого системного и прикладного программного обеспечения обобщаются и анализируются в банке данных угроз безопасности информации, сформированном ФСТЭК России.

Общая характеристика уязвимостей системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

– в микропрограммах, в прошивках ПЗУ, ППЗУ;
– в средствах операционной системы, предназначенных для управления локальными ресурсами системы (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т. п.), драйверах, утилитах;
– в средствах операционной системы, предназначенных для выполнения вспомогательных функций, – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиках и т. п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т. п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т. д.);
– в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

– функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
– фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

– отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т. п.);
– ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Общая характеристика уязвимостей прикладного программного обеспечения

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы. Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т. п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т. п. Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данной информационной системе (в том числе программные средства защиты информации, разработанные для конкретной информационной системы).

Уязвимости прикладного программного обеспечения могут представлять собой:

– функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
– функции и процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду информационной системы и вызова штатных функций операционной системы, выполнения несанкционированного доступа без обнаружения таких изменений операционной системой;

- фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т. п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

С веб-приложениями связаны следующие проблемы обеспечения безопасности:

- внедрение SQL-кода;
- применение форм и сценариев;
- файлы cookie и управление сеансом;
- общие атаки.

Общие уязвимости программных средств защиты информации

В ОВС в качестве средств защиты от несанкционированного доступа используют стандартные средства операционных систем и средства СУБД, у которых нет сертификата ФСТЭК России об отсутствии недекларированных возможностей. Это является угрозой существования фрагментов кода программ ("дыры", "люки"), введенных разработчиком, позволяющих обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в операционной системе. Следует также помнить, что появлению уязвимостей может способствовать некорректно выполненная настройка средств защиты, приводящая к отказам и сбоям в работе средств защиты информации.

Описание уязвимостей программного обеспечения ОВС

Выбор возможных уязвимостей информационной системы проводился с использованием банка данных угроз безопасности информации, сформированного ФСТЭК России, с учетом вендора программного обеспечения, наименования операционной системы, типа аппаратной платформы, названия и версии программного обеспечения. На степень критичности уязвимостей влияет

их тип воздействия на объект, существование предложенного производителем исправления или временного решения, наличие эксплоита и т. д. Уязвимости из банка данных угроз безопасности информации ФСТЭК России классифицируются по:

- классам,
- уровням опасности,
- статусам.

Согласно списку терминов, банка данных угроз безопасности информации ФСТЭК России, эти характеристики определяются следующим образом:

1. Класс уязвимости – характеристика уязвимости программного обеспечения, соответствующая причине ее появления. В банке данных используются следующие классы уязвимостей:
   - уязвимость кода. Возникает при разработке программного обеспечения без соблюдения требований безопасности информации;
   - уязвимость архитектуры. Возникает в результате выбора и соединения модулей программного обеспечения, которые содержат уязвимости;
   - многофакторная уязвимость. Вызвана наличием уязвимостей в программном обеспечении.
2. Базовый вектор уязвимости – строка, текстовая формализованная запись, информация о базовых метриках (критериях) уязвимости. Служит исходными данными для вычисления базовой оценки уязвимости.
3. Уровень опасности уязвимости. Это показатель опасности уязвимости, определяется с помощью базовой оценки уязвимости. В соответствии со значением базовой оценки уязвимости V применяются уровни опасности:
   - низкий, при $0{,}0 \leqslant V \leqslant 4$;
   - средний, при $4{,}0 \leqslant V \leqslant 7$;
   - высокий, при $7{,}0 \leqslant V \leqslant 9{,}9$;
   - критический, при $V = 10{,}0$.
4. Статус уязвимости – степень подтверждения факта наличия уязвимости. Значение поля "Статус уязвимости" принимает одно из следующих значений:
   - "уязвимость подтверждена производителем". Статус принимает это значение, в случае, если существование уязвимости

подтверждено производителем (разработчиком) программного обеспечения, в котором она содержится;

- "уязвимость подтверждена в процессе исследований". Существование уязвимости подтверждено исследователем, который не является производителем (разработчиком) программного обеспечения;
- "потенциальная уязвимость". Статус присваивается в остальных случаях.

В ИС наиболее распространены следующие уязвимости:

- не устраненные при обновлениях;
- заложенные в исходный код программного обеспечения недекларированные возможности обхода процедур аутентификации, выделения привилегий, прочие возможности, не входящие в функционал программного обеспечения;
- не обнаруженные при использовании защитных механизмов программного обеспечения, не прошедшего сертификацию в качестве средства защиты информации от несанкционированного доступа;
- возникающие при некорректном конфигурировании программного обеспечения, разграничивающего доступ к ресурсам;
- возможность получения несанкционированного доступа, обходя специальное программное обеспечение.

Меры, принимаемые для устранения уязвимостей в системе

Для устранения уязвимостей в ИС принимаются следующие меры:

- назначены ответственные специалисты (системные администраторы), отвечающие за проведение работ по установке обновлений разработчиков программного обеспечения, устраняющих выявленные разработчиком уязвимости программного обеспечения;
- имеется система защиты периметра ЛВС, где находится серверное оборудование, оснащенная сертифицированными средствами защиты. При этом исключена возможность доступа внешних нарушителей ко всему комплексу программного обеспечения ИС для использования заложенных в исходный код недекларированных возможностей обхода процедур аутентификации, выделения привилегий субъектом, а также прочих функций, не входящих в функционал программного обеспечения;

– используемые средства защиты имеют сертификаты соответствия ФСТЭК России и/или ФСБ России;
– конфигурирование программного обеспечения, которое разделяет доступ к объектам, проводится специалистами, прошедшими обучение по использованию средств защиты, и в соответствии с утвержденными инструкциями по настройке средств защиты;
– приняты все необходимые технические и организационные меры с целью исключения возможности получения доступа к базе данных в обход специального программного обеспечения.

1.4.3 Модель нарушителя безопасности информации в образовательных вычислительных сервисах

Модель нарушителя безопасности информации в соответствии с нормативными документами ФСТЭК России

Согласно нормативным документам ФСТЭК России по наличию права постоянного или разового доступа в контролируемую зону информационной системы нарушители подразделяются на два типа:

– внешние нарушители – нарушители, не имеющие доступа к информационной системе, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
– внутренние нарушители – нарушители, имеющие доступ к информационной системе, включая пользователей информационной системы, реализующие угрозы непосредственно в информационной системе.

Категории внутренних и внешних нарушителей, их способы и полномочия доступа к информационной системе, основные возможности представлены в Приложении А.

Внешний нарушитель принадлежит одной из следующих категорий:

– физические лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ;

– физические лица, имеющие возможность осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена.

Для реализации модели нарушителя были приняты ограничения и гипотезы, характеризующие поведение нарушителей:

– несанкционированный доступ может произойти по причине случайных или преднамеренных действий;
– планируя атаки, нарушитель пытается скрыть несанкционированные действия;
– проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа программного обеспечения для защиты информации, не будет приоритетной целью нарушителя по причине значительных трудозатрат на разработку средств атаки и отсутствием заметных негативных последствий атаки;
– в ИС не предусмотрена удаленный доступ;
– системные администраторы и администраторы безопасности ИС (категория нарушителя 5 и 6) относятся к привилегированным пользователям, так как имеют особые права доступа к защищаемой информации;
– сотрудники, осуществляющие поставку, поддержку и ремонт средств ИС (категория 8) относятся к привилегированным пользователям, так как имеют особые права доступа к защищаемой информации.

Наличие привилегированных пользователей требует реализации необходимых организационных мер для снижения риска информационной безопасности. В ИС применяются следующие организационные меры:

– регламентированы и внедрены процедуры управления доступом в контролируемую зону, к аппаратным и программным средствам обработки и защиты информации;
– определены должности сотрудников (роли), которым предоставляются привилегированные права доступа к информационным ресурсам;
– привилегированные пользователи назначаются из числа особо доверенных и ответственных лиц, и утверждаются приказом оператора информационной системы;

- в должностные инструкции привилегированных пользователей включены обязанности в области защиты информации;
- сформированы требования к кандидатам на трудоустройство на должности привилегированных пользователей;
- определены процедуры отбора и проверок кандидатов на трудоустройство на должности привилегированных пользователей;
- определены процедуры оформления приема сотрудников на должности привилегированных пользователей;
- определены процедуры увольнения сотрудников, занимавших должности привилегированных пользователей;
- организованы обучения и инструктажи в области защиты информации;
- организованы, документально оформлены и внедрены принципы разграничения полномочий и двойного управления для решения задач, связанных с администрированием программных и технических средств, в том числе средств обеспечения информационной безопасности;
- определены процедуры реагирования на нарушения информационной безопасности;
- определены процедуры контроля выполнения требований;
- определена ответственность за нарушения информационной безопасности.

В связи с отсутствием удаленного доступа, нарушители категории 3 исключены из числа потенциальных нарушителей. В связи с принятием в ИС указанных мер, нарушители категории 4, 5 и 6 (привилегированные пользователи группы администраторов) также не входят в число потенциальных нарушителей безопасности информации ИС. На должности работников – привилегированных пользователей (категория 8), которые занимаются поставкой, поддержкой, ремонтом, техническим обслуживанием средств информационной системы и специальных средств защиты информации (в том числе их настройка, конфигурирование, назначение паролей и документации между пользователями), должны назначаться из числа особо доверенных и ответственных лиц и утверждаться приказом оператора ИС. Эти сотрудники обладают полным доступом к настройкам сети и подсистемам защиты информации в случае восстановления, установки обновлений и т. п. Работоспособность системы безопасности информации во многом зависит от действий этих работников.

Поскольку обслуживание программных модулей информационной системы согласовывается с оператором ИС и контролируется ответственным за обеспечение безопасности информации, то нарушители категории 7 также должны быть исключены из числа потенциальных нарушителей безопасности информации ИС. Таким образом, потенциальными нарушителями безопасности информации в ИС могут быть признаны:

- физические лица, имеющие возможность осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена (внешний нарушитель);
- физические лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ (внешний нарушитель);
- обслуживающий персонал организации (внутренний нарушитель категории 1);
- работники инженерно-технических и административно-хозяйственных служб организации (внутренний нарушитель категории 1);
- сотрудники иных организаций, являющиеся зарегистрированными пользователями информационной системы, осуществляющие ограниченный доступ к информационным ресурсам ИС с рабочего места в рамках своих полномочий (внутренний нарушитель категории 2).

Определение потенциала нарушителей

В списке терминов, приведенных в банке данных угроз безопасности информации, сформированном ФСТЭК России, потенциал нарушителя определяется как мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе. Потенциал нарушителя может быть высоким, средним или низким.

При высоком потенциале нарушитель обладает возможностями уровня организации / группы организаций / государства для создания средств эксплуатации имеющихся уязвимостей. В случае среднего потенциала подразумевается наличие тех же возможностей, но на уровне группы лиц / организации. Низкий потенциал нарушителя соответствует наличию возможностей приобретения (в свободном доступе) и использованию средств эксплуатации уязвимостей на уровне одного человека.

Потенциал внешнего и внутреннего нарушителя, определяемого в соответствии с методикой ФСТЭК России, с учетом его оснащенности и мотивации и на основании приведенных выше определений потенциала внешнего и внутреннего нарушителей приведен в таблицах 3 и 4 соответственно.

Таблица 3 — Потенциал внешнего нарушителя

Внешний нарушитель	Потенциал нарушителя
Разведывательные службы государств	Высокий
Криминальные структуры	Средний
Конкуренты (конкурирующие организации)	Средний
Недобросовестные партнеры	Средний
Внешние субъекты (физические лица)	Низкий

Потенциал потенциальных нарушителей безопасности информации в ИС в соответствии со списком признанных вероятных нарушителей и на основании таблицы 4 приведен в таблице 5.

Анализ модели нарушителя, с учетом класса защищенности 1, присвоенного ИС, позволил сделать вывод об актуальности для ИС только внешних и внутренних нарушителей с **низким** и **средним** потенциалами.

Модель нарушителя безопасности информации в соответствии с нормативными документами ФСБ России

Согласно актуальным нормативным документам ФСБ России помимо защищаемой информации к объектам защиты относятся:

- средства криптографической защиты информации;
- среда функционирования (СФ) средств криптографической защиты информации (СКЗИ);
- информация, относящаяся к криптографической защите данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к информационным системам и их криптографической защите, включая документацию на СКЗИ и технические и программные компоненты СФ;
- носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты данных, носители клю-

чевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
- используемые информационной системой каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите информации.

Таблица 4 — Потенциал внутреннего нарушителя

Внутренний нарушитель	Потенциал нарушителя
Лица, имеющие санкционированный доступ к информационной системе, но не имеющие доступа к информации. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование информационной системы	Низкий
Зарегистрированные пользователи информационной системы, которые имеют ограниченный доступ с рабочего места к ресурсам информационной системы	Низкий
Зарегистрированные пользователи информационной системы, осуществляющие удаленный доступ к информационной системе по локальным и (или) распределенным информационным системам	Низкий
Зарегистрированные пользователи информационной системы (группа лиц), осуществляющие удаленный доступ к информационной системе по локальным и (или) распределенным информационным системам	Средний
Зарегистрированные пользователи информационной системы с полномочиями администратора безопасности сегмента (фрагмента) информационной системы	Низкий
Зарегистрированные пользователи с полномочиями системного администратора информационной системы	Средний
Зарегистрированные пользователи с полномочиями администратора безопасности информационной системы	Средний
Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	Средний
Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств в информационной системе	Средний

Классификация нарушителей (субъектов атак)

Согласно нормативным документам ФСБ России физических лиц, обладающих доступом к техническим и программным средствам информационной системы, можно разделить на две категории:

1. Категория I. Лица, не имеющие права доступа в контролируемую зону информационной системы..
2. Категория II. Лица, имеющие право постоянного/разового доступа в контролируемую зону информационной системы.

Таблица 5 — Потенциал нарушителей безопасности информации в ИС

Нарушитель	Тип нарушителя	Потенциал нарушителя
Физические лица, имеющие возможность осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена	Внешний	Низкий
Физические лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ	Внешний	Средний
Обслуживающий персонал организации	Внутренний категория 1	Низкий
Сотрудники иных организаций, являющиеся зарегистрированными пользователями информационной системы, осуществляющие ограниченный доступ к информационным ресурсам ИС с рабочего места в рамках своих полномочий	Внутренний категория 2	Низкий

Все потенциальные нарушители подразделяются на:

– внешних нарушителей. Реализуют атаки, находясь снаружи контролируемой зоны информационной системы. Это могут быть лица категорий I или II;
– внутренних нарушителей. Реализуют атаки, находясь внутри пределов контролируемой зоны информационной системы. Могут принадлежать только категории II;
– привилегированных пользователей (группа с правами администраторов). Назначаются из числа особо доверенных лиц, реализуют поддержку средств СКЗИ и СФ, в т. ч. настройку, конфигурирование и др.

Описание нарушителей (субъектов атак)

Лица, ответственные за безопасность информации в ИС, являются привилегированными пользователями. Эта категория не рассматривается в качестве потенциальных нарушителей, т. к. на эти должности назначаются лица из числа особо доверенных работников. Будем считать ограниченными возможности работников, имеющих доступ к информационной системе, действующими

в пределах контролируемой зоны факторами: режимными мероприятиями и организационно-техническими мерами, для пресечения несанкционированных действий.

Лица, относящиеся к обслуживающему персоналу (инженерно-технические и административно-хозяйственные службы), не являющиеся зарегистрированными пользователями ИС и посетители не обладают доступом в те помещения, где расположена информационная система, в отсутствие зарегистрированных пользователей системы, поэтому лица этой категории имеют возможность проведения атаки при нахождении в пределах контролируемой зоны, исключая помещения, где расположена информационная система. Иные сотрудники, легально находящиеся в пределах контролируемой зоны, но не являющиеся зарегистрированными пользователями системы, имеют возможность реализовать атаку, находясь физически в контролируемой зоне, кроме тех помещений, где расположена ИС. Другие работники, которые находятся легально в контролируемой зоне, но при этом не являются зарегистрированными пользователями системы, могут реализовать атаку при эксплуатации СКЗИ на помещения, где находятся программные и технические компоненты систем обработки данных на которых реализованы СКЗИ и СФ.

Будем считать, что только зарегистрированные пользователи ИС используют СКЗИ при передаче информации по каналам связи общего пользования. Прочие работники ведомств, организаций и учреждений, которые не являются зарегистрированными пользователями ИС, не могут использовать СКЗИ, следовательно, не входят в число потенциальных нарушителей.

Поскольку задачи, которые решает информационная система, не направлены на получение прибыли, а сама информационная система не связана с обработкой информации, составляющей государственную тайну, то для потенциальных нарушителей, которые могут нанять специалистов с опытом разработки и анализа СКЗИ (уровня группы лиц, организации, группы организаций, государства), ИС не представляет интереса. Эту категорию далее не будем рассматривать в числе потенциальных нарушителей.

Будем полагать, что в наличии у нарушителя есть все необходимые средства для реализации атак. Для доступа к желаемой информации внешний нарушитель может применять следующие средства доступа: свободно продаваемые аппаратные средства и программное обеспечение, специализированное

программное обеспечение и свободно продаваемые средства перехвата аудио- и визуальной информации.

Внутренний нарушитель для доступа к информации может применять те же средства доступа, что и внешний нарушитель, а также доступные ему штатные средства информационной системы. В таблице 6 представлены обобщенные возможности источников атак, выделенные на основе информации об информационной системе, объектах защиты и источниках атак.

Таблица 6 — Обобщенные возможности источников атак на ОВС

Обобщенные возможности источников атак	Предположение о возможности источников атак
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	+
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	–
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	–
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	–
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	–
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	–

Согласно нормативным документам ФСБ России реализация угроз безопасности защищаемой информации, обрабатываемой в информационной системе, определяется возможностями источников атак. Анализ уточненных возможностей нарушителей и направления атак можно представить в следующем виде:

1.1 **Проведение атаки при нахождении в пределах контролируемой зоны** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- проводятся работы по подбору персонала;
- доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом;
- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями информационной системы, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в информационной системе и ответственности за несоблюдение правил обеспечения безопасности информации;
- пользователи СКЗИ проинформированы о правилах работы в информационной системе, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;
- помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, двери помещений постоянно закрыты на замок и открываются только для санкционированного прохода;
- утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;
- утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;
- осуществляется разграничение и управление доступом пользователей к защищаемым ресурсам;
- осуществляется контроль целостности средств защиты;

- на АРМ и серверах, на которых установлены СКЗИ;
- используются сертифицированные средства защиты информации от несанкционированного доступа и средства антивирусной защиты.

1.2 **Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ, а также помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- проводятся работы по подбору персонала;
- доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом;
- документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе;
- помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, двери помещений постоянного закрыты на замок и открыты только для санкционированного прохода;
- утвержден перечень лиц, имеющих право доступа в помещения.

1.3 **Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы, а также сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- проводятся работы по подбору персонала;

- доступ в контролируемую зону и помещения, где располагаются ресурсы информационной системы, обеспечивается в соответствии с контрольно-пропускным режимом;
- сведения о физических мерах защиты объектов, в которых размещена информационная система, доступны ограниченному кругу сотрудников;
- сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации;
- существует регламент работы пользователей информационной системы;
- пользователи информационной системы проходят обучение в сфере безопасности информации, а также предупреждены об ответственности за несоблюдение мер безопасности информации.

1.4 **Использование штатных средств информационной системы, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- проводятся работы по подбору персонала;
- ответственными за обеспечение безопасности информации, администраторами информационной системы, ответственный пользователь криптографических средств могут быть назначены только особо доверенные лица;
- ремонт, обслуживание и поддержка всех видов средств информационной системы, включая средства защиты информации, осуществляется только доверенными лицами, с выполнением мер по обеспечению безопасности информации;
- существует регламент работы пользователей информационной системы;
- пользователи информационной системы проходят обучение в сфере безопасности информации, а также предупреждены об ответственности за несоблюдение мер безопасности информации;

- пользователи информационной системы не имеют возможности запуска стороннего программного обеспечения или установки, изменения настроек работающего программного обеспечения без контроля со стороны ответственного за обеспечение безопасности информации, помещения, где находятся документация на СКЗИ, СКЗИ и компоненты СФ, постоянно закрыты на замок, и их открывают только для санкционированного прохода;
- выполняются учет и регистрация действий пользователей;
- настройка программных, технических, программно-технических средств (в том числе средств защиты информации) информационной системы проводится согласно политике обеспечения безопасности информации;
- для обеспечения безопасности информационной системы применяются сертифицированные средства антивирусной защиты (регулярно обновляются базы вирусных сигнатур) и средства защиты информации от несанкционированного доступа.

2.1 **Физический доступ к СВТ, на которых реализованы СКЗИ и СФ** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- проводятся работы по подбору персонала;
- доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;
- в отсутствие пользователей информационной системы сотрудникам, обеспечивающим функционирование информационной системы и обслуживающему персоналу, запрещено находиться в помещениях, где находится информационная система;
- запрещено нахождение посторонних лиц в помещениях, где происходит обработка информации;
- помещения, где находятся документация на СКЗИ, СКЗИ и компоненты СФ, постоянно закрыты на замок, и их открывают только для санкционированного прохода.

2.2 **Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и**

направленными на предотвращение и пресечение несанкционированных действий – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- проводятся работы по подбору персонала;
- доступ в контролируемую зону, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;
- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;
- в помещениях, где происходит обработка информации, строго запрещено бесконтрольное нахождение посторонних лиц;
- помещения, где находятся документация на СКЗИ, СКЗИ и компоненты СФ, постоянно закрыты на замок, и их открывают только для санкционированного прохода.

3.1 **Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;
- высокая стоимость и сложность подготовки реализации возможности;
- проводятся работы по подбору персонала;
- доступ в контролируемую зону, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;
- обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компонен-

ты СФ, на замок и их открытие только для санкционированного прохода;

- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;
- осуществляется разграничение и управление доступом пользователей к защищаемым ресурсам;
- выполняются учет и регистрация действий пользователей;
- для обеспечения безопасности информационной системы применяются сертифицированные средства антивирусной защиты (регулярно обновляются базы вирусных сигнатур) и средства защиты информации от несанкционированного доступа.

3.2 **Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;
- высокая стоимость и сложность подготовки реализации возможности.

3.3 **Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

- высокая стоимость и сложность подготовки реализации возможности.

4.1 **Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что:

- не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;
- высокая стоимость и сложность подготовки реализации возможности;
- проводятся работы по подбору персонала;
- доступ в контролируемую зону, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;
- обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, на замок и их открытие только для санкционированного прохода;
- представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации;
- осуществляется разграничение и управление доступом пользователей к защищаемым ресурсам;
- выполняются учет и регистрация действий пользователей;
- для обеспечения безопасности информационной системы применяются сертифицированные средства антивирусной защиты (регулярно обновляются базы вирусных сигнатур) и средства защиты информации от несанкционированного доступа.

4.2 **Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ** – отсутствуют объективные предпосылки для осу-

ществления угрозы ввиду того, что не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

4.3 **Возможность воздействовать на любые компоненты СКЗИ и СФ** – отсутствуют объективные предпосылки для осуществления угрозы ввиду того, что не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

На основании оценки возможностей нарушителей и проведенного анализа уточненных возможностей нарушителей и направления атак, в соответствии с «Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (ФСБ России № 149/7/2/6-432, 2015 г.) и Приказом ФСБ России от 10 июля 2014 г. № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" определен необходимый уровень криптографической защиты информации – КС1 и выше.

Таким образом, была разработана модель угроз и модель нарушителя ОВС, основанной на распределенной информационной системе. Разработанная модель наиболее полно охватывает возможные сценарии реализации угроз потенциальными нарушителями и позволяет перейти к созданию научно-методического аппарата адаптивного риск-ориентированного управления доступом в распределенных информационных системах на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды в распределенных информационных системах, включающего в себя: **риск-ориентированную атрибутивную модель управления доступом, учитывающую значения риска при принятии решения о предоставлении доступа, метод количественной оценки рисков реализации угроз информационной безопасности на основе анализа событий, посту-**

пающих от агентов, метод непрерывной аутентификации на основе психологических реакций пользователей и метод оценки эффективности реализации защитных мер, основанный на анализе затрат ресурсов.

Разработанная модель угроз и модель нарушителя позволяет сформировать структуру разрабатываемого научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков.

1.5 Структура разрабатываемого научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков

Проведенный анализ научных источников позволил выявить ряд существенных проблем управлением доступом в распределенных информационных вычислительных системах дистанционного образования. Основными из них являются: разнообразие групп пользователей, которые обладают специфическими и иногда пересекающимися правами доступа к объектам: студенты, преподаватели, администраторы и прочие. Также следует отметить, что в системах дистанционного образования необходимо точно определять, к каким ресурсам и функциям имеет доступ каждый пользователь и, поскольку данные системы являются распределенными и предоставляют доступ пользователям из различных географических точек, то необходимо использовать динамическое управление правами: изменения в правах доступа в зависимости от курса, прогресса обучения, роли в системе, местоположения и других атрибутов безопасности. Сложность в координации доступа к ресурсам, распределенным между разными серверами, и облачными платформами и необходимость централизованного управления в условиях децентрализованных данных также являются факторами применения динамических систем управления доступом [112].

Для решения указанных проблем необходимо в первую очередь создать модель управления доступом, учитывающую значения риска и позволяющую гибко и незаметно для пользователя определять значение риска в каждом конкретном контексте доступа субъекта к объекту. Модель должна использовать

определенные атрибуты, которые наилучшим образом позволят с одной стороны описать субъект доступа и объект доступа и присущий им контекст, а с другой стороны динамически определять значение риска доступа. Описание созданной модели будет представлено в главе 2.

Традиционные модели управления доступом, как правило, статичны и не подходят для использования в такой динамической среде как система дистанционного образования (СДО). Разработанная модель использует атрибуты доступа, которые позволяют создать метод количественной оценки рисков реализации угроз информационной безопасности, основанный на оперативном анализе данных доступа к образовательным сервисам. Метод предполагает использование интеллектуальных агентов сбора и анализа событий безопасности с помощью нечетких правил и позволяет создать динамическую модель управления доступом, вычисляющую уровень риска при доступе субъекта к ресурсам СДО. Описание разработанного метода представлено в главе 3.

Для повышения надежности и устойчивости создаваемых методов адаптивного риск-ориентированного управления доступом в распределенных информационных системах необходимо разработать метод, позволяющий "на лету" осуществлять аутентификацию пользователя системы. Анализ предметной области показал, что наиболее подходящим функционалом обладают поведенческие методы аутентификации. В главе 4 представлен методы непрерывной аутентификации на основе психологических реакций пользователей, позволяющий повысить устойчивость системы управления доступом в СДО вуза. Разработанная риск-ориентированная атрибутивная модель, метод количественной оценки рисков реализации угроз информационной безопасности и метод непрерывной аутентификации на основе психологических реакций пользователей позволили создать научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков.

Для решения поставленных в диссертационном исследовании задач, в первую очередь, необходимо оценить эффективность реализации защитных мер с точки затрат ресурсов. Возможно создать абсолютно защищенную систему, которой будет невозможно пользоваться из-за постоянных проверок безопасности и многочисленных методов аутентификации пользователей или создать систему, которая требует больших затрат вычислительных ресурсов. Таким образом одним из ключевых преимуществ созданного научно-методического ап-

парата будет его эффективность с точки зрения затрат ресурсов, обеспечения безопасности данных и удобства использования СДО, поскольку в современном информационном мире наблюдается конкуренция за лояльность и приток новых пользователей информационных систем. Кроме того оценка эффективности позволит сделать вывод о целесообразности, рациональности и возможности использования интеллектуальных агентов сбора и анализа событий безопасности и их влиянии на производительность СДО вуза.

В разделе "Метод оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов" рассмотрена методология оценки эффективности защитных мер, с учетом затрат ресурсов. В разделе обоснована необходимость рационального распределения ресурсов при внедрении защитных мер с точки зрения анализа затрат ресурсов, критерия эффективности и процессов оптимизации. После проверки эффективности разработанного научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды необходимо подробно описать разработанное решение, объединяющее в себе разработанные атрибутивную модель, метод количественной оценки рисков и метод непрерывной аутентификации пользователей на основе их психологических реакций.

Для решения проблемы управления доступом в СДО вуза используется динамическая атрибутивная модель управления доступом. Созданная модель управления доступом имеет способность адаптироваться к изменениям атрибутов пользователей и контекста доступа субъекта к объекту. Описан процесс количественного анализа рисков, включая вероятностные модели и оценку последствий нарушений безопасности. Также разработаны способы интеграции динамических данных из различных источников, позволяющие адаптировать политику управления доступом в режиме реального времени. После успешного решения задачи эффективного использования вычислительных ресурсов и разработки научно-методического аппарата риск-ориентированного атрибутивного управления доступом необходимо оценить его эффективность в реальных СДО. Предполагается внедрение и опытная эксплуатация разработанных решений в СДО РТУ МИРЭА. В заключительном разделе необходимо привести статистические данные свидетельствующие об эффективности предложенного научно-методического аппарата на основе практического использования, опытной эксплуатации пользователями и результатов моделирования.

1.6 Выводы по первой главе

В первой главе проведен анализ объекта и предмета исследования, определены цель и научная проблема проводимого исследования. Разграничение доступа легитимных пользователей к защищаемым ресурсам, конфиденциальной информации и персональным данным образовательных вычислительных сервисов представляет собой одно из наиболее актуальных направлений обеспечения информационной безопасности распределенных информационных систем. Существующие решения в области управления доступом не позволяют своевременно модифицировать предоставляемые права доступа в зависимости от действий пользователей и существующих требований безопасности.

В ходе проведенного анализа объекта исследования рассмотрены основные подходы управления доступом распределенных информационных систем, на базе которых развертываются и функционируют образовательные вычислительные сервисы, определены их достоинства и недостатки. Анализ предмета исследования, основанный на сравнительном анализе существующих моделей управления доступом, позволил обосновать применение методов управления доступом на основе аттрибутов в процессе разработки научно-методического аппарата адаптивного риск-ориентированного управления доступом в распределенных информационных системах.

Для обоснования применяемого риск-ориентированного подхода управления доступом проведены исследования в области количественной оценки рисков, изучены достоинства и недостатки, обоснована необходимость разработки метода количественной оценки рисков реализации угроз информационной безопасности, основанный на анализе информации о событиях безопасности, поступающих от агентов, функционирующих в распределенных информационных системах. Кроме того разработана модель угроз и модель нарушителя безопасности информации, циркулирующей в образовательных вычислительных сервисах, базирующихся на распределенных информационных системах. Полученные результаты позволили перейти к разработке теоретических и практических решений научно-методического аппарата адаптивного риск-ориентированного управления доступом в распределенных информационных системах.

Глава 2. Риск-ориентированная атрибутивная модель управления доступом, основанная на анализе состояния изменяющихся условий среды и учете получаемых оценок значений риска

В главе представлено описание разработанной риск-ориентированной атрибутивной модели управления доступом, использующей в процессе предоставления доступа к объектам значения риска реализации угроз информационной безопасности образовательных вычислительных сервисов.

2.1 Исследования в области моделей управления доступом

Возросшее количество инцидентов информационной безопасности, связанных с утечкой конфиденциальной информации и персональных данных в частных и государственных учреждениях обусловлено как преднамеренными действиями внутренних нарушителей, так и недетерминированным (девиантным) поведением сотрудников организаций, имеющих легитимный доступ к защищаемым объектам. Стоит отметить тот факт, что зачастую недетерминированное (девиантное) поведение легитимных пользователей, представляющее собой легитимные запросы доступа на предоставление полномочий, не может быть своевременно обнаружено методами традиционных статичных моделей управления доступом [113].

Существующие традиционные модели управления доступом используют логику предоставления доступа к ресурсам и объектам на основе правил управления доступом. Применение указанного механизма управления доступом позволяет устранить большинство существующих проблем при разграничении доступа, однако имеет существенный недостаток, заключающийся в применении предопределенных (фиксированных) политик безопасности, которые не позволяют обеспечить требуемый уровень защищенность объектов доступа в динамически изменяющихся условиях. Вне зависимости от текущей ситуации модели, основанные на предопределенных политиках, формируют одно и то же решение по предоставлению доступом [114], что не отвечает динамически меняющимся требованиям безопасности [115; 116].

Указанная особенность не позволяет использовать существующие статические модели управления доступом в динамически изменяющихся условиях. С целую устранения указанного недостатка необходимо провести анализ исследований в области методов управления доступам, учитывающих динамически изменяющиеся условия. К указанным методам относятся атрибутивные и динамические модели (частный случай атрибутивных моделей) управления доступом.

2.1.1 Атрибутивные модели управления доступом

Атрибутивное управление доступом (ABAC, Attribute-Based Access Control) предоставляет собой класс методов управления доступом, которые могут быть применены как в исследовательских системах, так и в реально функционирующих системах, в том числе и образовательных вычислительных сервисах, базирующихся на распределенных информационных системах. Формально не описаны единая модель или стандарт моделей ABAC, но при этом существуют высокоуровневые определения и описания их функциональных особенностей. Одно из таких высокоуровневых описаний содержится в публикации Национального института стандартов и технологий (NIST, National Institute of Standards and Technology) "Руководство по атрибутивному управлению доступом (ABAC): определение и аспекты применения" [117]. Согласно [117] атрибутивное управление доступом – это метод, при котором атрибуты субъекта, объекта, окружающая обстановка, политики безопасности определяют разрешение/отклонение запросы субъектов на выполнение операций с объектами.

ABAC дает возможность разрабатывать политики доступа на основе существующих атрибутов пользователей и объектов в системе, без использования ручного назначения ролей, владения, меток безопасности администратором системы. Обеспечение безопасности ресурсов и сервисов ОВС должно с одной стороны гарантировать соблюдение всех свойств безопасности информации, а с другой – обеспечивать доступность ресурсов. Контекст использования ОВС обуславливает клиент-ориентированность образовательных ресурсов и их конкуренцию между собой. При этом стремление разработать "совершенную

защищенную" систему приведет к снижению удобства использования до нуля, что, в свою очередь, приведет к оттоку обучающихся, использующих ОВС [118].

Существующие в ABAC механизмы управления доступом устраняют необходимость ручного управления в процессе авторизации пользователей системы для выполнения необходимых ролей или уровней безопасности. Это делает более простым администрирование в сложных системах со значительным числом пользователей. Кроме того, появляется возможность автоматизации решений управления доступом для удаленных пользователей из внешних систем, что особенно актуально учитывая особенности современных ОВС и дистанционный формат образования. Несмотря на разнообразие работ по применению ABAC к существующим проблемам и попыткам дополнительной формализации ABAC, не все исследования предоставляют подробное и детализированное описание разрабатываемых решений в различных областях применения ABAC. С целью дальнейшего исследования моделей атрибутивного управления доступом проведен сравнительный анализ, направленный на выявление проблем, которые ограничивают внедрение и использование моделей ABAC в ОВС.

Атрибутивное управления доступом

Атрибутивное управление доступом (ABAC) базируется на атрибутах управления доступом, которые могут быть классифицированы по следующим категориям:

1. Атрибуты пользователя – характеристики субъектов (имя и фамилия, возраст, должность, роль, уровень доступа, адрес, дата приема на работу). Здесь же может быть указан уровень доверия, определяемый конечной системой.
2. Атрибуты объекта – характеристики ресурсов системы, метаданные (автор, дата создания, размер, тип файла) или содержание объекта (например, имя пациента для медицинских учреждений или шифр обучающегося для учебных учреждений).
3. Атрибуты окружения системы – свойства актуального состояния окружения (текущее время, день недели, число активных пользователей и т. д.

4. Атрибуты соединения – характеристики актуальной сессии пользователя (IP-адрес, физическое местоположение, дата и время начала сессии и др.).
5. Административные атрибуты – конфигурационные параметры, применяемые к системе в целом. Их вручную устанавливает администратором или установка происходит автоматически. Это могут быть: уровень угрозы, минимальный уровень доверия пользователя для получения доступа к системе, наибольшая продолжительность сессии и т. д.

В идеальном случае перечисленные атрибуты - свойства элементов системы, для них не нужен ручной ввод администратором (большинство атрибутов объекта можно получить из его метаданных). Политики доступа можно разработать с использованием языков политик при ограничении доступа к заданным ресурсам/объектам, на основе результата булевого выражения, которое сравнивает атрибуты, например, "*user.age >= 18 OR object.owner == user.id" или "TIME > 8:00AM AND TIME < 5:00PM*". Это позволяет более гибко применять политики реального мира, требуя при этом лишь знания некоторого подмножества атрибутов о заданном пользователе (в отличие от знания его идентификации и назначенных ему ролей или разрешений вручную).

Основная модель ABAC

Исходя из того, каждая модель ABAC имеет свою собственную специфику в формализации элементов, упрощенное описание базовой модели ABAC для ОВС может быть представлено через основные элементы, которые являются общими для широкого круга моделей. К ним относятся:

– Пользователи (U): множество всех участников, которым разрешен доступ к системе. Пользователи могут включать в себя как физических лиц, так и другие информационные системы или компоненты, которые могут взаимодействовать с системой. Важно отметить, что множество пользователей может быть динамическим и не обязательно ограничивается конкретным списком на момент создания системы. Это особенно важно для систем с динамическим набором пользователей, таких как

системы с открытым доступом или системы, которые могут взаимодействовать с другими внешними системами, к которым относятся ОВС.

– Объекты (O): множество всех ресурсов, которые подлежат защите в системе. Объекты могут включать в себя данные, файлы, устройства, сервисы или любые другие элементы, с которыми пользователи могут взаимодействовать или на которые они могут запрашивать доступ. Каждый объект имеет свои собственные атрибуты, которые определяют его характеристики и свойства, и используются для определения разрешений на доступ к нему.
– Атрибуты (A): совокупность всех характеристик и свойств, которые могут быть присвоены пользователям и объектам в ОВС. Атрибуты могут представлять собой разные типы информации: персональные данные субъектов, метаданные объектов, данные об окружении и т. д. Атрибуты имеют важное значение в процессе принятия решений о доступе, поскольку используются для определения, разрешается ли пользователю выполнение операции с объектом в определенном контексте.
– Разрешения ($PERM$): совокупность всех возможных правил и политик, которые определяют, какие действия могут быть выполнены пользователями с определенными атрибутами над объектами с определенными атрибутами. Разрешения могут включать в себя различные операции, такие как чтение, запись, выполнение, удаление и другие, а также дополнительные условия, учитываемые при принятии решения о доступе, например, ограничения по времени, местоположению или другим контекстуальным факторам. Эти основные элементы модели ABAC обеспечивают фундаментальные принципы для построения системы атрибутивного управления доступом и служат основой для разработки более конкретных моделей и архитектур, учитывая уникальные требования и особенности конкретных систем и организаций.
– Политики (P). Это набор всех политик, которые регулируют доступ в системе. Обычно эти политики написаны на языке политики и в некотором отношении связаны с разрешениями, которые они предоставляют.

Пользователям и объектам назначаются атрибуты и связываются через следующие отношения, представленные на рисунке 2.1:

Назначение атрибутов пользователям может быть представлено в виде выражения $\{a \in A, u \in U, \text{значения}\} \in UAA$. Это значит, что все

элементы UAA – это кортежи из 3 значений: имя атрибута из множества атрибутов (A); имя пользователя из множества пользователей (U); набор значений, соответствующих пользователю и паре атрибута. Например, если пользователю, $\{aa\_sidorov\_bbmo\_1\_22\}$, был назначен атрибут "группа" со значением $\{bbmo\_1\_22\}$ и атрибут "кафедра" со значением $\{IS\}$, запись в UAA будет выглядеть как $\{aa_sidorov, \{bbmo\_1\_22\}, \{IS\}\}$. В другом случае, если пользователю, $\{am\_petrov\}$, был назначен атрибут $\{tutor\}$, который содержит набор других пользователей, для которых он является наставником (в данном случае $\{ii\_stepanov\}$ и $\{ai\_ivanov\}$), запись в UAA будет $\{tutor, am\_petrov, \{ii\_stepanov, ai\_ivanov\}\}$.

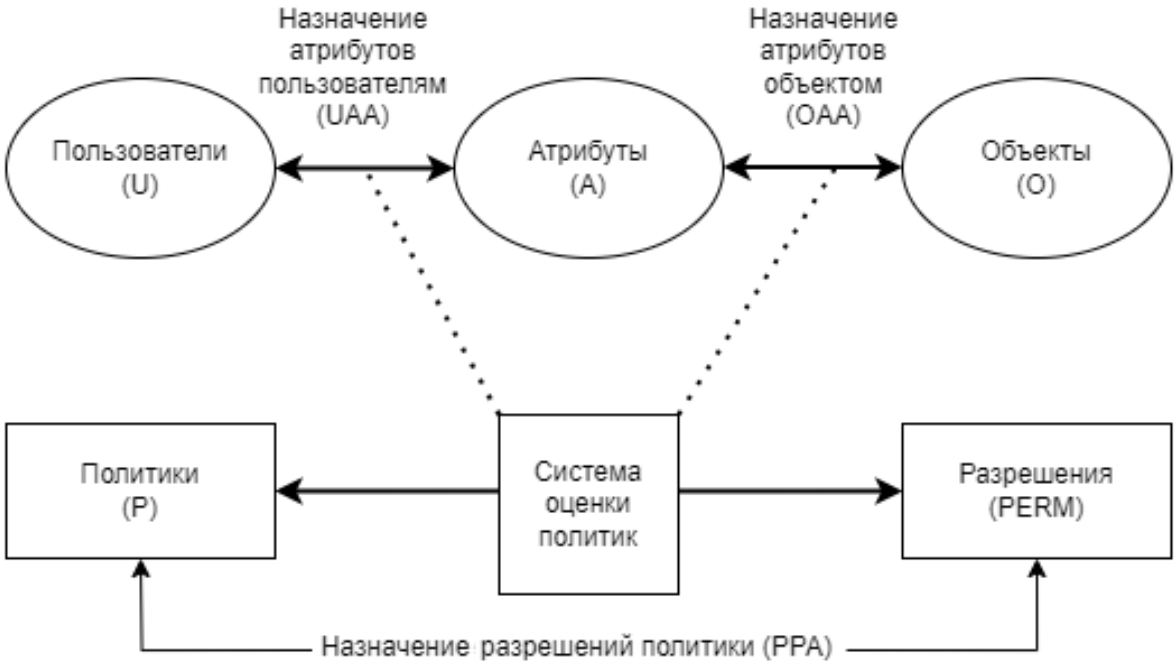


Рисунок 2.1 — Базовая модель ABAC для ОВС

Назначение атрибутов объектам может быть представлено в виде $\{a \in A, o \in O, \text{значения}\} \in OAA$ и функционирует также, как UAA, только применительно к объектам. Отношение между политиками и соответствующими разрешениями можно представить в виде $\{p \in P, \text{разрешение} \in PERM\} \in PPR$. Это назначение часто формулируется по-разному или вообще не формулируется во многих моделях в зависимости от того, как работает их язык политик (например, сам язык может указывать набор предоставляемых разрешений).

Политики в наборе P обычно представляют собой булевы выражения, включающие атрибуты и константы, такие как $user.group$ ==

$\{bbmo\_1\_22, bbmo\_2\_22\}$ (предоставляет доступ, если пользователь учится в группе $bbmo\_1\_22$ или $bbmo\_2\_22$) или $user.id == teacher$ (предоставляет доступ, если пользователь является сотрудником подразделения вуза). Когда пользователь делает запрос на доступ, его оценивают по набору политик (P) при этом учитываются атрибуты пользователя, который совершает запрос на доступ, и запрашиваемого объекта. Запросы на доступ часто не осуществляются самим пользователем, а происходят опосредованно через сеанс, содержащий возможные атрибуты пользователя.

Помимо атрибутивных и традиционных (основанных на статических правилах) моделей доступа широкое применение получили динамические модели управления доступом, которые позволяют изменять правила разграничения доступа в зависимости от изменяющихся условий.

2.1.2 Динамические модели управления доступом

Под динамическим управлением доступа в контексте исследования понимаются системы управления доступом, в которых решение о предоставлении доступа субъекта к объекту предоставляется по правилам сравнения в момент запроса доступа их атрибутов и по правилам действующих на момент доступа. С точки зрения существующих моделей управления доступом динамическое управление доступом представляет собой атрибутивное управление доступом при динамически изменяющихся атрибутах субъектов, объектов и устройств (среды) доступа.

Динамические модели управления доступом используют не только политики доступа, но также и параметры реального времени, которые рассчитываются во время запроса доступа и их значение определяет решение о предоставлении доступа. Поскольку значения атрибутов субъектов (пользователей) и объектов доступа, а также "утверждения-клаймы" по правилам доступа могут изменяться, то и результат удовлетворения запросов на доступ также может динамически меняться.

В работах [119; 120] предлагаются риск-ориентированные модели управления доступом к устройствам типа Internet of Things (IoT) и Internet of Vehicles (IoV). Значение риска рассчитывается на основе параметров: контекст пользо-

вателя и агента, ценности ресурса, критичность действия, базы данных рисков (история рисков). На основе полученного значения риска принимается решение о предоставлении доступа к объекту.

Авторы исследования [121] отмечают недостатки дискреционных (DAC), мандатных (MAC) и ролевых моделей управления доступом (RBAC) при функционировании в экосистемах больших данных. В статье описана риск-ориентированная модель управления доступом на основе контента (RCBAC), позволяющая решить проблему утечки конфиденциальных данных по вине внутренних нарушителей за счет применения риск-ориентированной модели управления доступом авторизованных пользователей к ресурсам. Разработанная авторами модель оценивает риск на основе содержимого данных, поведения пользователя при доступе к объекту и истории доступа пользователя. Поведение пользователя, атрибуты пользователя сравниваются с атрибутами объекта доступа, также учитывается контент запрашиваемого объекта. История доступа пользователя учитывает предыдущие запросы пользователя к объектам.

В работе [122] также отмечаются недостатки существующих моделей управления доступом для облачной инфраструктуры, поскольку статические методы описания правил доступа ведут к значительным рискам нарушения информационной безопасности и не могут полностью реализовать потребности и функционал облачных сервисов. Для решения обозначенных проблем авторы предлагают динамическую риск-ориентированную модель управления доступом. Модель состоит из четырех основных блоков: обнаружение аномалий на основе правил, оценка риска на основе потока данных, комплексное принятие решений, динамическая подстройка порогового значения риска.

В работе [123] приводится описание оценки риска как комплексного свойства, состоящего из идентификации, анализа и оценки риска. Цель идентификации риска заключается в определении событий, способных привести к потенциальной потере данных, и получить представление о причинах, способах и месте возникновения утечки данных. Идентификация риска включает риски независимо от того, находится ли их источник под контролем организации или нет, даже если источники или причины риска неочевидны.

Анализ риска определяет значения вероятности и последствия риска. Анализ рисков может быть выполнен с разной степенью детализации в зависимости от уязвимостей или инцидентов. Методология анализа риска включает в себя три подхода: качественный, количественный и комбинацию этих двух. Обычно

качественный анализ используется в качестве первого, поскольку он позволяет получить первую информацию об уровне риска и оценить, действительно ли риск критичен. После этого может быть проведена более подробная количественная оценка. Качественный анализ рисков использует шкалу, которая описывает степень риска (например, информативный, низкий, средний, высокий и критический) для воздействия на бизнес и вероятности возникновения угроз. Эта шкала может быть адаптирована к различным ситуациям и типам риска. Результат этого подхода представляется в виде строки данных (категории).

Количественный анализ риска использует числовое значение шкалы как для воздействия, так и для вероятности. Качество такого анализа зависит от качества входных данных (точности числовых значений) и достоверности используемых моделей (например, насколько они соответствуют поведению системы, корректируют данные измерений). Способ раскрытия воздействия и вероятности будет изменен в зависимости от типа риска и цели, для которой используется оценка риска. При анализе также следует учитывать неопределенность и изменчивость как влияния на бизнес, так и вероятности. Оценка риска – это процесс, используемый для сравнения результата оценки риска, достигнутого в ходе анализа, с заданными критериями риска, чтобы определить, является ли уровень риска приемлемым или нет.

Для определения риска в работе определяются 4 категории: место исходящего запроса (офис, дом, магазин, кинотеатр, аэропорт), время инициации запроса (8–16 ч., 16–22 ч., 22-6 ч., 6–8 ч.), сервис (банковский сектор, e-mail, серфинг сайтов, электронная коммерция), устройство (персональный компьютер, ноутбук, смартфон). Далее на основе веса контекста категории, веса безопасности контекста данных и фактора зависимости рассчитывается минимальный уровень безопасности объекта, который должен обеспечиваться.

Авторы исследования [124] описывают риск-ориентированную систему управления доступом с учетом конфиденциальности для систем обнаружения угроз. Каждый запрос на доступ оценивается системой путем сравнения риска конфиденциальности и надежности запроса. Когда риск слишком велик по сравнению с уровнем доверия, фреймворк может применять стратегии адаптивной корректировки для снижения риска (например, путем выборочного запутывания данных) или для повышения уровня доверия для выполнения заданной задачи (например, наложения на пользователя обязательных к исполнению

обязательств). Фреймворк может одновременно удовлетворять как требованиям конфиденциальности, так и требованиям полезности. Экспериментальные результаты, полученные авторами, показывают, что фреймворк приводит к значимым результатам и производительности в режиме реального времени в рамках решения для обнаружения промышленных угроз. Фреймворк состоит из 4 блоков: риск-ориентированный модуль управления доступом, блок оценки риска, модуль оценки доверия запроса, модуль управления доверием и риском.

Результаты сравнительного анализа традиционных и динамических моделей управления доступом представлены в таблице 7.

Таблица 7 — Сравнение основных параметров традиционных и динамических моделей управления доступом

	Традиционные модели	Динамические модели
Особенности	Используют предопределенные и статические политики для определения решения о доступе	Используют политики доступа и контекстные функции, которые собирают данные во время выполнения запроса на доступ
Решение о предоставлении доступа	Доступ предоставляется только в том случае, если он соответствует одному из правил политики доступа	Доступ предоставляется на основе контекста и политики. Решение может быть переопределено на основе контекста
Решение об отказе	Доступ отклоняется только в том случае, если есть несоответствие какому-либо правилу в политике доступа	Доступ отклоняется на основе контекста и политики. Изменение контекста может привести к немедленному изменению решения
Пример	ACL, DAC, MAC и RBAC являются распространенными и популярными подходами или примерами традиционного управления доступом	Известные примеры динамического управления доступом: на основе рисков, на основе доверия; сочетание риска с доверием
Применение	Приложения, которые не имеют доступа к функциям/атрибутам реального времени, таким как операционная система	Различным динамическим и распределенным системам требуется динамическое управление доступом для обеспечения большей гибкости, включая ОВС и др.

К достоинствам традиционных моделей управления доступом относятся: понятность и интерпретируемость; простота в тестировании и обслуживании; быстрое создание; данные модели отражают объективный метод, что позволяет получать более точный результат и им не требуются контекстные данные, что ускоряет принятие решений о доступе. Недостатки традиционных моделей управления доступом:

- не способны к адаптации в случаях изменения обстоятельств, влияющих на гибкость;
- в политике предусмотрены не все возможные условия, появление новых данных может привести к проблемам;
- решение не может быть масштабируемым, особенно при значительном объеме пользователей и объектов;
- существуют сложности с изменением/обновлением прав доступа некоторым пользователям.

При этом динамические модели управления доступом являются адаптированными к непредсказуемым ситуациям и условиям, которые не могут быть описаны стандартными политиками, позволяют повысить гибкость при доступе к системным ресурсам, обеспечивают устранение риска и угроз в режиме реального времени, особенно при работе с ранее не идентифицированной угрозой. При этом имеют следующие ограничения:

- более сложное определение, особенно при большом объеме контекстуальных атрибутов;
- домен/поле применения влияют на контекстуальные функции;
- есть сложности с выявлением эффективных контекстуальных функций;
- назначение веса контекстуальным функциям субъективно;
- обработка динамических объектов с учетом политики требует временных затрат;
- требуется больше вычислительной мощности.

Указанные недостатки не позволяют использовать традиционные (статические) модели управления доступом в распределенных информационных системах, в том числе в ОВС [125]. Для внедрения в ОВС, базирующихся на распределенных информационных системах, оптимальными являются динамические модели управления доступом, поскольку в них применяются не только политики доступа, но и механизмы учета контекста среды, которые функционируют в режиме реального времени и влияют на предоставление доступа к объекту ОВС. Стоит отметить, что динамические характеристики могут включать такие параметры как доверие, риск, контекст, историю и операционные потребности [62]. Что позволяет использовать наряду с динамическими моделями атрибутивные, в которых в качестве основного атрибута предоставления доступа предлагается значение риска реализации угроз информационной безопасности ОВС.

Представленные особенности позволяют перейти к разработке динамической атрибутивной модели управления доступом, основанной на анализе состояния динамически изменяющихся условий среды и учете получаемых оценок значений риска, для ОВС, базирующихся на распределенных информационных вычислительных системах, применяемых в организациях высшего образования.

2.2 Риск-ориентированная атрибутивная модель управления доступом для образовательных вычислительных сервисов организаций высшего образования

Для построения риск-ориентированной атрибутивной модели управления доступом для ОВС организаций высшего образования необходимо изучить функционирование и управление доступом в ОВС организаций высшего образования [126; 127].

2.2.1 Особенности управления доступом в организациях высшего образования

Влияние пандемии новой коронавирусной инфекции, а также существующие ограничения на использование ресурсов и информационных систем иностранного производства, позволили образовательным учреждениям осуществить переход на формат дистанционного обучения и использование новых сервисов и информационных технологий, функционирующих в распределенных информационных системах. В результате перехода разработано значительное число программ и информационных сервисов, ориентированных на глобальную информатизацию, которая способствовала бы эффективному управлению организацией, предоставлению учащимся образовательных услуг, в т. ч. с использованием дистанционных технологий. В результате чего остро встал вопрос об обеспечении информационной безопасности, обрабатываемой информации, в сочетании с поддержанием в актуальном состоянии предоставляемых

образовательных сервисов, возможности их модернизации, обновления и масштабируемости.

Информационная инфраструктура образовательных вычислительных сервисов учреждений высшего образования (образовательных учреждений) – совокупность программных, аппаратных, телекоммуникационных продуктов и ресурсов, необходимых для организации и реализации образовательного процесса, представлена на рисунке 2.2.

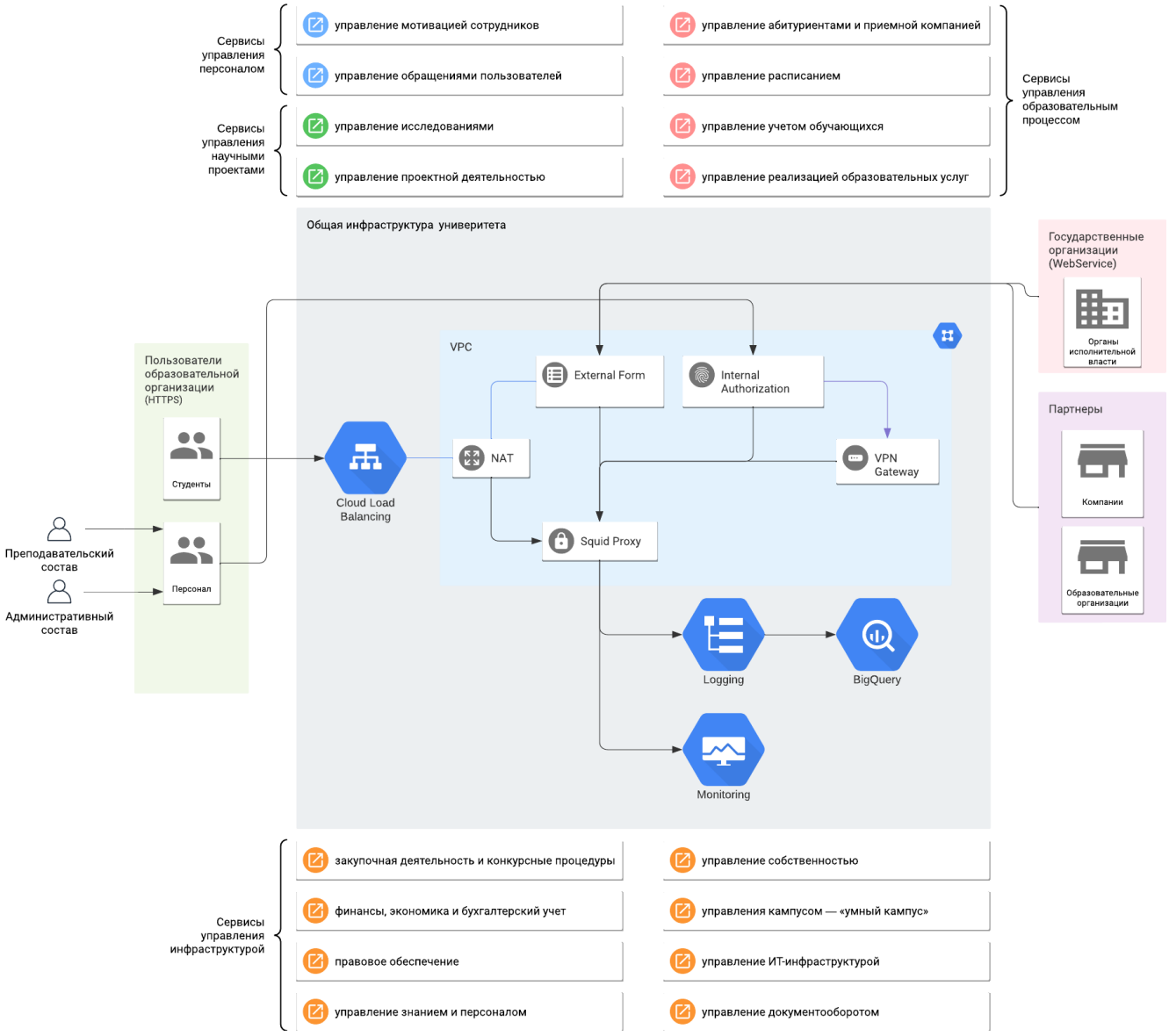


Рисунок 2.2 — Типовая структура информационной инфраструктуры сервисов высшего образования

К информационной инфраструктуре образовательных учреждений предъявляется требование обеспечения управления правами доступа всех пользователей, означающее, что в информационной системе должен быть разграничен

доступ пользователей к информационным ресурсам организации на основе заданных правил, при этом должен соблюдаться контроль выполнения указанных правил.

В схему управления доступом информационной инфраструктуры входят следующие компоненты:

1. Модели управления доступом (мандатные, дискреционные, ролевые).
2. Виды доступа (просмотр, внесение изменений, создание, удаление, выполнение).
3. Правила разграничения доступа, которые могут иметь привязку к ролям, спискам, значениям атрибутов меткам безопасности и др.

Каждая из классических моделей управления доступом обладает своими преимуществами и недостатками, наиболее распространенной (по причине доступности и простоты реализации) является ролевая модель управления доступом, в которой осуществляется создание ролей (пользователя), описывающих полномочия пользователей в соответствии с их должностными обязанностями. На основе ролей проводится проверка возможности выполнения того или иного действия пользователем. Если иерархия ролей задана согласно штатному расписанию (преподаватель, администратор, студент, и т. д.), то такой подход можно применять. Одной должности ставится в соответствие одна роль. Однако с увеличением сервисов, появлением новых кампусов, добавлением новых филиалов, ролевая структура усложняется и становится многомерной, что влечет за собой создание новых ролей, которые будут соответствовать комбинациям всех атрибутов. В результате чего будет сформировано большое количество ролей, которое приведет к стиранию границ контроля и предоставления доступа и сложности управления ввиду отсутствия четкой иерархии.

Представленные особенности позволяют сделать вывод, что использовании многомерной структуры, в которой реализуется управление доступом, ролевая модель становится не только бесполезной для управления доступом, но даже способствует появлению новых (ранее не существовавших) проблем. Для устранения ограничений ролевого управления доступом был разработан другой подход, основанный на атрибутах (ABAC) [128], главное отличие которого заключается в том, что отдельная ситуация оценивается не с позиции роли пользователя и действия, которое он планирует выполнить, а с точки зрения относящихся к нему атрибутов. При этом под регламентом в разработанной модели понимается набор условий, где разные атрибуты должны соответство-

вать требованиям, предъявляемым к ним для предоставления доступа. Для построения атрибутивной модели управления доступом сформированы атрибуты, применяемые в образовательных вычислительных сервисах организаций высшего образования.

2.2.2 Атрибуты безопасности управления доступом в образовательных вычислительных сервисах организаций высшего образования

Атрибутивная модель управления доступом не ограничивает сложность процессов. Из-за более простой реализации в рамках применения этого подхода стоимость поддержки при реализации более сложных правил не увеличивается. Кроме того, появляется возможность обеспечения управления доступом и к действиям, и к данным. Данная модель является набором условий, в которых атрибуты должны соответствовать требованиям, предъявляемым к ним. Можно явно выделить несколько категорий атрибутов:

- атрибуты ресурса (тип, создатель, стоимость, название и т. д.);
- атрибуты субъекта (имя, отдел, должность, лимит утверждений и т. д.);
- атрибуты действия (название);
- атрибуты среды (IP-адрес, время, устройство).

Для того чтобы выполнить авторизацию, сравнивают значения всех атрибутов в момент проверки прав и ожидаемые значения. Доступ к ресурсу обеспечивается при выполнении всех условий. Спроектируем информационную инфраструктуру образовательного учреждения с применением атрибутивной модели управления доступом. Инфраструктура образовательного учреждения включает в себя значительное число связанных между собой элементов, безопасность которых необходимо обеспечить:

- сервисы управления образовательным процессом;
- сервисы управления научными проектами;
- сервисы управления персоналом;
- сервисы управления доступом;
- сервисы бухгалтерского учета;
- сервисы управления инфраструктурой и т. д.

Среди угроз информационной инфраструктуре организации, работающей в сфере образования, можно назвать рассылку сообщений с вредоносными вложениями, попытки несанкционированного доступа к данным организации и многие другие. Злоумышленники разрабатывают все более совершенные механизмы атаки на информационные системы организаций, в т.ч. образовательных учреждений. Тогда в качестве атрибутов доступа информационных сервисов высшего образования можно выделить следующие атрибуты:

- 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.

Необходимым требованием к информационной инфраструктуре организации является обеспечение защиты информационной образовательной среды организации и постоянного мониторинга и верификации пользователей. При этом пользователь должен иметь возможность оставаться в сеансе доступа к информационному ресурсу в течение времени, необходимого для работы. Работы в области адаптивной безопасности [129] показали, как применять этот вид проверок на основе различных техник. В качестве такой техники может выступать контекстно-зависимая безопасность. Данный подход опирается на контекстно-зависимую информацию, такую как геолокация, время доступа, репутация определенного IP-адреса или домена, тип используемого устройства и т. д., для принятия решения о предоставлении доступа. Указанная информация, собранная и обработанная динамически, может обеспечить большую защищенность и гранулярность относительно статических методов. Кроме того,

представленная концепция может быть реализована в контексте аутентификации и авторизации в распределенных информационных системах, где решение о предоставлении доступа может быть основано на различных процедурах или атрибутах в зависимости от контекста конкретного запроса.

Дополнительной техникой является инкрементная (интеллектуальная) безопасность. Такой подход сочетает в себе различные методы и инструменты, такие как большие данные, аналитика или управление информацией и событиями безопасности (SIEM, Security information and event management), для обнаружения аномалий, выбросов или отклонений от стандартного поведения и принятия соответствующих мер. Инкрементальная/интеллектуальная безопасность основана на сборе, стандартизации и анализе данных, генерируемых сетями, приложениями, базами данных, журналами и другой инфраструктурой в режиме реального времени. Эта информация оценивается и обрабатывается (с помощью машинного обучения, распознавания образов и т.д.) для перевода данных в удобочитаемый формат, который поддерживает принятие обоснованных решений.

Рассмотренные атрибуты управления доступом в образовательных вычислительных сервисах организаций высшего образования могут быть применены в процессе построения риск-ориентированной атрибутивной модели управления доступом для образовательных вычислительных сервисов организаций высшего образования только совместно с атрибутом, связанным со значением риска реализации угрозы информационной безопасности.

2.2.3 Риск-ориентированная атрибутивная модель управления доступом в образовательных вычислительных сервисах организаций высшего образования, учитывающая оценки значений риска

Модель управления доступом на основе рисков является динамической моделью, которая функционирует в режиме реального времени и использует контекстную информацию в качестве атрибута доступа для принятия решений о предоставлении доступа к объекту. Данная модель основана на осуществлении расчета риска по каждому запросу на доступ к объекту и принятии решения в режиме реального времени (динамическое решение) на основе по-

лученного значения риска. Необходимость разработки риск-ориентированной модели управления доступом заключается в отсутствие механизмов обеспечения оперативного, надежного и точного метода оценки риска, в том числе при отсутствии исходных данных для количественного описания риска и оценки его воздействия на защищаемые информационные ресурсы в процессе предоставления доступа [130].

Обеспечение информационной безопасности в режиме реального времени образовательных вычислительных сервисов организаций высшего образования на основе рисков позволяет идентифицировать различные риски каждого из активов организации, расставляя приоритеты в отношении потенциальных убытков, размера нанесенного ущерба, возможности дальнейшего использования активов, сохранение функциональности и т. д., что позволяет осуществить уменьшение суммарного значения риска до требуемого уровня. В процессе обеспечения информационной безопасности в режиме реального времени также необходимо отслеживать, измерять и оценивать существующие риски для того, чтобы обеспечить требуемый уровень защищенности информации. Кроме того необходимо разработать методы противодействия обнаруженным рискам в процессе функционирования образовательных вычислительных сервисов.

На рисунке 2.3 представлена риск-ориентированная атрибутивная модель управления доступом для организаций высшего образования. Оценка риска реализации угроз производится на основе анализа событий безопасности в SIEM-системе и анализа поведения пользователей с учетом, выбранных ранее атрибутов управления доступом в образовательных вычислительных сервисах организаций высшего образования.

Выбор подхода к количественной оценке рисков должен быть основан на существующих ограничениях и допущениях, принятых в ОВС организации высшего образования, базирующихся на распределенных информационных системах, а также должен учитывать:

– существующие уязвимости и угрозы безопасности информации;
– потенциал нарушителя и его потенциальные возможности;
– используемые атрибуты безопасности управления доступом.

Разработка модели и ее валидация производилась в среде Security Policy Tool [134]. Для субъектов и объектов модели были заданы атрибуты, описанные в разделе 2.2.2 (рис. 2.4). Помимо этого заданы две политики атрибутивного

управления доступом, в одной из которых производился учет значения рисков, а в другой – нет (рис. 2.5).

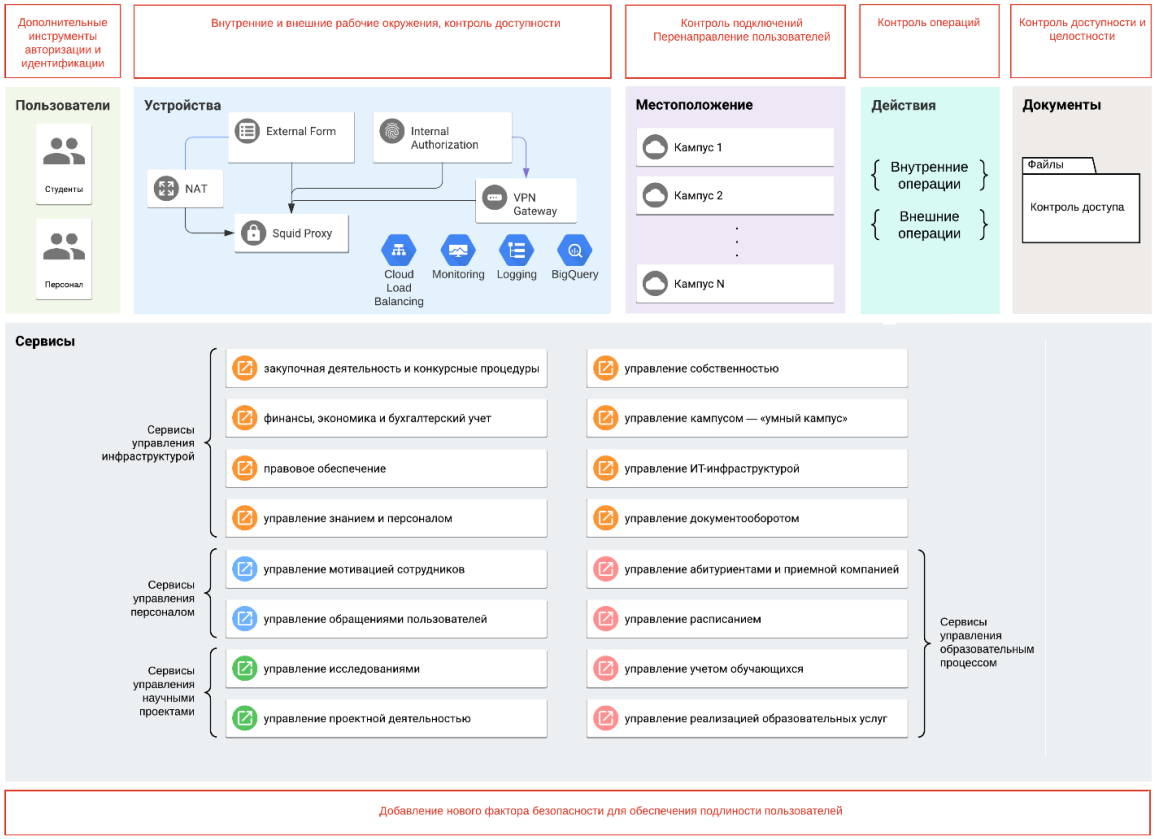


Рисунок 2.3 — Риск-ориентированная атрибутивная модель управления доступом для ОВС системы высшего образования

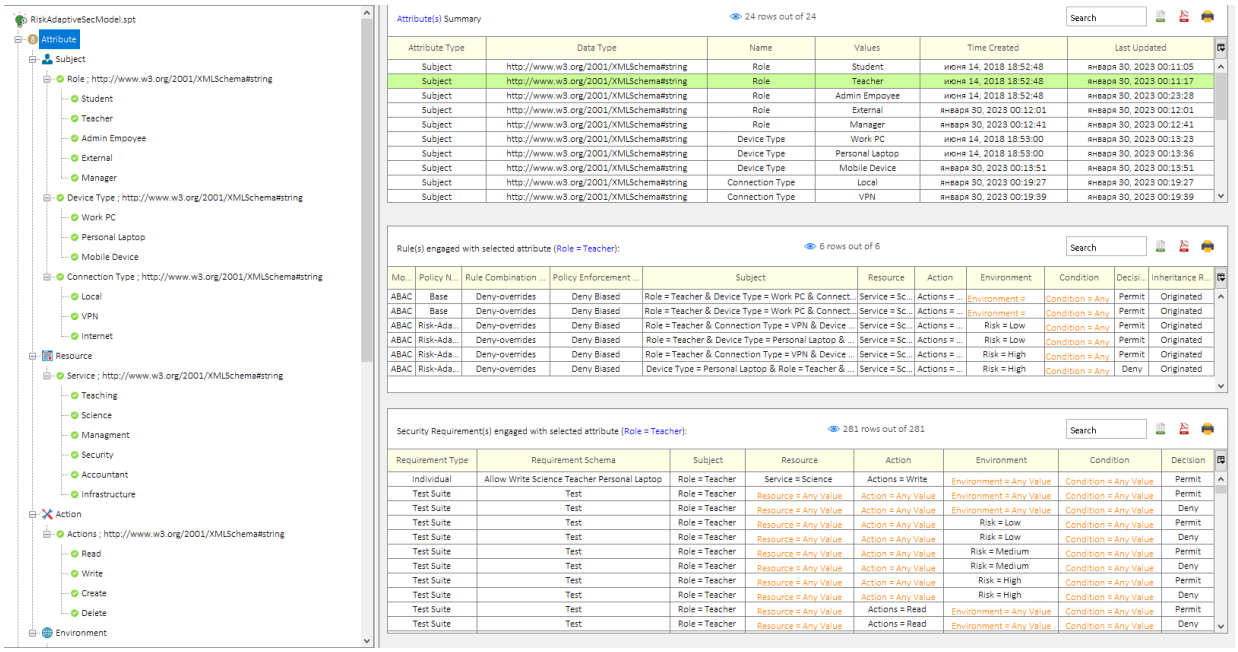


Рисунок 2.4 — Атрибуты объектов и субъектов модели управления доступом

ABAC(s) Summary — 2 rows out of 2 — Search

Model	Policy Name	Rule Combination Algorithm	Policy Enforcement Algorithm	No. of Rule(s)	Time Created	L
ABAC	Base	Deny-overrides	Deny Biased	2	января 30, 2023 00:23:01	января
ABAC	Risk-Adaptive	Deny-overrides	Deny Biased	4	января 30, 2023 00:26:16	января

Rule (s) defined with selected policy (Risk-Adaptive): — 4 rows out of 4 — Search

Sequence No	Subject	Resource	Action	Environment	Condition	Decision
1	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = Low	Condition = Any Value	Permit
2	Role = Teacher & Device Type = Personal Laptop & Connection Type = VPN	Service = Science	Actions = Write	Risk = Low	Condition = Any Value	Permit
3	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = High	Condition = Any Value	Permit
4	Device Type = Personal Laptop & Role = Teacher & Connection Type = VPN	Service = Science	Actions = Write	Risk = High	Condition = Any Value	Deny

Рисунок 2.5 — Политики атрибутивного управления доступом

В качестве приоритетного подхода к количественной оценке риска ОВС может быть использован подход к оценке рисков на основе нечетких множеств [131]. Предлагаемый подход может позволить осуществить переход от статичных правил управления [132; 133] к динамически изменяемым, при этом, описываемым атрибутивной моделью управления доступом, в которой значение риска является дополнительным атрибутом безопасности.

В риск-ориентированной модели управления доступом при доступе преподавателя к научным сервисам с личного ноутбука при подключении VPN и высоком значении риска доступ на запись запрещен. Для валидации корректности модели был задан инвариант безопасности, разрешающий доступ преподавателя к научным сервисам с личного ноутбука при подключении VPN на запись. Тестирование моделей позволило выявить невыполнение данного инварианта для риск-ориентированной модели управления доступом (рис. 2.6).

Policy Verification (января 30, 2023 00:31:53)(s) Summary — 1 rows out of 1 — Search

Status	Name	Verification T...	Verification Tech...	Number of Poli...	Combination Algo...	Enforcement Algor...	Policy List
Outdat...	Policy Verification (января 30, 2023 ...	Standard	Merged Policy	2	Deny-overrides	Deny Biased	ABAC:Base, ABAC:Risk-A...

Warning : Changes to following input parameter(s) may render previous verification result inaccurate.

Requirement Schema(s) : Allow Write Science Teacher Personal Laptop

Please Refresh Policy Verification (января 30, 2023 00:31:53)(s) to ensure recent changes are updated in your results.

Result(s) with selected verification (Policy Verification (января 30, 2023 00:31:53)) — 2 rows out of 2 — Search

Requirement Schema	Subject	Resource	Action	Environment	Condition	Decision	Verification Result
Test	Role = Teacher	Service = Science	Actions = Write	Environment = Any Value	Condition = Any Value	Permit	FALSE
Test	Device Type = Personal Laptop	Service = Science	Actions = Write	Environment = Any Value	Condition = Any Value	Permit	FALSE

Рисунок 2.6 — Результаты тестирования инварианта безопасности для заданных политик

Невыполнение указанного инварианта подтверждает корректную работу модели с учетом анализа рисков безопасности. Дополнительно была сгенерирована политика в формате XACML (eXtensible Access Control Markup Language) для обеспечения возможности использования ее в инфраструктуре образовательных организаций (рис. 2.7). Расширяемый язык разметки управления доступом (XACML) – это открытый стандарт для авторизации и управления доступом, который обеспечивает детальный контроль над тем, кто из пользователей имеет доступ к каким ресурсам и какие действия может выполнять. Он используется для определения политик управления доступом в распределенных системах и приложениях [135].

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicySetId="urn:infobeyondtech:securitypolicytool:Untitled1:ABAC" PolicyCombiningAlgId=
"urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable" Version="1.0">
  <Target></Target>
  <Policy PolicyId="urn:infobeyondtech:securitypolicytool:UniversityTestCase3.spt:ABAC:Base" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:ordered-deny-overrides"
    <Target></Target>
    <Rule Effect="Permit" RuleId="rule_1">
      <Target>
        <AnyOf>
          <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Teacher</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::subjectcategory:accesssubject" AttributeId="urn:oasis:names:tc:xacml:1.0:subject:Role" DataType="http://www.w3.org/
MustBePresent="true"></AttributeDesignator>
            </Match>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Work PC</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::subjectcategory:accesssubject" AttributeId="urn:oasis:names:tc:xacml:1.0:subject:Device Type" DataType=
"http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">VPN</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::subjectcategory:accesssubject" AttributeId="urn:oasis:names:tc:xacml:1.0:subject:Connection Type" DataType=
"http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Science</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::attributecategory:resource" AttributeId="urn:oasis:names:tc:xacml:1.0:resource:Service" DataType="http://www.w3.org/
MustBePresent="true"></AttributeDesignator>
            </Match>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Read</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::attributecategory:action" AttributeId="urn:oasis:names:tc:xacml:1.0:action:Actions" DataType="http://www.w3.org/2001
MustBePresent="true"></AttributeDesignator>
            </Match>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Any Value</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::attributecategory:environment" AttributeId="urn:oasis:names:tc:xacml:1.0:environment:Environment" DataType=
"http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/xmlschema#string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Any Value</AttributeValue>
              <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::attributecategory:condition" AttributeId="urn:oasis:names:tc:xacml:1.0:condition:Condition" DataType="http://www.w3.
MustBePresent="true"></AttributeDesignator>
            </Match>
          </AllOf>
        </AnyOf>
```

Рисунок 2.7 — Фрагмент риск-ориентированной политики управления доступом на языке XACML

Разработанная риск-ориентированная атрибутивная модель управления доступом позволяет осуществить переход от статических правил управления доступом, используемых в классических моделях управления доступом, к динамическим, изменяющимся правилам с учетом оценки рисков реализации угроз. В качестве разрабатываемого подхода к количественной оценке риска выступает подход на основе математического аппарата нечеткой логики.

Сформированная риск-ориентированная атрибутивная модель управления доступом позволяет осуществить управление доступом субъектов ОВС, базирующихся на распределенных информационных системах, посредством основных атрибутов защищаемого ресурса, субъекта доступа, осуществляемого

действия, атрибута среды, а также количественного атрибута, характеризующего количественное значение риска реализации угрозы информационной безопасности ОВС. Для практической реализации разработанной риск-ориентированной атрибутивной модели управления доступом необходимо разработать метод количественной оценки рисков реализации угроз информационной безопасности.

2.3 Выводы по второй главе

Во второй главе проведен анализ исследований в области моделей управления доступом. В ходе проведенного анализа рассмотрены основные подходы к построению моделей управления доступом, определены их достоинства и недостатки, обоснован выбор атрибутивной модели управления доступом для повышения защищенности образовательных вычислительных сервисов организаций высшего образования. В ходе разработки атрибутивной модели управления доступом доказана необходимость внедрения дополнительного атрибута безопасности, основанного на количественной оценке значения риска реализации угроз информационной безопасности образовательных вычислительных сервисов организаций высшего образования.

Для внедрения предлагаемой риск-ориентированной атрибутивной модели управления доступом проведено исследование построения систем управления доступом в организациях высшего образования, определены используемые атрибуты безопасности управления доступом в образовательных вычислительных сервисах организаций высшего образования. На основе полученных атрибутов и рассмотренных моделей управления доступом разработана риск-ориентированная атрибутивная модель управления доступом для образовательных вычислительных сервисов организаций высшего образования, позволяющая учитывать динамически меняющееся значение риска реализации угроз при принятии решения о предоставлении доступа к защищаемым ресурсам образовательных вычислительных сервисов.

Глава 3. Метод количественной оценки рисков реализации угроз информационной безопасности, основанный на анализе событий, создаваемых агентами информационной системы

В главе рассматривается разработанный метод количественной оценки рисков реализации угроз информационной безопасности для образовательных вычислительных сервисов организаций высшего образования, основанный на анализе событий, создаваемых агентами распределенной информационной системы, посредством применения математического аппарата нечеткой логики. Разработанный метод базируется на проведенном анализе существующих подходов к количественной оценке рисков и разработанной системе интеллектуальных агентов, осуществляющих сбор и агрегирование событий безопасности, соответствующим атрибутам разработанной риск-ориентированной атрибутивной модели управления доступом.

3.1 Базовые основы риск-ориентированного подхода

Минимизация рисков реализации угроз несанкционированного доступа к образовательным сервисам остается одной из наиболее актуальных проблем в области функционирования систем высшего образования, базирующихся на распределенных информационных системах [136]. При этом разработке специализированного решения, ориентированного на особенности использования вычислительных ресурсов и позволяющего учесть структуру данных, скорость и частоту обмена информацией, а также возможности вычислительных ресурсов и другие условия, посвящено большое количество исследований. Так представлены решения в области защиты данных систем интернета вещей (IoT) [137], анализа рисков для обеспечения безопасности Smart Grid [138], оценки рисков безопасности данных SCADA (Supervisory Control And Data Acquisition) [139; 140], защиты системы управления энергопотреблением EMS (Energy Management System) [141], оценки уровня конфиденциальности социальных сетей Интернета [142; 143], контроля соответствия требований информационной безопасности организации [144] и учреждений здравоохранения [145].

Стоит отметить, что организации защиты информации систем образования посвящены отдельные работы по нескольким направлениям исследований [146—148], что, в свою очередь, требует проведения дополнительных исследований в данной области. Одним из возможных решений по управлению уровнем защищенности являются анализ и оценка рисков [149]. Мониторинг, анализ и регулирование уровня риска при доступе к образовательным ресурсам является сложной задачей со многими неизвестными. Решением указанной проблемы может выступать применение разработанной риск-ориентированной атрибутивной модели управления доступом, динамически изменяющей правила доступа в зависимости от текущего значения риска реализации угроз информационной безопасности.

Концепция риска определяется согласно стандартам Международной организации по стандартизации (ISO) [150; 151] как эффект (положительное и/или отрицательное отклонение от ожидаемого) неопределенности на цели (которые могут иметь различные аспекты, такие как финансовые, здоровье, безопасность и т. д.) [152]. В практических случаях риск часто выражается как комбинация последствий, затрат или воздействия события, включая изменения обстоятельств, и соответствующая вероятность его возникновения. В информационной системе риск безопасности соответствует риску, который возникает из-за утраты конфиденциальности, целостности или доступности информации и данных, а также услуг или систем, определенных как основные требования безопасности. Риски кибербезопасности – это риски безопасности, которые могут возникнуть в киберпространстве в следствии реализации кибератак. Этот вид риска связан с негативными последствиями для пользователя, организации (активы, цели, репутация и т. д.) или государства [153].

В соответствии со стандартом ISO 31000 [150] оценка рисков – это процесс, который можно разделить на идентификацию, анализ и оценку рисков. К идентификации рисков относится распознавание и описание опасностей и факторов риска. Анализ рисков состоит из объяснения сути опасностей, выявлении уровней рисков и их оценке. Сравнение значений риска с учетом существующих критериев определения их значимости – это оценка риска, которая может основываться на различных подходах. Управление рисками представляет собой набор целенаправленных действий по управлению функционированием системы, проектом или организацией с учетом возможных рисков. В сфере безопасности и кибербезопасности процесс управления рисками состоит из ком-

плекса мероприятий, направленных на защиту данных, услуг и систем от киберугроз, таких как несанкционированный доступ, с целью: поддержания осведомленности о киберугрозах и киберугрозах, выявления аномалий, неправильных конфигураций и инцидентов, отрицательно влияющих на систему и/или данные и смягчения последствий, реагирования на инциденты и восстановления после них.

Как показано на рисунке 3.1, процесс управления рисками согласно ISO 31000 состоит в систематическом применении набора политик, процедур и практик к следующим действиям: коммуникация и консультация; установление контекста, оценка рисков (идентификация рисков, анализ и оценка), обработка рисков, мониторинг и рассмотрение рисков.

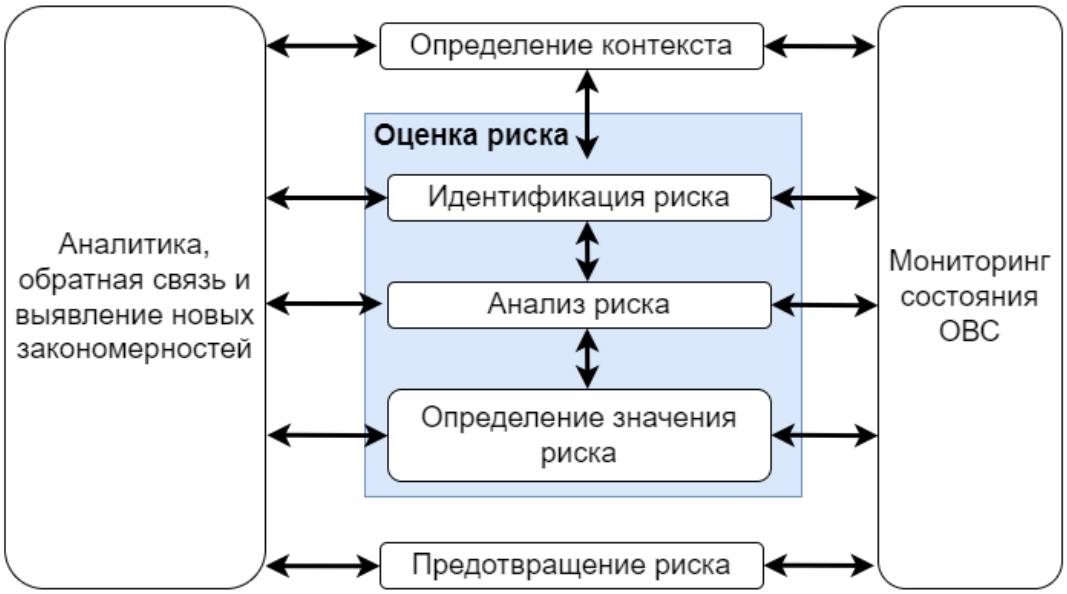


Рисунок 3.1 — Функциональная схема процесса управления рисками

Реализация требований ISO 31000 позволяет использовать методы анализа, оценки и управления рисками при разработке моделей управления доступом, базирующихся на количественных значениях риска в информационной системе.

3.2 Модель управления доступом, основанная на риске

В контексте информационной безопасности распределенных информационных систем под риском понимается вероятность возникновения инцидента в

будущем и соответствующие ему убытки. В [154] риск определен как "возможный ущерб, который может возникнуть в результате существующей операции или какого-либо предстоящего инцидента". Риск безопасности в сфере безопасности информационных технологий - это ущерб, влияющий на бизнес-процессы организации и информацию, связанную с ними. Процесс выявления, предупреждения и устранения инцидентов, которые могут привести к нарушению конфиденциальности, целостности или доступности информационной системы, называется управлением рисками [154].

В контексте управления доступом риск безопасности можно изучать как сочетание возможности утечки информации, которая может произойти при доступе к системным ресурсам, и ее ценности [63]. Модель управления доступом, основанная на рисках, использует оценку риска безопасности в качестве критерия для принятия решения о доступе для каждого запроса. Модель основана на динамической оценке значения риска безопасности, связанного с каждым запросом субъекта на доступ к объекту (рис. 3.2).

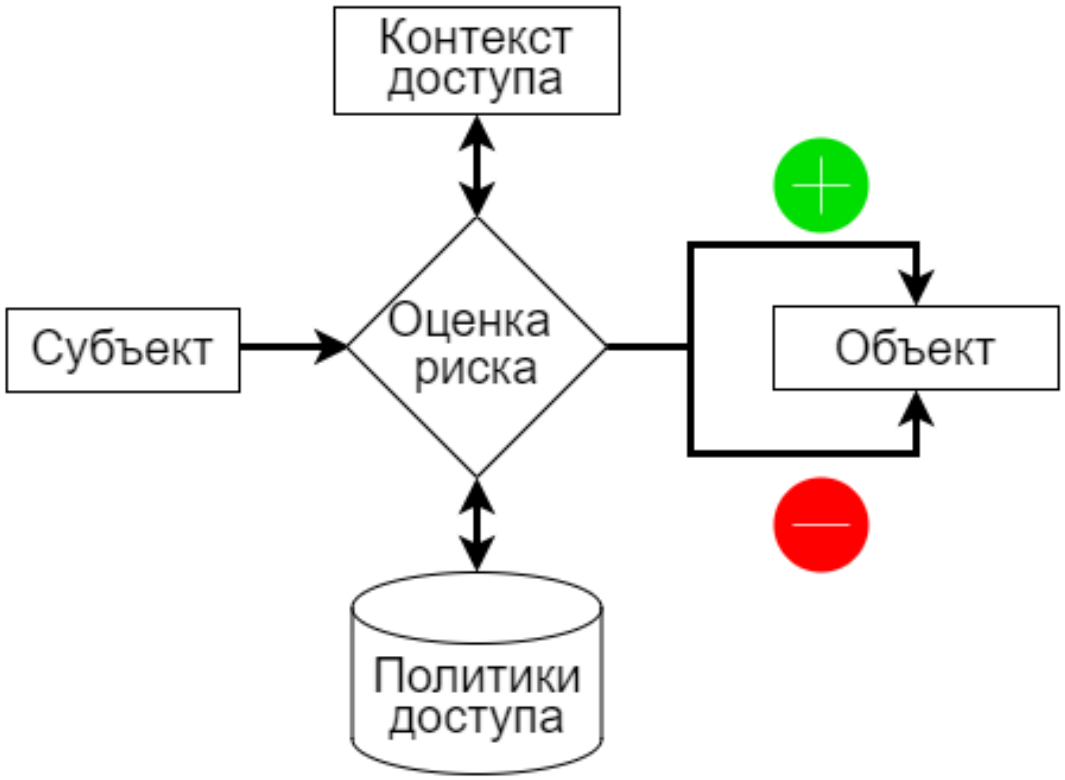


Рисунок 3.2 — Модель управления доступом на основе анализа риска

На рисунке 3.2 представлена модель управления доступом на основе анализа риска. Наиболее широко используемая формула количественного представления риска – это вероятность того, что инцидент произойдет, умноженная

на воздействие, связанное с этим инцидентом [155]. Модель управления доступом на основе рисков включает в себя три основных модуля. Главный модуль – это оценка рисков. Этот модуль собирает запросы на доступ от пользователей, анализирует их, получает информацию о факторах риска и оценивает величину риска для всех запросов. После этого оцененное значение риска сопоставляется с политиками доступа, для вынесения решение о доступе или отказе в доступе.

Основные проблемы, связанные с созданием динамической модели управления доступом в ОВС представлены на рисунке 3.3. К проблемам создания динамических моделей управления доступом в ОВС относятся:

1. Техническая надежность: связана с безопасностью ОВС и входящих в ее состав сервисов. Разнообразный и не унифицированный состав устройств доступа и расширяющийся перечень сервисов ОВС требует наличия динамических механизмов управления доступом пользователей.
2. Устаревшая/отсутствующая инфраструктура: многие вузы по-прежнему используют бумажные носители и имеют устаревшую цифровую инфраструктуру. Создание современной и безопасной ОВС требует наличия унифицированного и минимально необходимого состава оборудования и ПО. Кроме того, устаревшее ПО, неактуальные прошивки устройств, входящих в состав инфраструктуры, существенно снижают защищенность ОВС в целом.
3. Масштабируемость: современная ОВС требует работы в режиме реального времени и наличия обширного перечня доступных сервисов и устройств, подключенных одновременно. В результате система должна быть способна обрабатывать значительные объемы данных. Потребуются большие емкости хранилища и вычислительные ресурсы. Кроме того, необходимо предусмотреть легко настраиваемые и модифицируемые механизмы управления доступом.
4. Идентификация и анализ рисков: Определение потенциальных угроз безопасности и уязвимостей в системе дистанционного образования требует тщательного исследования. Это может включать в себя анализ возможных угроз для конфиденциальности личных данных студентов, целостности учебного контента и доступности системы.
5. Адаптация стандартных моделей к дистанционному образованию: многие существующие модели управления доступом разработаны для

корпоративных или административных сред, и они могут не полностью соответствовать уникальным требованиям систем дистанционного образования. Необходимо адаптировать такие модели для учета специфики образовательных процессов и потребностей студентов.

6. Управление доступом к контенту: эффективное управление доступом к учебному контенту требует учета различных ролей пользователей (студентов, преподавателей, администраторов) и соответствующих им разрешений. Проблемы могут возникнуть при определении, какой контент должен быть доступен для каждой группы пользователей, и каким образом это должно регулироваться.
7. Мониторинг активности пользователей: необходимость отслеживания и анализа активности пользователей для выявления подозрительного поведения или нарушений безопасности является важным аспектом риск-ориентированной модели управления доступом. Проблемы могут возникнуть в разработке эффективных механизмов мониторинга и обработке больших объемов данных.
8. Управление рисками: разработка методов оценки и управления рисками, специфичными для дистанционного обучения, требует учета особенностей такой среды обучения, а также уровня конкретных угроз и их влияния на учебные процессы и информационную безопасность.
9. Комплексность окружения: дистанционное обучение часто включает в себя различные виды информационных ресурсов, платформ, приложений и устройств, что увеличивает сложность управления доступом и рисками безопасности в таком разнообразном окружении.
10. Соблюдение нормативных требований: создание модели управления доступом должно учитывать соблюдение законодательства и нормативных требований в области безопасности данных и образования, что также может быть достаточно сложным процессом.
11. Адаптация к динамическому окружению: дистанционное образование подвержено быстрой эволюции технологий и изменениям в требованиях к безопасности. Модель управления доступом должна быть способной адаптироваться к таким изменениям и эффективно реагировать на новые угрозы.
12. Обеспечение удобства использования ОВС: важно найти баланс между безопасностью и удобством использования для студентов и препо-

давателей, чтобы не создавать излишней неудобства при доступе к образовательным ресурсам.

Рисунок 3.3 — Основные проблемы при создании динамической модели на основе рисков

Процесс управления рисками (риск-менеджмент) по существу связан с двумя фундаментальными концепциями: доверием и риском (рис. 3.4). Важно уточнить, что обе концепции (доверие и риск) тесно связаны друг с другом. Так субъект или система с низким уровнем доверия рассматривается как субъект с высоким уровнем риска и наоборот. Поэтому при рассмотрении доверия основной целью является установление и оценка достоверности рассматриваемой среды. Что касается интеграции оценки риска в ОВС, то процесс оценки риска может осуществляться одним из следующих методов анализа: качественным, количественным или их комбинацией. Качественные подходы основаны на определении качественных характеристик с целью описания потенциальных последствий с соответствующими вероятностями их возникновения. В практических случаях при использовании качественного подхода обычно происходит ориентация на снижении риска, без оценки его конкретного значения. В отличие от описательных характеристик, количественные подходы используют

числовые значения как для последствий, так и для связанных с ними вероятностей. В практических случаях при использовании количественного подхода обычно. ориентируются на оценку значения риска.

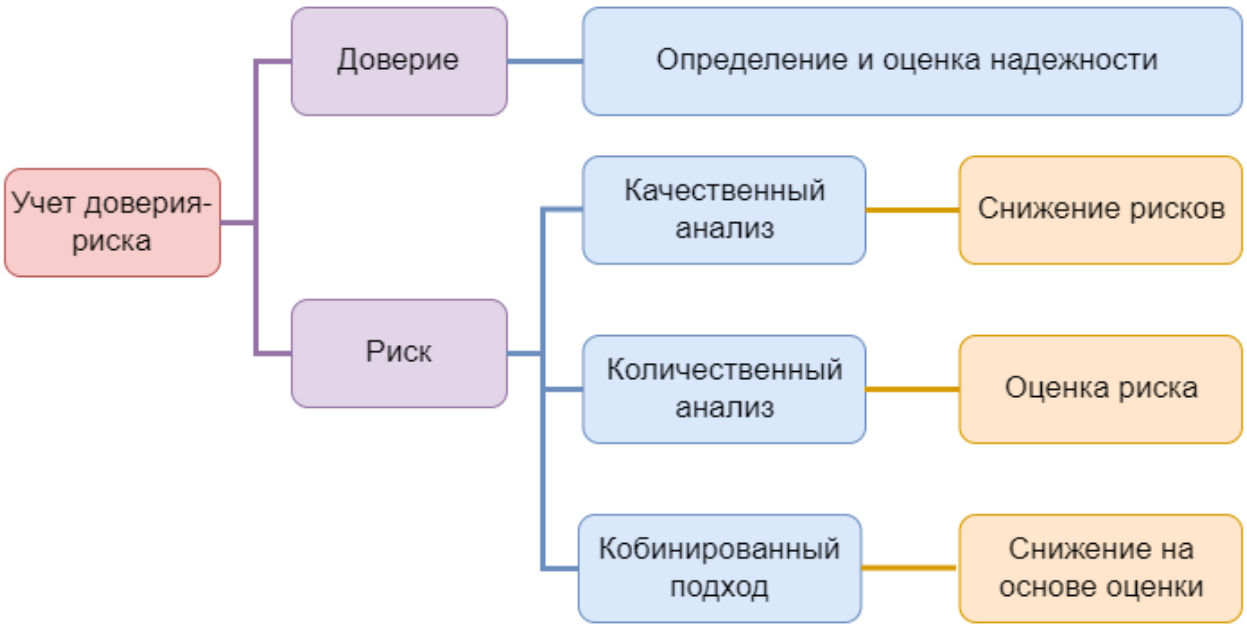


Рисунок 3.4 — Схема модели на основе рисков

В качестве реализации модели управления доступом на основе риска может применяться модель адаптивного управления доступом на основе рисков (AdRBAC, Adaptive Role Based Access Control).

3.3 Адаптивное управление доступом на основе рисков (AdRBAC)

Данная модель использует контекстные функции пользователя в реальном времени, чувствительность к ресурсам, серьезность действий и историю рисков в качестве входных данных для оценки величины риска безопасности каждого запроса на доступ. В существующих моделях управления доступом, основанных на оценке рисков, нет способа обнаружить вредоносные действия пользователей во время сеанса доступа. Данная модель устраняет указанный недостаток и отслеживает поведение пользователя во время сеанса доступа для обнаружения любых аномальных действий.

В ряде исследований оценка риска безопасности использовалась для создания динамических моделей управления доступом. В работе [156] предложены

три основных компонента для модели управления доступом, основанной на риске: оценка величины риска, связанного с запросом на доступ; определение уровней приемлемости риска и контроль обмена информацией на основе полученной величины риска и политик управления доступом. Макгроу [52] предложил механизм адаптируемого к рискам доступа. Данная модель оценивает риск безопасности и оперативные потребности для обеспечения доступа. Она оценивает риск, связанный с запросом на доступ, а затем сравнивает его с политикой управления доступом и оперативными потребностями для принятия окончательного решения о доступе. Однако модель не предоставляет подробной информации о том, как оценить риск и операционные потребности количественно. Кроме того, Кандала и др. [53] предложили подход, который идентифицирует различные компоненты риска модели, представленной в работе [156], используя подход к управлению доступом на основе атрибутов.

Модель гибкого управления доступом на основе рисков, предложенная в работе [54], использует оценку величины риска, связанного с запросом доступа, в зависимости от результатов действий с точки зрения доступности, конфиденциальности и целостности. Недостатками модели является отсутствие данных об оценке величины риска для каждого состояния системы и для каждого результата действия, соответственно в ней отсутствуют функции адаптации к риску. Хамбхамметту и другие авторы [55] предложили структуру, основанную на оценке ценности объекта, надежности субъекта и разнице между значением ценности объекта и надежностью объекта с использованием оценки риска. Однако в этой системе не предусмотрена оценка величины риска для каждой ситуации окружающей среды. Кроме того, данный подход требует от системного администратора присвоения разумного значения каждой входной функции на ранней стадии процесса оценки рисков, что создает сложность в использовании подхода в больших распределенных вычислительных системах. Также отсутствует функция адаптации к рискам.

Шарма и др. [61] предложили модель управления доступом на основе оценки величины риска, связанного с запросом доступа. Значение риска вычисляется с точки зрения различных действий и соответствующих намерений субъектов доступа. Результаты и вероятность риска определяются вместе с уровнем чувствительности данных. Полученное значение риска сравнивается с пороговым значением риска для определения решения о доступе. Однако в этой модели не используются механизмы, функционирующие в режиме реально-

го времени в процессе оценки риска и отсутствуют функции адаптации к риску. В работе Ли и др. [62] разработана контекстная модель управления доступом, основанная на риске. Модель извлекает весь возможный контекст и оценивает его с точки зрения безопасности. Оценка рисков с помощью многофакторного процесса оценки применяется для оценки величины связанного риска. Величина риска основана на результатах действий с точки зрения доступности, конфиденциальности и целостности. В модели игнорируется поведение пользователей в прошлом, а также отсутствуют функции адаптации к риску.

В работе [63] предложена модель управления доступом, основанная на оценке рисков, которая использует количественную оценку показателей риска и их агрегирование. Она основана на идее политик рисков, которые позволяют поставщикам услуг и владельцам ресурсов определять свои собственные показатели, обеспечивая большую гибкость системы управления доступом. Однако для обеспечения минимальной безопасности в этой модели требуется системный администратор. Модель не может функционировать в режиме реального времени, и в ней отсутствуют функции адаптации к рискам.

Представленные модели управления доступом, основанные на оценке рисков, концентрируются только на принятии решений о доступе, не предоставляя никакого способа предотвратить аномальный и нестандартный доступ к данным со стороны авторизованных пользователей. Для построения метода количественной оценки риска могут выступать подходы динамического управления доступом. Динамическое управление доступом использует контекст реального времени для принятия решения о доступе. Одной из этих функций является оценка риска безопасности, связанного с запросом на доступ, который является основным элементом модели управления доступом на основе рисков. Модель выполняет анализ рисков для принятия решения о доступе. Как показано на рисунке 3.5, модель AdRBAC имеет четыре входных сигнала, контекст пользователя/агента, чувствительность к ресурсам, серьезность действий и история рисков.

Входные данные (факторы риска) используются для оценки риска безопасности, связанного с каждым запросом на доступ. Оцененное значение риска затем сравнивается с политиками рисков для принятия решения о доступе. Для обеспечения адаптивных функций оценки поведение субъектов оценивается для обнаружения любых ненормальных действий во время сеанса доступа. Эта модель обеспечит соответствующий уровень безопасности, обеспечивая при этом

гибкость и масштабируемость системы управления доступом в ОВС. Кроме того, предлагаемая модель может хорошо работать в приложениях, где часто происходят непредвиденные ситуации нарушения политик безопасности. Это может произойти из-за того, что политики являются неполными или непоследовательными, иногда даже противоречивыми.

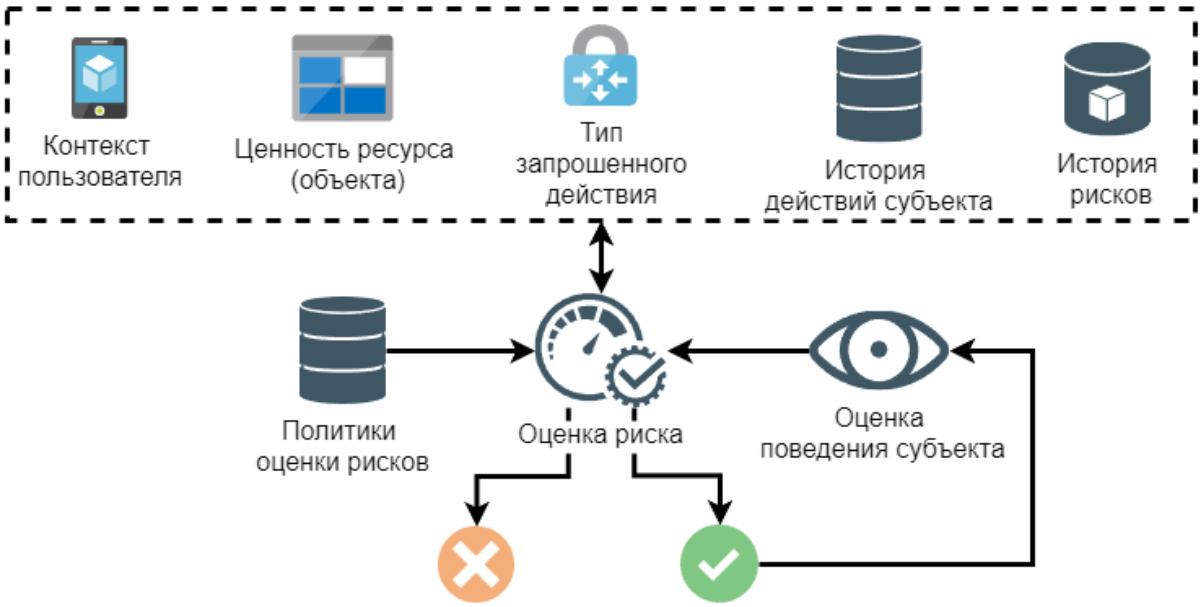


Рисунок 3.5 — Предложенная схема предоставления доступа на основе оценки риска

Предложенный механизм управления доступом на основе риска имеет ряд преимуществ относительно стандартных моделей:

1. Совместимость с несколькими пользователями: для обеспечения функциональной совместимости политики рисков будут разрабатываться с использованием контекстных функций в режиме реального времени, которые динамически изменяются. Таким образом, политики рисков будут более гибкими и смогут работать с несколькими подразделениями вуза и пользователями.
2. Динамическое взаимодействие: предлагаемая модель обеспечивает динамическую и гибкую модель управления доступом для ОВС. Для принятия решения о доступе используются контекстные функции в реальном времени. Таким образом, решение о доступе динамически изменяется на основе собранных характеристик среды.
3. Использование контекста: предлагаемая модель использует контекстные характеристики в реальном времени, собранные из среды ОВС, для принятия решения о доступе. Таким образом, предлагаемая модель

является моделью с учетом рисков, которая использует контекстную осведомленность об окружающей среде для принятия решения о доступе.

4. Удобство использования: реализация разработанной модели позволяет создать удобные интерфейсы для пользователя, которые легко администрировать и модифицировать.
5. Ограниченные ресурсы пользователей: в предлагаемой модели будет использоваться централизованная и контекстуальная архитектура управления доступом, в которой субъекты и объекты ОВС участвуют в принятии решений о доступе. Логика управления доступом будет реализована на центральном сервере со всеми необходимыми ресурсными возможностями. Контекстные функции будут отправляться центральному серверу системы управления доступом. Таким образом, ограничения ресурсов устройств доступа к ОВС не будут являться проблемой.
6. Масштабируемость: предлагаемая модель предназначена для использования в современных ОВС, количество пользователей в которых изменяется динамически, как правило, достаточно большое, поэтому при разработке модуля оценки рисков и политики управления рисками следует учитывать указанные свойства ОВС.
7. Возможность аудита: предлагаемая модель включает модуль мониторинга для записи и мониторинга всех действий субъектов с объектами, выполняемых предоставленным во время сеанса доступа. Данное свойство позволит осуществлять разбор спорных ситуаций и использовать центры мониторинга безопасности.

Язык описания политик

Язык политики играет ключевую роль в модели ABAC, поскольку он определяет правила доступа для системы. Несмотря на то, что они не являются моделями сами по себе (существует такое заблуждение), эти языки являются общими стандартами языков управления доступом (XACML) либо созданы специально для применения с конкретной моделью. Одним из наиболее широко упоминаемых и используемых стандартов является расширяемый язык разметки управления доступом (XACML), разработанный организацией по продвижению структурированных информационных стандартов OASIS. XACML представляет собой XML-основанный (eXtensible Markup Language) язык поли-

тики управления доступом, в котором поддержка политик осуществляется на основе атрибутов. Этот язык широко распространен в средствах управления доступом.

Кроме того, стоит отметить язык маркировки утверждений безопасности (SAML, Security Assertion Markup Language), авторства той же организации OASIS. Это стандартизированный язык разметки и протокол для обмена информацией об авторизации и аутентификации на основе атрибутов между различными участниками, включая поставщиков услуг, поставщиков идентификации/атрибутов и конечных пользователей. Однако, помимо этих стандартов, существует множество других языков политики, разработанных специально для определенных моделей ABAC или адаптированных для конкретных требований организаций и систем. Важно отметить, что выбор конкретного языка политики зависит от потребностей конкретной системы, ее характеристик и особенностей.

Помимо ABAC, в информационной безопасности существует важное направление, известное как Attribute-Based Encryption (ABE), представляющее метод шифрования данных, где доступ к зашифрованным объектам основывается на атрибутах их пользователей или других контекстных параметрах. В ABE существует два основных подхода: Key-Policy ABE (KP-ABE) и Ciphertext-Policy ABE (CP-ABE). Например, в KP-ABE данные шифруются с учетом определенной политики доступа, инкапсулированной в ключе пользователя. Это означает, что объект можно расшифровать только в случае, если пользователь обладает определенным набором атрибутов, соответствующих этой политике. С другой стороны, в CP-ABE шифрование выполняется на основе заданной политики доступа, и ключ пользователя содержит атрибуты, необходимые для доступа к данным, соответствующим этой политике.

Примеры применения ABE в распределенных информационных системах включают защиту данных в облачных сервисах, где пользователи могут иметь разные уровни доступа к информации в зависимости от их ролей и контекста использования. Например, в сфере здравоохранения ABE может быть использован для защиты медицинских записей, где доступ к конкретным данным зависит от роли и полномочий пользователя, а также от контекста запроса (например, время доступа, местоположение пользователя и т. д.). Другой пример – применение ABE в системах управления доступом к ресурсам Интернета вещей (IoT, Internet of things), где поступающие с устройств данные, можно зашифровать, учитывая атрибуты этих устройств или окружающей среды. Система

"умный дом" может применять ABE для обеспечения безопасности доступа к датчикам и устройствам в зависимости от роли и прав доступа пользователя.

Таким образом, ABE представляет собой мощный инструмент для обеспечения безопасности в распределенных системах, где требуется гибкое и контекстно-зависимое управление доступом к данным, имеющий следующие недостатки и ограничения:

1. Сложность управления политиками доступа: создание политик и управление доступом в ABE может быть сложным и трудоемким процессом. Это связано с необходимостью определения точных условий доступа, которые могут включать в себя множество атрибутов и их комбинаций.
2. Высокая вычислительная нагрузка: шифрование и расшифрование данных в ABE требует значительных вычислительных ресурсов, особенно при использовании сложных политик доступа и большого объема данных.
3. Сложность масштабирования: при увеличении количества пользователей и объектов доступа, а также усложнении политик доступа, становится сложнее обеспечить эффективное управление и масштабирование системе ABE.
4. Потенциальная утечка информации о структуре данных: в некоторых случаях структура атрибутов и политик доступа может раскрывать чувствительную информацию о структуре данных или организации, что может представлять угрозу конфиденциальности.
5. Ограничения в поддержке динамических изменений: в некоторых реализациях ABE может быть сложно или невозможно динамически изменять или обновлять политики доступа без перешифрования данных, что затрудняет адаптацию к изменяющимся потребностям и требует дополнительных ресурсов.

Указанные недостатки подчеркивают важность тщательного анализа требований и оценки применимости ABE перед его внедрением в конкретной среде. В данном исследовании внедрение моделей не рассматривается в виду невозможности адаптации данного механизма в ОВС, где динамически происходит изменение множества субъектов и объектов, что повлечет существенные затраты на обслуживание системы и существенно усложнит удобство использования образовательными сервисами. Для устранения отмеченных недостатков в ОВС могут быть применены модели ABAC.

Модели ABAC позволяют динамически управлять доступом в распределенных информационных системах и обладают рядом преимуществ:

1. Гибкость в определении прав доступа: возможность создания политик доступа на основе атрибутов пользователей, объектов и окружения.
2. Автоматизация: за счет использования атрибутов для определения доступа, ABAC облегчает автоматизацию процесса управления доступом, что уменьшает необходимость вручную назначать роли или разрешения.
3. Масштабируемость: модели ABAC могут эффективно масштабироваться для обработки больших объемов пользователей, объектов и политик доступа.
4. Гранулярность: ABAC позволяет создавать более детализированные политики доступа, основанные на атрибутах пользователей и объектов, что обеспечивает более точное управление доступом.
5. Аудит и отчетность: благодаря использованию атрибутов и структуре политик, ABAC облегчает аудит и отчетность в системе управления доступом.

Кроме того для моделей ABAC может быть разработана логическая модель, позволяющая реализовывать атрибутивное управление доступом.

Логические модели для атрибутивного управления доступом

В работе Ванга и соавторов, опубликованной в 2004 году, представлена одна из первых "чистых" и "общих" моделей ABAC в виде логического фреймворка на основе логического программирования, в котором политики определены как "стратифицированные программы логики ограничений, свободные от циклов" [157], при этом атрибуты и операции определяются в качестве множеств в вычислительной теории множеств [158]. Представлены методы оптимизации времени оценки политики ABAC, которые включают преобразование заданной политики ABAC в семантически эквивалентную, но сокращенную по времени выполнения и накладным расходам политику, когда это возможно. В то время как фреймворк Ванга и его коллег вводит иерархические атрибуты (что отсутствует в других моделях), он в основном сосредоточен на представлении, согласованности и производительности политик на основе атрибутов и их оценке. Несколько важных компонентов отсутствуют, включая отсутствие атрибутов объектов (рассматриваются только атрибуты пользователей) и от-

сутствие формализации аспектов ABAC вне политик и их оценки (например, рассматривается только управление доступом к службам/операциям).

В работе Чжана и соавторов 2005 года предложена уникальная модель ABAC на основе усовершенствованной матрицы доступа, называемая моделью "матрицы доступа на основе атрибутов" (ABAM, Attribute Based Access Matrix) [159]. ABAM определяет матрицу доступа, в которой каждая строка представлена парой, состоящей из субъекта и набора его атрибутов $(Si, ATTS(Si))$, каждому столбцу соответствует пара – объект и его набор атрибутов $(Oi, ATTS(Oi))$. Ячейка $([Si, Oi])$ представляет собой набор прав доступа субъекта (Si), которые он может осуществлять над объектом (Oi) при выполнении определенных политик. Операции (или "команды", как их называют в ABAM) могут выполняться субъектом над объектом только в том случае, если в матрице доступа найдены соответствующие права доступа, требуемые операцией, и атрибуты субъекта и объекта соответствуют набору политик на операцию.

Чжан и соавторы дополняют формализацию ABAM анализом безопасности для доказательства разрешимости ABAM, в случае конечности набора атрибутов, и если атрибуты не образуют циклы. В то время как уникальное использование ABAM матрицы доступа позволяет создать более аудиторные системы ABAC по сравнению с другими моделями (базовые проверки, какие пользователи могут получить доступ к определенному объекту, могут быть выполнены с помощью простого поиска по матрице, а не оценкой политик на большом наборе атрибутов и субъектов), в работе отсутствует детальное описание процесса администрирования, составления или оценки сформированной политики. Язык политик представлена на примерах, но полностью не формализован. Декларировано, но не доказано, что модель ABAM универсальная и включает в себя традиционные модели управления доступом; но не является очевидным, что ABAM может включать в себя MAC или RBAC. Следует отметить также, что в модели ABAM нет атрибутов соединения, окружения и иерархических, отсутствуют ограничения для разделения обязанностей или упрощения делегирования.

В работе Рубио-Медрано и др. [160] определены безопасные маркеры в абстрактной модели ABAC, определяющей ключевые компоненты и атрибуты для минимальной эталонной модели. В других моделях ABAC основанных на правилах, где решения об управлении доступом основаны на оценке политик и актуального состояния различных атрибутов, эта модель связывает атрибу-

ты сущностей управления доступом (субъекты, объекты и т. д.) с безопасными маркерами, проходя через определенный администратором "граф предоставления маркеров" (TP-Graph). TP-Graph является направленным, возможно, цикличным графом, вершины которого представляют собой наборы связанных атрибутов или безопасных маркеров (называемые семьями атрибутов или безопасных маркеров), а его ребра представляют собой "функции предоставления маркеров" (TP-Functions), отображающие семью атрибутов / безопасных маркеров в другую семью безопасных маркеров на основе определенных критериев, которым соответствуют значения атрибутов/маркеров. Поскольку администраторы системы могут назначать TP-Functions и связывать безопасные маркеры и разрешениями, обеспечивается принятие решений об управлении доступом. По мнению авторов эти решения лучше поддаются аудиту и открыты анализу безопасности с помощью методов теории графов.

В работе Рубио-Медрано и его коллег предложен новаторский подход к ABAC, который обеспечивает дополнительную аудиторскую возможность и анализ безопасности на основе графов, но это сопряжено с увеличением административной сложности и накладными расходами. В теории графы TP должны позволять разработать методы анализа безопасности на основе теории графов, но эта работа остается на будущее. Кроме того, модель ABAC сама по себе в значительной степени неформальна, описывая большинство концепций, но не определяя их формально. Неизвестно, каким образом TP-Functions и TP-Graph могут быть созданы администратором или в каком виде они могут быть приняты. В качестве направления дальнейших исследований назван язык политик. Нет четкого описания обработки циклов ABAC или алгоритма реализации TP-Graph.

Работа Джин и его соавторов [161] посвящена "разработке формальной модели ABAC, достаточно выразительной, чтобы охватить DAC, MAC и RBAC". В этой работе проведена формализация ключевых элементов ABAC (пользователи, объекты, политики и т. д.), их взаимоотношений и ограничений, с помощью которых можно эмулировать традиционные модели. Частичный язык политик и ограничений – "общий язык политики (CPL, Common Political Language)", созданный на основе обозначений теории множеств и булевой логики, определены и приведены примеры конфигураций для управления доступом в стиле DAC, MAC и RBAC в ABAC. Кроме того, указывается ограниченная функциональная спецификация, включающая минимальный набор администра-

тивных функций (хотя информация о конкретных условиях авторизации для административных функций не дана).

Язык CPL применяется и для спецификации политик, и для настройки ограничений в ABAC – при ограничении возможные назначений атрибутов и установке возможного диапазона и типа значений атрибутов. В примере 1 проиллюстрирована политика авторизации в CPL для обеспечения управления доступом в стиле RBAC. Здесь S – это множество всех субъектов, O – множество всех объектов, $srole$ – атрибут субъекта, содержащий роли субъектов, $rrole$ – атрибут объекта, содержащий множество ролей, дающих разрешение на чтение объекта, $wrole$ – атрибут объекта, содержащий множество ролей, дающих разрешение на запись в объект. Согласно политике авторизации субъект может читать объект только при наличии у него роли в множестве значений атрибута rrole объектов, и может записывать в объект только в том случае, если у него есть роль в множестве значений атрибута $wrole$ объектов.

Политика управления доступом определяет права доступа, когда пользователь ОВС подключается к системе. Политики управления доступом в первую очередь управляют всеми решениями о предоставлении доступе субъекта к объекту ОВС. Процесс формулирования политик должен соответствовать нескольким целям [162]. Процесс составления и назначения политики не должен быть слишком сложным, первостепенное значение должно иметь удобство использования [163]. При подключении пользователя к ресурсам ОВС, предоставление доступа должно быть гибким, чтобы соответствовать требованиям политики и позволяющим избегать распространения риска в сети ОВС. Разработка политик управления доступом зависит от домена. Политики должны адаптироваться к конкретной среде и ее характеристикам. Например, политики для ОВС должны не только обеспечивать безопасность объектов ОВС, но и быть гибкими в предоставлении ресурсов ОВС субъектам, чтобы максимизировать удобство использования ОВС пользователями. Сгенерированные политики могут быть не достаточно детализированными, что может привести к чрезмерным привилегиям пользователя [164; 165]. Решения на основе риска для управления доступом определяют контекст, который необходим для внедрения динамичности политик безопасности. Политики на основе ACL (Access Control List) являются ручным способом создания политик доступа, что является непригодным для создания ролей и разрешений при распределенной ОВС.

Спецификация динамических политик

Обзор спецификации политик безопасности показывает, что существующим решениям не хватает оперативности в формировании политики, принятии решений и оценке [166]. Машинное обучение может быть использовано для автоматизации использования политик. Благодаря автоматизации отпадает необходимость редактировать политики вручную при масштабном и постоянном изменении состава пользователей ОВС, что характерно для образовательной организации. Таким образом, использование машинного обучения напрямую поможет повысить оперативность в решении задач управления доступом. Традиционные подходы, основанные на модели управления доступом:

- Лю и др. предложили модель управления доступом для совместного использования ресурсов в [167]. Подход основан на RBAC. Механизм авторизации использует метод планирования на основе графиков для поиска оптимального маршрута авторизации для администраторов для предоставления привилегий субъекту. Политика охватывает роли пользователей, разрешения и ресурсы. Это решение сталкивается с проблемами с точки зрения эффективности использования ресурсов и масштабируемости.
- В [168] Альхрешех и др. разработали структуру динамического управления доступом на основе ABAC. В работе представлен новый алгоритм автоматического определения политики, в котором политика генерируется на основе извлечения атрибутов из субъекта, объекта и выполняемой процедуры и оценивается на основе набора примитивных фактов. Кроме того, алгоритм применения политики постоянно и автоматически корректирует политики.
- В [169] Габийон и др. предложили основанную на ABAC структуру для протокола MQTT (Message Queue Telemetry Transport). В их подходе язык политики основан на языке ограничений Shapes, представленном консорциумом WWW (World Wide Web). Хотя политики являются выразительными и контекстуальными с помощью атрибутов, администрирование по-прежнему статично.
- В [170] Риад и др. использовали расширенный язык XACML для применения в среде распределенного интернета вещей. Их архитектура соответствует модели ABAC и позволяет корректировать политики во время выполнения. Что может быть использовано в среде ОВС, поскольк-

ку ОВС имеет ряд схожих свойств с интернетом вещей: распределенный формат систем, множество пользователей и субъектов доступа, динамический характер функционирования. Сгенерированные политики в данной работе проверяются с использованием контрольной суммы алгоритма MD5 для дайджеста сообщений. Схема защищает сеть Интернета вещей от двух атак, т. е. маскарадной атаки и атаки "человек посередине".

– Аналогичным образом, концептуальная основа, которая обеспечивает соблюдение политик управления доступом в среде Smart Health, была предложена в [171]. Эта платформа использует централизованную архитектуру, но может уточнять политики во время выполнения для обеспечения динамичности. Язык политик основан на XML. XML был использован из-за его гибкости для обмена политиками между доменами. Фреймворк в [171] основан на модели ABAC. Фактически, многие подходы используют модель ABAC для обеспечения соблюдения политик управления доступом из-за ее поддержки нескольких атрибутов. Однако модель ABAC также может иметь проблемы с производительностью по сравнению с другими из-за множества атрибутов, используемых для управления доступом [172].

Подходы, основанные на искусственном интеллекте:

– Бертино и др. провел тематическое исследование политик XACML для анализа их модели, разработанной на основе символьного обучения в Generative Policy Model (GPM) в [173]. Общедоступный набор данных, включающий запросы политик XACML и ответы, были использованы для проведения исследования. На основе набора данных они сгенерировали набор примеров, содержащих параметры ABAC, которые были основаны на грамматике набора ответов.
– Каннингтон и др. предложили централизованную архитектуру на основе GPM для подключенных и автономных транспортных средств в [174]. Принятый метод основан на индуктивном логическом программировании. Их решение не генерирует политики управления доступом, но оно уточняет и сохраняет политики динамически.
– Лю и др. предложили модель управления доступом для Интернета транспортных средств (IoV, Internet of Vehicles) на основе прогнозирования рисков в [175]. В своем подходе они используют централизованную

архитектуру с моделью генерирующей состязательной сети, основанной на долговременной кратковременной памяти LSTM (Long short-term memory), для улучшения набора обучающих данных. Транспортное средство может получить доступ к запрошенному ресурсу, если риск ниже заданного порога

– Ю и др. предложили основанный на обучении подход, который изучает контекстные политики управления доступом на основе моделей поведения нескольких устройств "умного дома" в [176]. Этот подход использует федеративную структуру обучения, которая включает временное моделирование.
– В работе [177] Чу и др. предложили метод управления множественным доступом, основанный на прогнозировании заряда батареи с использованием сбора энергии в IoT. Предлагаемое решение использует глубокую нейронную сеть на основе LSTM. Оно разработано для беспроводной сети, в которой узлы датчиков географически распределены. Узлам предоставляется доступ к базовой станции на основе состояния батареи узла датчика. В предлагаемой двухуровневой сети LSTM первый уровень прогнозирует и генерирует уровень заряда батареи сенсорного узла. Второй уровень использует информацию о канале и прогнозируемые значения для формирования политик управления доступом.

Подходы к управлению доступом на основе блокчейна:

– Блокчейн был исследован для принятия решений по управлению доступом в IoT из-за его распределенной природы. Решение для управления доступом на основе смарт-контрактов было предложено в [178]. При подходе, основанном на блокчейне, политика, созданная владельцем ресурса, сохраняется в блокчейне в виде транзакции. Политика написана на XACML и преобразуется в смарт-контракт. Чтобы обновить или удалить политику, контракт заменяется новым смарт-контрактом.
– В работе [179] Лю и др. предложили подход, основанный на распределенных реестрах, для защиты конфиденциальности данных Интернета вещей. В рамках этого подхода обновления политик проводятся через пограничный узел путем добавления новой политики в блокчейн, что позволяет осуществлять динамическое управление доступом.
– В [180] предлагается распределенное решение для управления доступом на основе блокчейна для домена smart grid. Подход состоит из трех

уровней: первый уровень – это сетевой уровень, второй уровень состоит из необработанных политик RBAC и ABAC, а также третий уровень состоит из распределенной бухгалтерской книги. Обновления контекстной информации в PDP (Policy Decision Point) выполняются виртуальными аудиторами. Эти обновления помогают PDP принимать решения о динамическом управлении доступом.

– В [181] Чжан и др. предложили подход к управлению доступом на основе смарт-контрактов, использующий парадигму ABAC. Политики не жестко закодированы в смарт-контрактах, что позволяет использовать подход с меньшими накладными расходами. Это решение также содержит предопределенные функции для добавления, удаления и обновления политик, что способствует реализации концепции динамического управления доступом.

Политики, которые переносят данные:

– Учитывая контекстуальный характер и объем передаваемых и обрабатываемых конфиденциальных данных, устройства Интернета вещей также могут встраивать политики в данные. Эта встроенная политика в отношении данных позволяет осуществлять постоянный мониторинг и отменять доступ. Впервые представленные в [182], Sticky Policies обеспечивают подход к IoT, ориентированный на владельца данных, и позволяют пользователям встраивать политики в данные.
– Эта концепция применялась во многих подходах в области IoT. Например, подход, называемый данными, несущими политику, был предложен в [183]. При таком подходе политика может указывать информацию о разрешениях, обязательствах и ограничениях данных, что обеспечивает динамичность. Язык политики основан на логике первого порядка. Однако язык считается сложным, и существует потребность в централизованном сервере для оценки как производителей, так и потребителей данных.
– В [184] Сикари и др. использовали архитектуру промежуточного программного обеспечения для обработки запросов политики и ответов с использованием ABAC.
– Подходы, описанные в [185; 186], используют гибкие политики за счет использования архитектуры пограничных вычислений. Для определения политик использовался формат объектной нотации JavaScript.

Сквозное взаимодействие было зашифровано для сохранения конфиденциальности данных. Политики Sticky позволяют осуществлять интеллектуальный контроль над авторизацией ресурсов Интернета вещей. Однако у него также есть ограничения. Не существует установленного языка для политик из-за привязки политик к данным. Это также может увеличить вычислительные издержки на устройствах из-за шифрования, которое используется во время передачи данных [187].

Спецификация SAML и XACML

SAML (язык разметки утверждений безопасности) – это открытый стандарт, разработанный OASIS для обмена данными аутентификации и авторизации между взаимодействующими системами. Основное применение языка -объединение идентификаторов: для получения доступа к службам из разных доменов безопасности пользователь должен только один раз подтвердить свою идентичность в объединенной системе. Использование SAML позволяет клиентам получать доступ к службам без необходимости повторно подтверждать свои идентификационные данные каждый раз, когда они обращаются к новой службе. Это связано с тем, что SAML предоставляет механизм безопасной передачи информации об аутентификации и авторизации между системами, позволяя им обмениваться информацией и доверять друг другу. SAML может использоваться как язык разметки или механизм взаимодействия. Он состоит из 4 компонентов на основе XML, обеспечивающих защищенную и гибкую связь между системами: утверждения безопасности, протоколы, привязки и профили.

На рисунке 3.6 представлены основные компоненты SAML: Утверждающая и Проверяющая стороны и Принципал. Утверждающая сторона является административным доменом, где находятся один или несколько органов SAML, которые выдают утверждения.

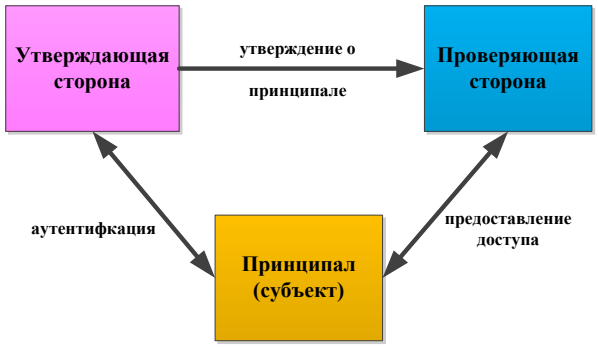


Рисунок 3.6 — Основные компоненты SAML

Проверяющая сторона полагается на Утверждающую сторону для получения утверждений, касающихся конкретного предмета. Принципал – это организация, личность которой может быть проверена. В профиле единого входа Подтверждающая сторона выступает в качестве поставщика удостоверений, управляя идентификационной информацией о Принципалах и обеспечивая аутентификацию Принципала. Проверяющая сторона функционирует как поставщик услуг. Предполагается, что между Проверяющей стороной и Утверждающей стороной существуют доверительные отношения. Утверждения SAML передают информацию о безопасности, относящуюся к определенному субъекту или сущности. Имеются 3 типа утверждений: аутентификация, атрибут и авторизация. Все утверждения защищены цифровыми подписями и шифрованием. В SAML заданы некоторые протоколы запроса/ответа. Протоколы определяют, как запрашиваются и принимаются элементы SAML (включая утверждения). При определенных привязках сообщения протокола SAML могут встраиваться и передаваться по протоколам, например по протоколу доступа к объектам SOAP (Simple Object Access Protocol). Профиль SAML описывает объединение утверждений, протоколов и привязки для отдельных случаев использования. Для обеспечения безопасности предполагается использование инфраструктуры открытых ключей (PKI, Public key Infrastructure) и безопасности транспортного уровня (TLS, Transport Layer Security). Также следует использовать цифровые подписи и взаимную аутентификацию. Исходная цель языка SAML – это разработка универсального языка для утверждений безопасности. Однако профили SAML были практически ориентированы на варианты использования аутентификации и единого входа (SSO, Single sign-on), поэтому авторизация объектов и протоколов оставалась за рамками процесса стандартизации SAML. Это было основой начала стандартизации языка разметки расширяемого управления доступом (XACML).

Язык XACML – это стандарт OASIS, реализующий и модель ABAC для оценки политики, а матрицу управления доступом для обеспечения соблюдения политики, содержащий язык и справочную архитектуру, включающую точки принятия политических решений, точки применения политики, точки администрирования политики и точки информации о политике. В XACML запросы к файловым системам или веб-серверам направляются в защищающую ресурс точку применения политики (PEP, Policy Enforcement Point). PEP создает запрос XACML на основе атрибутов запрашивающего, доступного ресурса,

запрашиваемого действия и другой соответствующей информации. Затем этот запрос отправляется в Центр принятия политических решений (PDP), который выдает ответ о том, следует ли предоставить доступ или отказать в нем на основании применимых политик. PEP уважает решение PDP при разрешении или блокировании доступа к ресурсу (рис. 3.7). Запрос на доступ ресурсу поступает в PEP, который для принятия решений связан с PDP. PDP использует полученные сведения, для разрешения/запрета доступа к ресурсу.

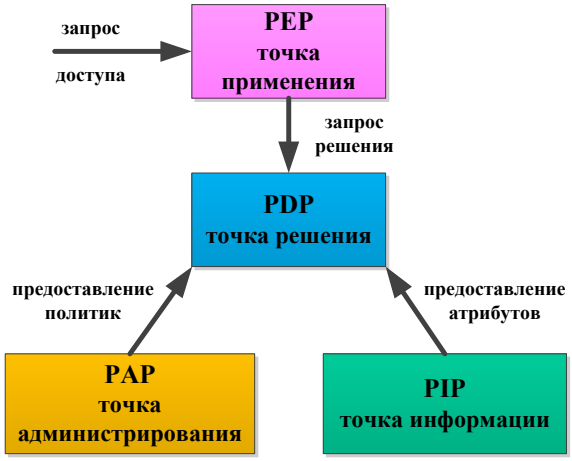


Рисунок 3.7 — Архитектура XACML

Система XACML дает возможность использования сложных политик, созданных на основе правил, обязательств и рекомендаций. Атрибуты (характеристики субъекта, ресурса, действия или среды) в XACML формируют основу политик. Имя пользователя, его членство в определенной группе, документ, к которому нужен доступ, и дата являются значениями атрибутов. Запрос на доступ, отправляемый в PDP из PEP, создается почти полностью из атрибутов, которые сравниваются с допустимыми значениями атрибутов согласно политике для обеспечения доступа. Механизм принятия решения об авторизации определяется алгоритмами объединения правил и политик с учетом результатов оценки набора правил и политик. Следует отметить, что при всех своих возможностях система XACML является достаточно сложной.

Существуют различные публикации, в которых предлагается использовать SAML и XACML для создания структуры авторизации для устройств Интернета вещей [188; 189]. SAML и XACML остаются наиболее широко используемыми в промышленности стандартами сети Интернет и управления доступом. В [190] представлена система авторизации для Интернета вещей,

позволяющая реализовывать детальное и гибкое управление доступом к устройствам с недостаточными вычислительной мощностью и объемом памяти. Авторами были созданы профили и адаптации XACML и SAML для их активации и оптимизации использования в случаях ограниченных возможностей устройств. В работе представлена полная эталонная архитектура и отдельные возможности оптимизации для адаптации протоколов к устройствам с ограниченными возможностями. В качестве примера, одна оптимизация устраняет многословие полного синтаксиса ответов XACML и утверждений SAML путем определения упрощенной нотации на основе JSON для утверждения авторизации.

Другая публикация по этой тематике основывается на определении точного утверждения авторизации в формате JSON, совместимого с протоколом авторизации и вычисляемого устройством с ограниченными возможностями [191]. Эти два подхода базируются на особенностях веб-шифрования IETF JSON (JWE, JSON Web Encryption) [192]. В то же время, выводы из этих исследований следующие: JWE значительно увеличивает накладные расходы для полезных нагрузок размером всего в несколько байт, которые распространены в протоколах интернета вещей с ограниченными возможностями, таких как протокол ограниченного применения CoAP (Constrainted Application Protocol).

Кроме того, рабочая группа IETF (Internet Engineering Task Force) по аутентификации и авторизации в ограниченных средах (ACE, Authentication and Authorization for Constrained Environments) работает над расширением OAuth 2.0, чтобы предоставить решение для Интернета вещей. В работе рассматриваются очень разные и ограниченные возможности устройств Интернета вещей в отношении доступной обработки и обмена сообщениями при поддержке различных вариантов использования авторизации [191]. Группа ACE основывается на:

- CoAP для обмена сообщениями (не исключая возможности использования протоколов MQTT (Message Queue Telemetry Transport) или QUIC (Quick UDP Internet Connections));
- краткое двоичное объектное представление (CBOR, Concise Binary Object Representation) и веб-токен CBOR (CWT, CBOR Web Token) [193] для представления токенов и подписи и шифрования объектов CBOR (COSE, Common Open Software Environment) и DTLS (Datagram

Transport Layer Security) для обеспечения безопасности приложений и транспортного уровня, соответственно.

Веб-токен CWT упрощает процедуру веб-шифрования JSON (JWE) для устройств с ограниченными возможностями (объектов Интернета вещей). ACE использует и другой тип токена, PoP (Proof of Product) токенами по сравнению с потоком устройств OAuth 2.0. Токены PoP – токены доступа с ключом PoP, связанным с токеном. Токен PoP дает возможность пользователю подтвердить серверу регистрации RS (Registration Server), что он является предполагаемым авторизованным владельцем токена. Пусть RS и клиент зарегистрированы на сервере авторизации (AS, Authentication Server). Тогда в ACE должны произойти следующие события, чтобы пользователь получил доступ к размещенному RS ресурсу. Пользователь отправляет запрос в AS. AS оценивает запрос токена и азрешает/отказывает в доступе, при этом возвращается токен PoP или сообщение об ошибке [194]. Клиент включает токен PoP в свой запрос ресурса. Используя токен PoP, RS аутентифицирует клиента. Также RS при наличии возможности локально оценивает токен. В другом случае для проверки токена он может связаться с AS. Этот процесс называется самоанализом токена. По результатам проверки токена RS может разрешить/запретить доступ к ресурсу [195]. ACE обрабатывает различные схемы связи, включая некоторую поддержку связи между устройствами. По сути, ACE ожидает, что устройства могут часто находиться в автономном режиме или они могут не поддерживать связь на основе IP, и, следовательно, они не всегда могут взаимодействовать с AS [196]. Затем более мощный сервер авторизации клиента может запросить токены у AS. Если устройство действует как RS, но у него нет постоянного подключения к Интернету, то может понадобиться локальная проверка токенов. При смене пользовательских политик токен становится недействительным, при этом не существует простого способа отозвать токен. Эта проблема может нанести ущерб безопасности всей системы, подчеркивая сложность обеспечения значимой авторизации в ограниченных и распределенных системах Интернета вещей.

Коллектив IETF разработал стандарт доступа, управляемого пользователем (UMA, User-Managed Access), в рамках инициативы Kantara [197]. Стандарт UMA определяет новое разрешение на авторизацию, которое дает возможность владельцам ресурсов управлять доступом к своим ресурсам клиентов, управляемых любыми сторонами, запрашивающими доступ (например, Алиса разрешает доступ к своим ресурсам с помощью служб Боба, в отличие от модели OAuth

2.0, где Алиса только с помощью своих служб может разрешать доступ к своим ресурсам). Стандарт определяет политику, основанную на возможностях, оценка политики находится за рамками его деятельности. Ресурсы могут находиться на любом количестве серверов ресурсов, а централизованный сервер авторизации управляет доступом к ресурсам на основе пользовательских политик. По сравнению с потоками OAuth 2.0, эти политики доступа используются для обработки асинхронных разрешений авторизации [198]. Типичный пример применение стандарта: веб-пользователь может авторизовать веб-сайт или собственное приложение (клиент) чтобы получить разовый/постоянный доступ к защищенному ресурсу, где содержится номер его телефона в хранилище персональных данных (сервер ресурсов). Пользователь должен при этом проинструктировать сервер ресурсов о соблюдении прав доступа, выданных сервером авторизации.

Блок-схема UMA представлена на рисунке 3.8. Владелец ресурса управляет онлайн-ресурсами на сервере ресурсов. Для защиты ресурсов, владелец подключает сервер ресурсов к серверу авторизации. Сервер ресурсов регистрирует ресурсы, которые необходимо защитить с помощью сервера авторизации. Для получения авторизации клиент направляет запрос к ресурсу на сервер ресурсов.

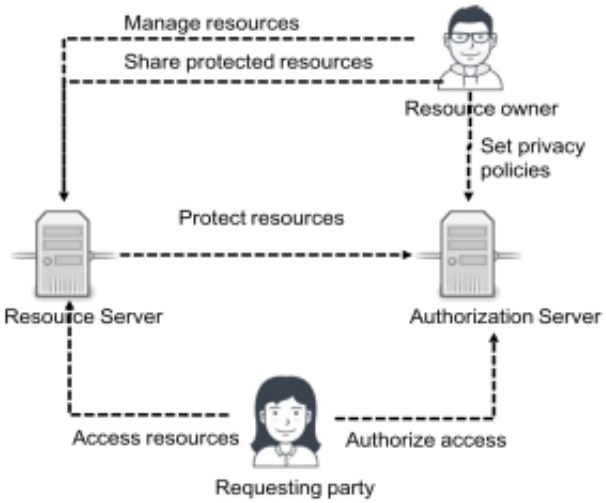


Рисунок 3.8 — Блок-схема управляемого пользователем доступа UMA

При попытке несанкционированного доступа сервер ресурсов регистрирует разрешение на сервере авторизации и возвращает клиенту запрос разрешения. Чтобы процесс авторизации начался клиент предоставляет этот запрос

разрешения серверу авторизации. В случае успешного завершения сервер авторизации возвращает клиенту токен запрашивающей стороны (RPT, Requesting Party Token). Для получения доступа к защищенному ресурсу клиент представляет токен RPT серверу ресурсов. После проверки токена сервером ресурсов клиент получает доступ к защищенному ресурсу. Стандарт UMA является централизованным решением, которое дает возможность реализации сложных политик на основе атрибутов. Решение UMA подходит для внутреннего обмена данными (рис. 3.8). Опубликованы исследований в сфере IoT стандарта UMA, посвященные сфере здравоохранения [199; 200].

Владелец ресурса (RO, Resource Owner) управляет принадлежащими ему ресурсами на сервере ресурсов (RS, Resource Server). RO представляет RS серверу авторизации (AS) в качестве объекта для RS для регистрации защищенных ресурсов. Кроме того, RO определяет политики в AS. Для доступа к ресурсам запрашивающая сторона обращается к RS, который фиксирует попытки доступа без токена как запросы разрешений в AS. После этого клиент обращается к AS, который использует запрос на разрешение и политики RO для выдачи клиенту токена запрашивающей стороны (RPT). Несмотря на то, что над управлением доступом ведется большая работа, в настоящее время отсутствуют универсальные решения, обеспечивающие высокий уровень безопасности и удобство использования. Основными факторами, влияющими на развитие систем управления доступом в ОВС являются:

1. Масштабируемость. ОВС находятся в постоянном развитии, увеличивается количество образовательных ресурсов, разрабатываются различные интерактивные модули и сервисы. Следовательно, подсистема управления доступом должна быть способна обрабатывать большое количество запросов от субъектов, обеспечивать соблюдение политик безопасности и быстро принимать решения о предоставлении доступа к объекту. Эффективным способом борьбы с масштабированием ОВС является децентрализация управления и делегирование полномочий. Таким образом, система управления доступом для распределенных вычислительных систем должна быть способна подстраиваться под разные структуры управления (сеть доверия, иерархическое управление и т. д.). В то же время значительная часть изученных работ основана на централизованном управлении, в которое может входить администрирование политик, выдача и анализ учетных данных для

принятия решений об авторизации (например, сервер авторизации в случае OAuth2.0, UMA и ACE или централизованный PDP/PEP в случае XACML). Эта централизация вызывает сомнения в плане возможности масштабируемости и проблем с единой точкой отказа. Что же касается полураспределенной архитектуры сервера авторизации, то часть ответственности передается периферийному устройству. Центральный орган по-прежнему может предоставлять сертификат или токен доступа для доступа к устройству или группе устройств, они применяются локально в точке доступа (ACE и UMA предоставляют эти опции). Относительно полностью распределенных подходов можно сказать, что существенная проблема заключается в ограниченности ресурсов в распределенных вычислительных системах.

2. Управление разнородностью. Новые протоколы сервера авторизации развертываются без обязательного отказа от старых. Повседневные сервисы имеют более длительный жизненный цикл, чем технические, что увеличивает продолжительность, в течение которой от новых объектов потребуется обратная совместимость. Более того, одни и те же сети ОВС могут продолжать использоваться все более сложными способами. Таким образом, механизмы управления доступом должны быть достаточно гибкими, чтобы адаптироваться к незапланированным случаям.
3. Открытость и гибкость, а также общее требование к унификации образовательных ресурсов, т. е. необходимо поддерживать решения от различных поставщиков и третьих сторон.
4. Разрешение идентификационных данных объектов. Рассмотренные подходы к управлению доступом анализируют идентификационные данные субъектов запрашивающих доступ к объектам. Однако подход, основанный исключительно на идентификаторах, может не полностью подходить для ОВС. Это связано с тем, что идентификационную информацию возможно легко подделать или попросту украсть. Кроме того, многие системы ОВС содержат информацию о пользователях в открытом доступе, например адреса электронной почты студентов, что способствует поиску информации по открытым источникам. Для преодоления данного недостатка должна использоваться комбинация атрибутов для подтверждения подлинности запрашивающего субъекта, например, текущее местоположение, владелец или производитель. При

совместном использовании атрибуты могут идентифицировать субъект более надежно чем отдельный атрибут. UMA v2.0 с его подходом, основанным на утверждениях, допускает этот тип аутентификации субъекта.

5. Управление персональными данными. Конечные пользователи несут ответственность за свои персональные данные вне зависимости от того, формирует их машина или нет. В ОВС должен содержаться элемент, управляющий конфликтующими интересами. Следует учитывать, что местоположение относится к персональным данным, особенно при использовании информации о местоположении с устройств. При сборе персональных данных на основе согласия "Общий регламент по защите данных" Европейского Союза (GDPR EU) [201] требует, чтобы процедура отзыва согласия была так же проста, как и процедура его подписи. При этом согласие считается действительным лишь в случае наличия у пользователя достаточных знаний о рисках и преимуществах раскрытия информации для принятия разумного решения.
6. Предоставление динамических политик. В политике конфиденциальности должно быть точно указано, кто взаимодействует с какими данными, когда, где, как и с какой целью. Это может противоречить удобству использования этих систем. Целью здесь должно быть создание простых для понимания политик, что затруднено из-за роста числа вариантов для многих потоков данных в ОВС. Перебор возможных сочетаний взаимодействия будет слишком трудоемким. Настройка управления доступом в ОВС должна быть динамической, чтобы соблюсти баланс между простотой и достоверностью, ограничив первоначальные политики набором правил. В [202] предложен пример динамической политики для систем контроля физического доступа (RFID, Physical Access Control System). В этой системе используются правила контроля физического доступа, которые обеспечивают следующие принципы: (1) местоположение пользователей видно им обоим, только при нахождении в одном и том же месте, и (2) местоположение объекта RFID видно его владельцу только если объект и его владелец находятся в одном месте. Данные принципы дополняются правилами, созданными для конкретного сценария. Например, в сценарии, где RFID-объект заимствован пользователем, владелец объекта

может проверить, находится ли RFID-объект этого пользователя. После этого возвращается информацию "пользователь x несет объект", без раскрытия информации о местоположении пользователя x. Хотя это исследование представляет собой шаг в правильном направлении, системы Интернета вещей нуждаются в политиках "точно в срок", которые разрешают запросы управления доступом к множеству объектов Интернета вещей.

7. Применимая безопасность. Обеспечение доступа к огромному числу объектов и их использование изучены недостаточно. Поэтому не было неожиданностью, когда ботнет из тысяч подключенных камер был использован для атаки типа "отказ в обслуживании" (DDoS) на французский хостинг. Современные решения для обеспечения безопасности используют криптографические методы и раскрывают ключи только авторизованным субъектам для защиты конфиденциальных данных ОВС от кибератак. Однако эти решения уязвимы ко многим типам кибератак. Кроме того, они не препятствуют авторизованным организациям выполнять определенные действия с подключенными объектами, о которых идет речь. Также использование криптографических методов является причиной значительных вычислительных затрат на устройстве, приводит к проблемам с распределением ключей и управлением ими. В ОВС необходимо автоматизированное и автономное управление доступом, которое снизит нагрузку на ресурсы ОВС и сделает использование более удобным.

В рассмотренных исследованиях представлены различные модели управления доступом: дискреционное управление доступом (DAC), мандатное управление доступа (MAC), управление доступом на основе ролей (RBAC) и т. д. Эти модели используются для реализации организационных политик, которые предотвращают несанкционированное раскрытие конфиденциальных данных, защищают целостность данных, обеспечивают безопасный доступ и совместное использование информации. Каждая модель имеет свои собственные методы принятия решений и обеспечения соблюдения политики. Однако из-за разнообразия моделей и различных проблем и ограничений важно найти метамодели с более высоким уровнем абстракции. Метамодели управления доступом служат объединяющей основой для определения любой политики и должны облегчить переход от одной модели к другой.

Для совместимости с разработанной риск-ориентированной атрибутивной моделью управления доступом [203] компоненты системы реализуются в виде агентов, которые предоставляют оценку состояния в своей зоне ответственности. Каждый агент наблюдает за отдельным аспектом работы защищаемой системы и сообщает свою оценку уровня риска. Оценка поступает в атрибутивную модель управления доступом в виде дополнительного атрибута, учитываемого при принятии решения о предоставлении доступа. Для систем с большим количеством элементов трудно задать все допустимые правила для риск-ориентированной атрибутивной модели управления доступом [204]. С другой стороны, за время функционирования защищаемых систем собирается большое число важных событий, содержащих полезную информацию о состоянии системы, действиях пользователей, нарушениях политики безопасности и других событий, которые также следует учитывать в модели. На основе данной информации могут производиться оценка и уточнение текущего значения риска в дополнение к существующим атрибутам, что позволит управлять риском в зависимости от состояния информации. В качестве метода количественной оценки риска, применяемого в разработанной риск-ориентированной атрибутивной модели управления доступом, выступает метод количественной оценки рисков реализации угроз несанкционированного доступа к образовательным сервисам на основе анализа событий безопасности с использованием математического аппарата нечеткой логики.

3.4 Метод количественной оценки рисков реализации угроз информационной безопасности на основе анализа событий, поступающих от агентов, с использованием нечеткой логики

Реализация риск-ориентированной атрибутивной модели основывается на интеллектуальных агентах. Интеллектуальные агенты создаются с применением методов машинного обучения на основе имеющихся данных и зависят от этих данных. Интеллектуальные агенты не обладают 100%-ным доверием, ввиду того, что требуется учитывать степень доверия при использовании показаний интеллектуальных агентов в процессе расчета значений риска. Доверие

назначается экспертным путем, учитывая факторы надежности используемой интеллектуальной технологии.

3.4.1 Интеллектуальные агенты анализа событий безопасности

Мониторинг, анализ, оценка и регулирование риска являются сложной задачей со многими неизвестными. Для систем с большим количеством элементов трудно задать все допустимые правила для риск-ориентированной атрибутивной модели управления доступом. С другой стороны, за время функционирования защищаемых систем собирается большое число важных событий, содержащих полезную информацию о состоянии системы, действиях пользователей, нарушениях политики безопасности и других событий, которые также следует учитывать в модели.

На основе данной информации может производиться оценка и уточнение текущего значения риска в дополнение к существующим атрибутам, что позволит управлять риском в зависимости от состояния информации. Для обработки накопленных данных предлагается использовать методы машинного обучения и искусственного интеллекта. Для совместимости с разработанной риск-ориентированной атрибутивной моделью управления доступом такие компоненты реализуются в виде интеллектуальных агентов, которые предоставляют оценку состояния системы в своей зоне ответственности [205].

Каждый агент наблюдает за отдельным аспектом работы защищаемой системы и сообщает свою оценку уровня риска. Оценка поступает в атрибутивную модель управления доступом в виде дополнительного атрибута, учитываемого при принятии решения о предоставлении доступа. Интеллектуальными агентами могут являться следующие типы механизмов:

- агенты наблюдения за субъектом (пользователем);
- агенты наблюдения за объектом (ресурсом);
- агенты наблюдения за инфраструктурой (средой).

Функционирование агентов осуществляется посредством реализации сценариев доступа, представленных на рисунке 3.9. Пример сценария, когда агент *KbdHwrt*, способный идентифицировать пользователя по клавиатурному почерку сообщает о несоответствии наблюдаемого пользователя его профилю (False):

Исходное правило:

Role=Teacher & ConnectionType = VPN & DeviceType=PersonalLaptop . . . Risk = Low / Decision = Permit

Измененное правило:

Role=Teacher & ConnectionType = VPN & DeviceType=PersonalLaptop & KbdHwrt=False, . . . Risk = High / Decision = Deny

Rule (s) defined with selected policy (Risk-Adaptive): 4 rows out of 4 Search

Sequence No	Subject	Resource	Action	Environment	Condition	Decision
1	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = Low	Condition = Any Value	Permit
2	Role = Teacher & Device Type = Personal Laptop & Connection Type = VPN	Service = Science	Actions = Write	Risk = Low	Condition = Any Value	Permit
3	Role = Teacher & Connection Type = VPN & Device Type = Personal Laptop	Service = Science	Actions = Read	Risk = High	Condition = Any Value	Permit
4	Device Type = Personal Laptop & Role = Teacher & Connection Type = VPN	Service = Science	Actions = Write	Risk = High	Condition = Any Value	Deny

Рисунок 3.9 — Сценарий доступа на основе нечеткой логики

Агенты могут анализировать действия пользователя для дальнейшей его идентификации и аутентификации. Пассивные агенты обрабатывают извлеченную ранее информацию, активные – предлагают пользователю совершить некие действия и анализируют полученный результат. Все агенты могут быть разделены на следующие группы:

1. Агент KbdHwrt – верификация пользователя по клавиатурному почерку, пассивный. Наблюдает за клавиатурным вводом пользователя, сравнивает наблюдения с записанным ранее профилем пользователя. Состояния *True* – пользователь верифицирован, *False* – пользователь определен как несовпадающий, *None* – отказ от верификации по любой причине (нет профиля, недостаточно данных, невысокий процент совпадения и т. п.).
2. Агент MouseHwrt – аналогичен KbdHwrt, но работает с мышью.
3. Агент FaceID – идентификация пользователя по изображению лица с веб-камеры, пассивный/активный. При наличии на устройстве пользователя веб-камеры получает изображение, проводит поиск лица, в случае обнаружения сравнивает его с профилем пользователя, выносит решение о совпадении. В некоторых случаях может просить пользователя включить камеру, показать лицо.
4. Агент VoiceID – аналогичен FaceID, но работает с голосом пользователя. Может просить пользователя включить микрофон, произнести заданную фразу.

5. Агент anBhvr – агент определения аномального поведения субъекта, пассивный. Создает типовые профили поведения субъекта, группы субъектов. Наблюдая за текущим поведением, определяет отклонение от типового поведения. Поскольку нетипичное поведение необязательно означает злоумышленные действия, то обладает невысоким доверием.

Помимо действий пользователя интеллектуальные агенты могут анализировать состояние среды, с которой взаимодействует пользователь. Интеллектуальные агенты наблюдения за средой могут разделяться:

– Агент IntrusDtct – наблюдает за защищаемой системой, определяет попытки или наличие атак на защищаемую систему или ее части, производит анализ и учет инцидентов, пассивный;
– Агент NwsMon – осуществляет мониторинг новостей/сообщений на профильных сообществах на предмет наличия информации о готовящихся злоумышленных действиях против защищаемой системы. Также осуществляет мониторинг общего ландшафта предполагаемых атак в регионе расположения защищаемой системы и отрасли, которой принадлежит защищаемая система и другие факторы (например, для вуза отмечается повышенная опасность DDoS атак во время приемных кампаний).

Наряду с информацией о субъекте и объекте интеллектуальные агенты способны анализировать объект доступа. В качестве основных интеллектуальных агентов наблюдения за объектом выступают:

– General – набор стандартных показателей и характеристик работы объекта (в том числе, но не ограничивающийся частотой использования ресурса, разнообразием пользователей, имеющих доступ к ресурсу, данных от систем мониторинга состояния объекта и т. п.), не обладает интеллектуальными свойствами.
– Агент AbUsng – определяет нетипичное использование ресурса, пассивный. Создает типовые профили использования ресурса или группы однотипных ресурсов, наблюдает за текущими сценариями использования, определяет аномалии. Поскольку нетипичное использование необязательно означает злоумышленные действия, то обладает невысоким доверием. Работает на уровне отдельного ресурса, группы однотипных ресурсов и группы ресурсов с одинаковой принадлежностью.

– Агент ChngDtct – наблюдает за изменениями состояния ресурса, определяет их допустимость, пассивный. Применяется к некоторым ресурсам.

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. Такая система позволяет использовать несколько экземпляров агентов, основанных на различных методах искусственного интеллекта и разных версиях их программных реализаций.

3.4.2 Формирование агентов на основе данных доступа к образовательным сервисам

Выбор данных для анализа при обеспечении безопасности определяется рядом факторов, одним из важнейших является аппаратно-вычислительное обеспечение, требование по оперативному расчету рисков и обработке больших объемов файлов журналов событий безопасности, а также отдельных ресурсов по их анализу. Выбираемые алгоритмы и агенты должны учитывать эти обстоятельство. Таким образом, алгоритмы обработки и формируемые агенты должны быть достаточно быстрыми и использовать имеющиеся вычислительные ресурсы. Общая схема работы процесса мониторинга представлена на рисунке 3.10 [206].

В системе аудита вуза содержатся описания событий. Событие описывается рядом признаков, которые могут быть использованы для формирования агентов:

– **Eventname** (object) – название события, например, вход пользователя в систему (*\core\event\user_loggedin*);
– **Objectid, relateduserid** (float64), **userid, contextid, contextinstanceid, courseid** (int64) – ID цели Eventname, ID пользователя, соотнесенного с событием, ID пользователя-источника события, ID контекста, instance контекста и курса, с которым происходит взаимодействие.
– **Crud** (object) – уровень работы с базой данных в методологии CRUD (create, read, update, delete);

– **Contextlevel** (int64) – положение в иерархии содержимого (всего 5-6 контекстов: отдельная дисциплина, группа дисциплин и т. п.);
– **Other** (object) – справочная информация о событии;
– **Timecreated** (int64) – время создания события;
– **Origin** (object) – источник события;
– **Ip** (object) – IP входного порта, к которому обращается событие;
– **Fileindex** (int64) – дополнительный признак, введенный для опознавания индексов файлов, из которых взяты события.

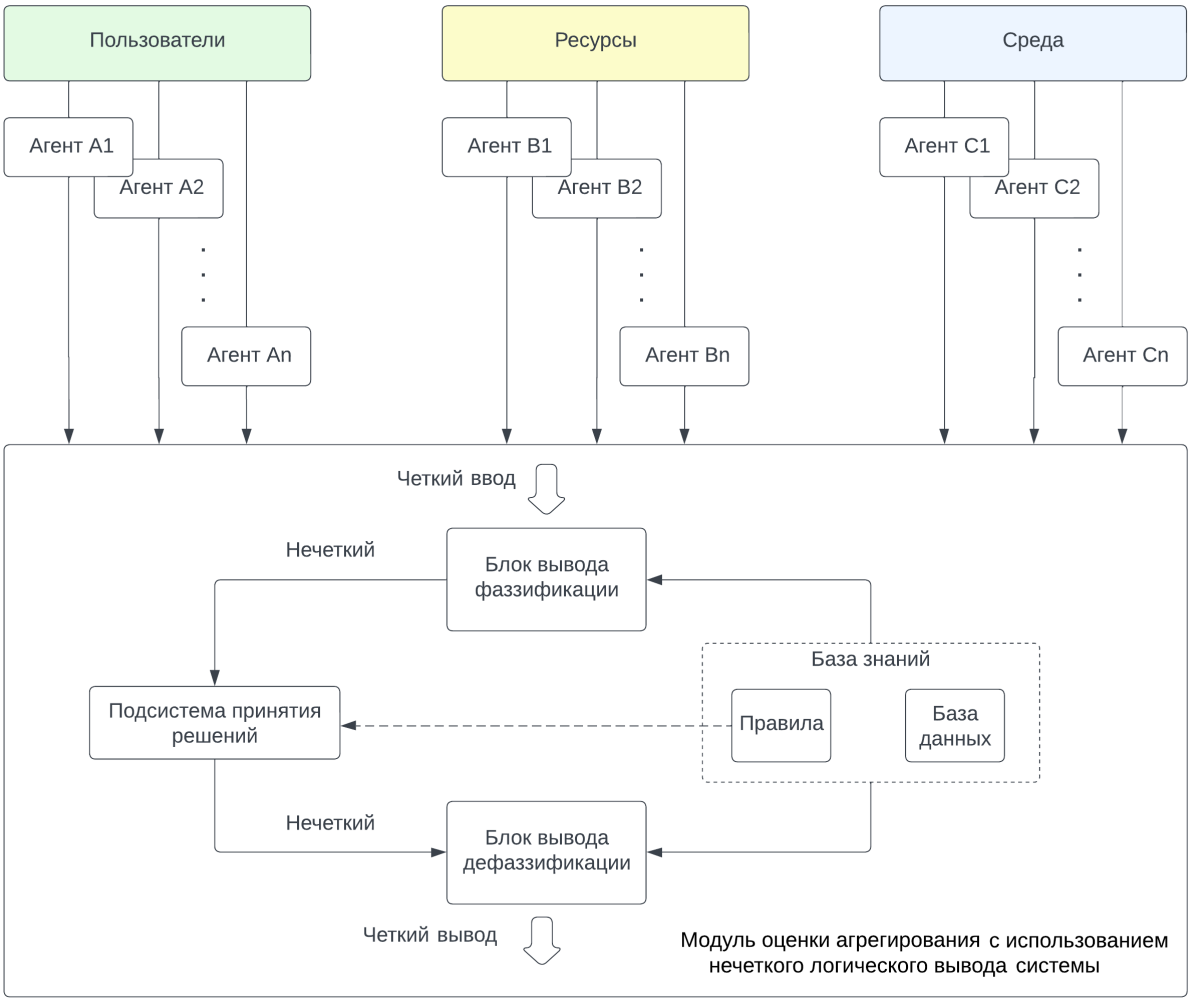


Рисунок 3.10 — Схема работы агрегирующей системы мониторинга

На основании анализа представленных данных выделено 4 типа агентов:

1. Агент 1 – Агент наблюдения за объектами – следит за количеством событий удаления пользователей и объектов.
2. Агент 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 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 4 – Агент наблюдения за пользователями – следит за количеством активных пользователей. В зависимости от количества пользователей высчитывается риск от 0 до 10. Нижняя и верхняя границы определяются задаваемой конфигурацией. Учитываются только изменения под конец 10-минутного периода. Время сессии одного пользователя – 30 минут.

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 $0 \ldots 1$ 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) [136]. Использование нечетких логических правил вместо четких позволяет учитывать недостаточное доверие к показаниям агентов, что регулируется функциями принадлежности их результатов. Реализация системы FIS возможна средствами библиотеки scfuzzy на языке Python. Работа FIS заключается в реализации следующих шагов:

1. Шаг 0. Составление баз данных правил и функций принадлежности (на этапе разработки/модификации системы).

2. Шаг 1. Фаззификация – перевод числовых показаний агентов в нечеткий вид согласно назначенным функциям принадлежности.
3. Шаг 2. Инференс – Выполнение нечетких правил, определение степени выполнения правила.
4. Шаг 3. Агрегирование результатов нечетких правил – возвращается нечеткая переменная с рассчитанной функцией принадлежности.
5. Шаг 4. Дефаззификация – перевод нечеткого результата в четкое число, интерпретируемое в дальнейшем как установленный уровень риска.

Здесь нечеткие логические правила следуют логике Мамдани, для которой нечеткие логические операции, аналогичные четкой логике, определены через операции с уровнем принадлежности нечетких значений. Каждый агент возвращает число, описывающее его состояние (табл. 8). Такое число задается либо в некоторой заранее известной шкале (например, от 0 до 10), либо нормируется к диапазону $0 \ldots 1$ и может быть интерпретировано как уверенность агента в появлении угрозы (в рамках его компетенции). Показания однотипных агентов агрегируются путем: усреднения, взвешенного усреднения, голосования (для категориальных).

Таблица 8 — Соответствие четких и нечетких логических операций

Boolean	Fuzzy
AND(x, y)	MIN(x, y)
OR(x, y)	MAX(x,y)
NOT(x)	$1 - x$

Сформированная система агентов, а также правил нечеткой логики, позволяющая осуществить переход от качественных значений, характеризующих величину значимости события, поступающего от агентов, в количественные значениям риска применяется в разработанном методе оценки риска, основанном на нечетких правилах.

3.4.3 Метод оценки риска на основе нечетких правил

Для всех агентов установим три градации нечетких значений риска: "низкий", "средний", "высокий".

Пусть i – номер агента $(1 \dots 4)$; I – число агентов имеющих 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 – (полу) ширина неоднозначности в оценке агентом риска "низкий"; a_i^C – (полу) ширина неоднозначности в оценке агентом риска "средний"; a_i^B – (полу) ширина 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" $S_i^H = \dfrac{D_i}{1 + [R_i - \frac{c_i^H}{a_i^H}]^{2b_i^H}}$;

– для риска "средний" $S_i^C = \dfrac{D_i}{1 + [R_i - \frac{c_i^C}{a_i^C}]^{2b_i^C}}$;

– для риска "высокий" $S_i^B = \dfrac{D_i}{1 + [R_i - \frac{c_i^B}{a_i^B}]^{2b_i^B}}$.

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:

$$W_j = F_I^j \circ S_I^{g_{jI}}(R_I) \circ \ \dots \ \circ F_i^j \circ S_i^{g_{ji}}(R_i) \circ \ \dots \ \circ F_1^j \circ S_1^{g_{j1}}(R_1). \qquad (3.1)$$

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 $\wedge$):

$$W_j = S_I^{g_{jI}}(R_I) \wedge \dots \wedge S_i^{g_{ji}}(R_i) \wedge \dots \wedge S_1^{g_{j1}}(R_1). \qquad (3.2)$$

Согласно правилам вычисления нечетких логических выражений (табл. 9):

$$W_j = \min \left[S_I^{g_{jI}}(R_I), \ \dots, S_i^{g_{ji}}(R_i), \ \dots, S_1^{g_{j1}}(R_1) \right]. \qquad (3.3)$$

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:

$$S^0(R) = \max_{j=1...J} \left[\min(S_j^0(R), W_j)\right]. \tag{3.4}$$

Таблица 9 — Нечеткие правила системы вывода

	ЕСЛИ				ТО
№	Агент 1	Агент 2	Агент 3	Агент 4	Заключение
1	Низкий	Низкий	Низкий	Низкий	Низкий
2	Высокий	Низкий	Низкий	Низкий	Высокий
3	Низкий	Высокий	Низкий	Низкий	Высокий
4	Низкий	Низкий	Высокий	Низкий	Высокий
5	Низкий	Низкий	Низкий	Высокий	Средний
6	Высокий	Высокий	Высокий	Высокий	Высокий
7	Средний	Средний	Средний	Средний	Высокий
8	Средний	Средний	Средний	Низкий	Высокий
9	Низкий	Средний	Средний	Средний	Средний
10	Средний	Низкий	Средний	Средний	Средний
11	Низкий	Средний	Средний	Низкий	Средний
12	Средний	Низкий	Низкий	Средний	Низкий
13	Низкий	Низкий	Низкий	Средний	Низкий
14	Низкий	Средний	Низкий	Средний	Средний
15	Средний	Низкий	Низкий	Низкий	Низкий

Решением уравнения (3.4), представляющим собой значением общего риска, является число, определяющее центр площадей. Общий риск R^* измеряется в тех же градациях "низкий", "средний", "высокий" (рис. 3.13):

$$R^* \equiv A_{R<R^*}(S^0(R)) = A_{R>R^*}(S^0(R)) \tag{3.5}$$

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

Таким образом (выражение (3.5)) определено значение общей оценки риска $R*$.

Визуализация результатов оценки риска согласно выражению (3.5) для следующих агентов:

– Агент VoiceID сообщает об уровне риска 2 (в 10-балльной шкале), с градациями степени принадлежности: "низкий": 0.7, "средний": 0.4, "высокий": 0.1;
– Агент NwsMon сообщает об уровне риска 5 (в 10-балльной шкале), с градациями степени принадлежности: "низкий": 0.3, "средний": 0.8, "высокий": 0.3;

представлена на рисунке 3.11. При этом общий риск измеряется в тех же градациях "низкий", "средний", "высокий", с колоколообразными функциями принадлежности по типу 2: S_H (голубой), S_C (оранжевая) и S_B (зеленый) и представлен на рисунке 3.12.

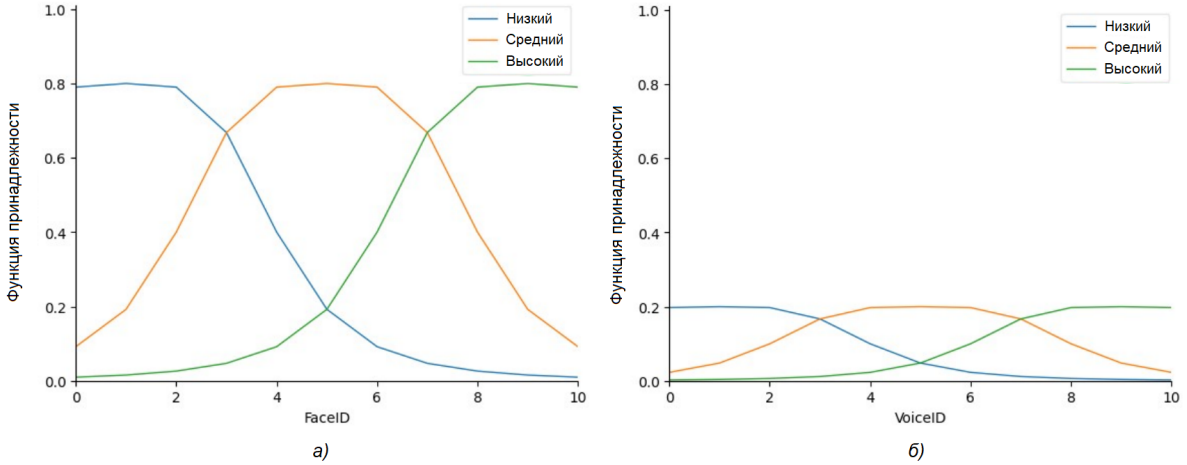


Рисунок 3.11 — Функции принадлежности: а) агента FaceID, б) агента VoiceID

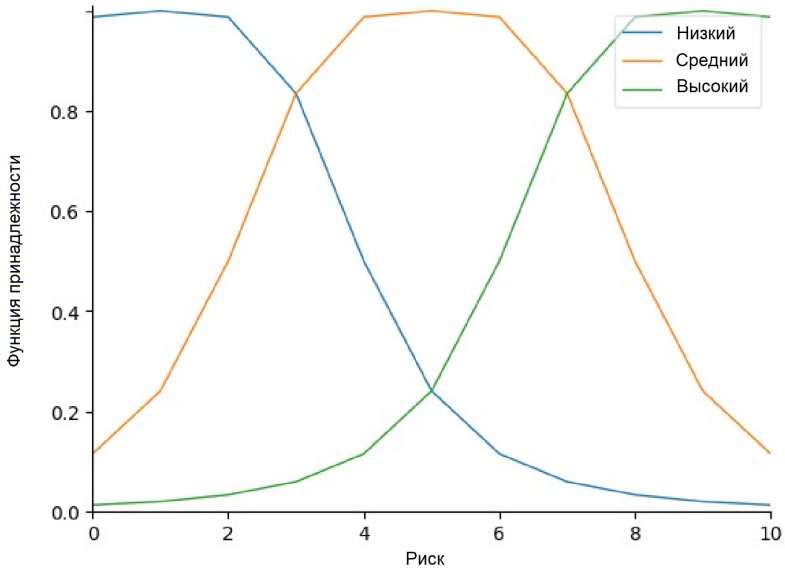


Рисунок 3.12 — Функции принадлежности общего риска $R*$ для агентов FaceID и VoiceID

В системе логического вывода заданы (для примера) 2 правила:

1. ЕСЛИ [риск VoiceID] "высокий" И [риск NwsMon] "высокий" ТОГДА [общий риск] "высокий";
2. ЕСЛИ [риск VoiceID] "низкий" И [риск NwsMon] "средний" ТОГДА [общий риск] "низкий".

Проведем расчет выполнения правил:

– для Правила 1 степень выполнения: С1= МИН(0.1, 0.3) = 0.1 (практически не выполняется);
– для Правила 2 степень выполнения: С2= МИН(0.7, 0.8) = 0.7 (довольно уверенно выполняется).

Решение возможно принять двумя вариантами:

– выбирать только самое уверенно выполняемое правило: тогда будет выбрано правило 2, общий риск "низкий" с уверенностью 0.7, после дефаззификации 2 по 10-балльной шкале;
– агрегировать все правила, выбирая МАКСИМАЛЬНУЮ степень принадлежности результата (рис. 3.13). Дефаззификация (способом расчета центра площадей) дает общий уровень риска 3 (по 10-балльной шкале).

Реализация системы нечеткой логики средствами библиотеки scfuzzy на языке программирования Python представлена на рисунке 3.14.

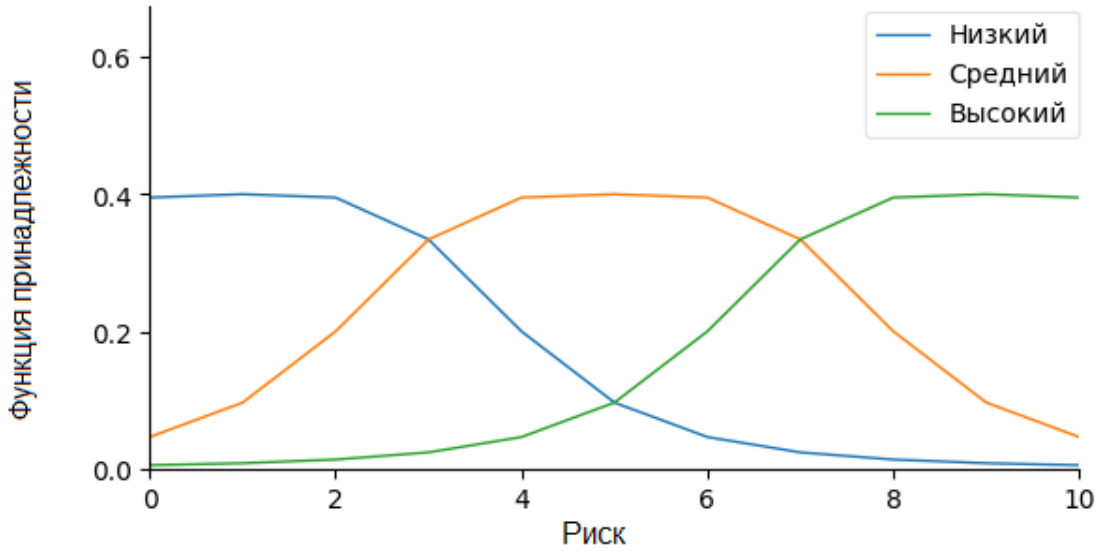


Рисунок 3.13 — Функции принадлежности агентов общего риска $R*$

Пример нечеткого логического вывода для расчета текущего риска.

Для работы с нечеткими множествами и нечеткими правилами есть библиотека skfuzzy. Ознакомьтесь с документацией и не забудьте установить библиотеку.

```
[15] # Установку надо сделать только раз.
     !pip install -q -U scikit-fuzzy
```

```
[16] import numpy as np # подключаем numpy
     import pandas as pd
     import skfuzzy as fuzz # подключаем библиотеку skfuzzy
     from skfuzzy import control as ctrl # и модуль control для задания переменных и правил
```

```
[17] scale=np.arange(0, 11, 1) # шкала измерения риска - показаний агентов 0-10
```

```
[18] # примеры значений риска, возвращенного агентами
     df=pd.DataFrame(columns=['Name','Risk','Conf']) #  Название агента / Величина риска / Степень доверия к агенту
     list_row = [["Агент1", 2, 0.4] ,["Агент2", 9, 0.8],["Агент3", 3, 0.2],["Агент4", 2, 0.5]]
     s=len(df.index)
     for i, row in enumerate(list_row):
       df.loc[s+i] = row
     df.head()
```

	Name	Risk	Conf
0	Агент1	2	0.4
1	Агент2	9	0.8
2	Агент3	3	0.2
3	Агент4	2	0.5

```
[19] # Зададим элементы для переменных - нечетких множеств для каждого агента
     Ant=[ctrl.Antecedent(scale, row) for row in df['Name']] # название переменной
```

```
[20] # выходная переменная - общий риск
     Con = ctrl.Consequent(scale, 'Диапазон риска') # название
```

```
[21] #df['Conf'][0]
```

```
     # функции принадлежности, здесь обобщенные функции Гаусса
     mf_dict={'Низкий': 1,'Средний': 5,'Высокий': 9} # лингвистические значения и положения центра для них
     A, B=3, 2 # определяют "крутизну" функций
     for i in range(len(Ant)):
       for mf, c in mf_dict.items():
         #print(mf,c)
         Ant[i][mf]=df['Conf'][i]*fuzz.gbellmf(Ant[i].universe,a=A,b=B,c=c) #  df['Conf'][i] - доверие
```

Рисунок 3.14 — Реализация системы нечеткой логики

Практическая реализация разработанного метода количественной оценки значения риска реализации угроз информационной безопасности на основе анализа событий, поступающих от разработанной системы агентов, позволяет перейти к экспериментальной оценке полученных значений разработанного метода.

3.5 Результаты оценки рисков на основе анализа данных доступа к образовательным сервисам

Результатом работы разработанной системы агентов, осуществляющих мониторинг событий безопасности, и метода количественной оценки риска яв-

ляется вычисляемое значение риска, в дальнейшем используемое в модели управления доступом для учета изменяющихся атрибутов модели. Для вычисления итогового значения риска необходимо агрегировать и кластеризовать информацию, полученную от разработанной системы агентов.

3.5.1 Кластеризация журналов событий безопасности, поступающих от агентов

Получены данные файлов журналов событий безопасности электронной системы вуза, содержащиеся в CSV-таблицах. Всего представлено 1289 фрагментов данных общим размером в 12 Гб. Каждый фрагмент данных содержит описания событий, зафиксированных в логирующей системе вуза. Событие описывается рядом признаков, часть которых пригодна для кластеризации. Ниже описаны признаки, отобранные для кластеризации [207]:

- Id (int64) – id события, не используется для кластеризации, так как все id событий уникальные и не отражают релевантных для кластеризации качеств событий;
- Eventname (object) – название события, например, /backslcore/event/user_loggedin, вход пользователя в систему. Признак является релевантным; предположительно, разделение по нему является ключевым в кластеризации предоставленных файлов журналов событий безопасности;
- Component, action, target, objecttable (object) – расшифровка компонентов Eventname события. Так, предложенный ранее пример /core/event/user_loggedin будет представлен как [core, loggedin, user, user]. Хотя эти признаки могли бы быть релевантными, при исследовании корреляции столбцов видно, что они низко информативны и обладают высокой корреляцией как между собой, так и с уже рассмотренным Eventname. Почти каждому значению Eventname сопоставляется ровно один набор значений [component, action, target, objecttable]. Кодирование этих признаков не добавляет эффективности кластеризации, только увеличивает вычислительную сложность

алгоритмов. Соответственно, данные столбцы были исключены из кластеризации;

- Objectid, relateduserid (float64), userid, contextid, contextinstanceid, courseid (int64) – id цели Eventname, id пользователя, соотнесенного с событием, id пользователя-источника события, id контекста, instance контекста и курса, с которым происходит взаимодействие. Данные признаки отличаются низкой кардинальностью большинства значений (много редких значений, мало популярных значений). При one-hot кодировании данных признаков был применен порог threshold для min_frequency значений – все значения с долей менее 1% в каждом признаке были объединены в категорию "нечастых" – infrequent;
- Crud (object) – уровень работы с базой данных в методологии CRUD (create, read, update, delete);
- Edulevel (int64) – принадлежность события в шкале учитель/ученик, 3 уровня;
- Contextlevel (int64) – положение в иерархии содержимого (всего 5-6 контекстов: отдельная дисциплина, группа дисциплин и т. п.);
- Anonymous (int64) – анонимность события. Бинарный признак с чрезвычайно редким значением 1 (да) – реже, чем в 40000 событиях. Был исключен из рассмотрения в кластерном анализе из-за низкой вариативности, но может быть значимым в дальнейшей работе по поиску аномалий;
- Other (object) – справочная информация о событии – трудно интерпретируемая, может быть значимой для поиска аномалий, но чрезвычайно тяжелая вычислительно из-за множества уникальных значений. Содержит дополнительную специфичную для события информацию о нем. Например, e-mail адрес пользователя для событий входа в систему, сообщение сервера для событий отказа в доступе и др. В целях конфиденциальности исключена из рассмотрения;
- Timecreated (int64) – время создания события. Данный признак является единственным числовым признаком (хотя многие другие признаки также закодированы float или int64, они отражают категории объектов, в то время как данный признак отражает время, когда происходило событие);

– origin (object) – источник события – web, ws или cli, зачастую (около 20% значений) неизвестный;
– Ip (object) – ip входного порта, к которому обращается событие, всего ip мало, не более двух-трех в каждом блоке из 10 фрагментов данных;
– Realuserid (float64) – реальный id пользователя. Вся колонка заполнена NaN – признаками отсутствия данных, поэтому в дальнейшем исключена из рассмотрения;
– Fileindex (int64) – дополнительный признак, введенный нами для опознавания индексов файлов, из которых взяты события.

Таким образом, из рассмотрения были исключены такие признаки как ID, realuserid, other, objecttable, component, action, target, anonymous. После этого число признаков снизилось с 22 до 14. Оставшиеся признаки были разделены на категориальные: eventname, objectid, crud, edulevel, contextid, contextlevel, contextinstanceid, userid, courseid, relateduserid, origin, ip, fileindex, и числовые: timecreated [208].

Для приведения признаков к нормализованному виду и осуществления анализа данных были применены следующие преобразования:

– в столбцах objectid, relateduserid, origin и ip были исключены NaN заменой на значения -1.0 (в числовых столбцах, предварительно проверено, что таких значений не присутствует в исходных данных) и на unknown (в строковых столбцах);
– к столбцу timecreated применено масштабирование MinMaxScaling для приведения признака к диапазону [0, 1]. Примечательно, что большая часть данных (более 80%) имеют значения более 90 для многих подмножеств файлов журналов событий безопасности. Это свидетельствует о неравномерном распределении логирования событий (много событий происходят в близкое время, малое число событий в другое время);
– к категориальным столбцам применено one-hot кодирование с отсечением значений с долей менее 1% в исходных данных (такие значения объединены в категорию infrequent).

Таким образом, в зависимости от взятого среза исходных данных после предобработки получается таблица из N * (80 . . . 120) ячеек, где N – размер взятого среза исходных данных, а 80-120 – среднее число признаков после предобработки. Это число можно регулировать установлением другого порога для infrequent данных, например, понизить долю с 1% до 0.1% или менее. Стоит

быть осторожным, так как без таких ограничений невозможно применять one-hot кодирование ко всем приведенным категориальным признакам (требуется 100-300 Гб оперативной памяти без infrequent threshold).

Для дальнейшего упрощения вычислений вместо рассмотрения всех исходных таблиц с данными брались подмножества файлов со случайными индексами. Для каждого размера подмножеств рассматривались несколько уникальных наборов индексов, результаты собранных метрик кластерного анализа усреднялись по данным наборам. Извлечение данных и их предобработка проводились с помощью средств Python, библиотеки для работы с табличными данными Pandas и инструментов библиотеки Scikit-learn [209].

После сбора и предобработки данных записи журнала событий безопасности рассматриваются как числовые последовательности, что можно считать аналогом токенизации в языковых моделях. Архитектура модели аналогична BERT, в которой:

- числовая последовательность векторизуется обучаемым слоем Embedding;
- векторная последовательность проходит через несколько блоков трансформер-подобных слоев, число блоков регулируется;
- на выходе получается другая векторная последовательность с таким же количеством элементов, но с регулируемой длиной вектора-элемента. При этом в силу свойств механизма внимания каждый элемент выходной последовательности связан с каждым элементом входной последовательности.
- случайно выбирается подмножество входных элементов (обычно 15%) и они заменяются на значение <MASK>;
- вычисляется контрастивная ошибка предсказания замаскированных элементов и модель обучается до тех пор пока не будет получено минимальное значение контрастивной ошибки;
- обученные веса модели сохраняются для последующего использования.

В процессе обучения используются следующие слои: слой векторизации Embedding, слой позиционного кодирования, блок трансформера, слой внимания, слой нормализации, слой персептрона, а также модуль расчет контрастивной ошибки.

Слой векторизации Embedding

На вход слоя подается векторная последовательность x_i , проходит через нелинейную функцию $tansig()$, возвращающую выход в диапазоне $-1, \ldots, +1$, с дополнительным множителем k_i регулирующим крутизну:

$$y_i = tansig(k_i * x_i). \tag{3.6}$$

Выход y поступает одновременно на два персептронных слоя нейронов. Первый имеет функцию активации $tansig()$ (рис. 3.15а), второй – $logsig()$ (рис. 3.15б). Число нейронов N в слоях одинаковое, назначается экспериментально и меньше, чем размерность входного элемента.

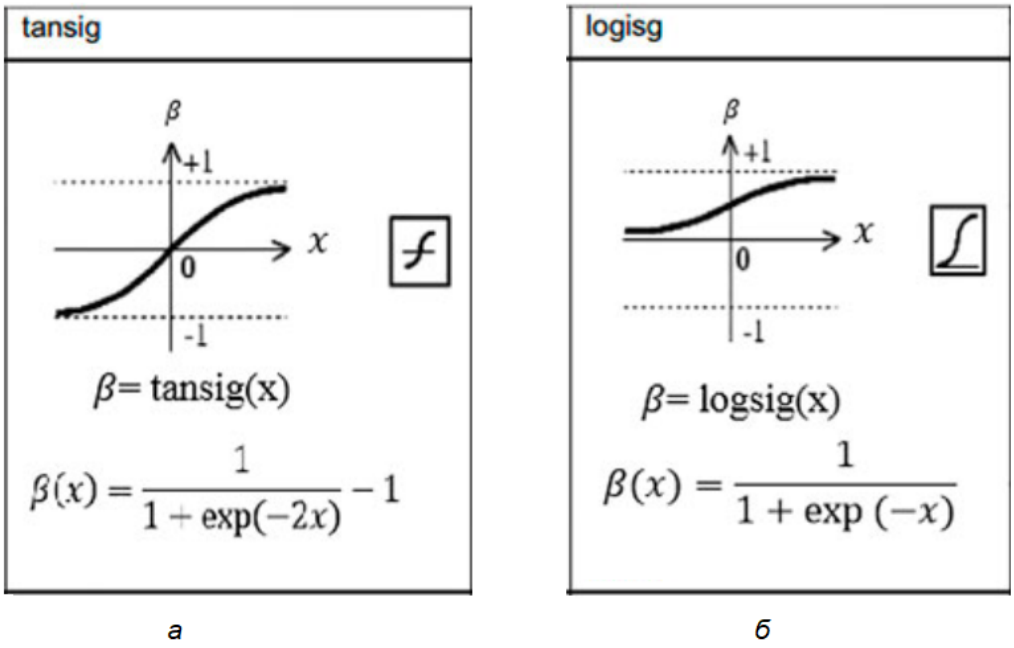


Рисунок 3.15 — Функция активации: а) $tansig()$, б) $logsig()$

Каждый такой слой выполняет линейное преобразование входа, используя обучаемые параметры и применяет нелинейную функцию активации: $z_1 = f_(W^1 * y + b^1)$ и $z_2 = f_(W^2 * y + b^2)$ соответственно, где W, b – параметры обучения (обучаемые параметры), $f()$ – выбранная функция активации.

Выход второго слоя с активацией $logsig()$ лежит в пределах $0, \ldots, 1$ и может интерпретироваться как коэффициент важности признака. Выходы обоих слоев перемножаются поэлементно, образуя обучаемый вентиль: $o = z^1 \circ z^2$.

Слой позиционного кодирования

Так как слои внимания не чувствительны к изменению порядка следования элементов последовательности, то необходимо позиционное кодирование,

которое бы вернуло такой порядок (рис 3.16). Здесь мы следуем рекомендациям позиционного кодирования для языковых моделей и используем матрицу позиционных кодов:

$$P(k, 2i) = \sin(\frac{k}{n^{2i/d}}),$$
$$P(k, 2i+1) = \cos(\frac{k}{n^{2i/d}}),$$

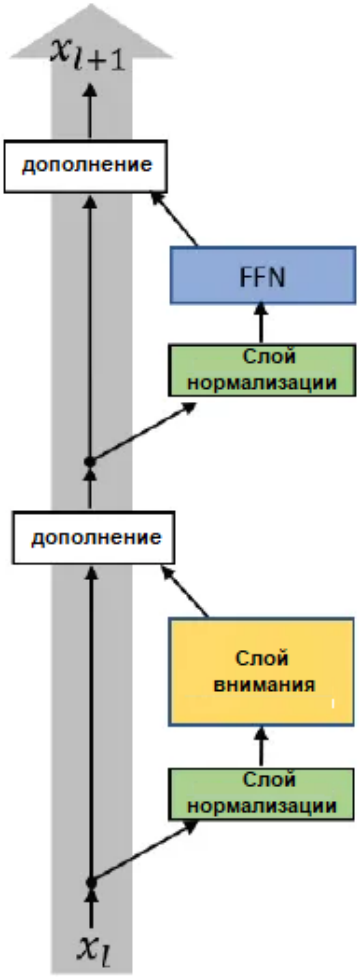
где K – номер элемента в последовательности, d – размерность векторов, совпадает с размерностью N слоя Embedding, n – подбираемый вручную параметр для повышения разнообразия кодов.

Рисунок 3.16 — Позиционное кодирование

Блок трансформера

Используется блок Pre-LN трансформера (рис. 3.17), который состоит из слоя внимания, слоев нормализации, слоя персептрона с нелинейной активацией и пропускающих связей, чтобы обеспечить стабильность градиента.

Слой внимания обеспечивает смешивание элементов входной последовательности с помощью обучаемых матриц W_Q (запросов), W_K (ключей), W_V (значений). Входной вектор X путем умножения на матрицы преобразуется в вектора Q, K, V (рис. 3.18).



Pre-LN Transformer

$$
\begin{aligned}
x_{l,i}^{pre,1} &= \text{LayerNorm}(x_{l,i}^{pre}) \\
x_{l,i}^{pre,2} &= \text{MultiHeadAtt}(x_{l,i}^{pre,1}, [x_{l,1}^{pre,1}, \cdots, x_{l,n}^{pre,1}]) \\
x_{l,i}^{pre,3} &= x_{l,i}^{pre} + x_{l,i}^{pre,2} \\
x_{l,i}^{pre,4} &= \text{LayerNorm}(x_{l,i}^{pre,3}) \\
x_{l,i}^{pre,5} &= \text{ReLU}(x_{l,i}^{pre,4} W^{1,l} + b^{1,l}) W^{2,l} + b^{2,l} \\
x_{l+1,i}^{pre} &= x_{l,i}^{pre,5} + x_{l,i}^{pre,3}
\end{aligned}
$$

Final LayerNorm: $x_{Final,i}^{pre} \leftarrow \text{LayerNorm}(x_{L+1,i}^{pre})$

Рисунок 3.17 — Блок Pre-LN трансформера

Находят попарные скалярные произведения векторов запросов на вектора ключей, нормируют их функцией $softmax()$ и получают коэффициенты внимания. Выходной вектор получается как взвешенная сумма векторов значений с соответствующим коэффициентами внимания (рис. 3.19).

Обучаемый слой нормализации задается выражением:

$$\text{LayerNorm}(\nu) = \gamma \frac{\nu - \mu}{\delta} + \beta,$$

$$\mu = \frac{1}{d} \sum_{k=1}^{d} \nu_k \text{and} \delta^2 = \frac{1}{d} \sum_{k=1}^{d} (\nu_k - \mu)^2,$$

где d – размерность входного вектора, γ, β – коэффициенты обучения (обучаемые коэффициенты).

Обучаемый слой персептрона, выполняющий линейное предобразование входного вектора и применяющий нелинейную функцию активации, представ-

ляет собой обучаемую функцию (рис. 3.20):

$$Swish_{\beta}(x) = x\delta(\beta x)$$
$$\delta(z) \sim sigmoid\, function.$$

Input vectors: X (shape $N_X \times D_X$)
Key matrix: W_K (Shape $D_X \times D_Q$)
Value matrix: W_V (Shape $D_X \times D_V$)
Query matrix: W_Q (Shape $D_X \times D_Q$)

Query vectors: $Q = XW_Q$ (Shape $N_X \times D_Q$)
Key vectors: $K = XW_K$ (Shape $N_X \times D_Q$)
Value vectors: $V = XW_V$ (Shape $N_X \times D_V$)
Similarity function: *scaled dot product*
Similarities: $E = QK^T$ (shape $N_X \times N_X$), $E_{i,j} = Q_i \cdot K_j / \sqrt{D_Q}$
Attention weights: $A = \text{softmax}(E, dim = 1)$ (shape $N_X \times N_X$)
Output: $Y = AV$ (shape $N_X \times D_V$) where $Y_i = \sum_j (A_{i,j}, V_j)$

Рисунок 3.18 — Алгоритм слоя внимания

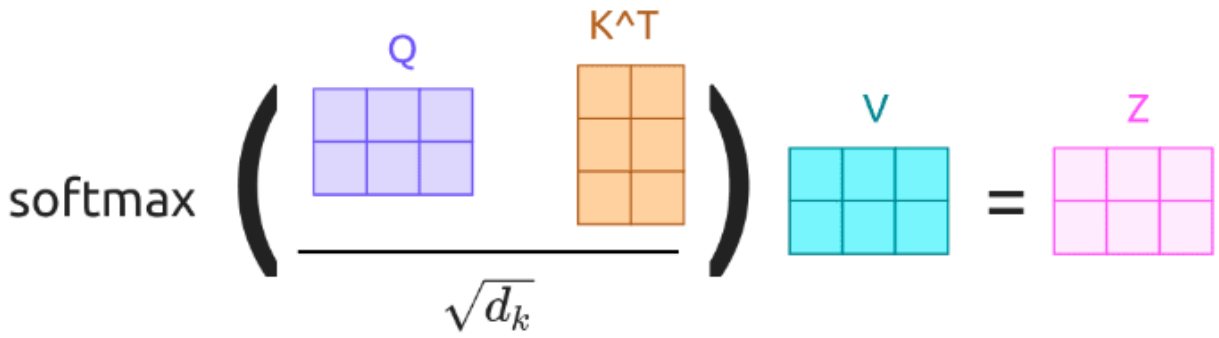


Рисунок 3.19 — Нормирование скалярного произведения векторов запросов на вектора ключей функцией $softmax()$

Расчет контрастивной ошибки

Модуль расчета ошибки маскировки выполняется также как для оригинальной сети BERT:

$$L_{MLM}^{(x)} = \frac{1}{|M_x|} \sum_{i \in M_x} \log P(x_i / (x \setminus M_x)), \tag{3.7}$$

где $x \setminus M_x$ – замаскированная последовательность, M_x – набор замаскированных элементов (их позиций).

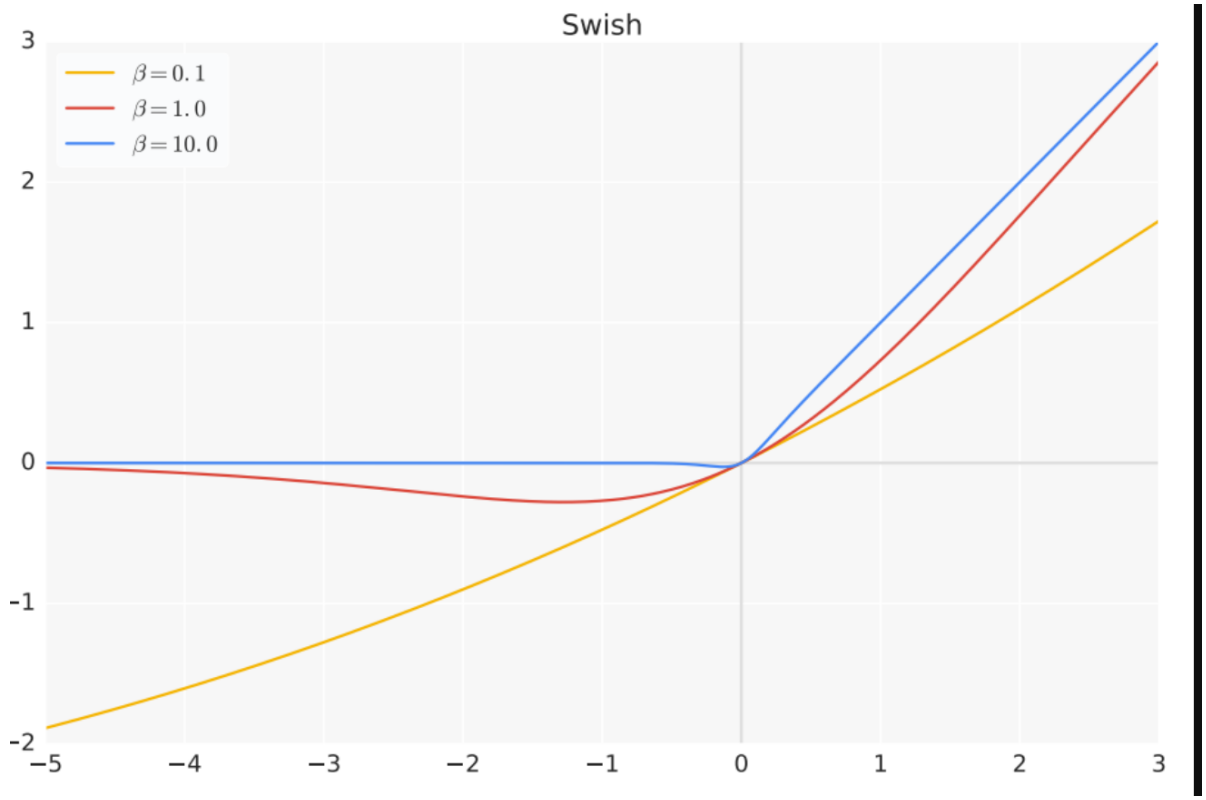


Рисунок 3.20 — Слой активации персептрона Swish

После обучения сформированная модель позволяет для любой записи файлов журнала событий безопасности сформировать векторную (самообученную) последовательность. Дальнейшая работа по кластеризации полученных результатов ведется в новом векторном пространстве [210].

Для решения задачи кластеризации векторного пространства использовались иерархические алгоритмы кластеризации. Алгоритмы иерархической кластеризации – подвид алгоритмов кластеризации без учителя, которые формируют иерархию (дерево) вложенных кластеров. Большинство алгоритмов являются агломеративными (agglomerative) – где итоговые кластеры образуются объединением более мелких кластеров. Также существуют дивизивные (divisive) методы, разделяющие большие кластеры на маленькие, но они не отличаются популярностью в применении. В данной работе фокус направлен на изучение именно agglomerative методов.

Для агломерации кластеров необходимо задать меру расстояния между кластерами. В силу ограничений метрик (которые будут рассмотрены ниже)

было принято решение использовать евклидову геометрию. Всего рассмотрены 4 вариации агломеративных алгоритмов, использующие различные методы соединения кластеров:

- Single linkage – расстояние между кластерами считается как минимальное из попарны расстояний между элементами различных кластеров: $\min\{d(a,b) : a \in A, b \in B\}$;
- Complete linkage – в противоположность single linkage, расстояние считается как максимальное из попарных расстояний между элементами кластеров: $\max\{d(a,b) : a \in A, b \in B\}$;
- Average linkage – в данном случае попарные расстояния между элементами различных кластеров усредняются для определения расстояния между кластерами: $\frac{1}{|A| \cdot |B|} \sum_{a \in A} \sum_{b \in B} d(a,b)$;
- Ward – метод Уорда. Данный метод более сложный, для оценки расстояния между кластерами используется следующая метрика: прирост суммы квадратов расстояний от всех элементов кластеров до полученного в результате объединения центра кластера: $\Delta' \sum_i (x_i - \overline{x})^2 - \sum_{x_i \in A} (x_i - \overline{a})^2 - \sum_{x_i \in B} (x_i - \overline{b})^2$.

Помимо этих агломеративных методов также применялся алгоритм BIRCH, который также является иерархическим, хотя и обладает более сложной структурой. Преимуществом данного метода является более сложная работа с деревом кластеров – алгоритм динамически балансирует дерево в зависимости от заданных параметров ветвления и порогов размеров поддеревьев. Алгоритм группирует переполненные подкластеры и удаляет лишние ветвления в дереве постепенно. Данный алгоритм эффективен для использования на больших массивах данных.

В качестве бэйзлайна для исследования алгломеративных методов был выбран классический центроидный алгоритм кластеризации K-means (K-средних). В ходе выполнения работы также рассматривался метод MeanShift – сдвига среднего значения, изучающий среднюю плотность в окне, задаваемую ядерной функцией. Данный метод обладает большой вычислительной сложностью и требует значительной калибровки. Более того, в алгоритме нельзя конфигурировать число кластеров, что затрудняет его сравнение с другими приведенными алгоритмами. По этим причинам после многочисленных попыток ускорить алгоритм, он был исключен из рассмотрения. Таким образом, в работе

рассматривались результаты выполнения 6 алгоритмов: K-means, Agglomerative Clustering (Ward, Single, Complete, Average Linkage), BIRCH.

Для оценки качества кластеризации необходимо ввести метрики. В случае обучения без учителя и отсутствия ground-truth labels объектов выбор значительно ограничен. Остается три популярных метрики:

- Silhouette Coefficient, рассматривающая отношение между средним расстоянием между точками внутри кластера и средним расстоянием от точек кластера до точек другого ближайшего кластера. Метрика ограничена отрезком [-1; 1], где большее значение отражает лучшее качество кластеризации;
- Davies-Bouldin Index – данная метрика сравнивает расстояния между точками кластеров с их размерами. Хотя и простая в вычислении, данная метрика может использоваться только в евклидовом пространстве, в связи с чем во всех алгоритмах также использовалось евклидово расстояние для вычисления дистанций между кластерами;
- Calinski-Harabasz Index (Variance Ratio Criterion) – изучает дисперсию расстояний внутри конкретных кластеров и между всеми кластерами. Больший счет отражает лучшее качество кластеризации.

Стоит заметить, что данные метрики достаточно просты в вычислении и отражают качество кластеризации. В то же время акценты в метриках направлены на разные качества кластеров (так, Davies-Bouldin напрямую учитывает размер кластеров и имеет смещение в сторону больших плотных кластеров). Все метрики также используют плотность кластеров для оценки качества кластеризации, так что некоторые алгоритмы, основанные на плотности (например, DBSCAN и его вариации), по умолчанию будут оказываться более эффективными.

3.5.2 Результаты анализа событий, поступающих от агентов

Рассматривая эффективность алгоритмов кластеризации, можно сделать вывод, что релевантными параметрами для калибровки алгоритмов прежде всего будут размер кластеров и размер входных данных, поступающих на вход в алгоритм. Agglomerative clustering имеет крайне мало параметров для ка-

либровки. Можно было бы рассматривать разные дистанции для вычисления расстояний, но это ограничивается вычислениями метрик, работающих только в евклидовом пространстве. Вместо n_clusters – размера кластеров – можно было бы рассматривать distance_threshold – порог расстояния между кластерами, но он работает очень ситуационно, часто возникают ситуации, когда точки не получается отнести ни к одному кластеру. Также итоговое число кластеров не определено, что вызывает дополнительные трудности при сравнении с другими алгоритмами.

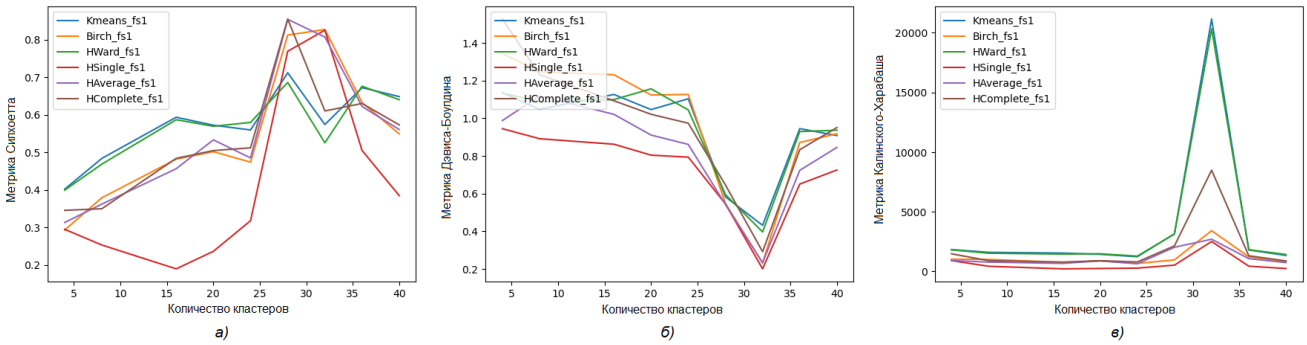


Рисунок 3.21 — Результаты кластерной оценки журналов событий безопасности по метрике: а) Силхоетта, б) Девиса-Боулдина, в) Калинского-Харбаша

Таким образом, сравнительный анализ по 3 приведенным метрикам применяется к срезам данных разного размера, а также конфигурируется число итоговых кластеров. На рисунке 3.21 приведены результатов метрик в зависимости от числа кластеров (взяты от 4 до 40 с периодом в 4). Стоит отметить, что более высокий счет Silhouette Score и Calinski-Harabasz отражает более высокое качество кластеризации, в то время как в Davies-Bouldin чем ближе счет к нулю – тем лучше. По графикам можно заключить, что оптимальное число кластеров близко к 32. Далее мы изучим это подробнее. Пока что можно заключить, что лучшие результаты показывают алгоритмы из агломерационного семейства – по Silhouette Score результаты почти всех вариаций (Single, Average, Complete), значительно превосходят K-means. В то же время Ward, показывающий близкие в K-means результаты, отличается высоким качеством по двум другим метрикам (причем, качество по Calinski-Harabasz значительно превосходит результаты всех других алгоритмов).

Изучим поближе число кластеров около 32. После многократного повторения сбора метрик были получены следующие выводы:

– При всех повторениях существовал точный оптимум числа кластеров, отражающийся на всех метриках для всех алгоритмов при фиксирован-

ном исходном наборе данных. Наиболее часто оптимум не превышает 34 с наиболее частым оптимумом при числе кластеров 33. Реже оптимум находится в окрестности 24-28, однако он также сопровождается понижением лучшего качества хотя бы по двум метрикам из трех.

– При любом оптимуме числа кластеров Agglomerative Ward обладает наилучшим качеством по метрике Galinski-Harabasz, достигая среднего пикового значения около 4600. Стоит также отметить, что данное значение не является медианным, медиана же находится около 2800. Это объясняется тем, что в отдельных случаях метрика доходит до значений в 20-40 тысяч, что отражает большое расстояние между маленькими плотными кластерами. Подробнее об этом случае мы поговорим далее;
– Также почти при любом оптимуме числа кластеров Agglomerative Average достигает максимума по метрике Silhouette Score, среднее пиковое значение 0.88, что близко к порогу качества 1 и свидетельствует о хорошем качестве кластеризации;
– Наиболее эффективным по Davies-Bouldin является алгоритм Agglomerative Single со средним минимальным значением в 0.83. Однако стоит заметить, что данный алгоритм зачастую проигрывает остальным по другим метрикам. Предполагаю, это связано с тем, что он генерирует чрезвычайно диспропорциональные по размеру классы, что сильно влияет на данную метрику, но не используется при подстчете других метрик.

Таким образом, вариации Agglomerative иерархических алгоритмов оказались наиболее эффективными на единичных срезах данных, в то время как K-means и BIRCH не показали выдающейся эффективности. При увеличении числа входных данных не удается получить более высокие результаты кластеризации, хотя ряд алгоритмов, например Birch и Ward, значительно повышают точность по ряду метрик. Наиболее заметно улучшение для Birch, который консистентно увеличивает результаты по всем метрикам, достигая прироста в 15-20%. Приведем примеры собранных метрик для увеличенного среза файлов (рис. 3.22).

Заметно, что во многом сохраняется схождение к оптимуму, хотя для отдельных алгоритмов (например, Single Linkage на втором графике) оптимум различается при разном размере файлов. В среднем алгоритмы, работающие с двойным срезом файлов, демонстрируют лучшие результаты, что видно на этих

графиках, хотя и не отражается так значительно при многократном повторении кластерного анализа (в среднем увеличение незначительно).

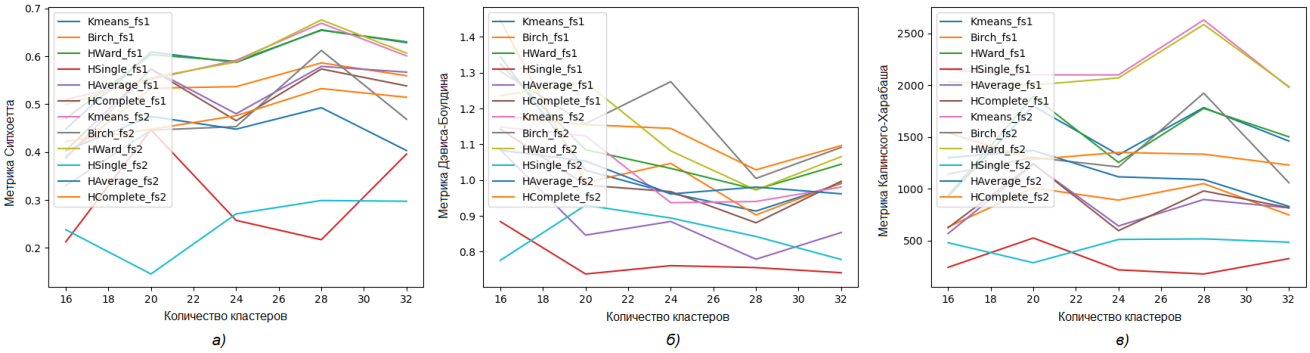


Рисунок 3.22 — Собранные метрики для увеличенного среза файлов:
а) Силхоетта, б) Девиса-Боулдина, в) Калинского-Харбаша

Для визуализации кластерного анализа можно применять технику PCA (Principal Component Analysis) – метод главных компонент (рис. 3.23). Применим данную технику для сжатия всех признаков к 2 признакам и рассмотрим их объясняемую Variance. Примечательно, что значение объясняемой Variance в среднем составляет около 17-19% для обоих компонент (первая компонента по определению обладает большей объясняемой Variance). Особенно это значимо, если взглянуть на визуализации кластеризаций (в графиках ниже число кластеров равно 8) [211].

Примечательно, что на каждом изображении присутствует 16000 точек (таким был размер среза файла). Точки расположены чрезвычайно кучно и это можно также связать и с высокой объясняемой Variance для первых компонент. В двумерной проекции, построенной с помощью PCA точки много точек расположено близко друг к другу – два признака хорошо дифференцируют данные. В ходе работы были проведены извлечение и предобработка исходных данных журналов событий безопасности. Рассмотрены релевантные алгоритмы иерархического кластерного анализа, подобраны метрики для сравнения их эффективности. В ходе проведенных экспериментальных исследований получены следующие результаты:

1. Методы Agglomerative Clustering обладают высокой эффективностью по всем метрикам, стоит подбирать необходимый Linkage в зависимости от выбора максимизируемой метрики.

2. Оптимум числа кластеров близок к 32 для большинства алгоритмов, причем оптимум един для рассмотренных алгоритмов кластеризации в подавляющем большинстве случаев.
3. Некоторые алгоритмы кластеризации чувствительны к размеру входных данных. Так, BIRCH алгоритм может значительно повысить качество при большом числе данных.
4. Применение PCA демонстрирует высокую плотность рассматриваемых событий в проекции на две главные компоненты. Чтобы более подробно изучить приложения Feature Selection в данном случае можно рассмотреть иерархический метод Feature Agglomeration.

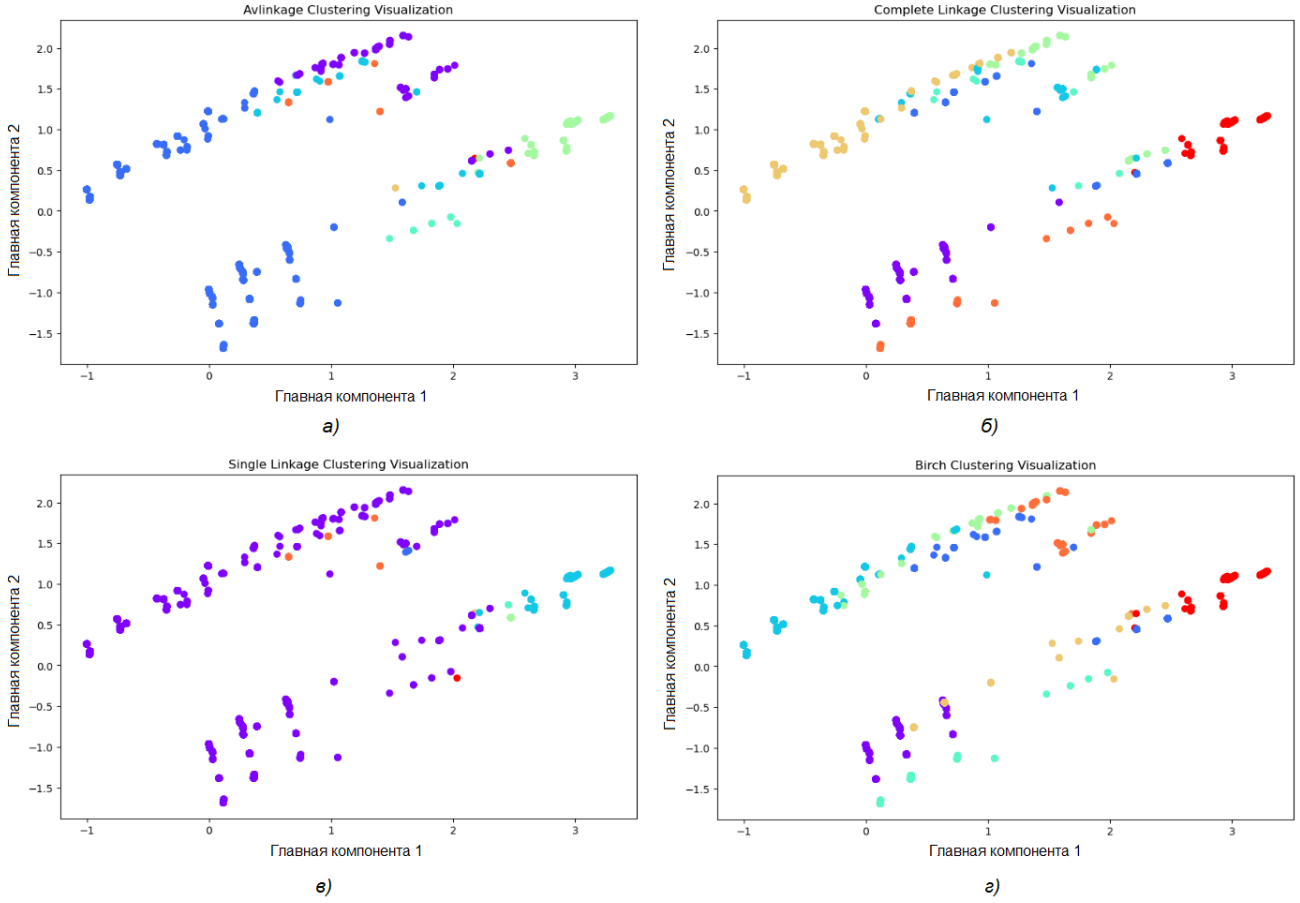


Рисунок 3.23 — Визуализация методов кластеризации

3.5.3 Оценка количественного значения риска на основе анализа событий, поступающих от агентов

Проведены экспериментальные исследования на основе данных, полученных с онлайн-системы РТУ МИРЭА. Определены значения уровней риска нарушения информационной безопасности для каждого рассматриваемого агента в заданные интервалы времени. Ниже, на графиках приведен обобщенный за день уровень риска по каждому агенту. Далее на рисунках по оси Y указаны уровень риска от 0 до 10, а по оси X – даты возникновения всплесков.

Агент 1 оценивает количество событий удаления пользователей и объектов. Если текущее количество удалений превышает среднее значение, то риск повышается в шкале от 1 до 10, где 10 – это верхняя граница разрешенного максимума. Если операций удаления меньше среднего, то риск равен 0. На рисунках 3.24 и 3.25 приведены результаты оценивания по экспериментальным данным с временными интервалами 10 минут и один месяц соответственно.

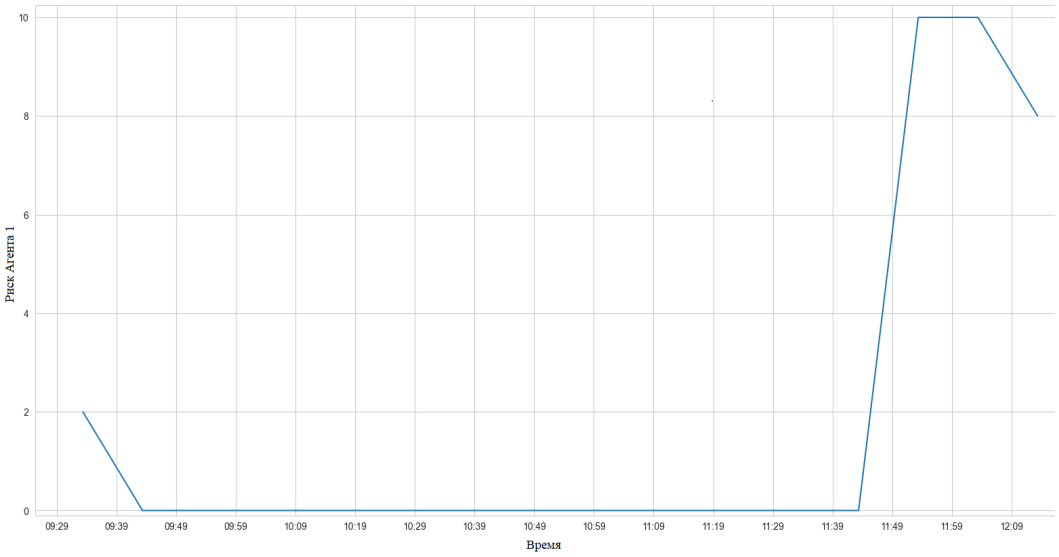


Рисунок 3.24 — Пример возвращаемого уровня риска Агентом 1, с заданным интервалом в 10 минут

Агент 2 оценивает количество неудавшихся попыток входа, при этом выдает уровень риска (от 0 до 10), сравнивая текущие значения со средними значениями таких попыток за определенный период времени. Пороговые значения для определения уровня риска настраиваются. Выдает уровень риска в зависимости от количества неудачных аутентификаций. На рисунках 3.26 и

3.27 приведены результаты для Агента 2 с интервалами 10 минут и один месяц соответственно.

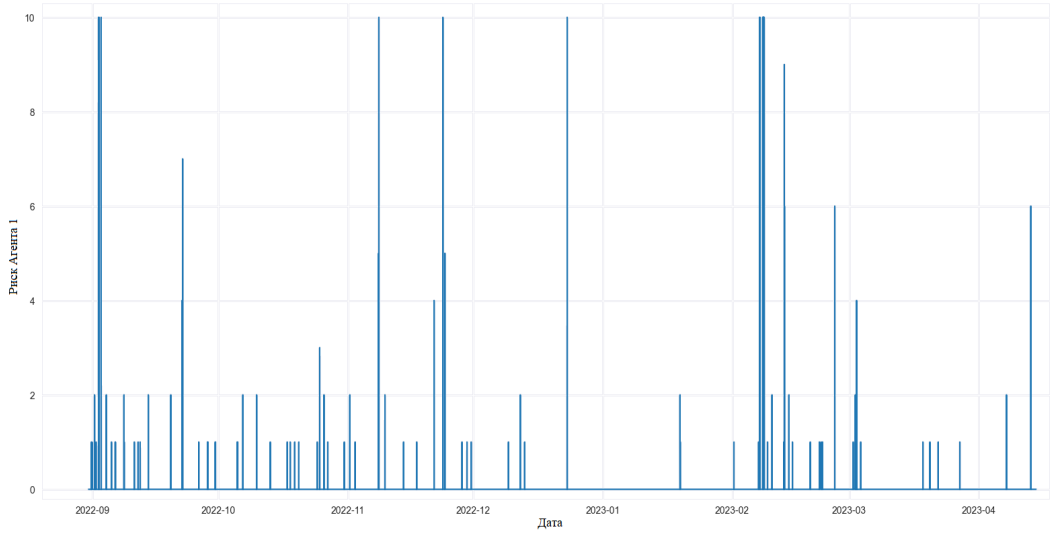


Рисунок 3.25 — Пример возвращаемого уровня риска Агентом 1, с заданным интервалом в один месяц

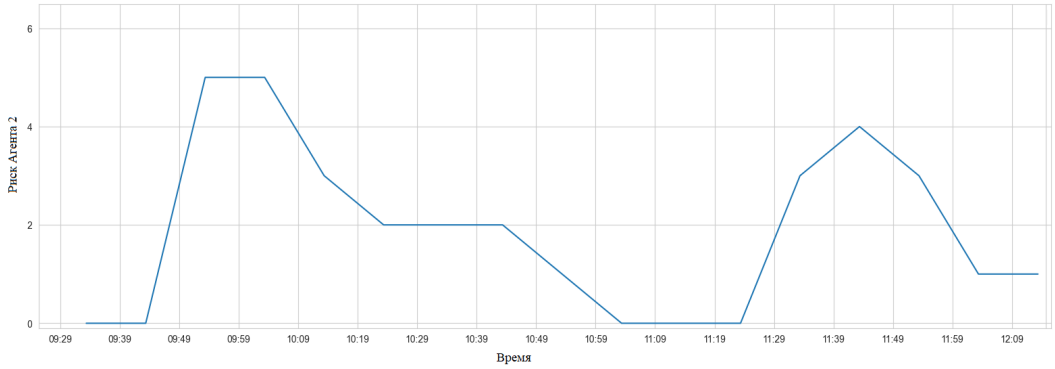


Рисунок 3.26 — Пример возвращаемого уровня риска Агентом 2, с заданным интервалом в 10 минут

Агент 3 оценивает количеством пользователей, одновременно обращающихся к ресурсу, возвращает риск при превышении частоты обращения заданного порога. В агенте задан словарь, содержащий имя сервиса, 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. На рисунках 3.28 и 3.29 приведен риск Агента 3 с интервалами 10 минут и один месяц соответственно.

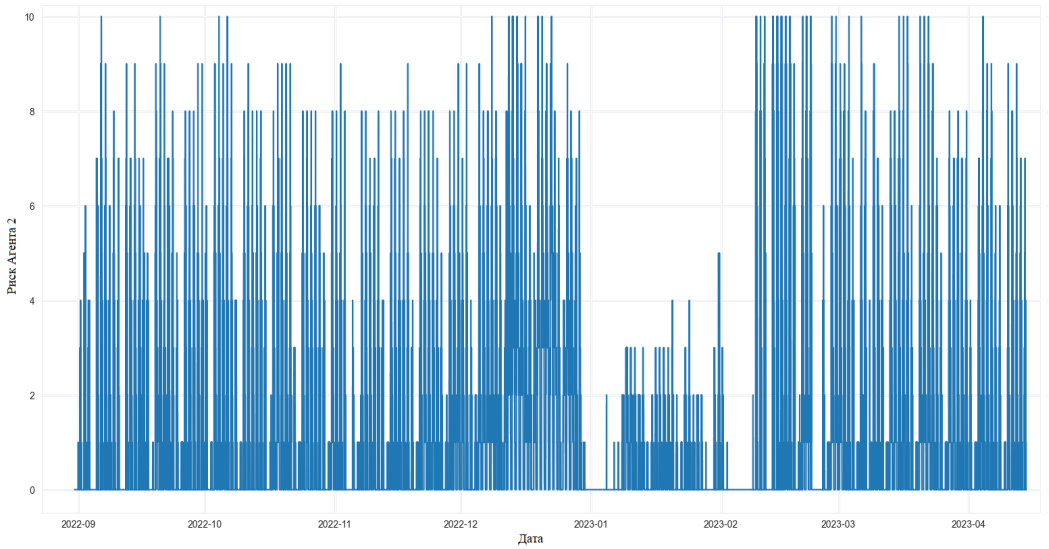


Рисунок 3.27 — Пример возвращаемого уровня риска Агентом 2, с заданным интервалом в один месяц

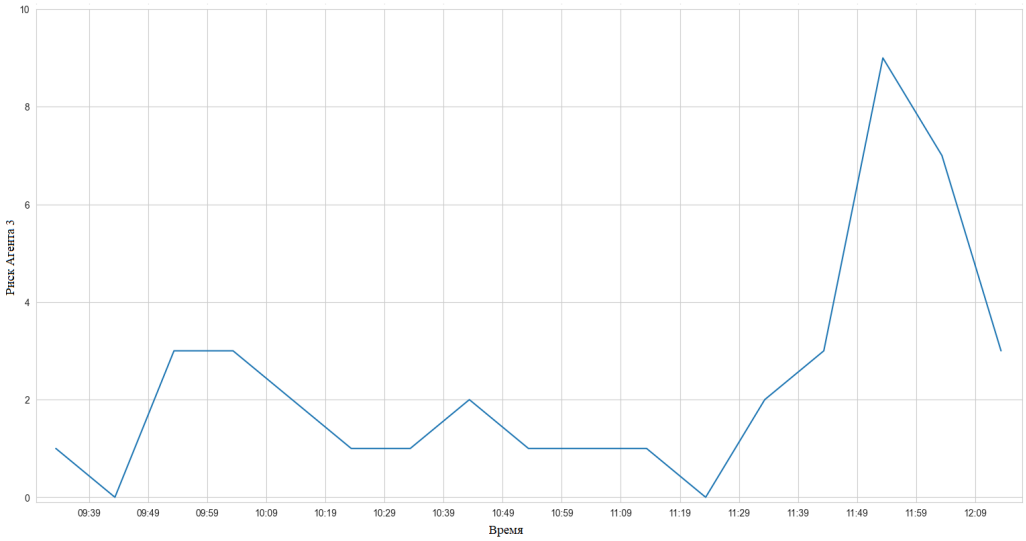


Рисунок 3.28 — Пример возвращаемого уровня риска Агентом 3, с заданным интервалом в 10 минут

Агент 4 оценивает количество активных пользователей. В зависимости от количества пользователей высчитывается риск от 0 до 10. Нижняя и верхняя границы определяются задаваемой конфигурацией. Учитываются только изменения под конец 10-минутного периода. Время сессии одного пользователя – 30 минут. На рисунках 3.30 и 3.31 приведен риск Агента 4 с интервалами 10 минут и один месяц соответственно.

Согласно разработанному методу, показания агентов 1–4 из шкалы $1 \ldots 10$ переводятся в нечеткий вид со значениями риска "низкий", "средний", "высокий". Обрабатываются текущие показания агентов и агрегируются в единое

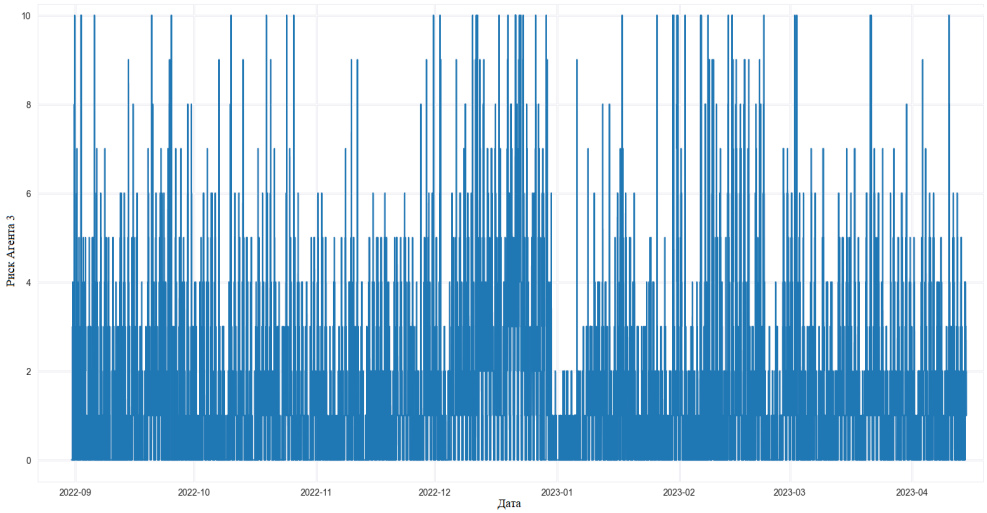


Рисунок 3.29 — Пример возвращаемого уровня риска Агентом 3, с заданным интервалом в один месяц

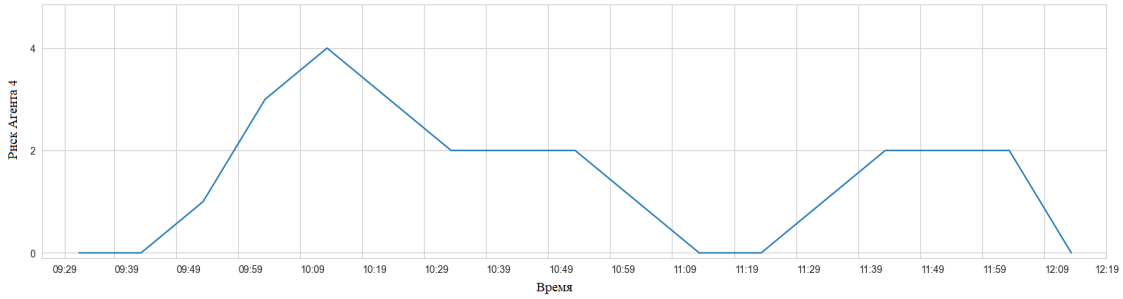


Рисунок 3.30 — Пример возвращаемого уровня риска Агентом 4, с заданным интервалом в 10 минут

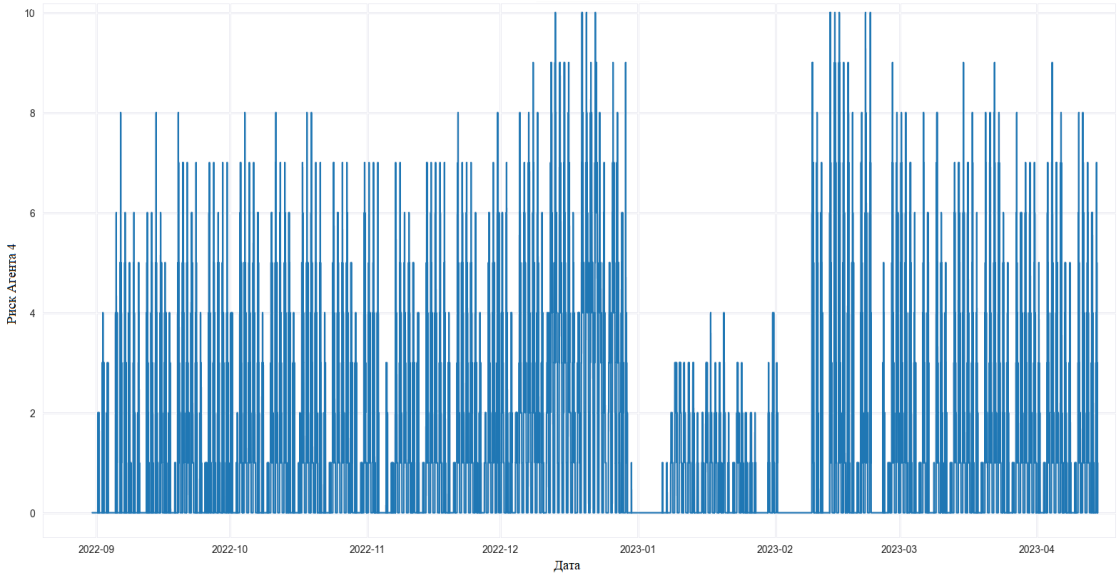


Рисунок 3.31 — Пример возвращаемого уровня риска Агентом 4, с заданным интервалом в один месяц

число – общий уровень риска, приведенный на рис. 3.33 за временной интервал по 10 минут и рис. 3.32 – за один месяц.

Полученные результаты представляют собой количественное значение оценки риска реализации угроз информационной безопасности, основанный на анализе событий передаваемых системой агентов, которое может быть использовано в качестве дополнительного атрибута в процессе управления доступа с целью принятия решения о предоставлении или отказе в предоставлении доступа пользователю к запрашиваемым информационным ресурсам ОВС, базирующимся на распределенных информационных системах.

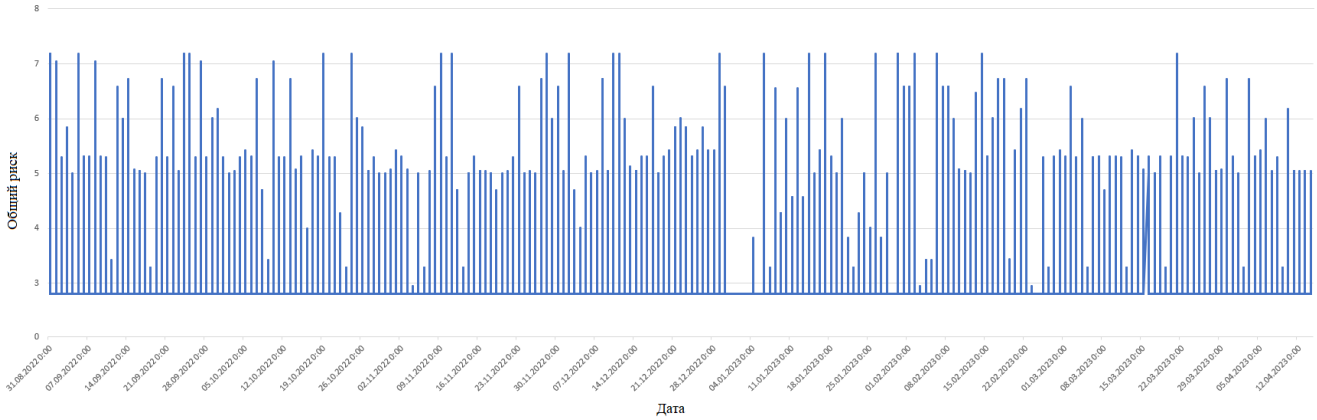


Рисунок 3.32 — Общий уровень риска согласно показаниям Агентов 1–4, с заданным интервалом один месяц

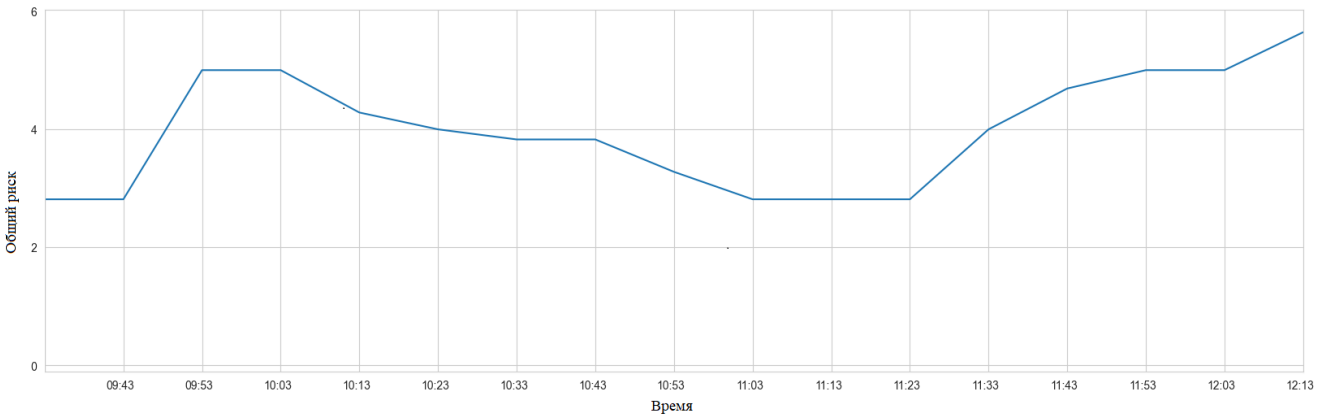


Рисунок 3.33 — Общий уровень риска согласно показаниям Агентов 1–4, с заданным интервалом 10 минут

3.6 Выводы по третьей главе

В третьей главе осуществлен анализ существующих решений и подходов к риск-ориентированному управлению доступом, рассмотрены основные понятия риск-ориентированного подхода, проведен сравнительный анализ адаптивных и динамических моделей управления доступом, обосновано применение адаптивной модели управления доступом для реализации риск-ориентированного подхода.

Для внедрения предлагаемой риск-ориентированной атрибутивной модели управления доступом проведено исследование построения систем управления доступом в организациях высшего образования, определены используемые атрибуты безопасности управления доступом в образовательных вычислительных сервисах организаций высшего образования. На основе полученных атрибутов и рассмотренных моделей управления доступом разработан метод количественной оценки рисков реализации угроз информационной безопасности.

Разработанный метод количественной оценки значения риска информационной безопасности основан на оперативном анализе событий, создаваемых агентами распределенной информационной системы, посредством математического аппарата нечеткой логики. Разработанная система агентов сбора информации отличается учетом возможных действий и событий как пользователя, так и объектов в образовательных вычислительных сервисах 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 решающего правила в процессе предоставления доступа пользователя к ресурсам.

Глава 4. Метод непрерывной аутентификации пользователей на основе их психологических реакций

В главе представлен метод непрерывной аутентификации пользователей распределенных информационных систем, основанный на использовании психологических реакций пользователей, которые могут быть измерены при работе с интерфейсами и взаимодействии с объектами данных систем. Применение в процессе аутентификации оцениваемых значений реакций пользователей обосновано посредством проведенного анализа и апробировано на тестовой выборке, сформированной на основе психологических реакций на различные действия студентов и преподавателей высшего учебного заведения. Приведено применение разработанного метода непрерывной аутентификации на основе психологических реакций пользователей в системах управления доступом.

4.1 Обзор способов и методов непрерывной аутентификации

Под аутентификацией согласно ГОСТ Р 70262.1-2022 [212] понимаются действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации. В зависимости от аутентификационной информации методы аутентификации принято разделять на:

- аутентификацию на основе знаний;
- аутентификацию на основе владения;
- биометрическая аутентификация: биологическая (физиологическая) и поведенческая.

Кроме того аутентификация может быть однофакторной (использование только одного метода аутентификации) или многофакторной (использование нескольких методов аутентификации разного типа).

Аутентификация на основе знаний – способ, основанный на использовании информации, известной только пользователю и системе управления доступом. В качестве идентификационной информации для аутентификации выступает,

как правило, последовательность цифр или букв. Информация может быть текстовой (PIN-код (Personal Identification Number), пароль из символов, цифр и букв) или графической (замок-шаблон) [213]. Основным преимуществом способов аутентификации на основе знаний является простота в использовании, настройке. К существующим недостаткам относится низкий уровень обеспечения безопасности, поскольку любой пользователь, обладающий паролем, может пройти аутентификацию, на что указывает ряд исследований [214—217]. Несмотря на озвученный недостаток аутентификация на основе знаний продолжает использоваться для проверки личности пользователя в качестве одного из факторов в многофакторных методах аутентификации. Для оценки стойкости паролей разработаны различные метрики, направленные на повышение безопасности [218].

Аутентификация на основе владения основана на физическом контроле какого-либо объекта, например смарт-карты или токена. Преимущества способа заключаются в высоком уровне безопасности, возможна организация физического и логического доступа. К недостаткам относятся: необходимость присутствия в системе управления доступом специального оборудования или программного обеспечения для обслуживания и использования токенов или смарт-карт, а также возможность утери или повреждения носителя. В работах [219; 220] рассмотрены методы биометрической аутентификации на основе биологических характеристик человека: радужная оболочка и сетчатка глаз, отпечатки и сосудистые карты пальцев, голос, лицо, походка, электрокардиограмма (ЭКГ) [221] и электроэнцефалограмма (ЭЭГ). Процедура аутентификации основана на обучении алгоритмов машинного обучения распознавать пользователей за счет полученных сигналов от сканера ЭЭГ и их предобработке. В работе описаны алгоритмы классификации: k-ближайших соседей и опорных векторов, а также модели глубокого обучения: сверточная нейронная сеть, рекуррентная нейронная сеть и долгая краткосрочная память. Метод аутентификации на основе энцефалограммы наиболее перспективен, поскольку в отличие от сгенерированных человеком паролей, обладающим энтропией в 20-22 бита, данный способ характеризуется энтропией в 83 бита, что положительно скажется на стойкости процедуры аутентификации.

В [222] авторы также разделяют биометрические показатели аутентификации на биологические и поведенческие, указывая на низкую стойкость методов аутентификации на основе знания/владения. Аутентификация на основе пове-

денческой биометрии анализирует уникальные поведенческие характеристики или привычки пользователя. Например, скорость набора текста на клавиатуре, амплитуда и направления движения курсора, движения пальцев по сенсорному экрану [223; 224]. Отмечается, что аутентификация на основе поведенческой биометрии более удобна и проста для пользователей, чем аутентификация на основе физиологической биометрии. Данный факт объясняется тем, что поведенческие признаки являются менее конфиденциальной информацией, по сравнению с неизмененными чертами тела, и пользователям проще их использовать, в том числе возможны варианты скрытой аутентификации. Например, при использовании мобильных устройств для получения поведенческих признаков, могут быть использованы сенсорный экран, микрофон и акселерометр [225].

В рамках концепции архитектур SIEM-систем в условиях больших данных [226; 227] получает распространение технология анализа поведения пользователей (UBA, User behavior analytics), относящаяся к биометрическим способам аутентификации [228]. Решения UBA изучают шаблоны человеческого поведения, а затем применяют алгоритмы обнаружения аномалий этих шаблонов. Например в [229] представлен пример, в котором злоумышленник в сети компании может использовать украденные учетные данные для незаметного сбора конфиденциальных данных. Такое поведение трудно обнаружить, если оно не вызывает предупреждение о нарушении доступа или утечке данных. Кроме того, атаки типа подмены или имитации, направленные на кражу учетных данных с помощью фишинга или перехвата сеанса пользователя, позволяют злоумышленникам получить доступ к личной информации или осуществлять действия под видом легитимного пользователя.

В ряде работ отмечается уязвимость физиологических биометрических данных, поскольку происходит их передача по каналам связи [230—232]. Кроме того в работах [233; 234] описаны способы подделки физиологической биометрической информации пользователя. Поскольку физиологические биометрические данные изменить невозможно, то они крайне чувствительны к компрометации и если такая информация будет получена злоумышленником, аутентификация на основе физиологических биометрических данных будет постоянно небезопасной, в связи с чем, многие пользователи отказываются использовать свои физиологические биометрические данные для аутентифика-

ции, что снижает эффективность биометрической аутентификации на основе физиологических признаков.

Указанных недостатков лишена поведенческая биометрия, которая получает характерные признаки из взаимодействия пользователя с системой управления доступом и защищаемой системой, например, ввод данных пользователем, переход по интерфейсам. В результате сбора признаков формируется цифровой шаблон поведения пользователя. В работе [235] отмечаются преимущества использования поведенческой биометрии относительно физиологической биометрической аутентификации. Кроме того, собранные поведенческие данные не нуждаются в какой-либо конкретной аппаратной архитектуре, что, в свою очередь, позволяет уменьшить сложность систем проверки и затрат на их реализацию. Исходя из проведенного анализа можно сделать вывод о необходимости использования биометрической аутентификации пользователей на основе поведенческих характеристик, что позволит повысить эффективность систем управления доступом.

Двухфакторная (многофакторная) аутентификация объединяет в себе два или более метода аутентификации с целью повышения уровня безопасности. Например, система управления доступом может запросить у пользователя несколько разных или однотипных аутентифицирующих данных: отпечаток пальца, радужная оболочка глаза, аудиоданные или секретные знания в виде пароля и другой идентификационной (аутентификационной) информации. Преимущества такого подхода заключаются в усилении безопасности за счет комбинирования двух и более методов аутентификации. К недостаткам относятся: дополнительные затраты на внедрение и обучение пользователей, возможные трудности в случае утери доступа к одному из факторов, повышенная сложность внедрения и управления, неудобство использования системы управления доступом. Несмотря на повышенный уровень безопасности, предоставляемый многофакторной аутентификацией, злоумышленник может подделать программный или аппаратный токен, и в то же время ввести украденную секретную или биометрическую информацию, основанную на знаниях.

Одной из перспективных методик поведенческой биометрии является сбор информации о динамике нажатия клавиш, иными словами изучение ритма ввода пользователя. Несколько исследований показали, что у пользователей есть определенный шаблон набора текста [236], который не сильно меняется даже при преднамеренных внешних раздражителях. Следовательно, это делает

динамику нажатий клавиш очень хорошим кандидатом для биометрической аутентификации в системах КД. Существует несколько комплексных обзорных работ, посвященных динамике нажатий клавиш [237]. Более того, процесс нажатия клавиш в основном зависит от времени нажатия и отпускания клавиш. Поведение при нажатии клавиш для пользователей может меняться в зависимости от раскладки клавиатуры [238] и модели поведения пользователя. Таким образом, возможно сделать вывод о сохранении многих поведенческих паттернов пользователей на разных устройствах, что делает данный способ пригодным для применения в системах управления доступом [239].

Следует отметить, что динамика нажатия клавиш подразделяется на анализ статического и динамического текстов. Анализ информации о нажатиях клавиш при наборе динамического текста позволяет осуществлять непрерывную или периодическую аутентификацию пользователя. Чтобы учесть изменение поведения пользователей с течением времени, были изучены различные подходы к машинному обучению для достижения цели проверки. Как и в случае с динамикой голоса и нажатий клавиш, было выявлено несколько угроз безопасности, которые, как правило, дают гораздо меньшую точность. В работе указано, что динамика нажатия клавиш на стационарном компьютере может быть использована для классификации активности на доброжелательную и враждебную. С использованием предложенного набора из 14 характеристик достигаются высокие показатели точности (от 93% до 97%) и низкие значения ошибок 1 и 2 рода (от 3% до 8%) при классификации образцов текста разного размера. Анализировались данные от 102 пользователей для доброжелательных активностей и от 103 пользователей для враждебных активностей, записано более 1,9 миллиона событий нажатия клавиш в общей сложности. Эксперименты показывают, что характер набора текста может раскрыть тип активности пользователя, тем самым предоставляя важные индикаторы уровня угрозы для системы [240].

Одна из новаторских работ в области анализа динамического текста была выполнена Гунетти и Пикарди [241]. Разработанная стратегия анализировала динамический текст для целей аутентификации, используя пользовательский интерфейс, в котором пользователь должен ввести любой текст объемом около 700–900 слов. Ритм набора текста изучается на основе информации о времени отдельных нажатий клавиш и сравнения n-графиков последовательных вводов текста. Если пользователь аутентифицирован, выдается запрос на ввод

пароля. Для аутентификации используется другой статистический метод, основанный на векторах взаимных признаков, который был предложен в работе [242]. На этапе обучения периодически собираются признаки нажатия клавиш аутентифицированного пользователя, и результаты сохраняются в базе данных. В дальнейшем, при аутентификации пользователя сравниваются характеристики нажатия клавиши с рассчитанными ранее и сохраненными векторами признаков и искажений. Были проведены эксперименты на основе множества паролей, введенных пользователем. Эта работа была сосредоточена на коротких фиксированных текстах и не учитывала возможность изменения поведения пользователя со временем.

В работе [243] описан подход, включающий получение характеристик действий пользователя (логин пользователя, движение мыши, среднее время между нажатием клавиши мыши и началом движения курсора, скорость набора текста и др.). Подобные исследования интересны, но носят ограниченный характер – для многопользовательских систем получение, передача, хранение и обработка данных вычислительно очень затратны. Кроме того, использование манипулятора мыши для анализа реакций сложно реализуемо – задержки сильно зависят от производителя и от поверхности, на которой в данный момент работает пользователь. Кроме того, веб-интерфейсы подразумевают использование их на разных устройствах, в том числе с сенсорными экранами.

Современные психологические исследования [244; 245] выявили достоверность данных по исследованию реакций, полученных с использованием веб-интерфейсов. Эти результаты дают основание для разработки метода непрерывной аутентификации пользователей информационной системы, использующего в качестве дополнительного идентификатора пользователя время реакций при работе с элементами интерфейса (время реакции – период времени от внешнего стимула до соответствующей реакцией индивидуума; оценка времени реакции – это один из важных методов изучения скорости обработки информации центральной нервной системой человека и скоординированной реакции периферических движений).

В работе [246] предлагается подход к построению системы анализа поведения пользователей, базирующейся на предлагаемой модели базы данных, для выявления аномального поведения пользователей в корпоративной компьютерной сети. Рассматриваются цели, задачи и варианты реализации систем аналитики поведения пользователей (UBA- и UEBA-систем или User and Entity

Behavior Analytics). Предлагается модель базы данных NoSQL (not only SQL) для анализа поведения пользователей в условиях корпоративной среды с целью выявления инсайдеров. Представляется реализация базы данных NoSQL для системы анализа поведения пользователей с использованием OrientDB, а также примеры ее использования. На основе предложенных правил разрабатывается эвристический алгоритм выявления аномалий и определения инсайдеров. Цели выполнения работы направлены на противодействие инсайдерам, однако методы анализа поведения пользователей могут быть применены для аутентификации в системах управления доступом высшего учебного заведения.

Проанализированные работы позволяют сделать вывод о перспективности применения поведенческих способов биометрии для внедрения в систему управления доступом высшего учебного заведения. К достоинствам данного способа относятся: доказанная точность выполнения процедуры аутентификации пользователей на основе поведенческих характеристик; постоянное присутствие "секрета" у пользователя, поскольку "секрет" – характеристика поведения конкретного человека; сложность подделки поведения пользователя, стойкость к атакам "человек посередине", простота реализации относительно физиологической биометрии.

Традиционные методы однофакторной аутентификации (SFA, Single-Factor Authentication), такие как текстовые пароли [247] или персональный идентификационный номер (PIN) [248], предназначены для проверки личности пользователя [249], но обладают рядом недостатков, в первую очередь определяемых низкой стойкостью против атак перебором. Рост вычислительных возможностей современного информационного оборудования и его доступность увеличивают количество атак, осуществляемых на информационные системы и сервисы. Оценки рисков SFA выявили несколько уязвимостей к атакам на безопасность, таким как брутфорс [250], словарные атаки [251], вредоносные программы [252], программы-кейлогеры [253] и другие [254]. В качестве решения многократная аутентификация (MFA, Multi-Factor Authentication) создает несколько уровней безопасности в дополнение к единичным входам [255].

Приложения и службы обычно имеют единую точку аутентификации (SSO, Single Sign-On), что представляет собой, метод аутентификации, при котором пользователь может использовать одни и те же учетные данные для доступа к различным системам или приложениям, не повторяя ввод логина и пароля. Это упрощает процесс аутентификации и предотвращает необходимость

повторного ввода учетных данных при доступе к разным ресурсам. SSO часто используется в корпоративных средах, где сотрудники имеют доступ к различным сервисам и приложениям, например в распределенных информационных система, в частности в системах дистанционного образования высшего учебного заведения. С этого момента система доверяет тому, что пользователи являются легитимными пользователями, которые наделяются соответствующими правами и привилегиями. Однако вместе с удобством использования и другими преимуществами SSO обладает рядом существенных недостатков, из которых наиболее значимыми в области безопасности являются следующие [256]:

1. пользователи могут осуществлять доступ в систему вне организации, что приводит к разработке сложной структуры каталогов, которые должны быть интегрированы с SSO;
2. неуправляемое и несанкционированное использование приложений SaaS (Software as a Service) представляет собой основные проблемы при внедрении SSO;
3. для повышения производительности и обеспечения безопасности информации SSO должен сочетаться с двухфакторной аутентификацией;
4. компрометация, перехват сессии или физического доступа к персональному компьютеру с активной сессией приводит к рискам для всей информации, присутствующей в системе.

Иногда эти приложения и сервисы включают второй фактор аутентификации, отправляя пользователю одноразовый пароль (OTP, One Time Password) на смартфон или используя аппаратный токен для выполнения первоначального входа в систему или выполнения действий с высоким риском [257]. Однако атака с перехватом сеанса может сделать эти дополнительные механизмы безопасности недостаточными, вследствие чего, они должны быть дополнены системами непрерывной аутентификации для обеспечения желаемых уровней безопасности [258]. На рисунке 4.1 представлен пример реализации перехвата сеанса в системах с единой точкой аутентификации.

Применение различных методов аутентификации позволяет осуществлять идентификацию и проверку подлинности пользователей для осуществления доступа к запрашиваемым ресурсам информационной сети. При этом, возросшее количество инцидентов информационной безопасности, обусловленных применением методов социальной инженерии, внедрение вредоносного программного обеспечения, а также безответственность сотрудников, связанная с предо-

ставлением своей идентификационной и аутентификационной информации, не позволяет в полной мере обеспечить защищенность как самой распределенной информационной системы, так и защищаемой в ней информации и различных ресурсов. Указанные особенности позволяют сделать вывод о необходимости использования дополнительного фактора аутентификации, основанного на времени реакций пользователя при работе с элементами интерфейса, в системах управления доступом метод для непрерывного отслеживания в режиме реального времени психологических характеристик пользователя с последующей аутентификацией.

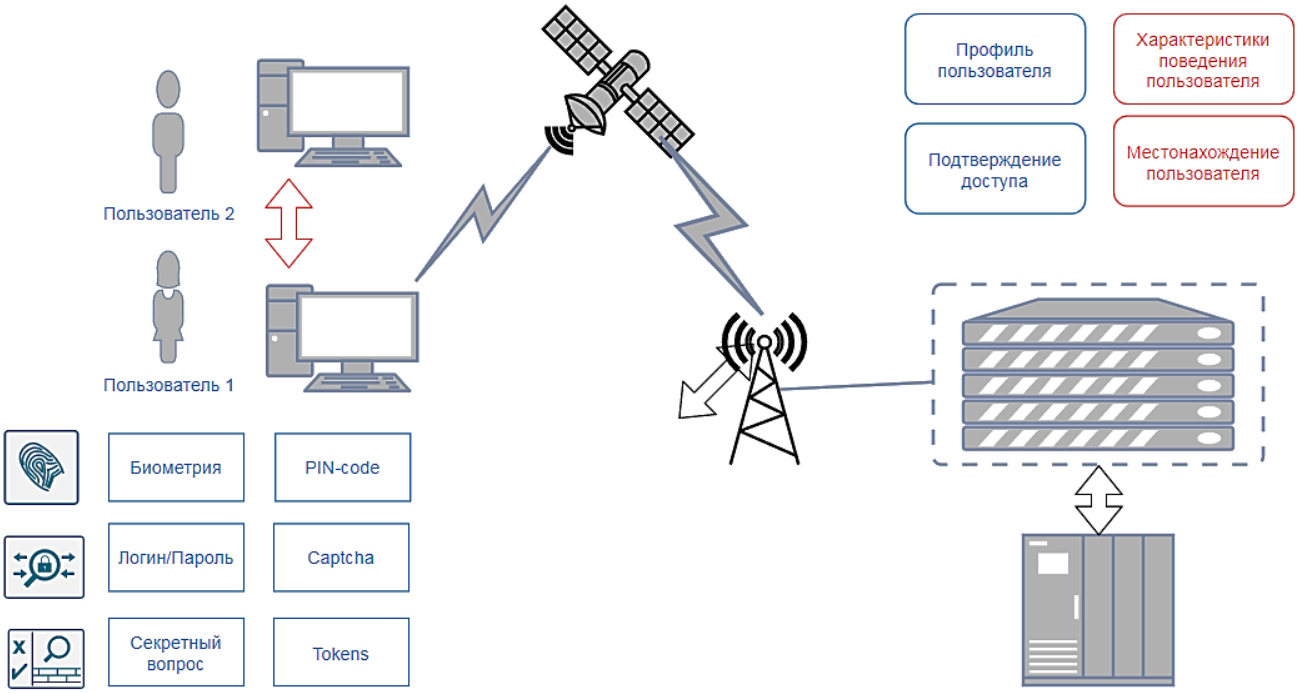


Рисунок 4.1 — Пример системы управления доступом

В работе [259] предложен метод непрерывной аутентификации пользователя дистанционной системы образования, в частности системы контроля пользователя при проведении экзаменов. Метод предполагает обучение модели нейронной сети для распознавания пользователя по изображению, получаемому с камеры, с последующей автоматической идентификацией пользователя. Система управления доступом прерывает сессию пользователя в следующих случаях: при наличии в кадре постороннего лица или нескольких лиц, а также при превышении времени отсутствия лица в кадре.

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. В случае обнаружения факта предоставления доступа с нарушением установленных правил осуществляется блокирование доступа и реализуются соответствующие меры защиты [260]. Основным преимуществом непрерывной аутентификации перед традиционными методами является предоставление дополнительного уровня защиты методов управления и предоставления доступа. Кроме того, в работах [261—263] отмечаются следующие достоинства:

- защита от взлома: методы непрерывной аутентификации позволяют минимизировать вероятность возникновения атак имитации. Статическая схема аутентификации позволяет идентифицировать пользователя только в начале сеанса. Таким образом, если атака имитации происходит позже, злоумышленник унаследует привилегии законного пользователя. Напротив, применение схемы непрерывной аутентификации позволяет верифицировать личность пользователя на каждом этапе [264];
- удобство использования: по сравнению с традиционной схемой аутентификации, непрерывная аутентификация предоставляет "бесшовный" (невидимый для пользователя) доступ к запрашиваемым ресурсам и информации (без осознания пользователем того, что происходит процесс аутентификации).

В работе [265] также отмечается, что непрерывная аутентификация пользователя является неотъемлемым требованием для проверки того, что пользователи являются теми, за кого они себя выдают, на постоянной основе. 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. Непрерывность использования пользователем системы делает поведенческие признаки естественным способом для осуществления непрерывной аутентификации без отвлечения для пользователей.

Проведенный анализ методов непрерывной аутентификации позволяет сделать вывод о том, что метод непрерывной аутентификации на основе поведенческой биометрии является наиболее актуальным для подходом к аутентификации пользователей в образовательных вычислительных сервисах организаций высшего образования (вузах), базирующихся на распределенных

информационных системах. Сбор аутентифицирующих признаков осуществляется посредством невидимого для пользователя анализа поведения, основанного на взаимодействий пользователя с ресурсами информационной системы системой и позволяет сформировать профиль пользователя (совокупность значений аутентифицирующих признаков) с последующей реализацией процедуры "тихой" аутентификации. В случае наличия значительных отклонений в анализируемых значениях аутентифицирующих признаков пользователя от эталонных пользователей, системой управления доступом формируется запрос на осуществление традиционной аутентификации пользователя с блокированием его текущего сеанса. В случае непрохождения пользователем аутентификации осуществляется выполнение защитных мер: сброс сессии, блокировка пользователя, оповещение администратора безопасности системы и др.

Для дальнейшего анализа возможности применения разработанного метода непрерывной аутентификации, основанной на психологических реакциях пользователя, необходимо провести экспериментальную оценку количественных значений аутентифицирующих признаков (времени реакции пользователей) и возможности практической реализации предложенного метода аутентификации пользователей в системах управления доступом.

4.2 Экспериментальные исследования психологических реакций пользователей

Исследования проводились с помощью цифровой платформы DigitalPsyTools [266]. Система является одновременно цифровой платформой с веб-интерфейсом и инструментом психодиагностики, используемым для популяционных исследований в системе образования. В вычислительной системе в элементы интерфейса встроены платформонезависимые функции оценки когнитивных реакций [267].

Между приложением внешнего стимула и соответствующей двигательной реакцией на стимул существует определенный период времени, называемый временем реакции (ВР). Оценка этого времени – один из важных методов изучения скорости обработки когнитивной информации человеком и скоординированной реакции периферических движений. Время реакции определяется как интервал

времени между предъявлением стимула и появлением у испытуемого соответствующей произвольной реакции. На время реакции влияют многие факторы, такие как пол, возраст, физическое состояние, утомляемость, состояние здоровья и т. п. Увеличенное время реакции означает снижение производительности. Время показа является временем от начала показа страницы, на которой можно сделать действие, до времени на момент, когда пользователь осуществил какое-либо действие в интерфейсе. Иными словами, ВР – это время от появления стимула до нажатия кнопки (на основании психологических терминов).

Время реакции пользователя для конкретного действия можно разделить на:

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

Для анализа использованы реакции 23102 студентов при ответе на 4 вопроса:

1. Основа обучения (выбор из трех вариантов: бюджетная, контрактная, целевая).
2. Вы поступили на ту специальность, которую хотели? (да, нет).
3. Укажите профиль Вашего образования (выбор из четырех вариантов: технический, гуманитарный, естественнонаучный, нет профиля).
4. Программа обучения (выбор из четырех вариантов: бакалавриат, магистратура, специалитет, аспирантура).

Анкета организована в виде веб-интерфейса. После получения архив с опросом на устройстве клиента распаковывается и загружается в браузер. 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". Проводимый опрос включал когнитивные тесты, мотивируя пользователя осуществлять переход на следующую страницу. Данные передавались в платформу после окончания всего опроса, либо после закрытия пользователем веб-страницы. Это гарантировало невмешательство сетей в оценку времени реакции. Также были собраны сведения об используемых операционных системах (рис. 4.2) и браузерах (рис. 4.3).

Гипотеза заключалась в том, что время реакции на разные ответы с разными элементами интерфейса различается. Гипотеза анализа данных о времени

реакции заключалась в возможности определения зависимости в реакциях пользователей при работе с элементами интерфейса при ответе на заданный вопрос, а также в возможности определения индивидуальных психомоторных реакций при работе с интерфейсом.

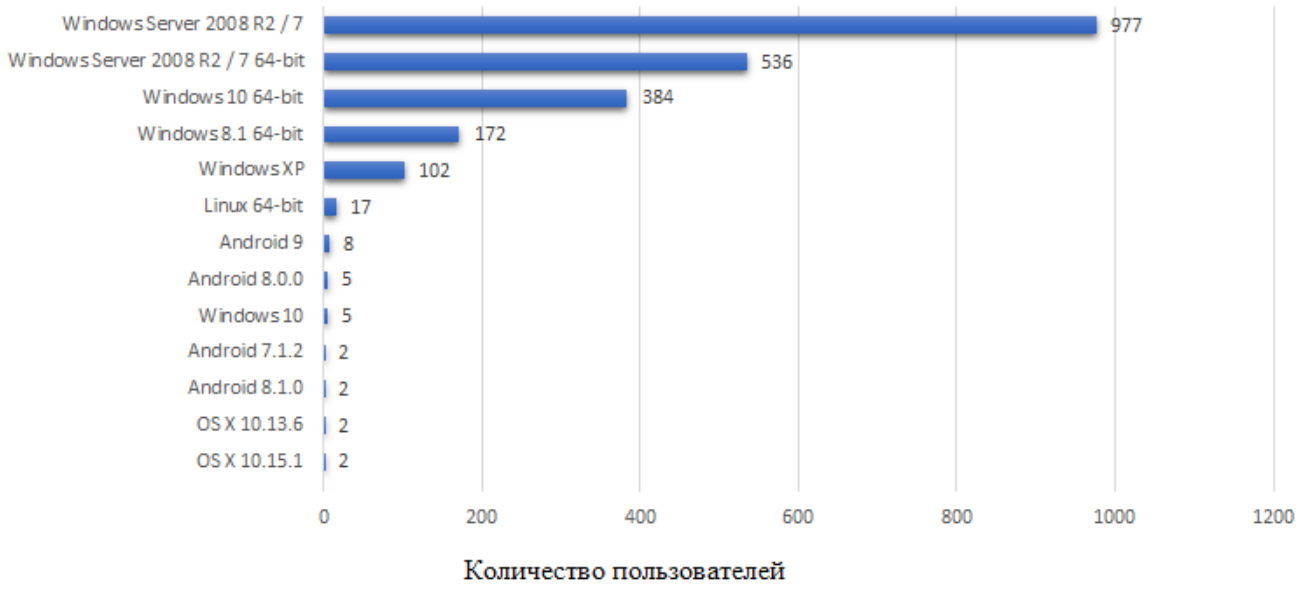


Рисунок 4.2 — Операционные системы, используемые пользователями в опросе

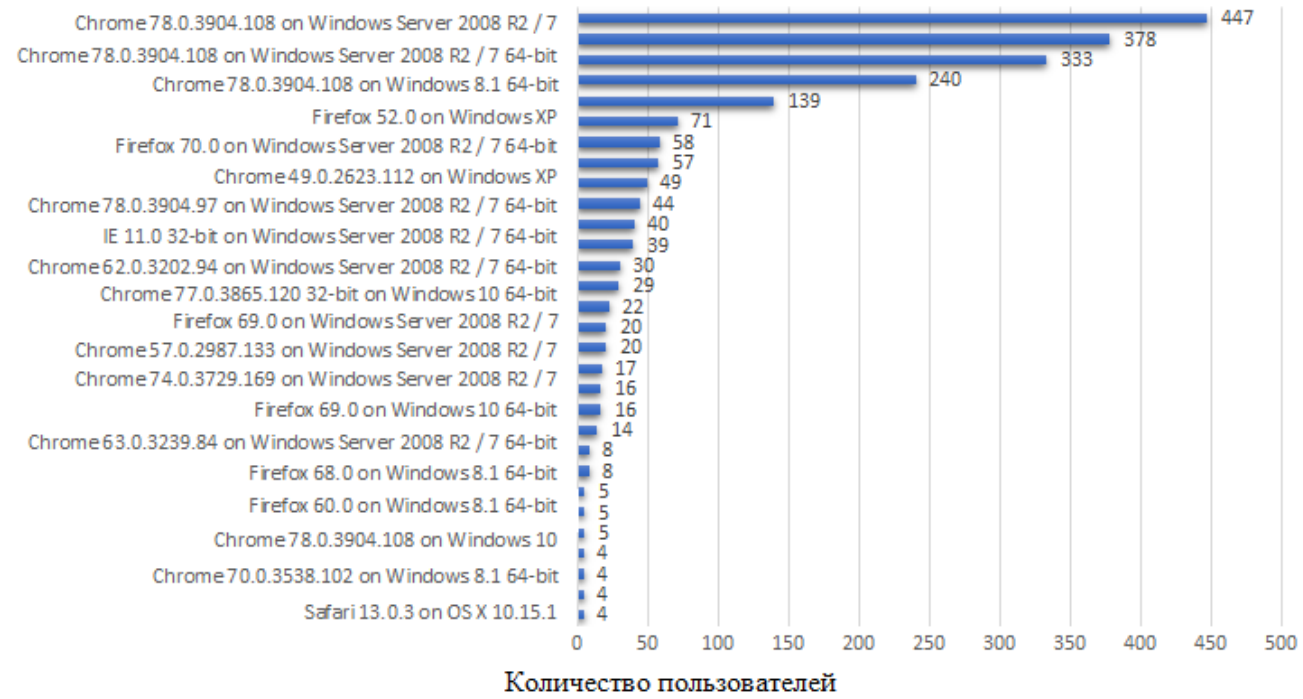


Рисунок 4.3 — Типы и версии браузеров, используемых пользователями в опросе

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, 2 задавались в начале взаимодействия с платформой, вопрос 3 – примерно через час после проведения различных когнитивных тестов. Общее количество респондентов, принявших участие в исследовании, равнялось 23102. Записи, содержащие пустые ответы или время реакции менее 2 секунд, были удалены из набора данных. Остальные 22357 записей были нормализованы, рассчитаны средние значения для каждого вопроса. Был создан новый набор данных, содержащий отклонение от среднего времени реакции для каждого студента по каждому вопросу. Гистограммы экспериментальных данных по каждому вопросу приведены на рисунке 4.4. Анализ гистограмм на основе методов психометрики подтверждает корректность психологического исследования.

Для качественной оценки отклонений времени реакции 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.

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.

Количественный анализ данных отклонений времени реакции показал достоверную корреляцию между отклонениями при ответах на вопросы 1–3. Коэффициенты корреляции представлены в таблице 10. Границы квартилей показаны в таблице 11.

При изучении взаимосвязи отклонений времени реакции для трех вопросов 1–3 был проведен тест Вальда (табл. 12) [268], демонстрирующий значительную линейную взаимосвязь между отклонениями.

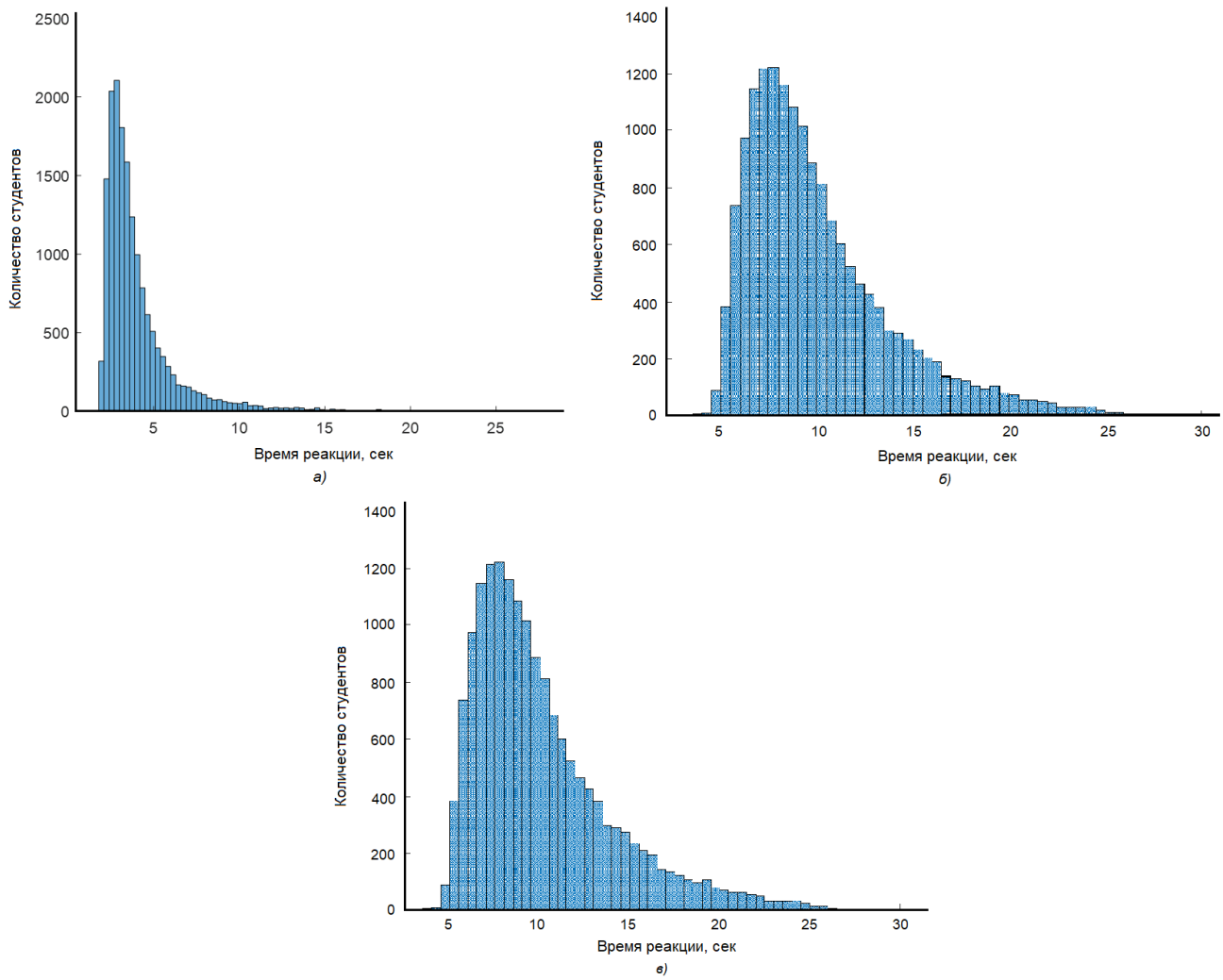


Рисунок 4.4 — Гистограммы экспериментальных данных

Таблица 10 — Коэффициенты корреляции отклонений времени реакции студентов на вопросы 1–3

Вид модели	Статистика Вальда	Критическое значение
R (1, 2)	R (1, 3)	R (2, 3)
0,9298	0,8039	0,8376

В ходе качественного анализа было обнаружено, что 17002 студентов (76%) принадлежали к одному квартилю по всем трем вопросам или не более чем один их квартиль находился рядом с двумя другими.

Из полученных гистограмм и приведенных результатов видно, что, несмотря на изменение времени реакций по всем данным, реакции у большинства пользователей остались неизменными. Для прогнозирования реакций были проверены возможности построения регрессионных зависимостей, проведен тест Вальда. Полученные зависимости демонстрируют допустимость постро-

ения достоверных прогнозных значений реакций пользователей. Это имеет важное значение для рассматриваемой задачи аутентификации пользователей. Например, для проверки того, работает ли с системой верифицированный пользователь, задается секретный вопрос или иной простой вопрос с анкетными данными. Анализ реакции пользователя по ответу на этот вопрос является также персональной информацией. Система управления доступом может сравнить прогнозируемое значение с полученным. 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.

Таблица 11 — 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

Таблица 12 — Статистика теста Вальда

Вид модели	Статистика Вальда	Критическое значение
$D_1 = \beta_0 + \beta_1 \cdot D_2 + \beta_2 \cdot D_3 + \varepsilon$	145 320	4,9915
$D_1 = \beta_0 + \beta_1 \cdot D_2 + \varepsilon$	142 700	3,8415
$D_1 = \beta_0 + \beta_2 \cdot D_3 + \varepsilon$	40 854	3,8415
$D_2 = \beta_0 + \beta_1 \cdot D_1 + \beta_2 \cdot D_3 + \varepsilon$	176 340	4,9915
$D_2 = \beta_0 + \beta_2 \cdot D_3 + \varepsilon$	52 547	3,8415
$D_3 = \beta_0 + \beta_1 \cdot D_1 + \beta_2 \cdot D_2 + \varepsilon$	53 735	4,9915

Уровень значимости равен 0,05, $\beta_0, \beta_1, \beta_2$ – постоянные значения, ε – нормально распределенная ошибка с $\mathbf{M} = 0$, $\sigma^2 = 1$.

Для вычислительной системы предлагается встроить в системы управления доступом и верификации вспомогательные индикаторы использования элементов интерфейса – время реакции при выполнении определенных, заранее зафиксированных действий. Это позволит использовать только персональные реакции, исключив ситуации смены пользователя в одном сеансе работы. Также возможно определение пользователя при использовании чужих паролей для входа в систему. При этом время реакции пользователей в распределенных информационных системах характеризуется наличием задержки, обусловленной наличием сетевого канала взаимодействия и особенностей распространения информационного сигнала. В ходе обоснования применения предложенного аутентификационного признака (время реакции пользователей) проведено исследование влияния задержек, возникающих в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределенных информационных системах

В исследовании [269] отмечается, что веб-технологии, применяемые в распределенных информационных системах, обеспечивают задержку ввода данных и отображения стимулов, но для большинства исследований задержка является приемлемой. Существуют исследования, показывающие сопоставимость точности результатов веб-инструментов и лабораторных исследований [270; 271]. Помимо различий, связанных с технологией, учитывается влияние аппаратной составляющей, различаются и средства ввода и вывода информации [272]. Следует отметить, что отвлекающие факторы (музыка на заднем плане, разговор и т. д.) в целом типичны для веб-приложений, поэтому при тестировании скорости реакции пользователь может измениться, также существуют и отвлечение пользователя на внешние факторы (упавший предмет, поправить одежду и т. д.). В целом, внешние отвлекающие факторы респондента с меньшей вероятностью повлияют на результаты эксперимента, чем задержки, вызванные ответами на приложение [273]. Наличие многозадачности и отвлечение ресурсов на другие процессы, осуществляемые в устройствах [274], также может оказать влияние на оценку. Показано, то что размер экрана, и оптимизация веб-страницы [275] лишь незначительно отвлекают пользователя.

Проведены экспериментальные исследования, направленные на выявление отклонений реакций при использовании различных технологий [245]. В качестве исходных данных были использованы результаты массового опроса учащихся системы образования. В исследовании приняли участие 3786 уча-

щихся 7–9 классов (45,8% мальчиков) общеобразовательных школ Российской Федерации. Возраст участников: 12–18 лет. Для оценки времени реакции были выбраны два вопроса: один из них помещался в начало психологической методики, второй был последним вопросом методики. Оба вопроса подразумевают выбор одного ответа из нескольких предложенных.

Ключевым критерием при выборе вопросов для анализа времени реакции была максимальная простота выбора ответа, то есть предполагается, что респондент должен дать ответ, не задумываясь. Отобранные вопросы формулируются следующим образом. Первый вопрос "Мне нравится проводить время с родителями" предполагает выбор одного из следующих ответов: "никогда", "иногда", "часто", "почти всегда", "всегда". Последний вопрос "Мои друзья мне помогут, если понадобится" предполагает выбор одного из следующих вариантов ответа: "никогда", "иногда", "часто", "почти всегда", "всегда".

Далее для каждой записи подсчитывалось общее время реакции. Время реакции участника R по каждому вопросу определялось по формуле $R = T_e - T_c$, где T_e – время, когда пользователь в последний раз менял свой ответ, T_c – время, когда вопрос впервые появился на экране. На основе операционных систем были сформированы три группы:

– мобильное устройство ("андроид" или "ios");
– устаревший ПК (Windows XP, Windows 7);
– современный ПК (Windows 8.1 и выше).

Исходные данные сортируются в хронологическом порядке, в группы отбираются первые записи из 1000 записей, найденных по заданному критерию. Также была сформирована группа "Все устройства", включающая результаты всех трех групп, в общей сложности содержащая 3000 записей. Для каждой из групп был проведен статистический анализ с целью определения связи между временем ответа при ответе на анкету и категорией используемых устройств [276]. По вопросу 1 статистическая оценка показала, что ответ с мобильных устройств занял у респондентов меньше времени, чем у современных пользователей ПК. При этом пользователям старых ПК, как правило, требовалось еще больше времени на выбор ответа. Полученные результаты приведены в таблице 13.

Полученные количественные значения оценок психологических реакций пользователей позволяют перейти к описанию и практической разработке метода непрерывной аутентификации, основанном на анализе психологических

реакций пользователей, осуществляющих взаимодействие с компонентами образовательных вычислительных сервисов организаций высшего образования, базирующихся на распределенных информационных системах.

Таблица 13 — Оценка времени ответа при ответе на один вопрос

	Мобильное устройство	Устаревший ПК	Современный ПК	Все устройства
Размер выборки	1000	1000	1000	3000
Первый квартиль	3,414	3,899	3,423	3,540
Третий квартиль	7,387	6,644	6,283	6,730
Среднее значение	8,115	7,732	6,877	7,575
Среднеквадратичное отклонение	11,670	12,008	10,480	11,416

4.3 Метод непрерывной аутентификации, основанный на психологических реакциях пользователей в образовательных вычислительных сервисах организаций высшего образования

Предлагается встроить в системы управления доступом и верификации вспомогательные индикаторы использования элементов интерфейса (время реакции) при выполнении определенных, заранее зафиксированных действий. Это позволит использовать только персональные реакции, исключив ситуации смены пользователя в одном сеансе работы. Также возможно определение пользователя при использовании чужих паролей для входа в систему. Возможные ситуации с изменением реакций из-за текущего психоэмоционального состояния требуют проведения дополнительных подтверждений личности пользователя. Так, в случаях, например, болезни или снижения концентрации пользователя в системы с критическим доступом допуск пользователя может быть проверен специальными службами.

На основе гипотез и проверенных экспериментальных исследований можно сформулировать метод непрерывной аутентификации, основанный на психологических реакциях пользователей. Метод состоит в следующем [245]:

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.

В общем виде разрабатываемую метод непрерывной аутентификации можно представить в следующем виде:

1. Технология реализуется вычислительным комплексом (ВК). ВК может предоставлять клиенту одну или несколько услуг.
2. ВК включает компьютерные сети, системы управления передачей данных, т. е. среду, используемую для обеспечения каналов связи между компьютерами, системами обработки данных и другими устройствами. Сеть может включать в себя соединения в виде проводных линий связи и каналов беспроводной связи.
3. ВК могут отправлять инциденты безопасности на облачную платформу для дальнейшего анализа приложением машинного обучения на основе идентифицированных характеристик инцидентов безопасности, обнаруженных во время локального анализа с помощью модуля безопасности и диспетчера событий. Идентифицированные характеристики могут включать, например, информацию о том, что наблюдаемые параметры имеют оценку риска безопасности выше порогового значения.
4. В ВК создается постоянное хранилище информации о безопасности и менеджер событий, который может быть аппаратным компонентом или комбинацией аппаратных и программных компонентов. Менеджер информации и событий безопасности управляет процессом выбора только определенных инцидентов безопасности для локального и удаленного анализа.
5. Интервал оценки психомоторных реакций пользователя представляет собой заранее определенный интервал времени, на основе которого формируются инциденты безопасности. Таким образом, элементы

интерфейса вместе со встроенными реакциями передаются в ВК, анализируются на уровне доступа (рис. 4.5).

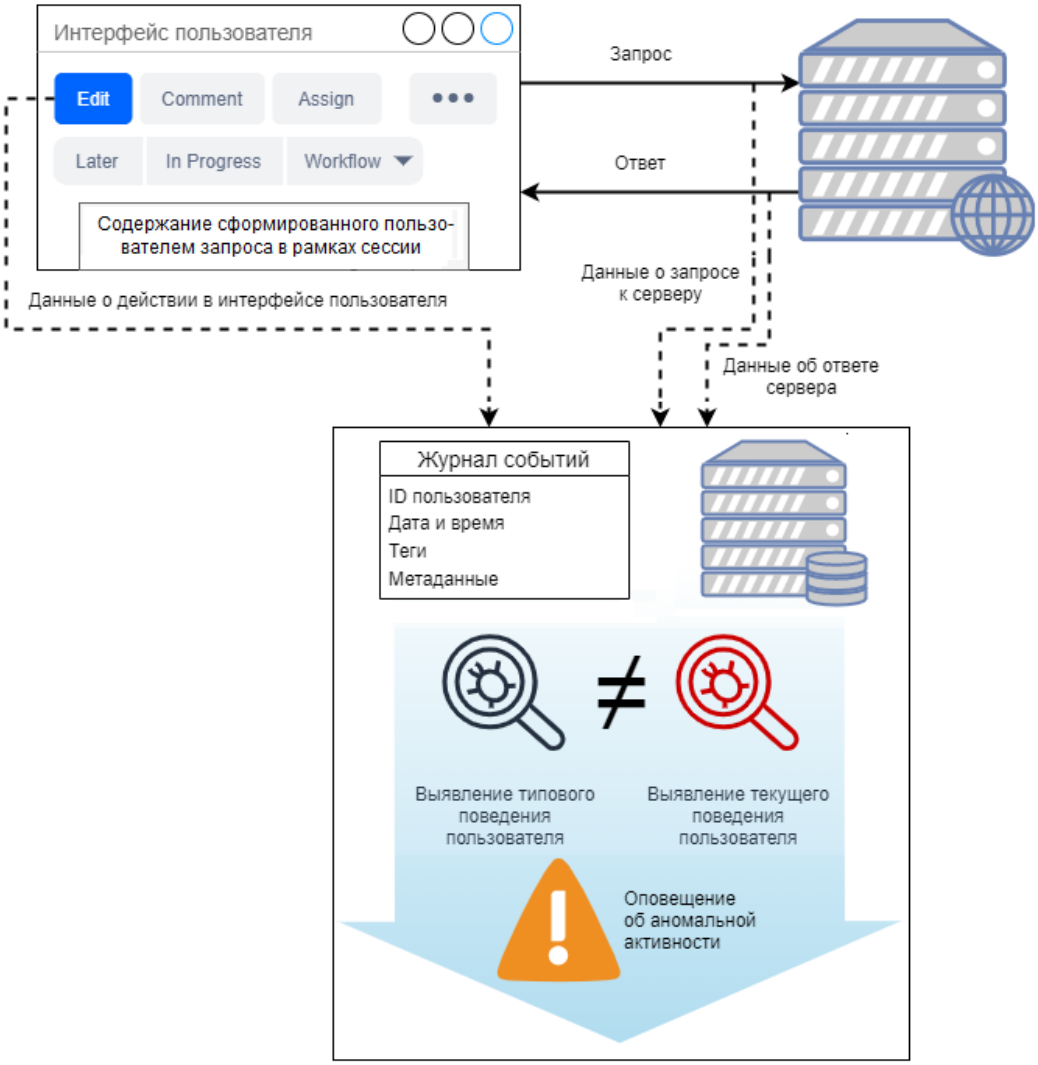


Рисунок 4.5 — Уровень анализа действий пользователя в архитектуре вычислительного комплекса

Концептуальная схема взаимодействия уровня управления и серверной части приведена на рисунке 4.6.

Разработанный метод непрерывной аутентификации на основе психологических реакций пользователей в образовательных вычислительных сервисах организаций высшего образования направлен на обеспечение дополнительного фактора защиты распределенных информационных систем, используемых в образовательных вычислительных сервисах и обеспечение конфиденциальности информации и ресурсов при осуществлении сетевого взаимодействия пользователей. Для обоснования применимости разработанного метода непрерывной аутентификации проведена экспериментальная оценка разработанного метода в образовательных вычислительных сервисах организации высшего образования.

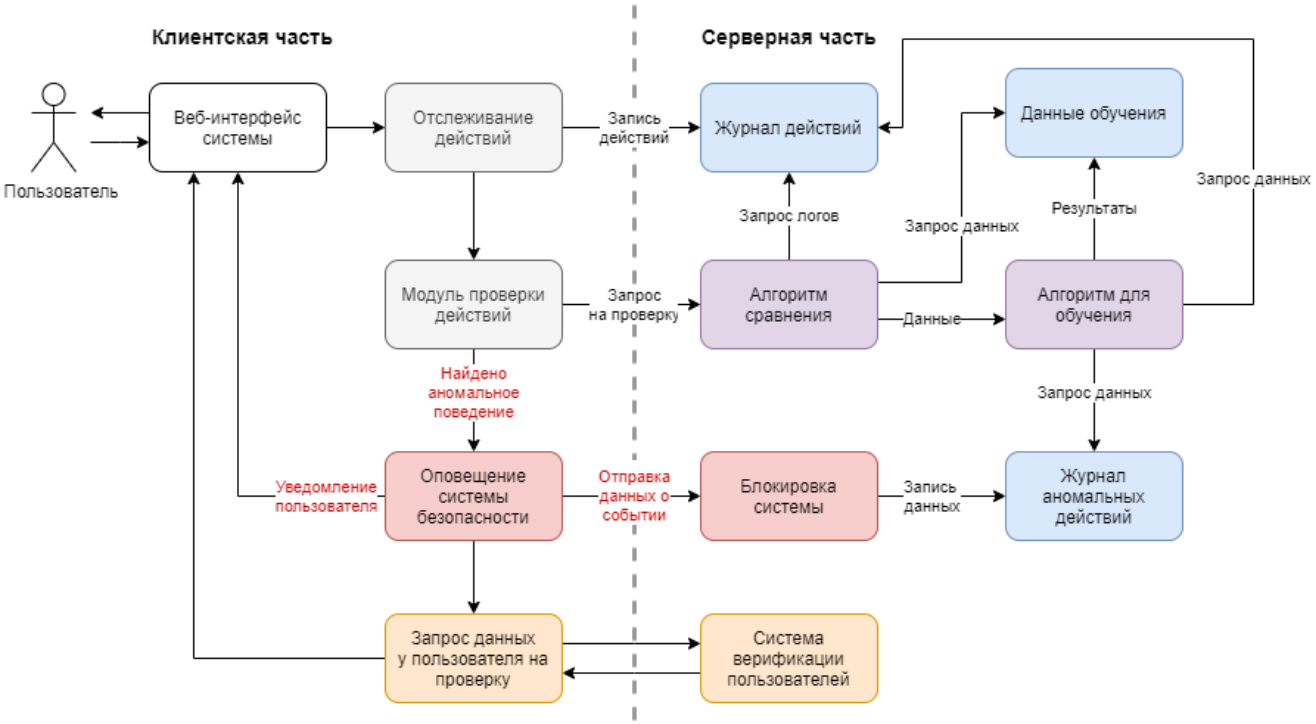


Рисунок 4.6 — Блок схема алгоритма метода непрерывной аутентификации

4.4 Экспериментальная оценка метода непрерывной аутентификации пользователей на основе анализа их психологических реакций

В дистанционном обучении значительное место отводится интерактивному взаимодействию пользователей с компонентами образовательных вычислительных сервисов организаций высшего образования (изучение учебных материалов по дисциплинам, сдача тестов, анкетирование и т. д.). Чтобы проанализировать уровень вовлеченности обучающегося в процесс обучения создаются специализированные технологии с использованием математических методов и алгоритмов. Показателем вовлеченности обучающегося в интерактивный образовательный процесс можно считать величину интервала времени между стимулом, совершаемым действием (прочитать определенный объем учебного материала, ответить на тестовое задание или вопрос) и фиксацией ответа с помощью клавиатуры или компьютерной мыши. Это и есть время реакции при интерактивном взаимодействии. Современные технологии, используемые в вузах позволяют регистрировать и сохранять информацию о времени реакции – временном интервале между выполнением задания и результатом, который фиксируется в веб-интерфейсе обучающимся.

Боты – это программный скрипт (робот), который каким-либо случайным или регулярным образом взаимодействует с цифровой платформой через веб-интерфейс посредством программного кода. Кликеры – это пользователи (образец пользовательского поведения), не участвующие в интерактивном процессе взаимодействия с платформой, которые просто "кликают" (осуществляют взаимодействие с различными элементами интерфейса программы или веб-приложения) по элементам веб-интерфейса, формально переходя по обучающим темам, не останавливаясь на изучение учебного материала.

В настоящее время существуют методы обнаружения кликеров с помощью машинного обучения при обработке результатов психологических опросов. Эти методы не используются в режиме реального времени [277], они применяются только при обработке полученных результатов [278]. Следует отметить также, что применение методов машинного обучения влечет за собой использование большого объема вычислительных ресурсов, следовательно, для значительных объемов данных, которые обрабатывают онлайн-системы в сфере образования, этот процесс достаточно ресурсоемкий. Метод выявления кликеров должен быть достоверным, легко воспроизводимым, без потребностей в значительных вычислительных затратах. Среди различных методов выявления кликеров одним из наиболее перспективных представляется метод, основанный на анализе аномалий времени реакции пользователя. Исходными данными для анализа вовлеченности пользователей может быть время реакции испытуемого на элементы веб-интерфейса с начала предъявления заданий для выполнения. В случае продолжительного взаимодействия множество реакций пользователя можно рассматривать как временной ряд и изучать его с помощью методов теории динамических систем. Подлинные участники интерактивного процесса, имеют определенные, присущие именно им реакции, однако, если интерактивное взаимодействие с цифровой средой достаточно продолжительно (более 2 ч.), то могут быть заметны задержки времени реакции: пользователя отвлек внешний шум, пользователь отошел попить и т. д.). Непостоянные, разовые задержки времени реакции невозможно предусмотреть и запрограммировать.

Отслеживание взаимодействия относится к косвенным методам исследования. Точными методами являются методы компьютерного зрения (в данном случае это изучение движений глаз, мимики, жестикуляции и положений тела), исследование данных, полученных с датчиков. Автоматические методы анализа вовлеченности пользователя могут дать более подробное и точное представле-

ние об обучающемся в плане уровня его вовлеченности в учебный процесс, но при этом необходимо использовать специальные датчики, что не всегда осуществимо в учебном процессе. Сенсорное наблюдение очевидно для учащегося и является дополнительным фактором стресса, например, знание того, что учащегося снимает веб-камера во время решения проблемы. Таким образом, актуальным является создание скрытых (полуавтоматических) методов оценки уровня вовлеченности пользователя с использованием вычислительно эффективных методов преобразования исходных данных о времени реакции обучающегося.

Динамические системы – это математическая модель развития системы (физической, биологической, экономической и т. д.), состояние которой в каждый момент времени точно определено начальным состоянием. Теория динамических систем изначально исследовала решения систем дифференциальных уравнений, представляя это решение в качестве изменений в фазовом пространстве и времени. В фазовое пространство входят фазовые переменные системы дифференциальных уравнений и производные этих переменных. Среди фазовых переменных нет переменной времени. Любому моменту времени сопоставляется набор значений фазовых переменных. Результатом является кривая (место точек) в пространстве состояний. Если система имеет одну фазовую переменную / один процесс, то рассматриваются фазовые траектории в двухмерном пространстве, причем координаты – это переменная и ее производная. Для данного дифференциального уравнения аналитически, чаще численно, может быть построено частное решение при данных условиях, называемое решением задачи Коши. Это уравнение, определяемое частным решением исходной системы. Численно или аналитически дифференцируя решение, получаем вид фазовой траектории. В теории динамических систем большое значение имеет тип фазовой траектории, ее геометрические свойства влияют на понимание и описание свойств системы. Фазовые траектории в колебательных системах - замкнутые, фазовые траектории устойчивых систем сходятся к точке равновесия.

В динамической системе состояние равновесия сопоставляется с точкой (вырожденной траекторией). Периодическое движение соответствует замкнутой кривой (квазипериодическому движению). Аттрактор (совокупность траекторий, притягивающих все близкие траектории) соответствует стационарному режиму (движению) диссипативной системы. Класс динамических систем имеет неустойчивые фазовые траектории, их хаотичным автоколебаниям со-

поставляется странный аттрактор – это множество неустойчивых траекторий. Динамические системы по виду уравнений и методам исследования можно классифицировать как: конечномерные системы с конечномерным фазовым пространством и бесконечномерные распределенные системы. Первый класс динамических систем также делится на консервативные и диссипативные в соответствии с их разной физической природой. Фазовый объем диссипативных систем не сохраняется, в их фазовом пространстве существует область (шар диссипации), в которую на любой траектории всегда попадает точка.

При обработке данных исследования в настоящее время применяются не только теории математической статистики, часто используемые в психометрии, но также динамические модели. Методы математической статистики базируются на статистическом представлении изучаемого процесса – основой служит понятие случайной величины, значения которой соответствуют определенному закону распределения. Предположение о виде распределения случайной величины проходит проверку как статистическая гипотеза, основанная на эмпирических данных. Применение статистического подхода дает возможность выявить вероятное значение случайной величины и разброс ее возможных значений. С помощью информации, полученной из статистических наблюдений, распределения дают возможность масштабировать значения измеряемых показателей. Что же касается динамических моделей, то можно получить следующее значение, имея текущее и уравнения эволюции (динамики). Задача построения уравнений по полученным данным (обратная задача динамики) некорректна с точки зрения математики, так как есть бесконечное число разных уравнений, имеющих решение одного вида. Известно значительное число методов восстановления уравнений, зная тип наблюдаемых процессов, а для систем с хаотической динамикой достаточно только иметь количественные оценки характеристик. Хаотические системы являются диссипативными - система, при попадании в область странного аттрактора, продолжает находиться на своих траекториях, она неустойчива, но включена в некоторую область фазового пространства. Будем рассматривать применение случайных величин и динамических систем в психометрике. При изучении набора тестов для группы испытуемых при статистическом подходе ответ на задание является случайной величиной. Ответы не связаны между собой, т. е. не зависят один от другого. Статистические гипотезы можно проверить проверенными методами, в соответствии с мощностью выборки и установленными правилами. Будем считать

исследуемым параметром время, которое тратится на получение верного ответа, то подход к анализу данных сильно не поменяется. Будем оценивать время реакции, приведя его к шкале, соответствующей распределению случайной величины .

При использовании динамического подхода следующий ответ пользователя оценивается с учетом предыдущего. Таким образом принимается во внимание степень утомления испытуемого, что может значительно влиять на результат в случае больших тестов. Если рассматривать динамику в качестве случайного процесса и проверить верность гипотезы о стационарности, то основываясь на теории случайных процессов и методах идентификации можно узнать среднее время реакции на тест, разброс значений и т. п. Если брать в качестве инструмента динамические модели, то можно изучить изменение траекторий личных реакций. У ботов и кликеров эти характеристики будут заметно отличаться. В динамических моделях для тестирования после 2 часов будут заметны отвлекающие факторы. Через 2 часа обучающийся точно отвлечется, возможно на длительное время. При статистической обработке эти значения (время реакции) отфильтруют как выбросы. В динамической модели зафиксируется информация о времени, в которое пользователь будет отвлекаться. Для каждого пользователя это будет индивидуально – один устанет раньше, другой - позже, но это обязательно произойдет. Следует отметить, что при моделировании ботов можно генерировать случайное значение распределения. Несмотря на то, что генерация будет основана на псевдослучайных числах, это трудно заметить для больших объемов данных в режиме реального времени. Генерация хаотического сигнала является трудоемкой задачей, в режиме реального времени его можно рассчитать в ходе длинной серии тестов.

Длительное интерактивное взаимодействие пользователя со средой обучения по динамике схоже с реакцией на прохождение тестирования. Элементы в среде обучения требуют определенного внимания, сам пользователь может остановиться или вернуться к более ранним учебным материалам. Это все естественно для человеческого поведения. Поэтому обоснованной будет гипотеза о возможности использования динамических моделей в процессе обезличенного оперативного анализа вовлеченности пользователя. В хаотической динамике используется множество характеристик, отдельные можно оценить без полных моделей динамических систем, например, с помощью временных рядов. В качестве такой характеристики рассмотрим старший показатель Ляпунова,

преимуществом его оценки является не его фактическое значение, а сигнатура (знак), при этом он может быть рассчитан на основе экспериментальных данных.

Определение показателей Ляпунова: есть система, заданная обыкновенным дифференциальным уравнением. Будем рассматривать возмущения, которые можно придать траектории этой системы. В случае, если амплитуда постоянно бесконечно мала относительно начального фазового пространства, то возмущения описываются линейным уравнением и их называют бесконечно малыми (вариации траектории). Бесконечно малые векторы являются касательными к траекториям исходной системы. Все касательные векторы представляют собой касательное пространство, которое имеет ту же размерность, что и фазовое пространство. Бесконечно малый вектор в зависимости от направления приложения возмущения и свойств системы может увеличиваться или затухать. Так как уравнение линейно, то поведение вектора примерно соответствует экспоненциальному закону. Согласно теореме Оселедца, существует набор чисел $\lambda_1 > \lambda_2 \ldots \lambda_m$, где m – размерность касательного пространства, такой, что для каждого начального возмущения существует показатель степени, принимающий значения из множества λ_i в соответствии с выбором касательного вектора. λ_i – это показатели Ляпунова. Из теоремы следует, что сумма первых k показателей Ляпунова является средним экспоненциальным сжатием или расширением k-мерного фазового объема. Для вычисления старшего показателя Ляпунова решают совместно линеаризованные уравнения, периодически выполняя перенормировки и накапливая логарифмы норм, после усредняя накопленные значения за время вычислений.

Сформулировать задачу формально. Пусть есть ряд реакций пользователей в течение продолжительного интерактивного сеанса с образовательным веб-сервисом. Надо определить пользователей, принявших участие в этом сеансе. Проведем мониторинг, выявляя 2 типов моделей поведения, не участвующих в интерактивном процессе:

1. Кликеры – слишком быстрая реакция на стимул (значительно меньшее время, чем нужно на изучение материала, ответа на вопрос и т. д.).
2. Боты – постоянное время реакции, вне зависимости от сложности задачи (может соответствовать некоторому закону распределения). Временной ряд реакций людей в течение интерактивного сеанса носит хаотичный характер.

Исходные данные для экспериментов – это результаты массового тестирования школьников и студентов посредством цифровой платформы [279]. Испытуемые должны были пройти тестирование, в которое входили вопросы, задачи и тесты. На рисунке 4.7 представлены примеры веб-страниц с заданиями, которые предъявлялись пользователям. Веб-интерфейс можно было открыть на любом устройстве с доступом в интернет. Кроме результатов ответа сохранилась информация о времени реакций пользователей. Эти данные представлены в настоящей работе.

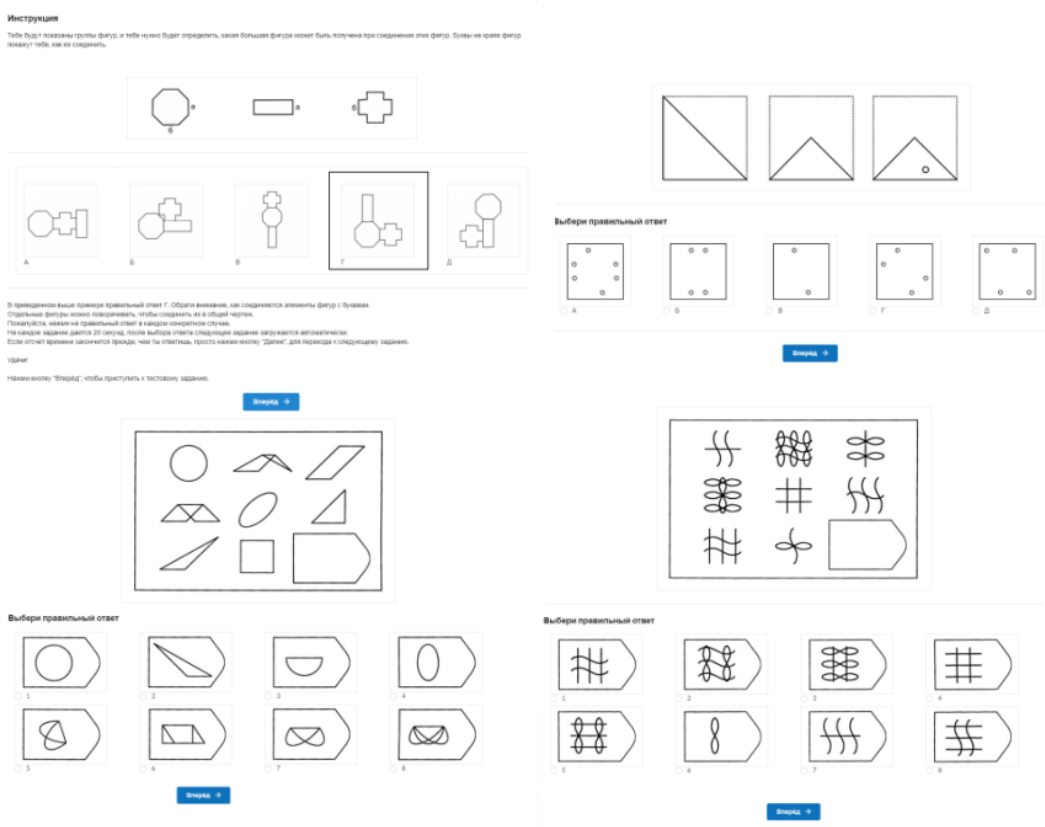


Рисунок 4.7 — Интерактивное взаимодействия образовательных платформы с использованием веб-интерфейса: вопросы тестов с кнопкой "Далее"

Число вопросов, представленных на странице, варьировалось, но для пользователей не менялось. Временем реакции пользователя считался интервал времени от появления изображения на экране до момента нажатия пользователем кнопки "Далее". Время реакции технически вычислялось как разница между последним фиксированным временем ответа (с учетом возврата на предыдущую страницу для изменения ответа) и временем первого показа задания.

Для каждого испытуемого был построен временной ряд, соответствующий времени реакций во время тестирования. На рисунке 4.8а представлен пример

такого временного ряда. Были выявлены пользователи с поведением кликера – с самого начала взаимодействия или либо после нескольких вопросов, такие испытуемые отвечали не думая. График, соответствующий временному ряду реакций кликера представлен на рисунке 4.8б.

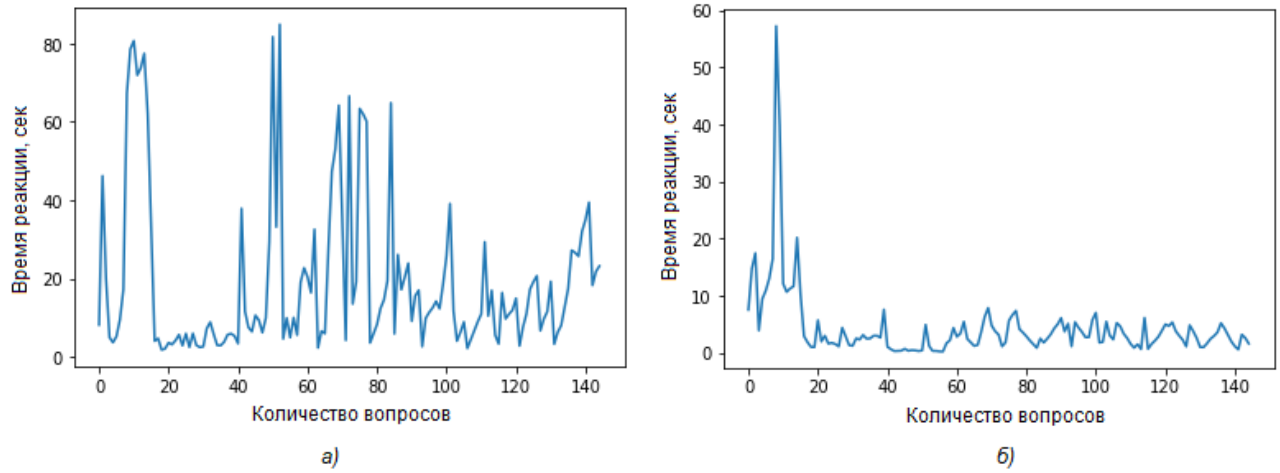


Рисунок 4.8 — Временной ряд типового пользователя: а) вовлеченного; б) не вовлеченного в интерактивное взаимодействие с платформой

Изучение показателей хаотической динамики помогло определить, что в качестве надежной характеристики для подобных рядов можно выбрать максимальное значение характеристического показателя Ляпунова (МПЛ). Применение теории динамических систем и хаоса для выявления и распознания динамики различных видов человеческой деятельности показало хорошие результаты [280]. Для пользователей, вовлеченных в интерактивный образовательный процесс, характерно хаотическое поведение (расходящиеся фазовые траектории) [281], следовательно, их значение λ будем неотрицательным, в то время как реакции кликеров и ботов людей будут характеризоваться сжимающимися фазовыми траекториями их значение λ будем отрицательным.

Пусть полученный временной ряд реакций пользователя $U = (T(q_1), \dots T(q_i), \dots T(q_n))$, где T – время реакции (сек.), q – вопрос, i – номер вопроса $[1, dotsn]$ – сформирован динамической системой с хаотической динамикой. Тогда при условии, что $n >> 2$n для временного ряда можно найти оценку МПЛ:

$$\lambda = \frac{1}{n} \sum_{i=1}^{n} \ln |U'(q_i)|, \tag{4.1}$$

где $U'(q_i) = (T(q_i) - T(q_{i-1})$.

Для экспериментального исследования рассматривалась выборка из 22236 записей веб-тестов студентов. Установлено, что из 22236 записей неотрицательный показатель λ имеют 21663 записи. На рисунке 4.9а показано распределение значений λ для всей выборки. Оранжевая линия – граница, справа от которой находятся положительные значения, то есть имеет место хаос. Имеется 573 записи с отрицательным λ.

Таким образом, доля отрицательных по показателю λ строчек (доля кликеров) составляет 2,48%. При сокращении исходной выборки (удалены данные пользователей, содержащие значения, выходящие за границы 3σ) до 13444 записей, проведены расчеты МПЛ. На рисунке 4.9б представлены значения λ по модифицированной выборке.

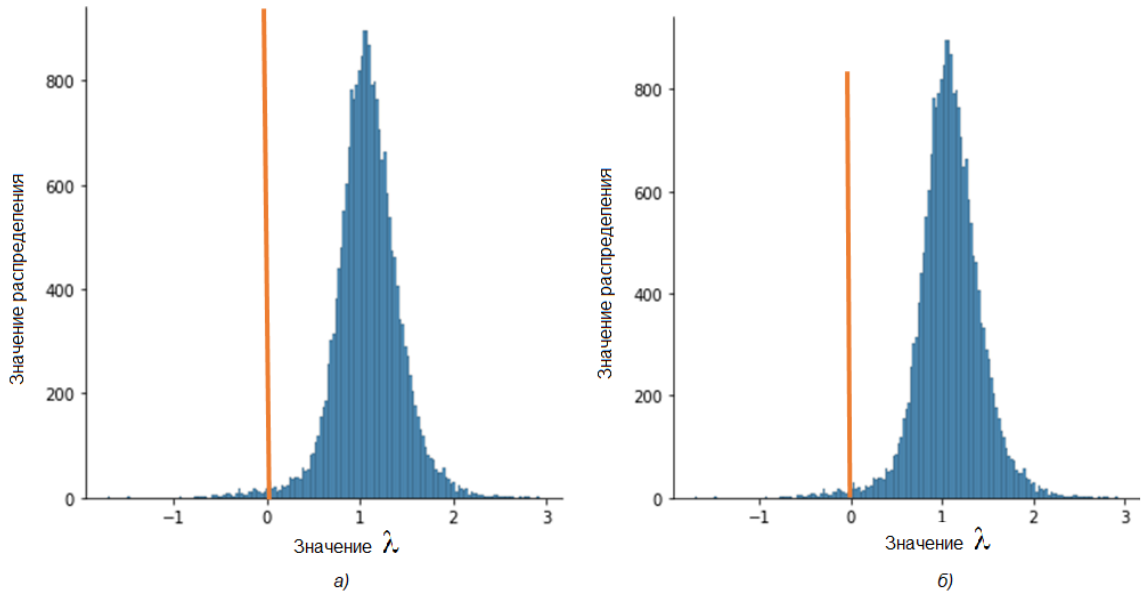


Рисунок 4.9 — Значения λ для эксперимента по выборке из: а) 22236 записей; б) 13444 записей

Неотрицательный показатель λ имели 13083 записи. Отрицательный показатель λ имела 361 запись. Доля отрицательных по Ляпунову строчек составила 2,68%. Фильтрация данных заметно уменьшила объем выборки. При этом соотношение кликеров не изменилось. Во втором эксперименте исследовалась выборка из 16350 записей о времени реакций. На рисунке 4.10а представлены значения λ для выборки.

Всего 27 записей из 16350 оказались выполненными невовлеченными пользователями (кликерами). Это согласуется с организационным сопровождением проведения данного исследования, которое осуществлялось администрациями

учебных заведений. Для заполнения веб-опроса в экспериментальном исследовании был разработан скрипт-бот, автоматически отвечающий на заданные вопросы. Применив вычисление λ к выборке данных из 688 записей, сгенерированных этим ботом (рис. 4.10б), получаем для всех записей отрицательные значение показателя λ, что, в свою очередь, подтверждает выдвинутую гипотезу.

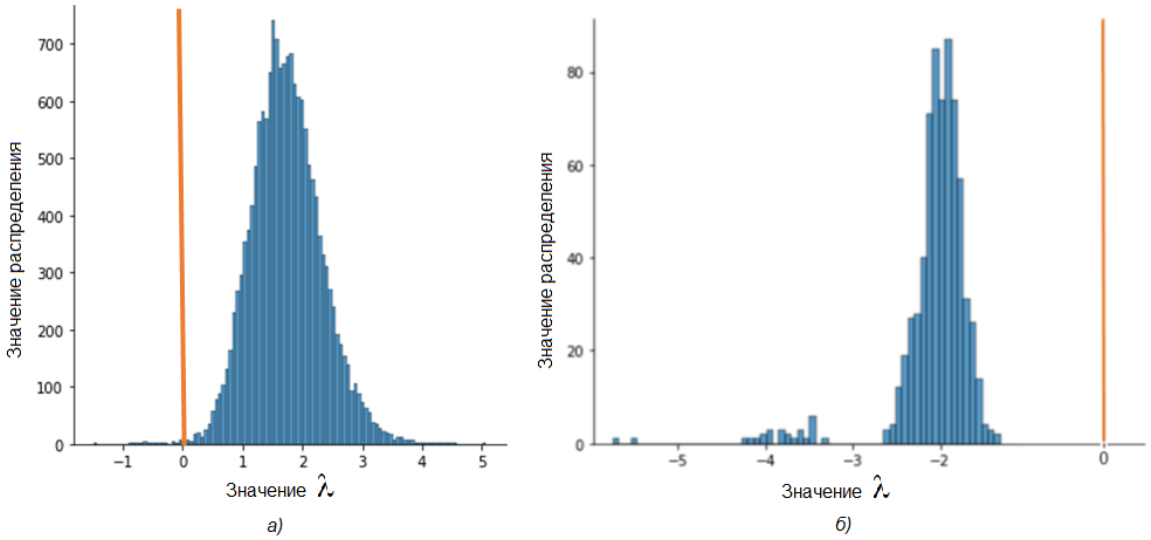


Рисунок 4.10 — Значения λ по выборке из: а) статьи экспериментального исследования; б) 688 сгенерированных ботом реакций

Таким образом, проведение экспериментов подтвердило гипотезу о выявлении невключенных в интерактивный процесс пользователей на основе неотрицательности МПЛ, как характеристик хаотической динамики. Для реализации задачи по контролю вовлеченности пользователя в интерактивный процесс образовательных веб-сервисов предлагается использовать реакции пользователя, представляющие собой фиксированные временные интервалы между предоставлением экранной формы и реакцией пользователя в веб-интерфейсе. Выделенные типы паттернов невовлеченного интерактивного поведения студентов – боты и кликеры и два типа, используемых характеристик хаотической динамики вычислительной характеристики. На больших данных были проведены вычислительные эксперименты, показавшие возможность выявления ботов и кликеров в общем объеме пользователей. Предложенные решения дадут возможность улучшить существующую систему контроля вовлечения обучающихся в цифровую среду, удалить лишние данные перед анализом реакций при применении метода непрерывной аутентификации на основе психологических реакций пользователей.

Методы компьютерного зрения и использование специальных датчиков для оценки вовлеченности пользователя могут дать более точное представление по сравнению с методами отслеживания вовлеченности по времени реакции. Но для их использование необходимо наличие специального оборудования, что не всегда может быть выполнимо. Кроме того, наблюдение для учащегося является дополнительным фактором стресса (знание того, что учащегося снимает веб-камера во время решения). Таким образом, дальнейшее развитие методов скрытой оценки вовлеченности является актуальным, а на основе полученных результатов могут быть разработаны новые вычислительно эффективные методы анализа времени реакции.

Разработанный метод непрерывной аутентификации на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы. Метод позволяет учитывать персональные реакции на основе только времени ответа на контрольные вопросы, что позволяет существенно сократить затраты ресурсов и объемы передаваемых данных, по сравнению с решениями, учитывающими все действия пользователей при взаимодействии с интерфейсом. Приведенные результаты экспериментальных исследований показали, что анализ психомоторных реакций пользователей может быть использован как модуль анализа управления доступом, при этом исследуемая характеристика пользователя может быть измерена без перегрузок каналов связи и независимо от используемого типа устройств, предложено время реакции.

4.5 Выводы по четвертой главе

В четвертой главе проведен обзор основных методов аутентификации пользователей, посредством сравнительного анализа существующих исследований в области непрерывной аутентификации, обоснован выбор метода аутентификации на основе поведенческой биометрии, использующий в качестве аутентифицирующего (идентификационного) признака время психологических реакций пользователей, в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределенных информационных системах.

Проведенные экспериментальные исследования значений психологических реакций пользователей позволили оценить применимость предложенного подхода для построения системы аутентификации образовательных вычислительных сервисах. Полученные количественные значения позволили установить пороговые значения и величины погрешностей времени реакции пользователей при обеспечении взаимодействия с сервисами и информацией, обрабатываемой в образовательных вычислительных сервисах организаций высшего образования.

На основе полученных экспериментальных значений и проведенных исследований в области непрерывной аутентификации разработан метод непрерывной аутентификации на основе психологических 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, а также обеспечить дополнительную защиту распределенных информационных систем в условиях высокого риска реализации угроз информационной безопасности. Проведенные экспериментальные исследования разработанного метода непрерывной аутентификации позволяют сделать вывод о возможности использования разработанного метода в системах управления доступом в качестве дополнительного фактора проверки подлинности пользователей.

Глава 5. Научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков

В главе представлен разработанный метод оценки эффективности реализации защитных мер на основе анализа затрат ресурсов, позволяющий обнаруживать факты избыточного использования ресурсов существующими средствами защиты информации в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределенных информационных системах. Кроме того представлен 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 доступом и методах количественной оценки рисков, непрерывной аутентификации и оценки эффективности.

5.1 Метод оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов

Одним из критериев оценки эффективности систем и мер обеспечения информационной безопасности вычислительных сервисов можно признать производительность таких систем. В контексте проводимого исследования под производительностью понимается способность систем безопасности хранить данные о деятельности пользователей и обрабатывать данные в режиме реального времени. Таким образом, в системах безопасности для гарантированного обеспечения заданного уровня эффективности, необходимо выявить производительность и вычислительные ресурсы, необходимые для выполнения средствами защиты своих функций по фиксированию действий пользователей и выявления рисков безопасности [282].

Эффективность использования ресурсов возможно оценить на основе анализа сложности алгоритмов и с использованием синтетических тестов. Первый подход может предоставить информацию о производительности отдельных ча-

стей алгоритма программного обеспечения во времени, но вряд ли применим для анализа сложных программных систем. Второй – хорошо известный подход к анализу эффективности использования ресурсов программного обеспечения, однако он не учитывает специфику вычислительной инфраструктуры и планируемый объем запросов данных. Для решения поставленных задач необходимо построить модель и разработать методику, основанную на использовании экспериментальных оценок в среде [283], имитирующей функционирование системы управления доступом в заданных условиях и ограничениях.

Задачу анализа затрат ресурсов компонентов архитектуры модернизированной системы КД возможно сформулировать следующим образом [284], исходя из необходимости оценить возникающие затраты в связи с внедрением метода непрерывной аутентификации пользователей. Пусть заданы технико-экономические характеристики функционирования системы управления доступом, представляющие собой набор заданных желаемых диапазонов значений при заданном уровне обслуживания QoS (Quality of Service), и планируемую форму и интенсивность запросов к системе. Тогда для пользовательских запросов $x \in X_K$ к системе управления доступом с архитектурой V, для компонента Z_k с допустимыми технико-экономическими характеристиками, может быть задано отображение:

$$Z_k \subset V : x \xrightarrow{\Phi} R_k \in \mathbf{R}^n, k = \overline{1,q}, \tag{5.1}$$

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

Отображение Φ в условиях виртуальности ресурсов может быть получено путем построения экспериментального стенда по технологии "инфраструктура как код", то есть получено в результате испытаний конфигурации Z_k при имитационном моделировании входного потока X. Иными словами отображение Φ представляет собой программно-конфигурационный код, содержащий виртуальную инфраструктуру, с входным сигналом в форме потока X и измеряемым скалярным выходом вектора измеряемых значений характеристик.

Для построения потока может быть использовано имитационное моделирование. В работах [285—287], посвященных построению математических моделей функционирования веб-порталов, показано, что стохастические процессы, описывающие доступ пользователей, могут быть идентифицированы на

основе типовых запросов. Для построения моделей трафика широко используются динамические модели. Существует направление, связанное с генерацией хаотического сигнала [288—291], имитирующего протокол TCP/IP. Для оценки ресурсов нет необходимости строить точные прогнозные модели процессов, поскольку искомые значения запасов вычислительных ресурсов зависят только от диапазона и интенсивности процессов, что может быть реализовано имитационным моделированием случайной величины с заданной функцией распределения [292; 293]. В случае, если технико-экономические характеристики не сильно сужают канал, целесообразно использовать бета- или гамма-распределение, для узких каналов – распределение с "тяжелыми хвостами".

Для оценки 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 средств управления доступом – выбор вариантов, имеющих 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 системы 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 [294].

Технология реализации предложенного метода состоит в использовании виртуальных стендов, обеспечивающих имитационную среду использования вычислительного комплекса. Такой подход позволяет учитывать особенности современной цифровой среды и технико-экономические требования, предъявляемые к вычислительному комплексу. Рассмотрим, например, задачу оценки вычислительных затрат при записи событий в базе данных при работе с веб-сервисами по компьютерным сетям с логированием действий пользователей, т. е. с созданием их профиля поведения. Предполагается, что запись действий пользователей будет осуществляться в журнал событий. Из-за разных видов интерфейсов, меняющихся в зависимости от типа устройства, для каждого устройства предлагается вести свою запись журнала действий. Пусть каждое действие в журнале событий включает следующие данные [295]:

- идентификатор пользователя;
- устройство (идентификатор конкретного устройства);
- действие (уникальное название или идентификатор, чтобы отличать действия);
- время совершенного действия.

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 (ВМ) (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 5.1, в таблице 14 приведены параметры виртуальных машин.

После создания виртуальных машин, установки и запуска серверного программного обеспечения и системы управления базами данных (СУБД) начинается сам эксперимент. Исходные данные загружаются в оперативную память ВМ Client. После их полной загрузки начинается отправка данных с заданными параметрами.

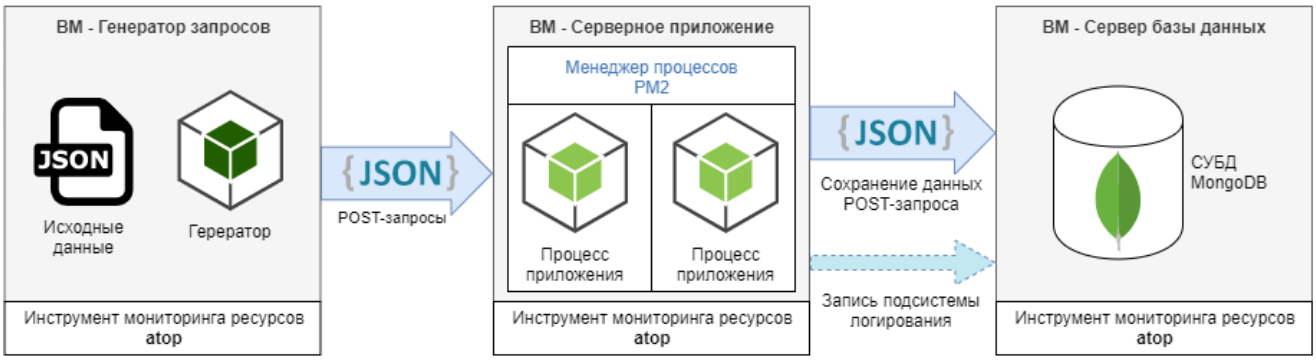


Рисунок 5.1 — Структурная схема экспериментального стенда

Таблица 14 — Основные характеристики виртуальных машин

	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 производится отправка POST-запросов к серверу на получение записей ResearchSubject, представляющих собой сохраненные журналы событий безопасности действий пользователя на основе анализа нажатий клавиш клавиатуры. На втором этапе эксперимента производится отправка POST-запросов к серверу на сохранение записей ResearchResult, представляющих собой результаты сравнение 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. Для логирования к запросу добавляется код, приведенный в листинге 5.1.

Эксперимент производится с двумя различными конфигурациями серверного ПО. В первом случае производится только сохранение данных (примеры записей данных приведены в листингах 5.2, 5.3). Во второй конфигурации добавлен программный код (листинг 5.4), осуществляющий логирование каждого запроса, полученного серверным ПО. При этом на каждый поступивший запрос в базе данных создается дополнительная запись, общий вид которой представлен в листинге 5.3. Эти записи создаются после выполнения каждого POST-запроса [296].

Листинг 5.1: Исходный код алгоритма логирования запросов к серверному ПО

```
Model.afterRemote('**', (ctx, modelInstance) => {
        const params = ctx.req.body.data || ctx.req.body;
        const { id, researchSubjectId } = params;
        const userId = researchSubjectId || id;
        if (!userId) {
                return Promise.resolve();
        }
        return Model.app.models.ResearchSubject.findById(userId)
        .then((researchSubject) => {
                Model.app.models.ActionLog.logEvent(modelInstance, ctx, userId,
                !!researchSubject);
        });
});
```

Листинг 5.2: Пример записи ResearchSubject

```
{
        "_id": ObjectId("5dce6295ef49df9ad703df17"),
        "sessionId": "cPbEMLwbr16DH2ySQWELHoUSHPZ3faAqVrp59jvKQWEESOE4N6Ue2mOBYnTD
        "login": "abcd1234541104000",
        "researcherId": ObjectId("5db81cb3db867f7f119baabb"),
        "alias": "abcd00001",
        "privateResearchSampleId": "5dce608e83d1929b0423aaaa",
        "createdAt": "2019-11-15T08:32:21.370Z",
        "updatedAt": "2019-11-28T10:43:50.744Z"
}
```

Сбор данных об используемых ресурсах осуществляется с помощью утилиты Atop с интервалом в 1 секунду; отправка запросов осуществляется в 4 потока, до 10 одновременных запросов; задержка между отправками пакетов по 10 запросов равна 300 мс, а задержка между этапами эксперимента – 60 с; максимальное ожидание ответа от сервера – 10 с; код исполняется с использованием Node.JS версии 12.x.

Серверное ПО запущено под управлением менеджера процессов PM2 со следующими параметрами: *pm2 start /vagrant/application/index.js –node-args="–max_old_space_size=1024i max –restart-delay=5 –max-restarts=1000.* Это означает, что объем выделенной для процесса ОЗУ не превышает 1024 Мб, количество параллельно работающих процессов равно числу ядер центрального процессора (то есть 2). Задержка перед повторным запуском процесса в случае

отказа 5 с. Максимальное число перезапуска процесса – 1000 раз. Код исполняется с использованием Node.JS версии 12.x. Установлена MongoDB версии 3.2.

Листинг 5.3: Пример записи ResearchResult

```
{
"_id": ObjectId("5dd90de7c383bff471725ac9"),
"embeddedPsychotestId": "5dce5d89ef49df9ad703db2a",
"embeddedPsychotestIndex": 4,
"data": {
        "answers": [
        // Multiple Objects
        ],
        "scales": [
        // Multiple Objects
        ],
        "metadata": {
                "platformOs": "Windows 10 64-bit",
                "userAgent": "Mozilla/4.0 (Windows NT 10.0; Win64; x64)
                AppleWebKit/536.36 (KHTML, like Gecko) Chrome/63.0.3282.140
                Safari/536.36 Edge/17.17763",
                "platformDescription": "Microsoft Edge 17.17763
                on Windows 10 64-bit",
                "startTime": "2019-11-23T10:43:06.095Z",
                "endTime": "2019-11-23T10:44:19.021Z"
                }
        },
"researcherId": ObjectId("5db81cb3db867f7f119baabb"),
"researchSampleId": ObjectId("5dce608e83d1929b0423aaaa"),
"researchSubjectId": ObjectId("5dce6295ef49df9ad703df1b"),
"createdAt": "2019-11-23T10:45:59.107Z",
"updatedAt": "2019-11-23T10:45:59.107Z"
}
```

Содержание основного конфигурационного файла (mongod.conf): *storage: dbPath: /var/lib/mongodb journal: enabled: true systemLog: destination: file logAppend: true path: /var/log/mongodb/mongod.log net: port: 27017 bindIp: 0.0.0.0 processManagement: timeZoneInfo: /usr/share/zoneinfo*

Диаграмма последовательностей для эксперимента для оценки ресурсной эффективности записи действий пользователей в журнал событий приведена на рисунке 5.2.

Листинг 5.4: Пример записи ActionLog

```
{
    "_id": ObjectId("5fc8e399f50a5851737b43af"),
    "userId": "5dce6295ef49df9ad703df17",
    "exists": true,
    "method": "POST",
    "request": "ResearchSubject.create",
    "createdAt": ISODate("2020-12-03T13:09:44.173Z"),
    "updatedAt": ISODate("2020-12-03T13:09:44.173Z")
}
```

Экспериментальный фреймворк размещен на хост-системе и выполняет управление экспериментом на всех приведенных этапах. Сперва производится инициализация всех виртуальных машин стенда. Она включает создание виртуальной машины из базового образа, запуск виртуальной машины, установку программного обеспечения и его конфигурирование. В ходе инициализации устанавливаются также характеристики виртуальных машин и ограничения по выделенным ресурсам.

Первой производится инициализация виртуальной машины сервера базы данных, затем серверного приложения, в конце – генератора запросов. Такая очередность обусловлена тем, что СУБД должна быть запущена и способна принимать запросы до того, как это потребуется серверному приложению. Когда все три виртуальные машины запущены и сконфигурированы, экспериментальный фреймворк фиксирует в оперативной памяти время начала эксперимента. Далее внутри виртуальной машины генератора запросов производится запуск программы, считывающей с диска исходные данные в оперативную память для последующей отправки по протоколу HTTP. На этом этапе данные разделяются также на две части *ResearchSubjects* и *ResearchResults*, соответствующие двум отдельным типам записей.

Когда весь объем данных загружен в оперативную память, начинается процесс отправки запросов. От виртуальной машины генератора запросов одновременно отправляется набор из HTTP-запросов, передающих записи *ResearchSubjects* по методу POST на API серверного приложения, размещенного в соответствующей виртуальной машине. Один запрос содержит одну запись. Далее серверное приложение выполняет сохранение каждой полученной записи и, если включен процесс логирования запросов, следом создается запись

ActionLog, которая также сохраняется в базу данных. Это происходит до формирования ответа генератору запросов. Когда серверное приложение завершило сохранение данных, оно возвращает положительный ответ генератору запросов. В свою очередь, генератор запросов дожидается получения ответов на все переданные запросы и после паузы в 300 мс выполняет отправку следующего набора запросов. Процедура повторяется до тех пор, пока не будут отправлены все записи *ResearchSubjects*.

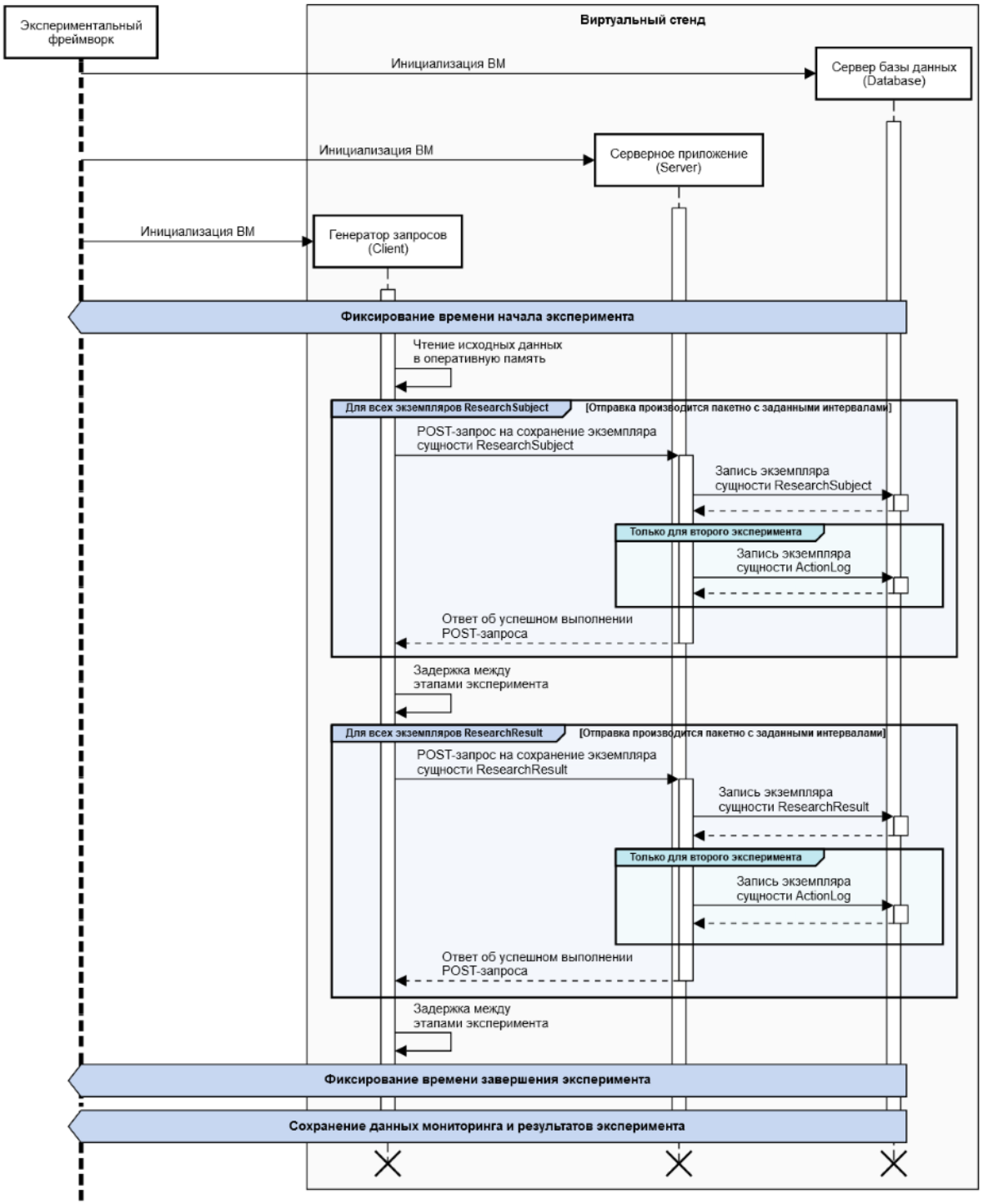


Рисунок 5.2 — Диаграмма последовательностей эксперимента

Когда все записи *ResearchSubjects* сохранены, программа генератора запросов переходит в режим ожидания длительностью 60 секунд. Затем для записей *ResearchResults* производится аналогичная процедура отправки запросов с последующим ожиданием. После этого экспериментальный фреймворк фиксирует в оперативной памяти время завершения эксперимента. С использованием полученных временных рамок из каждой виртуальной машины экспортируются данные об использовании вычислительных ресурсов на протяжении эксперимента для последующей обработки, визуализации и анализа. В конце все три виртуальные машины удаляются.

Результаты вычислительного эксперимента приведены на рисунках 5.3–5.5 и в таблице 15.

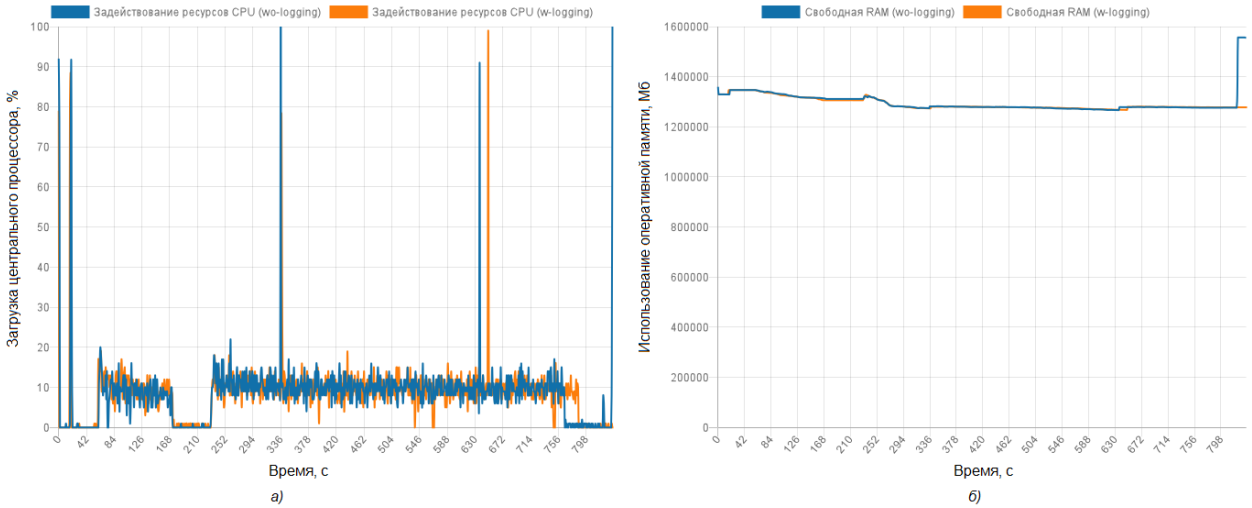


Рисунок 5.3 — Использование ресурсов виртуальной машины Client:
а) центрального процессора, б) оперативной памяти

Таким образом, для рассматриваемого примера экспериментально установлено, что использование разработанного метода непрерывной аутентификации пользователей существенно влияет только на загрузку процессоров Server и сервера Mongodb, незначительно увеличивает загрузку памяти сервера. Внедрение разработанного метода в системы управления доступом требует внесения соответствующих запасов ресурсов в вычислительный комплекс.

Для оценки ресурсной эффективности разработанного метода непрерывной аутентификации в зависимости от объема и типа запросов воспользуемся экспериментальным стендом, с параметрами, приведенными в таблице 14. На каждой виртуальной машине установлена ОС Linux Ubuntu 20.04.6 LTS. Сбор данных об используемых ресурсах осуществляется с помощью утилиты Atop

с интервалом в 1 секунду. Код серверного ПО исполняется с использованием Node.JS версии 18.17.1. Серверное ПО запущено под управлением менеджера процессов PM2 с параметрами, приведенными в таблице 16.

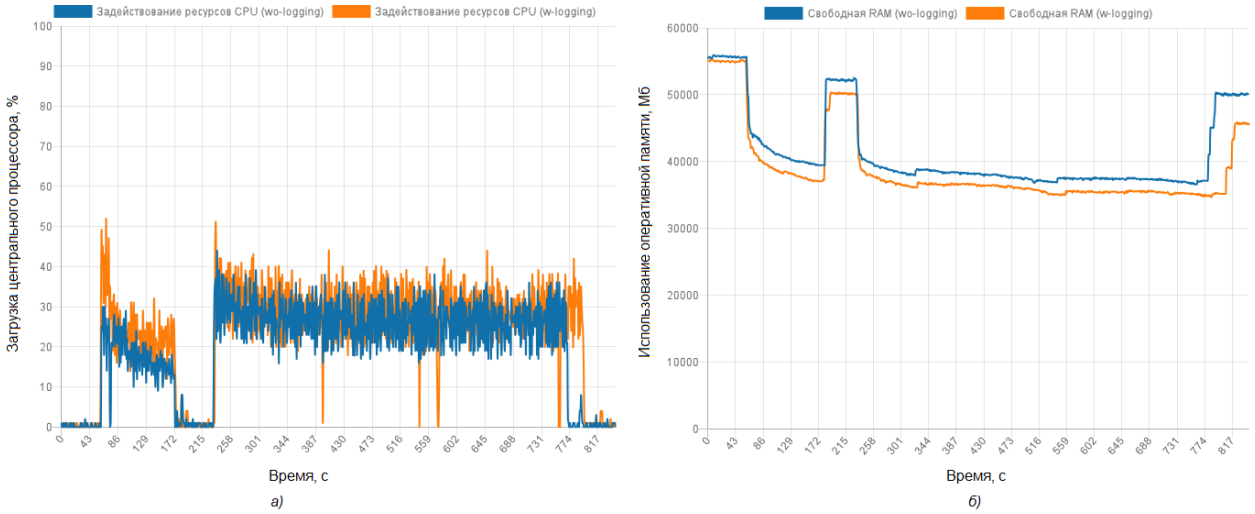


Рисунок 5.4 — Использование ресурсов виртуальной машины Server: а) центрального процессора, б) оперативной памяти

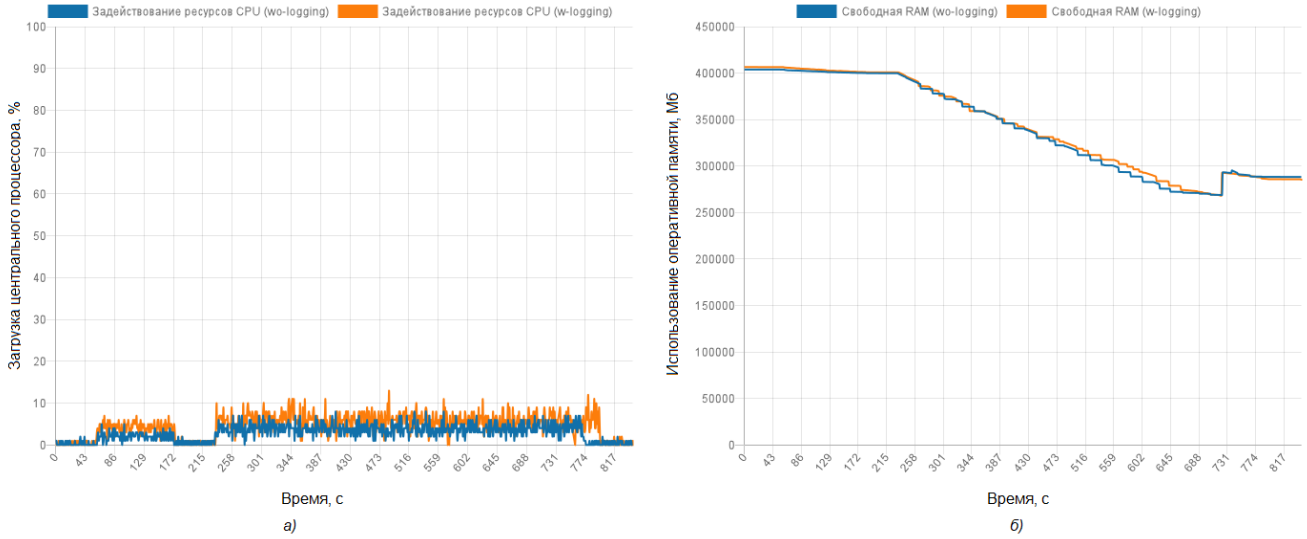


Рисунок 5.5 — Использование ресурсов виртуальной машины Mongodb: а) центрального процессора, б) оперативной памяти

Программное обеспечение виртуальной машины Database: СУБД MongoDB версии 4.4.29. Содержание основного конфигурационного файла (mongod.conf): *storage: dbPath: /var/lib/mongodb journal: enabled: true systemLog: destination: file logAppend: true path: /var/log/mongodb/mongod.log net: port: 27017 bindIp: 0.0.0.0 processManagement: timeZoneInfo: /usr/share/zoneinfo.*

Таблица 15 — Показатели ресурсных затрат на применение метода непрерывной аутентификации пользователей

Ресурсной преподаватель	Значение без использования метода непрерывной аутентификации	Значение с использования 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

Таблица 16 — Параметры запуска серверного программного обеспечения

Параметр	Значение	Пояснения
Max old space size	1024	Объем используемой процессом памяти не должен превышать 1024 Мб
Restart delay	5	2048 Перезапуск процесса в случае отказа выполняется с задержкой в 5 секунд
Max restarts	1000	Максимальное число перезапусков процесса равно 1000
Instances	1	Количество запущенных процессов серверного программного обеспечения равно 1

Программное обеспечение виртуальной машины Client. В качестве инструмента генерации нагрузки использован Locust 2.25.0. Код исполняется интерпретатором Python версии 3.8.10. Сценарии нагрузочных испытаний выполняют отправку POST-запросов к серверному ПО по протоколу HTTP. Проведены серии нагрузочных испытаний для следующих конфигураций сервера и типов записей:

1. Сохранение *ResearchSubject* без логирования действий пользователя.
2. Сохранение *ResearchSubject* с логированием действий пользователя.
3. Сохранение *ResearchResult* без логирования действий пользователя.

4. Сохранение *ResearchResult* с логированием действий пользователя.

Общая диаграмма последовательности для экспериментов с логированием и без логирования действий пользователя, представлена на рисунке 5.6.

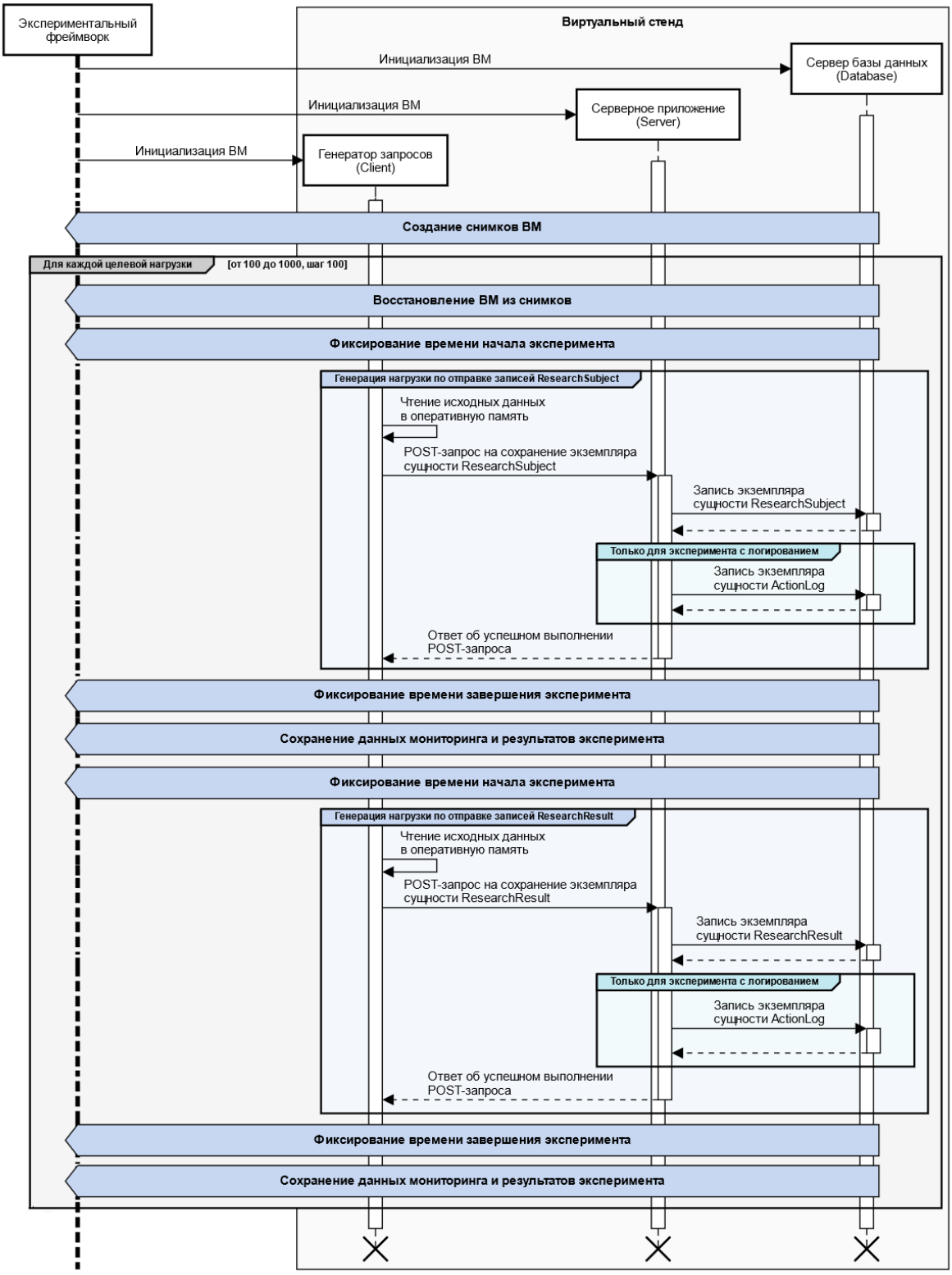


Рисунок 5.6 — Диаграмма последовательности серии нагрузочных испытаний

Каждая серия состояла из 10 нагрузочных испытаний с целевой нагрузкой от 100 до 1000 запросов. В ходе каждого испытания создавались от 20 до 200

виртуальных пользователей Locust с заданной постоянной целевой нагрузкой в 5 запросов в секунду. В случае длительного задержки ответа сервера виртуальный пользователь ожидал ответа перед тем, как отправить следующий запрос. Продолжительность каждого испытания – 10 минут. Испытания для двух типов записей проводились без перезапуска виртуальных машин. Для сбора оценок с разным уровнем целевой нагрузки производилось предварительное восстановление виртуальных машин из предварительно созданных снимков. Для разных настроек серверного ПО виртуальный стенд формировался заново.

Получены результаты нагрузочных испытаний для двух типов записей нагрузки, представленные в таблице 17.

Таблица 17 — Оценки производительности (пропускной способности)

Целевая нагрузка, зап/сек	Пропускная способность, зап/сек			
	Записи *ResearchSubject*		Записи *ResearchResult*	
	Без логирования	С логированием	Без логирования	С логированием
100	100,02	99,87	100,01	99,92
200	200,01	199,89	199,94	185,59
300	299,9	282,37	252,47	216,44
400	400,01	356,87	264,34	217,18
500	492,86	394,56	230,96	210,36
600	589,82	444,82	271,58	223,26
700	637,97	445,61	260,92	216,14
800	675,25	440,74	268,7	210,42
900	748,85	438,07	279,71	211,92
1000	775,43	444,89	265,91	203,74

На рисунке 5.7, приведены полученные значения пропускной способности разработанного метода при сохранении записей *ResearchSubject*, видно, что в случае логирования действий пользователя предельная пропускная способность достигается при целевой нагрузке в 600 запросов в секунду. При логировании производительность модели значительно ниже, чем без него: при нагрузке в 1000 запросов в секунду разница составила 42,62%.

Использование ресурсов центрального процессора при логировании действий пользователя значительно выше (табл. 18), что обуславливает разницу в производительности. Сравнивая данные о нагрузочных испытаниях до достижения предела пропускной способности (целевая нагрузка до 600 запросов в секунду включительно) в одной из конфигураций, можно отметить, что среднее использование ресурсов центрального процессора BM Server при логировании

выше на 48,22%, а для ВМ базы данных – на 83,74%. Из рисунка 5.8 видно, что использование ресурсов центрального процессора ВМ Server не достигает предела выделенных ресурсов. Это связано с тем, что серверное ПО запущено в единственном процессе Node.JS, что не позволяет задействовать более 1 ядра центрального процессора.

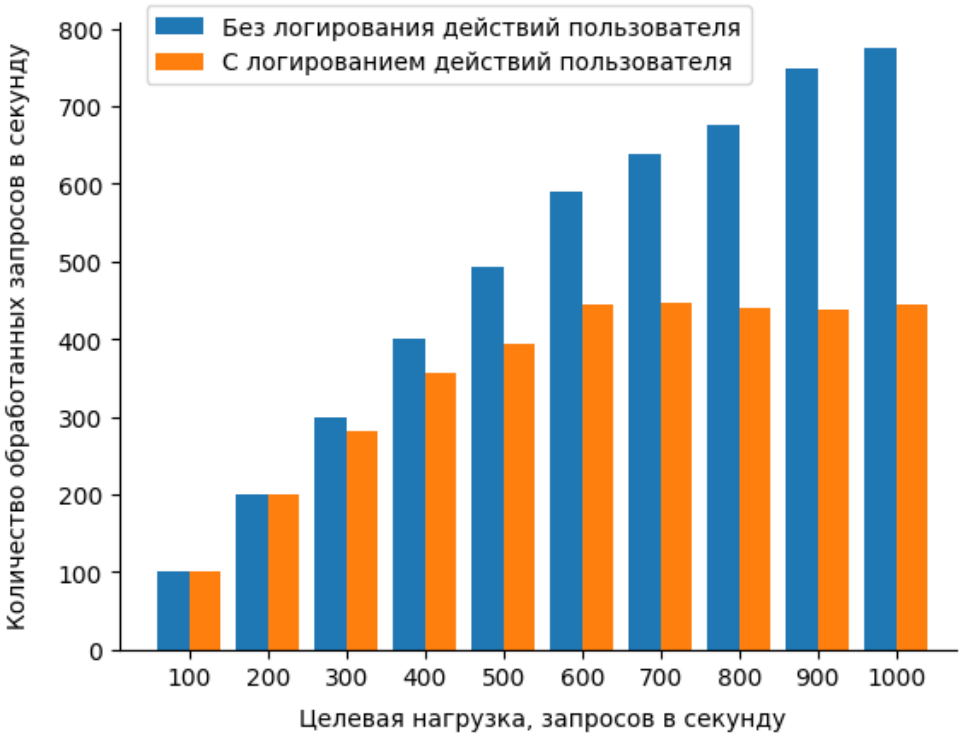


Рисунок 5.7 — Пропускная способность при сохранении записей *ResearchSubject*

Таблица 18 — Оценки использования ресурсов центрального процессора при сохранении записей *ResearchSubject*

Целевая нагрузка, зап/сек	Использование ресурсов центрального процессора			
	Server		Database (MongoDB)	
	Без логирования	С логированием	Без логирования	С логированием
100	25,35	42,88	14,44	29,33
/hline 200	42,04	74,34	25,58	55,24
300	60,86	103,33	36,58	70,46
400	83,47	119,28	48,9	89,96
500	110,31	127,2	57,47	91,64
600	117,54	135,63	65,81	96,97
700	126,12	133,07	70,79	96,3
800	135,06	131,48	75,6	96,37
900	138,85	130,42	73,61	96,17
1000	141,48	131,87	79,36	94,49

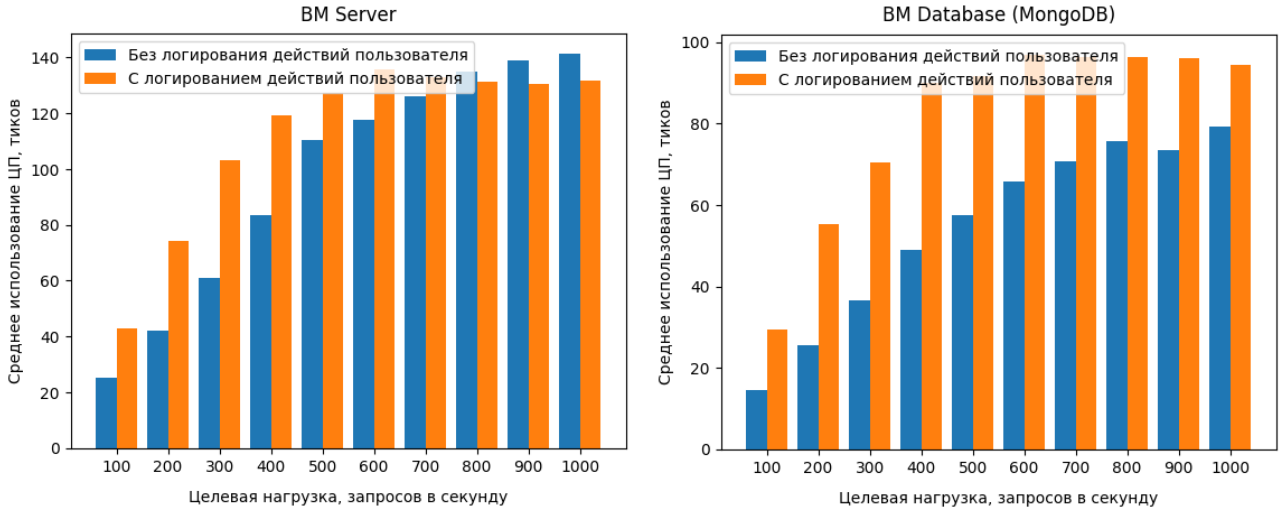


Рисунок 5.8 — Использование ресурсов центрального процессора при сохранении записей *ResearchSubject*

При анализе полученных результатов пропускной способности метода непрерывной аутентификации при сохранении записей *ResearchResult*, представленных на рисунке 5.9, видно, что добавление логирования действий пользователя также снижает производительность модели, однако, ввиду того что записи *ResearchResult* значительно больше по объему, предел достигается уже при целевой нагрузке в 300 запросов в секунду в обоих случаях.

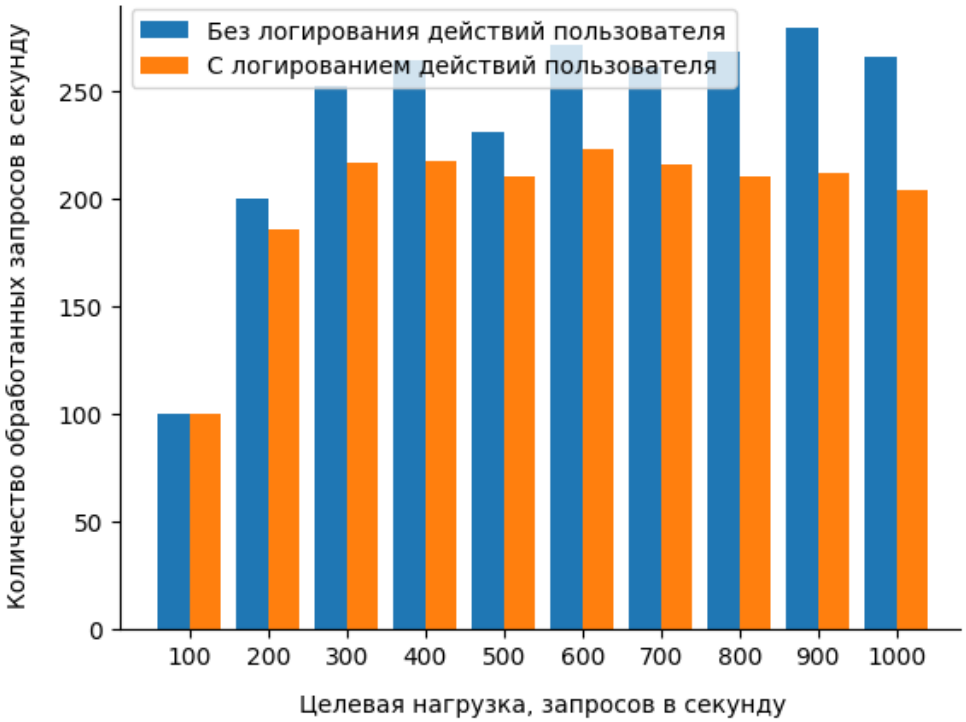


Рисунок 5.9 — Пропускная способность модели при сохранении записей *ResearchResult*

При логировании пропускная способность модели не превышает 224 запроса в секунду, тогда как без него – 280 запросов в секунду. При нагрузке в 1000 запросов в секунду разница в производительности модели составляет 23,38%. Использование ресурсов центрального процессора при логировании действий пользователя также выше, чем без него (табл. 19), что обуславливает разницу в производительности.

Таблица 19 — Оценки использования ресурсов центрального процессора при сохранении записей *ResearchSubject*

Целевая нагрузка, зап/сек	Использование ресурсов центрального процессора			
	Server		Database (MongoDB)	
	Без логирования	С логированием	Без логирования	С логированием
100	52,86	71,21	24,84	40,33
200	103,94	113,97	51,06	67,82
300	119,69	122,55	57,68	72,11
400	122,48	122,02	58,51	70,68
500	117,87	120,22	53,02	69,38
600	122,83	123,63	58,92	69,98
700	121,37	120,59	57,88	69,45
800	122,56	119,51	58,06	68,92
900	123,95	120,31	53,9	69,44
1000	121,33	119,32	56,9	68,92

Сравнивая данные о нагрузочных испытаниях до достижения предела пропускной способности (целевая нагрузка до 300 запросов в секунду включительно) в одной из конфигураций, можно отметить, что среднее использование ресурсов центрального процессора ВМ сервера при логировании выше на 15,58%, а для ВМ базы данных – на 40,06%. На рисунке 5.10 показано, что при достижении предельной пропускной способности затраты ресурсов ВМ Server практически идентичны, так как это предел возможностей для одного процесса Node.JS, но для ВМ Database разница в потребляемых ресурсах сохраняется.

Таким образом, на основе предложенного метода построен экспериментальный стенд, который позволил определить зависимость производительности от ресурсов, выделенных на каждый компонент, реализующий логирование действий пользователей в системах информационной безопасности. В рамках оценки рассмотрены затраты ресурсов центрального процессора и производительность системы в условиях различной нагрузки. Введение логирования действий пользователей повышает затраты ресурсов центрального процессора.

Для более ресурсоемких операций (в рассмотренном эксперименте – сохранение записей *ResearchResult*) логирование может требовать незначительный объем дополнительных ресурсов, в то время как для более тривиальных (сохранение записей *ResearchSubject*) на логирование может требоваться объем ресурсов, сопоставимый с выполнением самой операции.

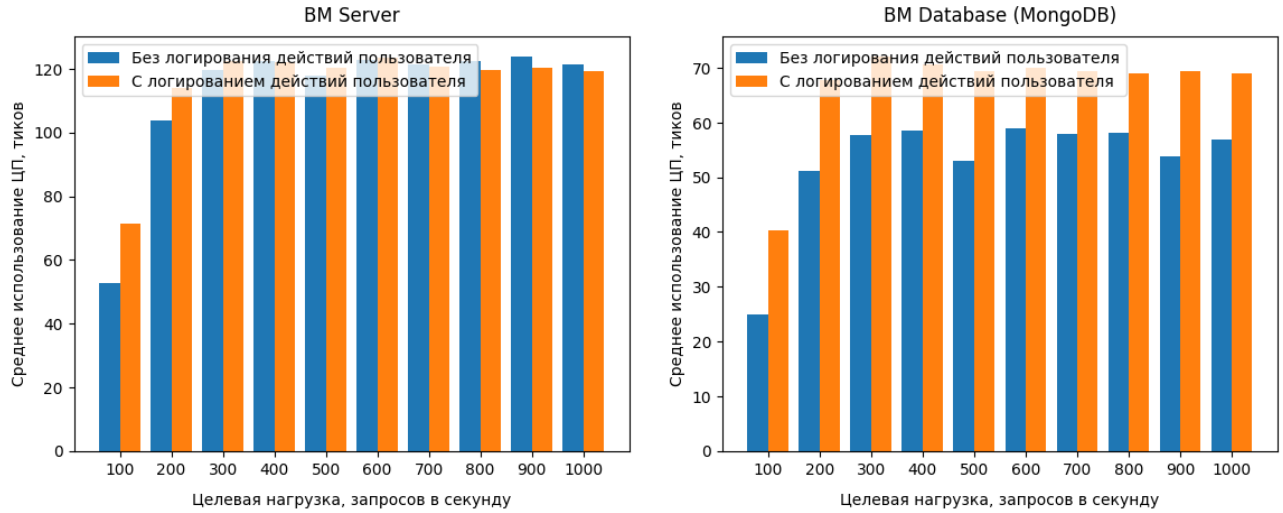


Рисунок 5.10 — Использование ресурсов центрального процессора при сохранении записей *ResearchResult*

Разработанный метод непрерывной аутентификации, реализованный в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределенных информационных системах, не оказывает влияния на производительность и функционирование, используемых систем защиты информации (реализованных защитных мер). Поэтапное повышение нагрузки с последующим сбором оценок позволяют определить уровень производительности реализованных защитных мер при выделенных вычислительных ресурсах, а средства мониторинга – выявить требуемый компонентами системы информационной безопасности объем ресурсов.

Полученные количественные значения оценки эффективности реализации защитных мер на основе анализа затрат ресурсов позволили перейти к разработке и реализации научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды.

5.2 Научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды

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 образовательный вычислительный сервис организаций высшего образования. Обобщенная схема разработанных предложений по практической реализации научно-методического аппарата представлена на рисунке 5.11.

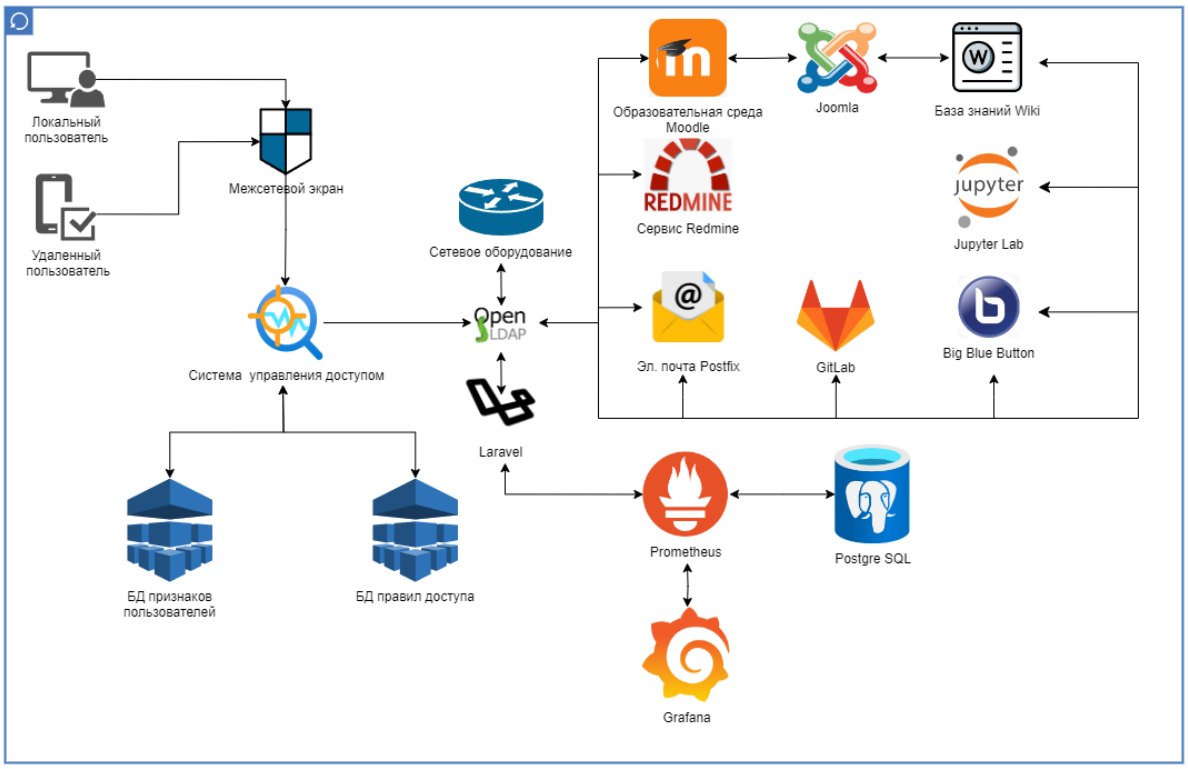


Рисунок 5.11 — Обобщенная схема разработанных предложений по практической реализации научно-методического аппарата

В состав сформированных предложений для реализации научно-методического аппарата риск-ориентированного атрибутивного управления входят: модуль сбора метрик и мониторинга систем Prometheus-Grafana, система управления контентом Joomla, фреймворк для разработки веб-приложений Laravel, платформа для создания и управления вики-сайтами MediaWiki, система для

совместной работы, хранения и обмена файлами Nextcloud, веб-сервер Nginx-PHP-FastCGI, система управления реляционными базами данных PostgreSQL, веб-приложение для управления проектами Redmine, система управления контентом WordPress и платформа проведения дистанционных занятий Moodle.

Prometheus-Grafana: используется для сбора метрик и мониторинга систем, а Grafana – для визуализации этих данных. Prometheus может интегрироваться с большинством веб-сервисов и серверов баз данных для сбора метрик. Grafana использует эти данные для создания дашбордов. Основная цель использования – мониторинг доступности и производительности веб-платформ СДО, анализ пользовательской активности и ресурсов сервера.

Достоинства:

- Подробный мониторинг: отслеживание производительности и доступности сервисов в реальном времени.
- Гибкая визуализация: настройка дашбордов для различных метрик и индикаторов безопасности.
- Тревоги: возможность настройки оповещений о критических изменениях или аномалиях.

Недостатки:

- Сложность в настройке: требует глубоких технических знаний для эффективного использования.
- Ограниченная функциональность управления доступом: не является инструментом для прямого управления доступом к ресурсам.

Joomla – система управления контентом (CMS, Content Management System), используемая для создания и управления веб-сайтами. Взаимодействие с другими сервисами: Joomla может интегрироваться с базами данных (например, PostgreSQL), системами аутентификации (OpenLDAP) и расширениями для различных функций. В СДО применяется для создания образовательных веб-сайтов, управление контентом курсов, публикацией материалов и информационных ресурсов.

Достоинства:

- Гибкая система управления контентом: удобный интерфейс для создания и управления содержимым сайта.
- Расширяемость: большое количество плагинов и тем для улучшения функциональности.

- Управление доступом: возможность настройки уровней доступа для разных пользователей.

Недостатки:

- Потенциальные проблемы безопасности: уязвимости, связанные с плагинами и сторонними компонентами.
- Требовательность к ресурсам сервера, особенно при использовании множества расширений.

Laravel – фреймворк для разработки веб-приложений на языке PHP (Hypertext Preprocessor). Взаимодействие с другими сервисами: Laravel может использоваться вместе с веб-серверами (например, Nginx), базами данных (PostgreSQL) и системами аутентификации (OpenLDAP). В СДО используется для разработки настраиваемых веб-приложений, управления курсами, регистрации пользователей и интерактивных элементов обучения.

Достоинства:

- Современная архитектура: MVC-паттерн обеспечивает четкую организацию кода.
- Встроенные средства безопасности: хорошая поддержка аутентификации и защиты данных.
- Расширяемость и гибкость: подходит для создания разнообразных веб-приложений.

Недостатки:

- Кривая обучения: требуется время для освоения фреймворка.
- Зависимость от экосистемы Laravel: необходимость использования определенных пакетов и инструментов.

MediaWiki – платформа для создания и управления вики-сайтами. MediaWiki может интегрироваться с различными серверами баз данных и системами аутентификации. Применяется для создания образовательной базы знаний для студентов и преподавателей, управления документацией и учебными материалами.

Достоинства:

- Мощный инструмент для совместной работы над документами.
- Широкие возможности кастомизации и расширения функционала.
- Поддержка истории изменений и версионности документов.

Недостатки:

- Интерфейс может показаться неинтуитивным новым пользователям.
- Требует тщательной настройки прав доступа и безопасности.

Nextcloud – платформа, которая предлагает решения для совместной работы, хранения и обмена файлами. Может быть интегрирована в LDAP/AD (Lightweight Directory Access Protocol/Active Directory) для аутентификации и серверами баз данных для хранения информации. В структуре СДО – это платформа для совместной работы студентов и преподавателей, хранения и обмена учебными материалами.

Достоинства:

- Широкий набор функций для совместной работы и обмена файлами.
- Возможность интеграции с множеством внешних сервисов и приложений.
- Высокий уровень контроля над данными и их безопасностью.

Недостатки:

- Может требовать значительных ресурсов сервера при большом количестве пользователей.
- Некоторые функции могут быть излишне сложными для простых пользовательских задач.

Nginx-PHP-FastCGI – веб-сервер, используемый для размещения веб-сайтов и веб-приложений. PHP-FastCGI обеспечивает обработку PHP-скриптов. Nginx часто используется в сочетании с PHP-приложениями (например, WordPress, Joomla), поддерживает взаимодействие с системами баз данных и аутентификации. Использование в СДО: размещение и обслуживание веб-сайтов и платформ СДО, обеспечение быстрой и надежной доставки контента пользователям.

Достоинства:

- Высокая производительность и надежность в обслуживании веб-сайтов.
- Гибкость в настройке сервера под различные нужды и окружения.
- Хорошая поддержка современных веб-технологий.

Недостатки:

- Конфигурация может быть сложной, особенно для начинающих пользователей.
- Требует регулярного обслуживания и обновления для поддержания безопасности.

OpenLDAP – реализация протокола LDAP, предназначенная для управления учетными записями и идентификацией пользователей, интеграция с веб-приложениями, CMS и базами данных для единой аутентификации и управления правами доступа. Использование в СДО: централизованное управление учетными записями студентов и преподавателей, интеграция с образовательными платформами для единого входа.

Достоинства:

- Централизованное управление учетными записями и политиками доступа.
- Хорошо масштабируется и поддерживает большое количество записей.
- Гибкость в настройке и интеграции с другими системами.

Недостатки:

- Сложность настройки и администрирования, особенно в больших организациях.
- Может потребовать дополнительного обучения администраторов.

PostgreSQL: система управления реляционными базами данных. Взаимодействие с другими сервисами: может использоваться с любым веб-приложением или CMS, поддерживающим реляционные базы данных. Использование в СДО: хранение данных об учебных курсах, пользовательских данных, результатов тестов и другой информации СДО.

Достоинства:

- Надежность и мощные функции управления данными.
- Поддержка сложных запросов и транзакций.
- Высокий уровень безопасности и управления доступом к данным.

Недостатки:

- Может быть излишне сложным для простых приложений.
- Необходимость регулярного обслуживания базы данных для оптимальной производительности.

Redmine: веб-приложение для управления проектами, интеграция с системами контроля версий, базами данных и системами аутентификации. Использование в СДО: управление образовательными проектами, планирование заданий и отслеживание прогресса студентов в рамках курсов.

Достоинства:

- Функциональная система управления проектами с поддержкой трекера задач и документации.
- Гибкость в настройке рабочих процессов и управлении доступом.
- Поддержка плагинов для расширения функциональности.

Недостатки:

- Интерфейс может показаться устаревшим.
- Требует времени для настройки и освоения системы.

WordPress – система управления контентом, легко интегрируется с различными плагинами, темами, базами данных и системами аутентификации. Использование в СДО: создание отдельных тем занятий, курсовых проектов, информационных порталов и образовательных веб-сайтов, публикация учебных материалов и ведение онлайн-журналов

Достоинства:

- Широкие возможности для создания и управления контентом.
- Огромное сообщество и множество доступных плагинов и тем.
- Доступность и простота использования для пользователей всех уровней.

Недостатки:

- Уязвимости безопасности, особенно связанные с плагинами и темами.
- Потенциальные проблемы производительности при неправильной настройке или использовании большого количества плагинов.

Moodle – платформа проведения дистанционных занятий в СДО, интегрируется с системами аутентификации, базами данных и различными плагинами и модулями. Использование в СДО: создание и управление онлайн-курсами, проведение тестирований и опросов, форумы для обсуждений и групповая работа.

Достоинства:

- Широкие возможности для дистанционного обучения и создания образовательного контента.
- Поддержка различных типов активностей и ресурсов для курсов.
- Гибкость в настройке прав доступа и возможностей для пользователей.

Недостатки:

- Интерфейс может быть сложен для новых пользователей.
- Требует регулярного обновления и поддержки для обеспечения безопасности и стабильности.

Для оценки возможности практической реализации разработанного научно-методического аппарата риск-ориентированного атрибутивного управления доступом осуществлена оценка эффективности внедрения разработанных научно-технических предложений в существующую систему управления доступом системы дистанционного образования (СДО) РТУ МИРЭА.

Основной целью проводимых экспериментов является подтверждение соответствия разработанной системы управления доступом требованиям современного дистанционного образования, способности обеспечивать безопасность данных и доступ, а также проведение нагрузочного тестирования для установления значений производительности используемых сервисов безопасности и их совместного функционирования. Проверка позволит выявить потенциальные уязвимости и недостатки системы при ее непосредственном использовании в существующей СДО РТУ МИРЭА.

Эксперименты направлены на проверку следующих направлений:

- Интеграция разработанного научно-методического аппарата управления доступом на основе анализа рисков и динамически изменяющихся атрибутов доступа в существующую систему дистанционного образования вуза: оценка гладкости интеграции и удобства использования сервисов, используемых и планируемых к внедрению в РТУ МИРЭА для осуществления образовательного процесса: Joomla, Moodle, WordPress и сервисами централизованного управления доступом и идентификацией, такими как OpenLDAP. Например: проверка единого входа (Single Sign-On) для Moodle и WordPress, использующего учетные данные из OpenLDAP.

- Безопасность и управление доступом: проверка надежности механизмов аутентификации и авторизации, а также способности разработанных подходов адекватно реагировать на угрозы безопасности.
- Оценка эффективности работы научно-методического аппарата в реальных условиях системы дистанционного обучения: оценка стабильности работы системы управления доступом при различных нагрузках, проверка производительности ключевых компонентов, таких как базы данных и веб-серверы.
- Проверка совместимости научно-методического аппарата с различными сервисами и компонентами, используемыми в системе дистанционного образования (prometheus-grafana, django, joomla, laravel, mediawiki, nextcloud, nginx-php-fastcgi, openldap, postgresql, redmine, wordpress, moodle).
- Сбор метрик и данных для анализа достижения целей по повышению безопасности и гибкости управления доступом в системе дистанционного образования.

Для оценки результатов экспериментов будут использоваться следующие показатели:

- Уровень интеграции: успешная связь и совместимость различных компонентов системы.
- Безопасность данных и доступа: отсутствие уязвимостей в механизмах аутентификации и авторизации, эффективность системы защиты от внешних атак. Например: имитация попыток несанкционированного доступа к административным разделам Joomla, используя различные методы атак.
- Стабильность и производительность: минимальное время отклика сервисов, отсутствие сбоев или простоев при максимальных нагрузках. Например: моделирование пиковой нагрузки на сервер Moodle с одновременным доступом большого числа пользователей.

Описание исходных данных обеспечит структурированный и объективный подход к оценке функциональности и надежности интегрированной системы управления доступом в рамках СДО и возможность воспроизвести описанные эксперименты. Исходные данные для экспериментов включают в себя:

– Конфигурации сервисов: полный список настроек каждого сервиса, включая информацию об интеграции и параметрах безопасности. Например: конфигурации доступа в Joomla, настройки LDAP в Moodle.
– Тестовые сценарии: сценарии, охватывающие стандартные и критические ситуации использования системы, включая авторизацию пользователей, доступ к ресурсам и управление контентом. Например: регистрация нового пользователя через OpenLDAP и доступ к курсам в Moodle.
– Данные о пользователях: информация о тестовых пользователях, включая различные роли и уровни доступа. Пример: аккаунты студентов, преподавателей и администраторов.
– Инструменты мониторинга: набор инструментов для отслеживания производительности системы, таких как Prometheus и Grafana. Пример: настройка дашбордов для мониторинга нагрузки на серверы и время отклика сервисов.
– Критерии оценки безопасности: спецификации и требования безопасности, которым должна соответствовать система. Пример: соответствие GDPR, проверка на уязвимости с помощью специализированного ПО.
– Разработанный научно-методический аппарат управления доступом на основе анализа рисков и динамически изменяющихся атрибутов доступа.
– Данные о текущем состоянии безопасности и управления доступом в системе дистанционного образования (журналы аудита, статистика инцидентов безопасности, отчеты о рисках и уязвимостях).

Метрики оценки достижения целей:

1. Успешность интеграции научно-методического аппарата в существующую систему дистанционного образования и его совместимость с различными сервисами и компонентами.
2. Изменение уровня рисков и количества инцидентов безопасности, связанных с управлением доступом, после внедрения научно-методического аппарата.
3. Гибкость и эффективность управления доступом с использованием научно-методического аппарата (время реакции на изменения атрибутов доступа, возможность динамического изменения политик доступа).

4. Удовлетворенность пользователей и администраторов системы дистанционного образования новым подходом к управлению доступом (опросы, отзывы, статистика использования).
5. Производительность и нагрузка на систему дистанционного образования после внедрения научно-методического аппарата (метрики мониторинга, времена отклика, пропускная способность).

Результаты эксперимента будут проанализированы и использованы для дальнейшего совершенствования научно-методического аппарата и повышения безопасности системы дистанционного образования вуза. Для создания интегрированной системы управления доступом в СДО были разработаны практические решения в следующих направлениях:

- Централизованное управление и анализ рисков: использование Prometheus и Grafana для мониторинга всей сетевой инфраструктуры, включая веб-сервисы и серверы баз данных. OpenLDAP используется для централизованного управления учетными записями и интеграции с Joomla, Moodle и другими CMS.
- Управление доступом и безопасность: настройка Nginx для безопасного доступа к веб-приложениям, интеграция с PHP-FastCGI для эффективной обработки запросов. Laravel может использоваться для разработки пользовательских веб-приложений, с интеграцией в систему управления базами данных PostgreSQL и учетными записями через OpenLDAP.
- Управление документами и совместная работа: использование MediaWiki и Nextcloud для хранения и обмена документами, включая возможности совместной работы и контроля версий. Разделение доступа и управление правами пользователей через интеграцию с OpenLDAP.
- Управление проектами и контентом: Redmine для управления проектами и задачами, интегрированное с OpenLDAP для управления пользователями. Joomla, WordPress и Moodle используются для создания и управления контентом образовательного портала, с интеграцией управления доступом и безопасности через централизованные системы.

5.3 Оценка эффективности разработанного научно-методического аппарата риск-ориентированного атрибутивного управления доступом

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. 5.12) в "Подсети-1" и "Подсети-2" с задействованием центра безопасности операций.

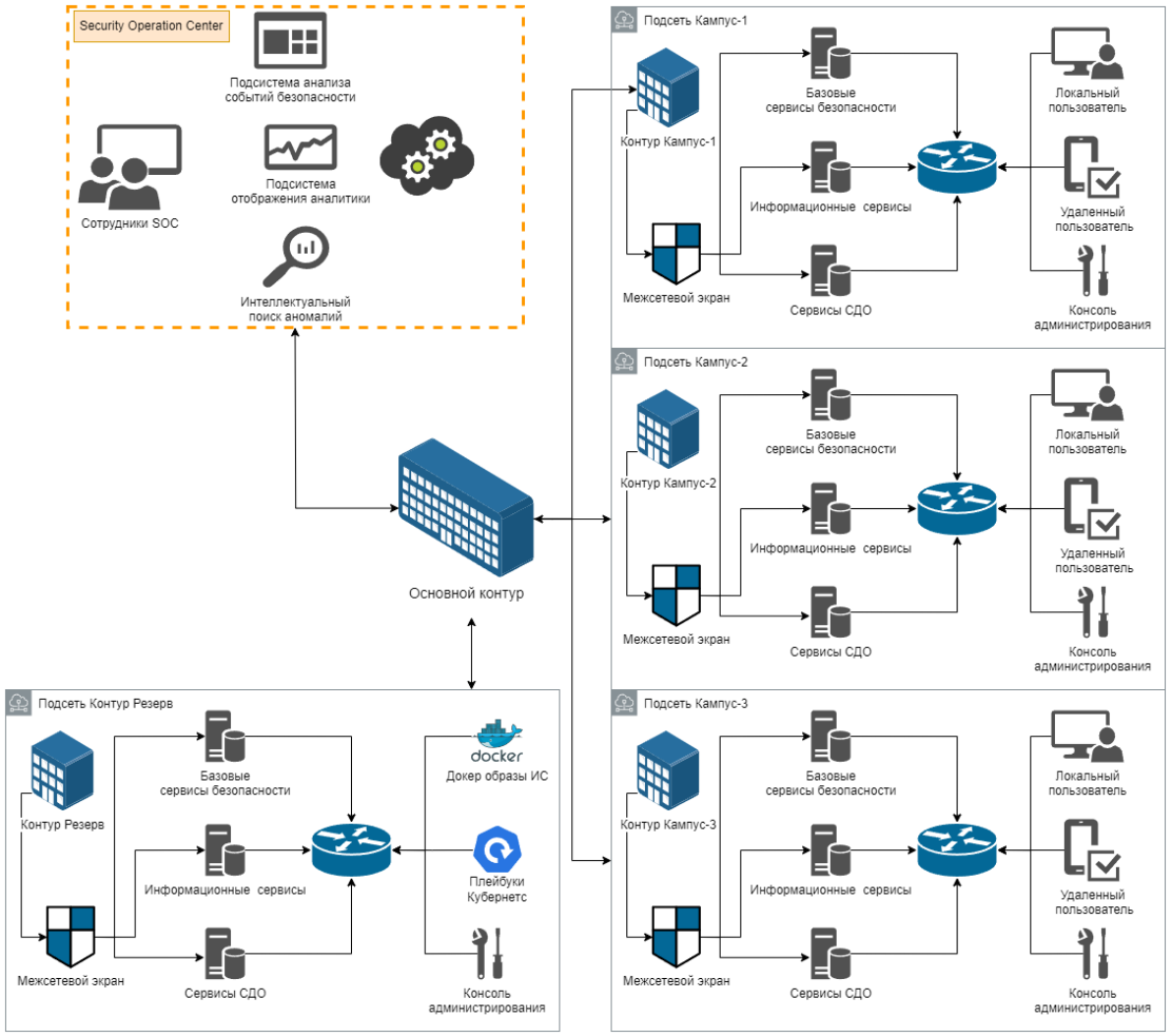


Рисунок 5.12 — Обобщенная схема системы дистанционного образования РТУ МИРЭА

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 5.13 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.

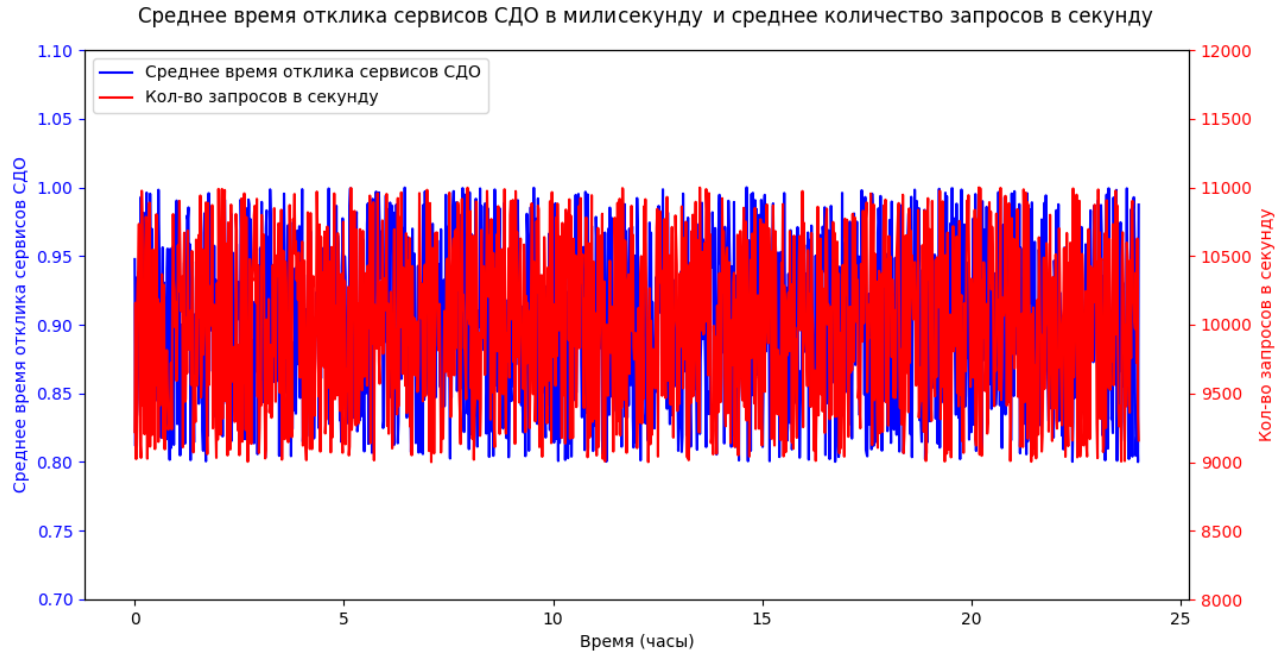


Рисунок 5.13 — Тестирование разработанной системы управления доступом в СДО МИРЭА

В ходе дальнейшей оценки эффективности разработанного научно-методического аппарата проанализированы риски реализации угроз, атрибутов безопасности, производительность и масштабируемость, а также возможности по мониторингу и формирования отчетности.

5.3.1 Анализ показателей риска, безопасности и атрибутов

Анализ рисков является составной частью любой системы управления доступом. Он включает в себя идентификацию потенциальных рисков и уязвимостей в системе и оценку вероятности и последствий этих рисков. В контексте разработанной системы управления доступом в СДО риски могут включать несанкционированный доступ к конфиденциальным данным

студентов/преподавателей, утечку образовательных данных или нарушение конфиденциальности. Для оценки рисков были предприняты следующие шаги:

1. определены потенциальные риски и уязвимости системы в рамках модели нарушителя и модели безопасности СДО;
2. определены вероятности и последствия этих рисков;
3. проверена способность системы управления доступом обнаружить и реагировать на эти риски;
4. оценена эффективность стратегий минимизации рисков системы.

В рамках тестирования была проведена проверка функциональности системы по анализу рисков, определены различные сценарии, в которых могут возникнуть риски, связанные с несанкционированным доступом к данным, утечкой информации или нарушением конфиденциальности. Система успешно выявила все рассмотренные сценарии риска, при этом функционирование системы происходило в штатном режиме без снижения среднего времени отклика сервисов СДО [297].

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 5.14.

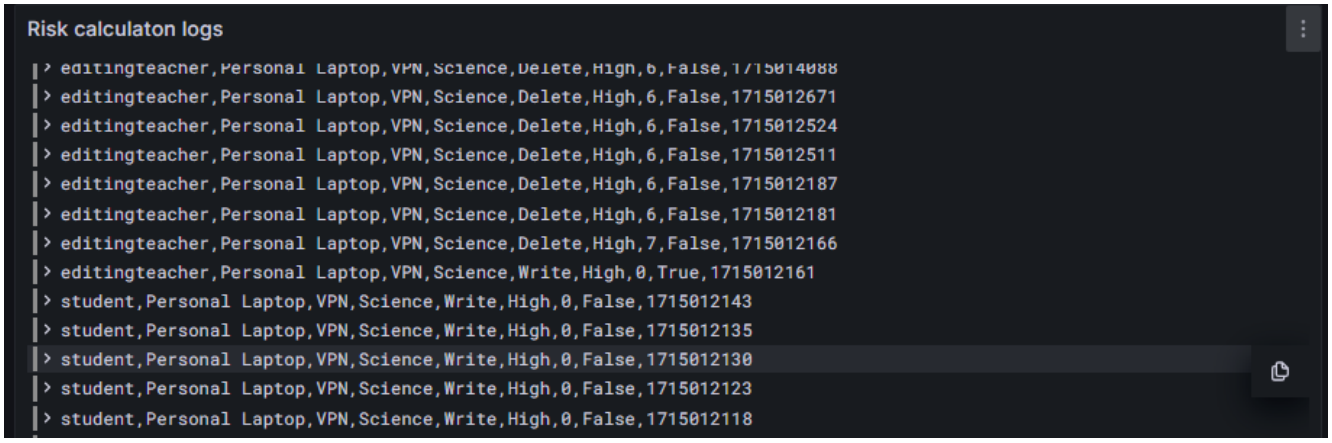


Рисунок 5.14 — Результаты мониторинга и отображения данных о текущем значении риска разработанной системы управления доступом

Помимо расчета значений риска для каждого запроса доступа субъекта к объекту системы управления доступом осуществляется логирование всех полученных атрибутов от агентов сбора данных (рис. 5.15).

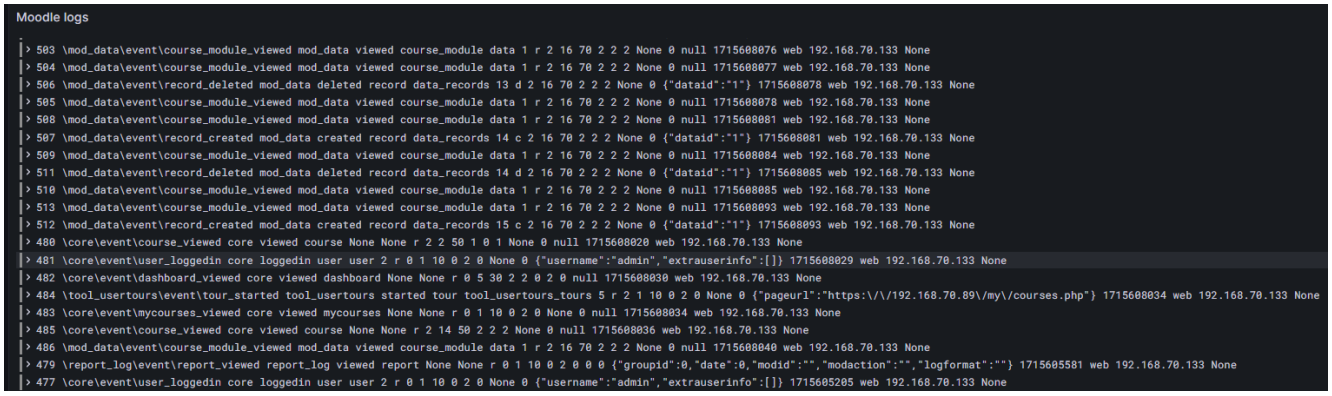


Рисунок 5.15 — Логирование атрибутов, полученных от агентов сбора данных

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). Для проверки способности системы обрабатывать динамические атрибуты были предприняты следующие шаги:

1. определены наиболее значимые динамические атрибуты, которые имеют значение для системы;
2. проверена способность системы обнаруживать аномалии и реагировать на изменения этих атрибутов;
3. оценена эффективность политик управления доступом на основе динамических атрибутов.

Например, если местоположение пользователя является значимым динамическим атрибутом, система отслеживает изменения местоположения пользователя и корректирует доступ к ресурсам в соответствии с политиками управления доступом.

Система управления доступом успешно продемонстрировала свою способность изменять динамические атрибуты доступа в зависимости от контекста и ситуации. 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 заданны-

ми критериями. Одним из элементов динамических атрибутов является модель поведения пользователя [298].

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:

1. Клик (нажатие на кнопку, значок или область) по элементу.
2. Переход по ссылке.
3. Заполнение форм или отдельных полей.
4. События аутентификации.

Однако данный список сильно упрощен, так как, при должном уровне технического вмешательства, возможно отслеживать любые события в браузере. Мониторинг действий на веб-странице возможно проводить несколькими способами:

1. Первый способ – внедрение на веб-странице специального скрипта для прослушивания определенных событий на странице, как в примере с interactor. Такой подход является наиболее простым, но также менее удобным для обработки и настройки, так как передаваться будут все события с перечисленным типом. Все события затем передаются на сервер мониторинга для хранения и последующей обработки.
2. Второй способ – установка прослушивания на определенные элементы на странице и сбор событий с них. Например, установить прослушивание событий с кнопки для передачи введенных значений. Такой способ более сложен с точки зрения имплементации, однако предлагает наиболее гибкую настройку собираемых событий, если их перечень ограничен.

Во всех случаях подразумевается внедрение нового кода в структуру приложения. Как правило, для первого способа необходимо внедрение JS (JavaScript) кода на корневом уровне HTML (HyperText Markup Language) страницы. Для второго же требуется модификация всех точек сбора данных и дополнительный импорт кода для передачи данных к каждому файлу, содер-

жащему анализируемый HTML компонент. Передача событий осуществляется посредством отправки HTTP запросов. Со стороны сервера предусмотрена схема передачи и соответствующий интерфейс API. Пример интерфейса REST API, /monitoring/event, включающий исчерпывающий набор полей для последующей обработки в соответствии со схемой, представленной в листинге 5.5:

Листинг 5.5: Пример интерфейса REST API /monitoring/event

```
{
        "user_session_id": "1234567abcd",
        "user_id": "123",
        "user_source_ip": "1.2.3.4",
        "event_type": "btn-click",
        "event_message": "clicked button 1 time",
        "event_element": "#sidebar-quicklinks > nav > div > div.sidebar-body >
        > ol > ol > li:nth-child(9) > em > a",
        "event_timestamp_unix": "1712149848"
}
```

Для внутренних переходов предусмотрена схема, представленная в листинге 5.6 и интерфейс /monitoring/href:

Листинг 5.6: Пример интерфейса REST API /monitoring/href

```
{
        "user_session_id": "1234567abcd",
        "user_id": "123",
        "user_source_ip": "1.2.3.4",
        "redirect_source": "https://example.com/page1",
        "redirect_target": "https://example.com/page2",
        "event_message": "user redirected",
        "event_element": "#sidebar-quicklinks > nav > div > div.sidebar-body >
        > ol > ol > li:nth-child(9) > em > a",
        "event_timestamp_unix": "1712149848"
}
```

Для последующей обработки событий от сенсоров применяется токенизация пользовательского ввода. Например, события нажатия на определенный элемент на странице будут токенизированы меткой "А", а событие отправки формы будет токенизировано меткой "Б". Затем, используя алгоритмы машинного обучения, в частности выполняя процедуру эмбеддинга с применением словарей, создаются векторы пользовательских действий на веб-странице и анализируются на наличие определенных поведенческих признаков.

Для событий открытия или закрытия страницы также существуют события JS, которые отслеживаются на интерфейсе /monitoring/visits, листинг 5.7:

Листинг 5.7: Пример интерфейса REST API /monitoring/visits

```
"user_session_id": null,
"user_id": null,
"user_source_ip": "1.2.3.4",
"page_url": "https://example.com/init_page",
"event_message": "new user visited the website",
"event_timestamp_unix": "1712149848"
```

Для создания такого вектора из базы данных событий извлекаются последовательности из одной сессии и кодируются события из них в едином формате. Также для составления полной истории действий пользователя можно использовать данные из всех источников событий, отфильтрованных по IP-адресу или ID пользователя. Для хранения пользовательских сессий на веб-странице используется несколько общепринятых подходов:

1. Доступные на стороне клиента:
   - local storage – хранит пользовательские данные в локальном хранилище браузера (не очищается при закрытии);
   - session storage – хранит пользовательские данные в сессионном хранилище браузера (очищается при закрытии сессии/браузера/вкладки).
2. Доступные на стороне сервера:
   - cookie header – хранит пользовательские данные в cookie хранилище браузера, управляется сервером.

В каждом случае для отслеживания пользовательской сессии используется сессионный идентификатор, такой как, например, ID сессии или пользователя. Возможно также отслеживать сессию по полному значению ключа, в случае, если он не модифицируется. Кроме сессии, для идентификации пользователя также используется IP-адрес или цифровой отпечаток браузера (с помощью библиотеки fingerprintjs). Для более тонкого наблюдения за перемещением пользователя по странице необходимо отслеживать положение указателя на странице. Сбор таких событий реализован с помощью браузерного события mousemove. Следующий элемент скрипта непрерывно отслеживает положение курсора на странице:

```
{
        addEventListener("mousemove", (event) => {
                let x = event.pageX;
                let y = event.pageY;
        })
}
```

Обработчик данных событий размещается на корневом элементе и осуществляет мониторинг всех событий данного типа на странице. Постоянно собирая изменения в позиции курсора и периодически отправляя их на сервер управления возможно построить карту перемещения курсора пользователя, пример представлен на рисунке 5.16:

Рисунок 5.16 — Карта перемещения курсора пользователя для создания модели поведения пользователя

Каждый пользователь имеет уникальную карту движения курсора мыши в виду наличия индивидуальных психологических и биологических особенностей. Данная модель имитирует цифровой отпечаток, наподобие отпечатка пальцев в дактилоскопии. Добавив несколько дополнительных фильтров для извлечения необходимых последовательностей для пользовательских сессий, возможно более тонко изучать поведения отдельных пользователей в 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 на основе нечеткой логики 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:

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

База данных политик: база данных политик содержит правила и политики доступа, которые используются для принятия решений о доступе. Агенты сбора данных передают информацию о различных факторах риска. Далее модуль оценки риска использует нечеткую логику для оценки уровня риска с помощью информации, полученной от сенсоров риска. Этот модуль выявляет значение уровня риска: низкое, среднее или высокое. Следующий модуль – модуль принятия решений использует полученные результаты оценки риска и политики доступа для принятия решений о доступе к ресурсам.

Выдача доступа производится в соответствии с заданными политиками доступа. В результате, риск-ориентированная модель на основе нечеткой логики позволяет найти баланс между безопасностью и доступностью услуг. Проведя анализ существующих решений было выявлено, что программных реализаций риск-ориентированных моделей управления доступом не представлено. Наиболее близкой к теме исследований является фреймворк атрибутного управления доступом на основе стандарта XACML. Необходимость практической реализации обусловлена потребностью в универсальном решении с целью создания простого и удобного механизма управления доступом. Были выдвинуты функциональные и нефункциональные требования к разрабатываемому решению.

К программной реализации метода управления доступом были выдвинуты следующие требования:

Функциональные требования:

1. Аутентификация и авторизация: реализация возможности регистрации и аутентификации пользователей и гибкая система управления доступом на основе ролей пользователей.
2. Управление данными: функционал Create-Read-Update-Delete (создание, чтение, обновление, удаление) данных в базе MongoDB и применение политик риск-ориентированной модели управления доступом для безопасного доступа к данным.
3. Взаимодействие с файлами: возможность загрузки и хранения файлов в базе данных MongoDB и редактирования хранящихся внутри MongoDB файлов.

Нефункциональные требования:

1. Безопасность: гарантированная защита данных с использованием механизмов шифрования и аутентификации и соблюдение стандартов безопасности при работе с чувствительной информацией.
2. Производительность: высокая скорость обработки запросов и отзывчивость системы и оптимизированные запросы к базе данных для уменьшения нагрузки.
3. Масштабируемость: возможность горизонтального масштабирования для обработки роста нагрузки и эффективное управление ресурсами для обеспечения стабильной работы при росте пользовательской базы.
4. Надежность: гарантированная доступность приложения и целостность данных и резервное копирование данных и мониторинг работоспособности системы.
5. Интеграция: возможность интеграции приложения в уже существующие системы

Научно-методический аппарат реализован на базе фреймворка Flask, в качестве хранилища данных используется MongoDB, хранящая события, которые анализируются в ходе реализаций политик управления доступом на основе фреймворка Py-ABAC (рис. 5.17). [299].

Рисунок 5.17 — Структурная схема реализации риск-ориентированной атрибутивной модели научно-методического аппарата исследования

Выбор Flask в качестве фреймворка для создания API объясняется его простотой в использовании, а также гибкостью и расширяемостью. Flask, как микрофреймворк, обладает минималистичной структурой, что увеличивает скорость развертывания сервисов. Также Flask обладает возможностью простой и удобной интеграции сторонних библиотек. В качестве хранилища данных выбрана MongoDB. Основным аргументом ее применения является документо-ориентированная структура, которая позволяет хранить информацию в формате документов, что упрощает работу с данными. Для обработки одной транзакции – в данном случае процесс принятия решения займет кратно больше времени.

В Py-ABAC определяются политики, содержащие условия для одного или нескольких атрибутов этих четырех элементов. Если эти условия удовлетворены, решение о доступе возвращается PDP с использованием алгоритма оценки. Поддерживаются три различных алгоритма оценки:

– AllowOverrides: возвращается allow если какое-либо решение оценивается как allow; и возвращает значение deny, если все решения оцениваются как deny;
– DenyOverrides: возвращается deny если какое-либо решение оценивается как deny; возвращается allow, если все решения оцениваются как allow;
– HighestPriority: возвращает решение с наивысшим приоритетом, которое оценивается как allow или deny. Если существует несколько конфликтующих решений с одинаковым наивысшим приоритетом, то DenyOverrides алгоритм будет применяться среди этих решений с наивысшим приоритетом.

Политика состоит из следующих полей: uid, description, rules, targets, effect, priority. Схема JSON задается массивом: *"uid": <string>, "description": <string>, "rules": <rules_block>, "targets": <targets_block>, "effect": <string>, "priority": <number>*, где *<rules_block>* и *<targets_block>* – блоки JSON. По сути, поля "targets" и "rules" используются для определения условий атрибутов

элементов управления доступом. Если эти условия удовлетворены, применяется политика и значение поля "effect" возвращается методом PDP. Таким образом, "effect" это возвращаемое решение политики, которое может быть либо "allow" или "deny". Поле "uid" представляет собой строковое значение, которое однозначно идентифицирует политику. Как следует из названия, в этом "description" поле хранится описание политики, "priority" предоставляет числовое значение, указывающее вес политики, когда ее решение конфликтует с другой политикой в рамках HighestPriority алгоритма оценки. По умолчанию это поле установлено 0 для всех политик.

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 все возможные варианты доступа к ресурсам СДО, фрагмент расчета представлен на рисунке 5.18.

```
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Management', 'Risk-Adaptive'), Risk Score: 1.95
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Management', 'Behaviour'), Risk Score: 2.2
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Security', 'Base'), Risk Score: 1.8
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Security', 'Risk-Adaptive'), Risk Score: 2.05
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Security', 'Behaviour'), Risk Score: 2.3
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Accountant', 'Base'), Risk Score: 1.9
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Accountant', 'Risk-Adaptive'), Risk Score: 2.15
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Accountant', 'Behaviour'), Risk Score: 2.4
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Infrastructure', 'Base'), Risk Score: 2.0
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Infrastructure', 'Risk-Adaptive'), Risk Score: 2.25
Combination: ('Manager', 'Internet', 'Work PC', 'Create', 'Infrastructure', 'Behaviour'), Risk Score: 2.5
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Teaching', 'Base'), Risk Score: 0.75
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Teaching', 'Risk-Adaptive'), Risk Score: 1.0
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Teaching', 'Behaviour'), Risk Score: 1.25
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Science', 'Base'), Risk Score: 0.85
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Science', 'Risk-Adaptive'), Risk Score: 1.1
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Science', 'Behaviour'), Risk Score: 1.35
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Management', 'Base'), Risk Score: 0.95
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Management', 'Risk-Adaptive'), Risk Score: 1.2
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Management', 'Behaviour'), Risk Score: 1.45
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Security', 'Base'), Risk Score: 1.05
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Security', 'Risk-Adaptive'), Risk Score: 1.3
Combination: ('Manager', 'VPN', 'Personal laptop', 'Read', 'Security', 'Behaviour'), Risk Score: 1.55
```

Рисунок 5.18 — Просчет возможных комбинаций атрибутов доступа и определение граничных значений для политик управления доступом

Стоит отметить, что модель поведения пользователя системы включает в себя ряд признаков:

1. Статистика динамики набора текста: время, необходимое для нажатия и отпускания клавиш, давление на клавиши и ритм набора текста могут

быть использованы для идентификации уникальных шаблонов набора каждого пользователя.

2. Статистика движений мыши: способ перемещения мыши пользователем, включая скорость, ускорение и направление движения, может использоваться для создания уникального поведенческого профиля.
3. Статистика взаимодействия с экраном касания: способ взаимодействия пользователя с экраном касания, включая давление, шаблоны прокрутки и шаблоны нажатий, может использоваться для создания уникального поведенческого профиля.
4. Контекстная информация окружения: местоположение, время суток и другие факторы окружающей среды могут использоваться для создания уникального поведенческого профиля для каждого пользователя.
5. Статистика использования приложений: способ взаимодействия пользователя с различными приложениями, включая частоту и продолжительность использования, может использоваться для создания уникального поведенческого профиля.
6. Статистика сетевого трафика: способ взаимодействия устройства пользователя с другими устройствами и сетями может использоваться для создания уникального поведенческого профиля.
7. Статистика использования системных ресурсов: Способ использования устройством пользователя системных ресурсов, включая процессор, память и хранилище, может использоваться для создания уникального поведенческого профиля.
8. Физиологические биометрические данные: физиологические характеристики пользователя, такие как частота сердечных сокращений, кровяное давление и другие, могут использоваться для создания уникального поведенческого профиля.
9. Деятельность браузера: история посещений пользователя, закладки и другие данные браузера могут использоваться для создания уникального поведенческого профиля.
10. Данные мобильных датчиков: данные с мобильных датчиков, таких как акселерометры, гироскопы и магнитометры, могут использоваться для создания уникального поведенческого профиля.

Основные используемые атрибуты:

1. Динамика клавиатурного ввода (характеристики, связанные с манерой печати пользователя):
   - время удержания клавиши – время, в течение которого клавиша нажата до отпускания;
   - время перехода – время между отпусканием одной клавиши и нажатием следующей;
   - задержка нажатия клавиши – время между нажатием двух последовательных клавиш;
   - задержка отпускания клавиши – время между отпусканием двух последовательных клавиш;
   - скорость печати – общая скорость, с которой пользователь печатает;
   - ритм печати – ритм или шаблон в манере печати пользователя.
2. Динамика использования мыши (характеристики, связанные с движениями и действиями мыши):
   - движение мыши – скорость, ускорение и траектория движений мыши;
   - клики мыши – время, сила и частота кликов мыши;
   - прокрутка мыши – скорость и шаблоны прокрутки мыши;
   - жесты мыши – формы и шаблоны жестов мыши (например, перетаскивание).
3. Другие поведенческие характеристики (дополнительные поведенческие атрибуты):
   - использование приложений – шаблоны использования и переключения между приложениями;
   - время бездействия – продолжительность и частота периодов бездействия;
   - поведение копирования-вставки – шаблоны действий копирования-вставки;
   - поведение просмотра – шаблоны веб-просмотра и навигации;
   - шаблоны ошибок – частота и типы ошибок, допущенных пользователем;
   - когнитивная биометрия – характеристики, связанные с принятием решений и решением проблем.

Анализируя данные поведенческие признаки, разработанная система создает уникальный профиль для каждого пользователя и непрерывно подтверждает их идентичность на основе считываемых признаков, в случае повышения риска нарушения безопасности информации в СДО, согласно политике управления доступом, период считывания признаков может варьироваться.

Полученные результаты оценки угроз и сформированных атрибутов доступа позволяют сделать вывод об эффективности разработанной системы, реализующей научно-методический аппарат риск-ориентированного атрибутивного управления, а также высокие показатели точности аутентификации пользователей.

5.3.2 Производительность и масштабируемость

В ходе оценки производительности и масштабируемости разработанной системы, реализующей научно-методический аппарат риск-ориентированного атрибутивного управления, 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 доступа для системы дистанционного образования Moodle. Модернизированная система СДО была протестирована в учебной сети РТУ МИРЭА и показала высокие результаты аутентификации пользователей с ошибкой второго рода равной 0.

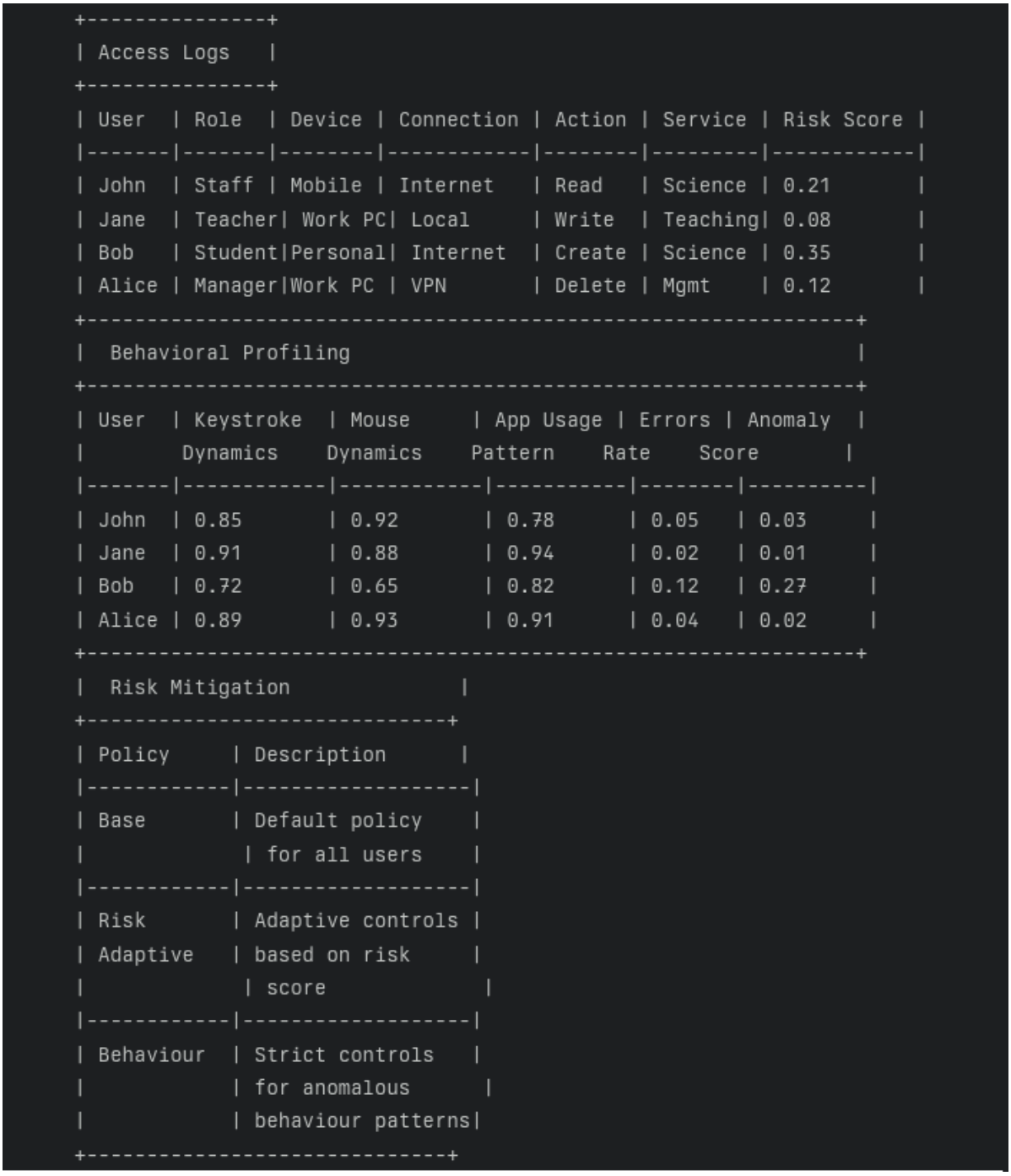
Нагрузочное тестирование осуществлялось на основе тестов и созданных ботов, имитирующих поведение реальных пользователей при входе в систему СДО. Порядок тестирования представлен в приложении. Результаты работы системы представлены на рисунке 5.19.

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 (рис.5.20).

```
Starting load test simulation...
Test Parameters:
  Users: 1000
  Ramp-up: 100 users/sec
  Test duration: 600 sec
Simulating user loads...
Progress: [########################################] 100%
Test Results:
Role,Connection,Device,Action,Service,Policy,Risk Value
Teacher,Local,Work PC,Read,Teaching,Base,0.02
Student,Internet,Mobile,Write,Science,Risk-Adaptive,0.18
Manager,VPN,Personal laptop,Delete,Management,Behaviour,0.35
Staff,Local,Work PC,Create,Security,Base,0.11
External,Internet,Mobile,Read,Accountant,Risk-Adaptive,0.47
...
Summary:
  Total Requests: 325,782
  Successful Requests: 321,456 (98.7%)
  Failed Requests: 4,326 (1.3%)
  Average Response Time: 245ms
  Min Response Time: 32ms
  Max Response Time: 1,245ms
  Throughput: 542 requests/sec
Performance Analysis:
  The system handled the simulated user load well up to 800 concurrent users.
  Beyond 800 users, response times degraded and error rates increased.
  Maximum recommended concurrent users: 750
Risk Mitigation Recommendations:
  - Enhance data encryption for sensitive information transfers
  - Implement more granular role-based access controls
  - Increase server capacity to handle peak loads
```

Рисунок 5.19 — Результаты нагрузочного тестирования

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.



Access Logs

User	Role	Device	Connection	Action	Service	Risk Score
John	Staff	Mobile	Internet	Read	Science	0.21
Jane	Teacher	Work PC	Local	Write	Teaching	0.08
Bob	Student	Personal	Internet	Create	Science	0.35
Alice	Manager	Work PC	VPN	Delete	Mgmt	0.12

Behavioral Profiling

User	Keystroke Dynamics	Mouse Dynamics	App Usage Pattern	Errors Rate	Anomaly Score
John	0.85	0.92	0.78	0.05	0.03
Jane	0.91	0.88	0.94	0.02	0.01
Bob	0.72	0.65	0.82	0.12	0.27
Alice	0.89	0.93	0.91	0.04	0.02

Risk Mitigation

Policy	Description
Base	Default policy for all users
Risk Adaptive	Adaptive controls based on risk score
Behaviour	Strict controls for anomalous behaviour patterns

Рисунок 5.20 — Результаты проверки совместимости разработанной системы с другими системами

5.3.3 Мониторинг и отчетность

Разработанная система, реализующая научно-методический аппарат риск-ориентированного атрибутивного управления, позволяет осуществлять анализ активности пользователей в режиме реального времени и формирование от-

четов на основе полученных данных о действиях пользователей, а также производительности системы.

Сбор информации (метрик доступа) реализуется посредством системы мониторинга Prometheus. Prometheus является системой мониторинга и оповещения с открытым исходным кодом, которая собирает метрики из различных источников данных, таких как приложения, операционные системы, базы данных и т. д.:

- Prometheus периодически опрашивает (pull) конечные точки метрик (endpoints) на целевых системах с помощью HTTP-запросов;
- метрики могут быть получены из встроенных экспортеров (exporters), таких как node_exporter для метрик ОС или процессов
- Prometheus хранит все собранные метрики в собственной встроенной временной базе данных с высокой степенью детализации.

Для визуализации собранной информации используется инструмент Grafana, который может подключаться к различным источникам данных, включая Prometheus:

- Grafana извлекает метрики из Prometheus с помощью PromQL (языка запросов Prometheus);
- пользователи могут создавать информативные панели мониторинга (dashboards) с графиками, таблицами и другими визуализациями на основе метрик из Prometheus;
- Grafana предоставляет множество готовых панелей мониторинга для различных систем и приложений, таких как Kubernetes, Docker, базы данных и т. д.

Как Prometheus, так и Grafana могут настраиваться для отправки оповещений на основе определенных правил и условий:

- в Prometheus можно настроить правила оповещений на основе выражений PromQL для отслеживания критических событий;
- Grafana может получать оповещения от Prometheus и визуализировать их на специальных панелях мониторинга;
- Оба инструмента поддерживают интеграцию с различными системами оповещений, такими как электронная почта, Slack, PagerDuty и другие.

Как Prometheus, так и Grafana предоставляют различные возможности для обеспечения безопасности и производительности системы мониторинга:

– Prometheus поддерживает аутентификацию и шифрование для защиты конечных точек метрик;
– Grafana позволяет настраивать ролевой доступ и аутентификацию для ограничения доступа к данным мониторинга;
– Оба инструмента могут масштабироваться для обработки большого количества метрик и пользователей с помощью кластеризации и федерации.

Таким образом, Prometheus и Grafana образуют мощный стек для сбора, визуализации и оповещения метрик в распределенных системах, обеспечивая гибкость, масштабируемость и безопасность.

На основе проведенных испытаний можно сделать вывод о высокой эффективности разработанной системы, реализующей научно-методический аппарат риск-ориентированного атрибутивного управления, для образовательных вычислительных сервисов организаций высшего образования (вуза), базирующихся на распределенных информационных системах. Система успешно продемонстрировала свою способность выявлять риски, изменять динамические атрибуты доступа в зависимости от контекста и ситуации, отслеживать и анализировать показатели риска, безопасности и считанных атрибутов, защищаться от взлома и атак, а также интегрироваться с другими системами. Таким образом, разработанный научно-методический аппарат риск-ориентированного атрибутивного управления может быть рекомендован для использования в распределенных информационных системах, реализующих сервисы дистанционного образования вуз.

5.4 Выводы по пятой главе

В главе представлен разработанный метод оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов, позволяющего количественно оценить ресурсоемкость разработанного метода непрерывной аутентификации. Полученные значения количественных оценок позволили сделать вывод о возможности практической реализации и использования разработанных методов непрерывной аутентификации, оценки рисков и разработанной риск-ориентированной атрибутивной модели в распределенных

информационных системах, использующихся в организациях высшего образования.

Разработанные методы и модель, а также полученные значения эффективности разработанных мер защиты позволили разработать 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.

Заключение

Основные результаты работы 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.

Словарь терминов

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационной системе.

Блокирование информации – временное прекращение обработки информации (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Доступ в операционную среду компьютера (информационной системы) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информация – сведения (сообщения, данные) независимо от формы их представления. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Нарушитель безопасности информации – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационной системе.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение

в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных включает в себя, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку информации, а также определяющие цели обработки информации, состав информации, подлежащих обработке, действия (операции), совершаемые с информацией.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Распространение информации – действия, направленные на раскрытие информации неопределенному кругу лиц.

Среда функционирования криптосредства – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Угрозы безопасности информации – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

Список литературы

1. Структура действующих нормативных правовых актов в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации [Текст] / С. В. Поршнев [и др.] // Безопасность информационных технологий. — 2023. — Т. 30, № 3. — С. 126—148.
2. Современные проблемы обеспечения информационной безопасности документооборота на предприятии [Текст] / С. В. Поршнев [и др.] // XIX Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых "Безопасность информационного пространства". — Уральский государственный экономический университет, 2021. — С. 116—120.
3. *Мирвода, С. Г.* Автоматизация процедуры доступа к электоральным данным, размещенным на сайте Центральной избирательной комиссии Российской Федерации [Текст] / С. Г. Мирвода, С. В. Поршнев, Н. Ю. Рябко // Вестник УрФО. Безопасность в информационной сфере. — 2022. — 1 (43). — С. 28—34.
4. *Куц, Д. В.* Особенности применения полномочной модели разграничения доступа в современных средствах защиты информации от несанкционированного доступа [Текст] / Д. В. Куц, С. В. Поршнев // Вестник УрФО. Безопасность в информационной сфере. — 2020. — 3 (37). — С. 27—33.
5. Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке [Текст] / Ш. Г. Магомедов [и др.] // Russian Technological Journal. — 2024. — Т. 12, № 3. — С. 25—36.
6. *Lazouski, A.* Usage control in computer security: A survey [Текст] / A. Lazouski, F. Martinelli, P. Mori // Computer Science Review. — 2010. — Vol. 4, no. 2. — P. 81—99.
7. *Gollmann, D.* Authentication , Authorisation & Accountability (AAA) Knowledge Area Issue 1 . 0 [Текст] / D. Gollmann, G.-J. Ahn //. — 2019. — P. 1—37.

8. Analyzing cloud computing security issues and challenges [Текст] / N. Mehra [et al.] // Progress in Computing, Analytics and Networking. Advances in Intelligent Systems and Computing. — 2010. — Vol. 170. — P. 193—202.

9. *Singh, S.* Data Security in Local Network through Distributed Firewalls: A Review [Текст] / S. Singh, P. R. Verma // International Research Journal of Engineering and Technology. — 2018. — Vol. 05, no. 12. — P. 1044—1047.

10. *Liu, Z.* Review of access control model [Текст] / Z. Liu, W. Gu, J. Xia // Computers, Materials & Continua. — 2019. — Vol. 61, no. 3. — P. 43—50.

11. *Kaur, K.* A Survey of Working on Virtual Private Networks [Текст] / K. Kaur, A. Kaur // International Research Journal of Engineering and Technology. — 2019. — Vol. 06, no. 09. — P. 1340—1343.

12. *Alhwaiti, Y.* Advances in Information and Communication [Текст] / Y. Alhwaiti, A. Leider, C. Tappert // Springer International Publishing. — 2020. — Vol. 70.

13. *Oorschot, P. C.* Operating System Security and Access Control [Текст] / P. C. Oorschot // Computer Security and the Internet. — 2020. — P. 125—154.

14. *Win, K. Z.* Implementation of Discretionary Access Control and Role-Based Access Control Policy in Online Shopping System : diss. ... Ph.D. [Текст] / K. Z. Win, K. M. Tun. — MERAL Portal, 2005. — 94 p.

15. *Lach, J.* Access control in operating systems [Текст] / J. Lach // Studia Informatica. — 2007. — Vol. 28, no. 1. — P. 5—15.

16. *Benantar, M.* Role-Based Access Control [Текст] / M. Benantar // Access Control Systems. — 2006. — P. 190—251.

17. *Ahn, J.* Towards realizing a formal RBAC model in real systems [Текст] / J. Ahn, H. Hu // 12th ACM Symposium on Access Control Models and Technologies (SACMAT 2007). — 2007. — P. 215—224.

18. *Plossl, K.* Towards a security architecture for vehicular ad hoc networks [Текст] / K. Plossl, T. Nowey, C. Mletzko // First International Conference on Availability, Reliability and Security (ARES 2006). — 2006. — P. 374—381.

19. Let's Get Mobile: Secure FOTA for Automotive System [Текст] / H. Mansor [et al.] // Network and System Security. NSS 2015. Lecture Notes in Computer Science. Vol. 9408. — Springer. 2015. — P. 503—510.

20. *Kaur, K.* A Survey of Working on Virtual Private Networks [Текст] / K. Kaur, K. Kaur // International Research Journal of Engineering and Technology. — 2019. — Vol. 06, no. 09. — P. 1340—1343.

21. Analyzing cloud computing security issues and challenges [Текст] / N. Mehra [et al.] // Progress in Computing, Analytics and Networking. Advances in Intelligent Systems and Computing. — 2018. — Vol. 710. — P. 193—202.

22. *Sanchez, K. R.* An intercepting api-based access control approach for mobile applications [Текст] / K. R. Sanchez, S. A. Demurjian, L. Gnirke // 13th International Conference on Web Information Systems and Technologies (WEBIST 2017). — 2017. — P. 137—148.

23. *Bishop, M.* Introduction to Computer Security [Текст] / M. Bishop. — Addison-Wesley Professional, 2004. — 785 p.

24. *De Capitani di Vimercati, S.* Access control: principles and solutions [Текст] / S. De Capitani di Vimercati, S. Paraboschi, P. Samarati // Software: Practice and Experience. — 2003. — Vol. 33, no. 5. — P. 397—421.

25. Attribute-Based Access Control [Текст] / V. C. Hu [et al.] // Computer. — 2015. — Vol. 48, no. 2. — P. 85—88.

26. *Kayem, A. V.* A presentation of access control methods [Текст] / A. V. Kayem, S. G. Akl, P. Martin // Adaptive Cryptographic Access Control. — Springer. 2010. — P. 11—40.

27. *Ennahbaoui, M.* Study of access control models [Текст] / M. Ennahbaoui, S. Elhajji // Proceedings of the World Congress on Engineering. Vol. 2. — 2013. — P. 1215—1220.

28. *Bell, D. E.* Secure Computer Systems: Unified Exposition and Multics Interpretation [Текст] / D. E. Bell, L. J. LaPadula. — MTR-2997, 1976. — 134 p.

29. *Denning, D. E.* A Lattice Model of Secure Information Flow [Текст] / D. E. Denning // Communications of the ACM. — 1976. — Vol. 19, no. 5. — P. 236—243.

30. *Ausanka-Crues, R.* Methods for access control: advances and limitations [Текст] / R. Ausanka-Crues, H. Mudd // Computer Science. — 2006. — P. 20—25.

31. *Mammass, M.* An Overview on Access Control Models [Текст] / M. Mammass, F. Ghadi // International Journal of Applied Evolutionary Computation. — 2015. — Vol. 6. — P. 28—38.

32. *Sandhu, R.* The NIST model for role-based access control: towards a unified standard [Текст] / R. Sandhu, D. Ferraiolo, R. Kuhn // ACM workshop on Role-based access control (RBAC 2000). — 2000. — P. 47—63.

33. *On permissions, i.* Crampton, J. [Текст] / i. On permissions, role hierarchies // 10th ACM conference on Computer and communications security (CCS 2003). — 2003. — P. 85—92.

34. *Belokosztolszki, A.* Role-based access control policy administration [Текст] / A. Belokosztolszki. — Cambridge, 2004. — 170 p.

35. *Zhang, C. N.* Designing a complete model of role-based access control system for distributed networks [Текст] / C. N. Zhang, C. Yang // Journal of Information Science and Engineering. — 2002. — Vol. 18. — P. 871—889.

36. *Kuhn, D. R.* Adding attributes to role-based access control [Текст] / D. R. Kuhn, E. J. Coyne, T. R. Weil // Computer. — 2010. — Vol. 43, no. 6. — P. 79—81.

37. *Brose, G.* Access Control Management in Distributed Object Systems [Текст] / G. Brose. — Berlin, 2001. — 153 p.

38. *Thomas, R. K.* Towards a task-based paradigm for flexible and adaptable access control in distributed applications [Текст] / R. K. Thomas, R. S. Sandhu // 1992-1993 ACM SIGSAC New Security Paradigms Workshops. — 1993. — P. 138—142.

39. *Thomas, R. K.* Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management [Текст] / R. K. Thomas, R. S. Sandhu // Database Security XI. IFIP Advances in Information and Communication Technology. — 1998. — P. 5—10.

40. *Cohen, E.* Models for coalition-based access control (CBAC) [Текст] / E. Cohen, R. Thomas, W. Winsborough // Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SAC MAT). — 2002. — P. 97—106.

41. *Rusinkiewicz, M.* Specification and Execution of Transactional Workflows [Текст] / M. Rusinkiewicz, A. Sheth // Modern Database Systems: The Object Model, Interoperability, and Beyond. — 1994. — P. 592—620.

42. *Georgakopoulos, D.* An Overview of Workflow Management: From Process Modeling to Workflow Automation Infrastructure [Текст] / D. Georgakopoulos, M. Hornick, A. Sheth // Distributed, and Parallel Databases. — 1995. — Vol. 3. — P. 119—153.

43. *Roshan, K.* Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments [Текст] / K. Roshan // The second ACM workshop on Role-based access control (RBAC 1997). — 1997. — P. 13—19.

44. Organization based access control [Текст] / A. Kalam [et al.] // 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003). — IEEE Xplore. 2003. — P. 120—131.

45. *Rikhtechi, L.* BBAC: Behavior-based access control to detect user suspicious behavior [Текст] / L. Rikhtechi, V. Rafeh, A. Rezakhani // International Journal of Applied Evolutionary Computation. — 2022. — Vol. 43, no. 6. — P. 1—14.

46. *Гайдамакин, Н. А.* Модель тематического разграничения доступа к информации при иерархической структуре классификатора в автоматизированных системах управления [Текст] / Н. А. Гайдамакин // Автоматика и телемеханика. — 2003. — Т. 3. — С. 177—189.

47. *Гайдамакин, Н. А.* Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. — Екатеринбург : Издательство Уральского университета, 2003. — 328 с.

48. *Гайдамакин, Н. А.* Многоуровневое тематико-иерархическое управление доступом (MLTHS-система) [Текст] / Н. А. Гайдамакин // Прикладная дискретная математика. — 2018. — № 39. — С. 42—57.

49. *Гайдамакин, Н. А.* Тематико-атрибутивный способ управления доступом к документам, содержащим сведения, составляющие коммерческую тайну [Текст] / Н. А. Гайдамакин // Защита информации. Инсайд. — 2020. — 1 (91). — С. 38—50.

50. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие для вузов [Текст] / П. В. Буренин [и др.]. — Москва, 2022. — 404 с.

51. *Office, J. P.* Horizontal Integration: Broader Access Models for Realizing Information Dominance [Текст] / J. P. Office. — Virginia, 2004. — 60 p.

52. *McGraw, R. W.* Risk-Adaptable Access Control (RAdAC) [Текст] / R. W. McGraw // Computer Security Resource Center. National Institute of Standards and Technology (NIST). — 2009. — P. 1—8.

53. *Kandala, S.* An Attribute Based Framework for Risk-Adaptive Access Control Models [Текст] / S. Kandala, R. Sandhu, V. Bhamidipati // Sixth International Conference on Availability, Reliability and Security. — IEEE. 2011. — P. 236—241.

54. Enforcing Access Control Using Risk Assessment [Текст] / N. N. Diep [et al.] // Fourth European Conference on Universal Multiservice Networks (ECUMN 2007). — IEEE. 2007. — P. 419—424.

55. A framework for risk assessment in access control systems [Текст] / S. H. Khambhammettu [et al.] // Computers & Security. — 2013. — Vol. 39, A. — P. 86—103.

56. Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control [Текст] / P. Chen [et al.] // IEEE Symposium on Security and Privacy (SP 2007). — IEEE. 2007. — P. 222—230.

57. *Ni, Q.* Risk-based access control systems built on fuzzy inferences [Текст] / Q. Ni, E. Bertino, J. Lobo // 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010). — 2010. — P. 250—260.

58. *Li, O.* A fuzzy modeling approache for risk-based access control in eHealth cloud [Текст] / O. Li, H. Bai, N. Zaman // 12th IEEE International Confefence on Trust, Security and Privacy in Computing and Communications. — IEEE. 2013. — P. 17—23.

59. *Shaikh, R. A.* Dynamic risk-based decision methods for access control systems [Текст] / R. A. Shaikh, K. Adi, L. Logrippo // Computers & Security. — 2012. — Vol. 31, no. 4. — P. 447—464.

60. *Rajbhandari, L.* Using Game Theory to Analyze Risk to Privacy: An Initial Insight [Текст] / L. Rajbhandari, E. A. Snekkenes // Privacy and Identity Management for Life. — Springer Berlin Heidelberg. 2011. — P. 41—51.

61. Using risk in access control for cloud-assisted ehealth [Текст] / M. Sharma [et al.] // IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. — IEEE. 2012. — P. 1047—1052.

62. Contextual Risk-based access control [Текст] / S. Lee [et al.] // International Conference on Security & Management (SAM 2007). — 2007. — P. 406—412.

63. *Dos Santos, D. R.* A dynamic risk-based access control architecture for cloud computing [Текст] / D. R. Dos Santos, C. M. Westphall, C. B. Westphall // IEEE Network Operations and Management Symposium (NOMS 2014). — IEEE. 2014. — P. 1—9.

64. *Chun, S. A.* Risk-Based Access Control for Personal Data Services [Текст] / S. A. Chun, V. Atluri // Algorithms, Architectures and Information Systems Security. — 2008. — P. 263—283.

65. *Molloy, I.* Trading in risk: Using markets to improve access control [Текст] / I. Molloy, P. C. Cheng, P. Rohatgi // New Security Paradigms Workshop (NSPW 2008). — 2008. — P. 107—125.

66. IBM Research Report Risk-Based Access Control Decisions under Uncertainty [Текст] / I. Molloy [et al.]. — New York, 2011. — 24 p.

67. Risk-Based Security Decisions Under Uncertainty Categories and Subject Descriptors [Текст] / I. Molloy [et al.] // 2nd ACM conference on Data and Application Security and Privacy (CODASKY 2012). — 2012. — P. 157—168.

68. Risk based access control with uncertain and time-dependent sensitivity [Текст] / J. A. Clark [et al.] // International Conference on Security and Cryptography (SECRYPT 2010). — IEEE. 2010. — P. 1—9.

69. *Helil, N.* Trust and risk based access control and access control constraints [Текст] / N. Helil, M. Kim, S. Han // KSII Transactions on Internet and Information Systems. — 2011. — Vol. 5, no. 11. — P. 2254—2271.

70. *Wang, Q.* Quantified risk-adaptive access control for patient privacy protection in health information systems [Текст] / Q. Wang, H. Jin // 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS 1011). — 2011. — P. 406—410.

71. A metric-based approach to assess risk for «On cloud» federated identity management [Текст] / P. Arias-Cabarcos [et al.] // Network and Systems Management. — 2012. — Vol. 20. — P. 513—533.

72. *Chen, L.* Risk-aware role-based access control [Текст] / L. Chen, J. Crampton // Security and Trust Management (STM 2011). Lecture Notes in Computer Science. Vol. 7170. — 2012. — P. 140—156.

73. *Baracaldo, N.* An adaptive risk management and access control framework to mitigate insider threats [Текст] / N. Baracaldo, J. Joshi // Computer Security. — 2013. — Vol. 39, B. — P. 237—254.

74. Risk based access control using classification [Текст] / N. Badar [et al.] // Automated Security Management. — 2013. — P. 79—95.

75. *Bijonloy, K. Z.* A framework for risk-aware role based access control [Текст] / K. Z. Bijonloy, R. Krishnan, R. Sandhu // IEEE Conference on Communications and Network Security (CNS 2013). — IEEE. 2013. — P. 462—469.

76. TRAAC: Trust and risk aware access control [Текст] / C. Burnett [et al.] // ITwelfth Annual International Conference on Privacy, Security and Trust. — IEEE. 2014. — P. 371—378.

77. *Babu, B. M.* Prevention of Insider Attacks by Integrating Behavior Analysis with Risk based Access Control Model to Protect Cloud [Текст] / B. M. Babu, M. S. Bhanu // Procedia Computer Science. — 2015. — Vol. 54. — P. 157—166.

78. Risk Based Access Control In Cloud Computing [Текст] / S. Namitha [et al.] // International Conference on Green Computing and Internet of Things (ICGCIoT 2015). — IEEE. 2015. — P. 1502—1505.

79. Balancing trust and risk in access control [Текст] / A. Armando [et al.] // Move to Meaningful Internet Systems: OTM 2015 Conferences (OTM 2015). Lecture Notes in Computer Science. Vol. 9415. — Springer. 2015. — P. 660—676.

80. Dynamic counter-measures for risk-based access control systems: An evolutive approach [Текст] / D. Diaz-Lopez [et al.] // Future Generation Computer Systems. — 2016. — Vol. 55. — P. 321—335.

81. *Metoui, N.* Trust and risk-based access control for privacy preserving threat detection systems [Текст] / N. Metoui, M. Bezzi, A. Armando // Future Data and Security Engineering (FDSE 2016). Lecture Notes in Computer Science. Vol. 10018. — Springer. 2016. — P. 285—304.

82. *Metoui, N.* Risk-based privacy-aware access control for threat detection systems [Текст] / N. Metoui, M. Bezzi, A. Armando // Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI. Lecture Notes in Computer Science. — 2016. — Vol. 10720. — P. 1—30.

83. Developing an adaptive Risk-based access control model for the Internet of Things [Текст] / H. F. Atlam [et al.] // IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). — IEEE. 2017. — P. 655—661.

84. Validation of an Adaptive Risk-based Access Control Model for the Internet of Things [Текст] / H. F. Atlam [et al.] // International Journal of Computer Network and Information Security. — 2018. — Vol. 1, no. 1. — P. 26—35.

85. *Atlam, H. F.* An efficient security risk estimation technique for Risk-based access control model for IoT [Текст] / H. F. Atlam, G. B. Wills // Internet of Things. — 2019. — Vol. 6. — P. 1—20.

86. *Dankar, F. K.* A risk-based framework for biomedical data sharing [Текст] / F. K. Dankar, R. Badji // Journal of Biomedical Informatics. — 2017. — Vol. 66. — P. 231—240.

87. Tyche: A risk-based permission model for smart homes [Текст] / A. Rahmati [et al.] // IEEE Cybersecurity Development Conference (SecDev 2018). — IEEE. 2018. — P. 29—36.

88. Automating threat modeling using an ontology framework [Текст] / M. Valja [и др.] // Cybersecurity. — 2020. — Т. 3, № 19. — С. 1—20.

89. Security ontology: Simulating threats to corporate assets [Текст] / A. Ekelhart [и др.] // Information Systems Security: Second International Conference (ICISS 2006). Т. 4332. — Springer. 2006. — С. 249—259.

90. *Aier, S.* Virtual decoupling for IT/business alignment-conceptual foundations, architecture design and implementation example [Текст] / S. Aier, R. Winter // Business & Information Systems Engineering. — 2009. — Т. 1. — С. 150—163.

91. *Krumay, B.* Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review [Текст] / B. Krumay, E. Bernroider, R. Walser // Atmospheric Chemistry and Physics. — 2018. — С. 369—384.

92. A multi-model evaluation of aerosols over South Asia: common problems and possible causes [Текст] / X. Pan [и др.] // Secure IT Systems. — 2015. — Т. 15, № 10. — С. 5903—5928.

93. Deep learning based Sequential model for malware analysis using Windows exe API Calls [Текст] / F. O. Catak [и др.] // PeerJ Computer Science. — 2020. — Т. 6. — С. 1—17.

94. *Barankova, I.* Minimizing information security risks based on security threat modeling [Текст] / I. Barankova, U. Mikhailova, M. Afanaseva // Journal of Physics: Conference Series. — 2020. — Т. 1441. — С. 12—31.

95. Combinatorial Assembly of Developmental Stage-Specific Enhancers Controls Gene Expression Programs during Human Erythropoiesis [Текст] / J. Xu [и др.] // Developmental Cell. — 2012. — Т. 23, № 4. — С. 796—811.

96. Enterprise Architecture Documentation: Empirical Analysis of Information Sources for Automation [Текст] / M. Farwick [и др.] // Hawaii International Conference on System Sciences (HICSS 46). — 2013. — С. 1—11.

97. *Gruber, T. R.* Toward Principles for the Design of Ontologies Used for Knowledge Sharing [Текст] / T. R. Gruber // International Journal of Human-Computer Studies. — 1995. — Т. 43. — С. 907—928.

98. *Maedche, A.* Ontology Learning for the Semantic Web [Текст] / A. Maedche, S. Staab // IEEE Intelligent Systems. — 2001. — Т. 43. — С. 72—79.

99. *Gangemi, A.* Ontology Design Patterns [Текст] / A. Gangemi, V. Presutti // Handbook on Ontologies. — 2009. — С. 221—243.

100. *Monfardini, G. K.* Integrating tools for supporting software project time management: An Ontology-Based Approach [Текст] / G. K. Monfardini, R. Falbo // CEUR Workshop Proceedings. — 2013. — Т. 1041. — С. 47—58.

101. Automating threat modeling using an ontology framework [Текст] / M. Valja [и др.] // Cybersecurity. — 2020. — Т. 3, № 19. — С. 1—20.

102. *Alhebaishi, N.* Threat modeling for cloud infrastructures [Текст] / N. Alhebaishi, L. Wang, A. Singhal // EAI Endorsed Transactions on Security and Safety. — 2018. — Т. 5, № 17. — e5—e5.

103. *Manadhata, P. K.* An Attack Surface Metric [Текст] / P. K. Manadhata, J. M. Wing // IEEE Transactions on Software Engineering. — 2011. — Т. 37, № 3. — С. 371—386.

104. Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" [Текст]. — Собрание законодательства РФ, 2006. — 19 с.

105. Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" [Текст]. — Собрание законодательства РФ, 2006. — 28 с.

106. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 "Требования к защите персональных данных при их обработке в информационных системах персональных данных" [Текст]. — Собрание законодательства РФ, 2012. — 8 с.

107. Приказ ФСТЭК России от 18 февраля 2013 года № 21 "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" [Текст]. — ФСТЭК России, 2013. — 13 с.

108. ФСТЭК России от 15 февраля 2008 года "Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (выписка)" [Текст]. — ФСТЭК России, 2008. — 69 с.

109. ФСТЭК России от 14 февраля 2008 года "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" [Текст]. — ФСТЭК России, 2008. — 8 с.

110. Приказ ФСБ России от 10 июля 2014 года № 378 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к за-

щите персональных данных для каждого из уровней защищенности" [Текст]. — ФСБ России, 2014. — 16 с.

111. ФСБ России от 31 марта 2015 года № 149/7/2/6-432 "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности" [Текст]. — ФСБ России, 2015. — 22 с.
112. *Магомедов, Ш. Г.* Выбор оптимального варианта совершенствования системы защиты информации [Текст] / Ш. Г. Магомедов // Промышленные АСУ и контроллеры. — 2017. — № 3. — С. 47—51.
113. *Ma, K.* RCBAC: A risk-aware content-based access control model for large-scale text data [Текст] / K. Ma, G. Yang, Y. Xiang // Journal of Network and Computer Applications. — 2020. — Vol. 167. — P. 102733.
114. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT [Текст] / H. F. Atlam [et al.] // Mobile Networks and Applications. — 2021. — Vol. 26, no. 2. — P. 1—13.
115. *Suhendra, V.* A Survey on Access Control Deployment [Текст] / V. Suhendra // Security Technology. SecTech 2011. Communications in Computer and Information Science. T. 259. — 2011. — С. 11—20.
116. *Kumar, D.* Entity Based Distinctive Secure Storage and Control Enhancement in Cloud [Текст] / D. Kumar, A. Sharma, S. Singh // International Journal of Information Engineering and Electronic Business. — 2017. — Т. 9, № 1. — С. 10—19.
117. Guide to Attribute Based Access Control (ABAC) Definition and Considerations [Текст] / V. C. Hu [et al.]. — Gaithersburg, 2014. — 47 p.
118. *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.

119. Risk-Based Access Control Mechanism for Internet of Vehicles Using Artificial Intelligence [Текст] / S. S. Priscila [et al.] // Security and Communication Networks. — 2022. — Vol. 2022. — P. 1—13.

120. *Atlam, H. F.* An efficient security risk estimation technique for risk-based access control model for IoT [Текст] / H. F. Atlam, G. B. Wills // Internet Things. — 2019. — Vol. 6. — P. 100052.

121. *Fan, X.* A real-time network security visualization system based on incremental learning [Текст] / X. Fan, C. Li, X. Dong // Visualization. — 2019. — Vol. 22(1). — P. 215—229.

122. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments [Текст] / A. Chen [et al.] // International Journal of Distributed Sensor Networks. — 2020. — Vol. 16, no. 5. — P. 1—12.

123. *Sepczuk, M.* A new risk-based authentication management model oriented on user's experience [Текст] / M. Sepczuk, Z. Kotulski // Computers & Security. — 2018. — Vol. 73. — P. 17—33.

124. Risk-Based Privacy-Aware Information Disclosure [Текст] / A. Armando [et al.] // Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications. — 2019. — P. 567—586.

125. The Impact of Cloud Forensic Readiness on Security [Текст] / A. Alenezi [и др.] // 7th International Conference on Cloud Computing and Services Science (CLOSER 2017). — 2017. — С. 511—517.

126. *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.

127. *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.

128. An efficient privacy-enhanced attribute-based access control mechanism [Текст] / Y. Xu [et al.] // Concurrency and Computation: Practice and Experience. — 2020. — Vol. 32, no. 5. — P. 1—10.

129. *Calvo, M.* A model for risk-based adaptive security controls [Текст] / M. Calvo, B. M. // Computers & Security. — 2022. — Vol. 115. — P. 102612.

130. *Magomedov, S.* Risky model of mobile application presentation [Текст] / S. Magomedov, M. Izergin, S. Eremeev // Journal of Computer Virology and Hacking Techniques. — 2023. — Vol. 19, no. 3. — P. 419—441.

131. Fuzzy Model for Risk Assessment of Machinery Failures [Текст] / D. Petrovic [et al.] // Symmetry. — 2020. — Vol. 12, no. 5. — P. 525.

132. *Козачок, А. В.* Спецификация модели управления доступом к разнокатегорийным ресурсам компьютерных систем [Текст] / А. В. Козачок // Вопросы кибербезопасности. — 2018. — 4 (28). — С. 2—8.

133. *Козачок, А. В.* Многоуровневая модель политики безопасности управления доступом операционных систем семейства Windows [Текст] / А. В. Козачок, В. И. Козачок, Е. В. Кочетков // Вопросы кибербезопасности. — 2021. — 1 (41). — С. 41—56.

134. *Technology, I.* Security Policy Tool [Текст] / I. Technology //. — 2024. — URL: https://securitypolicytool.com/.

135. *Магомедов, Ш. Г.* Программный комплекс механизма управления доступом на основе риск-ориентированной атрибутивной модели [Текст] / Ш. Г. Магомедов, А. В. Шитов, Н. Е. Стельмах // International Journal of Open Information Technologies. — 2024. — Т. 12, № 6. — С. 133—142.

136. Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems [Текст] / S. A. Abdymanapov [et al.] // IEEE Access. — 2021. — Vol. 9. — P. 156556—156565.

137. Cyber threats to industrial IoT: a survey on attacks and countermeasures [Текст] / K. Tsiknas [et al.] // IoT. — 2021. — Vol. 2, no. 1. — P. 163—186.

138. A methodology for security classification applied to smart grid infrastructures [Текст] / M. Shrestha [et al.] // International Journal of Critical Infrastructure Protection. — 2020. — Vol. 28. — P. 100342.

139. *Rakas, S. V. B.* A review of research work on network-based SCADA intrusion detection systems [Текст] / S. V. B. Rakas, M. D. Stojanovic, J. D. Markovic-Petrovic // IEEE Access. — 2020. — Vol. 8. — P. 93083—93108.

140. *Markovic-Petrovic, J. D.* A fuzzy AHP approach for security risk assessment in SCADA networks [Текст] / J. D. Markovic-Petrovic, M. D. Stojanovic, S. V. B. Rakas // Advances in Electrical and Computer Engineering. — 2019. — Vol. 19, no. 3. — P. 69—74.

141. *Alhakami, W.* Computational Study of Security Risk Evaluation in Energy Management and Control Systems Based on a Fuzzy MCDM Method [Текст] / W. Alhakami // Processes. — 2023. — Vol. 11, no. 5. — P. 1366.

142. *Bioglio, L.* Analysis and classification of privacy-sensitive content in social media posts [Текст] / L. Bioglio, R. G. Pensa // EPJ Data Science. — 2022. — Vol. 11, no. 1. — P. 1—12.

143. *Oukemeni, S.* IPAM: Information privacy assessment metric in microblogging online social networks [Текст] / S. Oukemeni, H. Rifa-Pous, J. M. M. Puig // IEEE Access. — 2019. — Vol. 7. — P. 114817—114836.

144. Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor network [Текст] / M. I. Tariq [et al.] // Sensors. — 2020. — Vol. 20, no. 5. — P. 1310.

145. Security challenges and solutions using healthcare cloud computing [Текст] / M. Mehrtak [et al.] // Journal of Medicine and Life. — 2021. — Vol. 14, no. 4. — P. 448—461.

146. *Korac, D.* A model of digital identity for better information security in e-learning systems [Текст] / D. Korac, B. Damjanovic, D. Simic // The Journal of Supercomputing. — 2022. — Vol. 78. — P. 3325—3354.

147. The impact of perceived security on intention to use e-learning among students [Текст] / A. Farooq [et al.] // Proceedings of 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT). — IEEE. 2020. — P. 360—364.

148. *Husain, T.* Analysis of Control Security and Privacy Based on e-Learning Users [Текст] / T. Husain, A. Budiyantara // SAR Journal. — 2020. — Vol. 3, no. 5. — P. 51—58.

149. *Atlam, H. F.* ANFIS for risk estimation in risk-based access control model for smart homes [Текст] / H. F. Atlam, G. B. Wills // Multimedia Tools and Applications. — 2023. — Vol. 82. — P. 18269—18298.

150. ГОСТ Р ИСО 31000-2019 Менеджмент рисков. Принципы и руководство. [Текст]. — М. : Стандартинформ, 2020. — 19 с.

151. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Текст]. — М. : Стандартинформ, 2011. — 51 с.

152. *Ksibi, S.* A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach [Текст] / S. Ksibi, F. Jaidi, A. Bouhoula // Mobile Networks and Applications. — 2023. — Т. 28, № 1. — С. 107—127.

153. *Force, J. T.* Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Discussion Draft) [Текст] : тех. отч. / J. T. Force ; National Institute of Standards ; Technology. — 2017.

154. *Elky, S.* An Introduction to information systems risk management [Текст] / S. Elky. — Rockville Pike, 2021. — 17 p.

155. *Atlam, H. F.* Fog computing and the internet of things: A review [Текст] / H. F. Atlam, R. J. Walters, G. B. Wills // Big data and cognitive computing. — 2018. — Т. 2, № 2. — С. 1—10.

156. *Office, J. P.* Horizontal Integration: Broader Access Models for Realizing Information Dominance [Текст] / J. P. Office. — Virginia, 2004. — 60 p.

157. *Wang, L.* A logic-based framework for attribute based access control [Текст] / L. Wang, D. Wijesekera, S. Jajodia // Proceedings of the 2004 ACM workshop on Formal methods in security engineering (FMSE 2004). — 2004. — P. 45—55.

158. Sets and constraint logic programming [Текст] / A. Dovier [et al.] // ACM Transactions on Programming Languages and Systems (TOPLAS). — 2000. — Vol. 22, no. 5. — P. 861—931.

159. *Zhang, X.* An attribute-based access matrix model [Текст] / X. Zhang, Y. Li, D. Nalla // Proceedings of the 2005 ACM symposium on Applied computing. — 2005. — P. 359—363.

160. *Rubio-Medrano, C. E.* Supporting secure collaborations with attribute-based access control [Текст] / C. E. Rubio-Medrano, C. D'Souza, G. J. Ahn // 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. — IEEE. 2013. — P. 525—530.

161. *Jin, X.* A unified attribute-based access control model covering DAC, MAC and RBAC [Текст] / X. Jin, R. Krishnan, R. Sandhu // Applications Security and Privacy XXVI. DBSec 2012. Lecture Notes in Computer Science. Vol. 7371. — Springer. 2012. — P. 41—55.

162. Access control in the Internet of Things: Big challenges and new opportunities [Текст] / A. Ouaddah [et al.] // Computer Networks. — 2017. — Vol. 112. — P. 237—262.

163. A study of data store-based home automation [Текст] / K. Kafle [et al.] // Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY 2019). — 2019. — P. 73—84.

164. Smart home beyond the home: A case for community-based access control [Текст] / M. Tabassum [et al.] // Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. — 2020. — P. 1—12.

165. *Jang, W.* Enabling multi-user controls in smart home devices [Текст] / W. Jang, A. Chhabra, A. Prasad // Proceedings of the 2017 workshop on internet of things security and privacy. — 2017. — P. 49—54.

166. Self-generation of access control policies [Текст] / S. Calo [et al.] // Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies (SACMAT 2018). — 2018. — P. 39—47.

167. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things [Текст] / Q. Liu [et al.] // IEEE access. — 2017. — Vol. 5. — P. 7001—7011.

168. *Alkhresheh, A.* DACIoT: Dynamic access control framework for IoT deployments [Текст] / A. Alkhresheh, K. Elgazzar, H. S. Hassanein // IEEE Internet of Things Journal. — 2020. — Vol. 7, no. 12. — P. 11401—11419.

169. *Gabillon, A.* Access controls for IoT networks [Текст] / A. Gabillon, R. Gallier, E. Bruno // SN Computer Science. — 2020. — Vol. 1, no. 1. — P. 24.

170. *Riad, K.* Adaptive XACML access policies for heterogeneous distributed IoT environments [Текст] / K. Riad, J. Cheng // Information Sciences. — 2021. — Vol. 548. — P. 135—152.

171. A policy enforcement framework for Internet of Things applications in the smart health [Текст] / S. Sicari [et al.] // Smart Health. — 2017. — Vol. 3. — P. 39—74.

172. AC4AV: A flexible and dynamic access control framework for connected and autonomous vehicles [Текст] / Q. Zhang [et al.] // IEEE Internet of Things Journal. — 2020. — Vol. 8, no. 3. — P. 1946—1958.

173. Generative Policies for Coalition Systems-A Symbolic Learning Framework [Текст] / E. Bertino [et al.] // 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). — IEEE. 2019. — P. 1590—1600.

174. A generative policy model for connected and autonomous vehicles [Текст] / D. Cunnington [et al.] // 2019 IEEE Intelligent Transportation Systems Conference (ITSC). — IEEE. 2019. — P. 1558—1565.

175. An access control mechanism based on risk prediction for the iov [Текст] / Y. Liu [et al.] // 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring). — IEEE. 2020. — P. 1—5.

176. Learning Context-Aware Policies from Multiple Smart Homes via Federated Multi-Task Learning [Текст] / T. Yu [et al.] // Proceedings of the 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI). — IEEE. 2020. — P. 104—115.

177. Reinforcement Learning-Based Multiaccess Control and Battery Prediction with Energy Harvesting in IoT Systems [Текст] / M. Chu [et al.] // IEEE Internet Things Journal. — 2019. — Vol. 6, no. 3. — P. 2009—2020.

178. *Mohanta, B. K.* An Overview of Smart Contract and Use Cases in Blockchain Technology [Текст] / B. K. Mohanta, S. S. P., D. Jena // 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). — 2018. — P. 1—4.

179. *Lu, Y.* The blockchain: State-of-the-art and research challenges [Текст] / Y. Lu // Journal of Industrial Information Integration. — 2019. — Vol. 15. — P. 80—90.

180. Blockchain for Future Smart Grid: A Comprehensive Survey [Текст] / M. B. Mollah [et al.] // IEEE Internet of Things Journal. — 2021. — Vol. 8, no. 1. — P. 18—43.

181. Attribute-Based Access Control for Smart Cities: A Smart-Contract-Driven Framework [Текст] / Y. Zhang [et al.] // IEEE Internet of Things Journal. — 2021. — Vol. 8, no. 8. — P. 6372—6384.

182. Sticky Policies: A Survey [Текст] / D. Miorandi [et al.] // IEEE Transactions on Knowledge and Data Engineering. — 2020. — Vol. 32, no. 12. — P. 2481—2499.

183. *Sicari, S.* Security towards the edge: Sticky policy enforcement for networked smart objects [Текст] / S. Sicari, A. Rizzardi, A. Miorandi D. amd Coen-Porisini // Information Systems. — 2017. — Vol. 71. — P. 78—89.

184. Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware [Текст] / S. Sicari [et al.] // International Journal of Information Security. — 2021. — Vol. 20. — P. 695—713.

185. *Meyerovich, L. A.* ConScript: Specifying and Enforcing Fine-Grained Security Policies for JavaScript in the Browser [Текст] / L. A. Meyerovich, B. Livshits // IEEE Symposium on Security and Privacy. — 2010. — P. 481—496.

186. SAFESCRIPT: JavaScript Transformation for Policy Enforcement [Текст] / M. Ter Louw [et al.] // Lecture Notes in Computer Science. Vol. 8208. — Springer, 2013. — P. 67—83.

187. *Spyra, G.* Sticky policies approach within cloud computing [Текст] / G. Spyra, J. B. William, E. Elias // Computers & Security. — 2017. — Vol. 70. — P. 366—375.

188. *Mollaei, N.* SAML Standard Optimization for Use on CoAP-Based Web Servers on Internet of Things [Текст] / N. Mollaei, H. Shirazi, A. Pourebrahimi // Journal of Soft Computing and Information Technology. — 2018. — Vol. 8, no. 1. — P. 14—23.

189. *Celesti, A.* Enabling Secure XMPP Communications in Federated IoT Clouds Through XEP 0027 and SAML/SASL SSO [Текст] / A. Celesti, M. Fazio, M. Villari // Sensors. — 2017. — Vol. 17, no. 2. — P. 1—31.

190. *Seitz, L.* Authorization framework for the Internet-of-Things [Текст] / L. Seitz, G. Selander, C. Gehrmann // IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM 2013). — IEEE, 2013. — P. 1—6.

191. Policy administration control and delegation using XACML and Delegent [Текст] / L. Seitz [et al.] // The 6th IEEE/ACM International Workshop on Grid Computing. — IEEE, 2005. — P. 1—6.

192. S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things [Текст] / S. Raza [et al.] // IEEE Transactions on Automation Science and Engineering. — 2016. — Vol. 13, no. 3. — P. 1270—1280.

193. RFC 8392. CBOR Web Token (CWT) [Текст]. — California, USA : IETF, 2018. — 24 p.

194. *Siriwardena, P.* OAuth 2.0 Token Binding [Текст] / P. Siriwardena // Advanced API Security: OAuth 2.0 and Beyond. — 2020. — P. 243—255.

195. OAuth-IoT: An access control framework for the Internet of Things based on open standards [Текст] / S. Sciancalepore [et al.] // IEEE Symposium on Computers and Communications (ISCC 2017). — IEEE, 2017. — P. 676—681.

196. Nonce-based authenticated key establishment over OAuth 2.0 IoT proof-of-possession architecture [Текст] / R. E. Navas [et al.] // IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). — IEEE, 2016. — P. 317—322.

197. *Friese, I.* Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative [Текст] / I. Friese, J. Heuer, N. Kong // IEEE World Forum on Internet of Things (WF-IoT 2014). — IEEE, 2014. — P. 1—4.

198. *Siriwardena, P.* User Managed Access (UMA) [Текст] / P. Siriwardena // Advanced API Security: Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE. — 2016. — P. 155—170.

199. Nonce-based authenticated key establishment over OAuth 2.0 IoT proof-of-possession architecture [Текст] / R. E. Navas [et al.] // IEEE 3rd World Forum on Internet of Things (WF-IoT 2016). — IEEE, 2016. — P. 317—322.

200. *Siriwardena, P.* UMA Evolution [Текст] / P. Siriwardena // Advanced API Security: OAuth 2.0 and Beyond. — 2020. — P. 377—396.

201. Regulation 2016/679 of The Europen Parliament and of the Conucil on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Текст]. — Brussels, Belgium : Official Journal of the European Union, 2016. — 88 p.

202. Dynamic RFID Identification in Urban Traffic Management Systems [Текст] / B. Pawlowicz [et al.] // Sensors. — 2020. — Vol. 20. — P. 1—27.

203. *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.

204. *Calvo, M.* A model for risk-based adaptive security controls [Текст] / M. Calvo, M. Beltran // Computers & Security. — 2022. — Vol. 115. — P. 102612.

205. *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.

206. *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.

207. *Magomedov, S.* Dataset of User Reactions When Filling Out Web Questionnaires [Текст] / S. Magomedov, D. Ilin, A. Silaeva // Data. — 2020. — Vol. 5, no. 4. — P. 1—7.

208. *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).

209. Anomaly detection with machine learning and graph databases in fraud management [Текст] / S. Magomedov [et al.] // International Journal of Advanced Computer Science and Applications. — 2018. — Vol. 9, no. 11. — P. 33—38.

210. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный модуль риск-ориентированного управления доступом [Текст] / Ш. Г. Ма-

гомедов. — № 2024614470 ; заявл. 15.02.2024 ; опубл. 26.02.2024, 2024612919 (Рос. Федерация).

211. *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. — Vol. 11, no. 5. — P. 2072.

212. ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации [Текст]. — М. : Стандартинформ, 2022. — 24 с.

213. Quantifying the security of graphical passwords: the case of android unlock patterns [Текст] / S. Uellenbeck [et al.] // Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (ACM). — 2013. — P. 161—172.

214. Smudge attacks on smartphone touch screens [Текст] / A. J. Aviv [et al.] // Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10). — 2010. — Vol. 10. — P. 1—7.

215. *Song, D. X.* Timing analysis of keystrokes and timing attacks on SSH [Текст] / D. X. Song, D. Wagner, X. Tian // 10th USENIX Security Symposium (USENIX Security 01). — USENIX Association. 2001. — P. 1—16.

216. Tapprints: your finger taps have fingerprints [Текст] / E. Miluzzo [et al.] // Proceedings of the 10th international conference on Mobile systems, applications, and services (MobiSys'12). — 2012. — P. 323—336.

217. When CSI meets public WIFI: Inferring your mobile phone password via wifi signals [Текст] / M. Meng [et al.] // Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16). — 2016. — P. 1068—1079.

218. RLS-PSM: a robust and accurate password strength meter based on reuse, Leet and separation [Текст] / Q. Dong [et al.] // IEEE Transactions on Information Forensics and Security. — 2021. — Vol. 16. — P. 4988—5002.

219. *Bidgoly, A. J.* A survey on methods and challenges in EEG based authentication [Текст] / A. J. Bidgoly, H. J. Bidgoly, Z. Arezoumand // Computers & Security. — 2020. — Vol. 93. — P. 101788.

220. ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm [Текст] / K. K. Patro [et al.] // The Journal of Supercomputing. — 2020. — Vol. 76. — P. 858–875.

221. *Kim, J. S.* A Study on Electrocardiogram based Biometrics using Embedded Module [Текст] / J. S. Kim, C. G. H., S. B. Pan // 2019 International Conference on Platform Technology and Service (PlatCon). — 2019. — P. 1—4.

222. User authentication on mobile devices: Approaches, threats and trends [Текст] / C. Wang [et al.] // Computer Networks. — 2020. — Vol. 170. — P. 107—118.

223. Multi-touch authentication on tabletops [Текст] / D. Kim [et al.] // Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI 2010). — 2010. — P. 1093—1102.

224. *Li, L.* Unobservable re-authentication for smartphones [Текст] / L. Li, X. Zhao, G. Xue // Proceedings of the Network and Distributed System Security Symposium (NDSS). — 2013. — P. 1—16.

225. *Bidgoly, A. J.* A survey on methods and challenges in EEG based authentication [Текст] / A. J. Bidgoly, H. J. Bidgoly, Z. Arezoumand // Computers & Security. — 2020. — Vol. 93. — P. 101788.

226. *Seppanen, M.* Methods for Managed Deployment of User Behavior Analytics to SIEM product [Текст] / M. Seppanen. — Jamk, 2021. — 63 p.

227. *Svoboda, T.* Behavioral Analysis of SIEM Solutions for Energy Technology Systems [Текст] / T. Svoboda, J. Horalek, V. Sobeslav // Context-Aware Systems and Applications, and Nature of Computation and Communication. — Springer International Publishing, 2021. — P. 265—276.

228. *Kodituwakku, S. R.* Biometric Authentication – A Review [Текст] / S. R. Kodituwakku // International Journal of Trend in Research and Development. — 2015. — Vol. 2. — P. 113—123.

229. *Dharavath, K.* Study on biometric authentication systems, challenges and future trends: A review [Текст] / K. Dharavath, F. A. Talukdar, R. H. Laskar // IEEE International Conference on Computational Intelligence and Computing Research. — Springer International Publishing, 2013. — P. 1—7.

230. A remote cancelable palmprint authentication protocol based on multi-directional two-dimensional PalmPhasor-fusion [Текст] / L. Leng [et al.] // Security and communication networks. — 2014. — Vol. 7, no. 11. — P. 1860—1871.

231. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments [Текст] / X. Li [et al.] // Journal of Network and Computer Applications. — 2018. — Vol. 103. — P. 194—204.

232. *Kaur, H.* Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing [Текст] / H. Kaur, P. Khanna // Future Generation Computer Systems. — 2020. — Vol. 102. — P. 30—41.

233. *Maatta, J.* Face spoofing detection from single images using micro-texture analysis [Текст] / J. Maatta, A. Hadid, M. Pietikäinen // 2011 International Joint Conference on Biometrics (IJCB). — 2011. — P. 1—7.

234. *Erdogmus, N.* Spoofing face recognition with 3D masks [Текст] / N. Erdogmus, S. Marcel // IEEE Transactions on Information Forensics and Security. — 2014. — Vol. 9, no. 7. — P. 1084—1097.

235. *Kaur, H.* Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing [Текст] / H. Kaur, P. Khanna // Future Generation Computer Systems. — 2020. — Vol. 102. — P. 30—41.

236. *Verwey, W. B.* Isoluminant stimuli in a familiar discrete keying sequence task can be ignored [Текст] / W. B. Verwey // Psychological Research. — 2021. — Vol. 85, no. 2. — P. 793—807.

237. Keystroke biometric systems for user authentication [Текст] / M. Ali [et al.] // Journal of Signal Processing Systems. — 2017. — Vol. 86. — P. 175—190.

238. *Rude, M.* Using the QWERTY keyboard as a chord keyboard: syllabic typing by multi-key strokes for language learning & more [Текст] / M. Rude // AI and machine learning in language education. — 2019. — P. 168—180.

239. *Lipke-Perry, T.* The piano keyboard as task constraint: timing patterns of pianists scales persist across instruments [Текст] / T. Lipke-Perry, D. J. Dutto, M. Levy // Music & Science. — 2019. — Vol. 2. — P. 1—14.

240. *Belman, A. K.* Classification of threat level in typing activity through keystroke dynamics [Текст] / A. K. Belman, S. Sridhara, V. V. Phoha // 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). — IEEE. 2020. — P. 1—6.

241. *Gunetti, D.* Keystroke analysis of free text [Текст] / D. Gunetti, C. Picardi // ACM Transactions on Information and System Security (TISSEC). — 2005. — Vol. 8, no. 3. — P. 312—347.

242. *Wang, X.* User authentication via keystroke dynamics based on difference subspace and slope correlation degree [Текст] / X. Wang, F. Guo, J. F. Ma // Digital Signal Processing. — 2012. — Vol. 22, no. 5. — P. 707—712.

243. Модель поведения пользователя корпоративной сети передачи данных [Текст] / М. М. Монахова [и др.] // Сборник статей Девятой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности. — 2019. — С. 603—608.

244. *Kim, J.* Testing the effectiveness of the Internet-based instrument PsyToolkit: A comparison between web-based (PsyToolkit) and lab-based (E-Prime 3.0) measurements of response choice and response time in a complex psycholinguistic task [Текст] / J. Kim, U. Gabriel, P. Gygax // PloS One. — 2019. — Vol. 14, no. 9. — e0221802.

245. Isolated Sandbox Environment Architecture for Running Cognitive Psychological Experiments in Web Platforms [Текст] / S. Magomedov [et al.] // Future Internet. — 2021. — Vol. 13, no. 10. — P. 1—17.

246. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA [Текст] / И. В. Котенко [и др.] // Защита информации. Инсайд. — 2019. — № 5. — С. 26—35.

247. *O'Gorman, L.* Comparing passwords, tokens, and biometrics for user authentication [Текст] / L. O'Gorman // Proceedings of the IEEE. — 2019. — Vol. 91, no. 12. — P. 2021—2040.

248. *Dodge, M.* Codes of life: Identification codes and the machine-readable world [Текст] / M. Dodge, R. Kitchin // Environment and Planning D: Society and Space. — 2005. — Vol. 23, no. 6. — P. 851—881.

249. *United States Patent.* Authentication and authorization protocol for secure web-based access to a protected resource [Текст] / H. M. Hinton, M. Vandenwauver. — No. US 7,478,434 B1 ; 01/13/2009 (US).

250. *Owens, J.* A study of passwords and methods used in brute-force SSH attacks [Текст] / J. Owens, J. Matthews // USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). — 2008. — P. 1—8. — URL: https://api.semanticscholar.org/CorpusID:15340523.

251. *Sood, S. K.* Cryptanalysis of password authentication schemes: Current status and key issues [Текст] / S. K. Sood, A. K. Sarje, K. Singh // 2009 Proceeding of International Conference on Methods and Models in Computer Science (ICM2CS). — IEEE. 2009. — P. 1—7.

252. An experimental investigation of malware attacks on SCADA systems [Текст] / I. N. Fovino [et al.] // International Journal of Critical Infrastructure Protection. — 2009. — Vol. 2, no. 4. — P. 139—145.

253. *Kim, J. J.* A method of risk assessment for multi-factor authentication [Текст] / J. J. Kim, S. P. Hong // Journal of Information Processing Systems. — 2011. — Vol. 7, no. 1. — P. 187—198.

254. *Tari, F.* A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords [Текст] / F. Tari, A. Ozok, S. H. Holden // Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS). — ACM. 2006. — P. 56—66.

255. *Chaudhari, S.* Design, implementation and analysis of multi layer, multi factor authentication (mfa) setup for webmail access in multi trust networks [Текст] / S. Chaudhari, S. S. Tomar, A. Rawat // 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). — IEEE. 2011. — P. 27—32.

256. *Pandey, P.* Challenges in single sign-on [Текст] / P. Pandey, T. N. Nisha // Journal of Physics: Conference Series. — 2021. — Vol. 1964, no. 4. — P. 042016.

257. *Aravindhan, K.* One time password: A survey [Текст] / K. Aravindhan, R. R. Karthiga // International Journal of Emerging Trends in Engineering and Development. — 2013. — Vol. 1, no. 3. — P. 613—623.

258. Combining user behavioural information at the feature level to enhance continuous authentication systems [Текст] / A. G. Martin [et al.] // Knowledge-Based Systems. — 2022. — Vol. 244. — P. 108544.

259. *Asep, H. S. G.* A design of continuous user verification for online exam proctoring on M-learning [Текст] / H. S. G. Asep, Y. Bandung // 2019 international conference on electrical engineering and informatics (ICEEI). — 2019. — P. 284—289.

260. *Gonzalez-Manzano, L.* Leveraging user-related internet of things for continuous authentication: A survey [Текст] / L. Gonzalez-Manzano, J. M. D. Fuentes, A. Ribagorda // ACM Computing Surveys. — 2019. — Vol. 52, no. 3. — P. 1—38.

261. *Shahzad, M.* Continuous authentication and authorization for the Internet of Things [Текст] / M. Shahzad, M. P. Singh // IEEE Internet Computing. — 2017. — Vol. 21, no. 2. — P. 86—90.

262. *Shahzad, M.* Continuous authentication and authorization for the Internet of Things [Текст] / M. Shahzad, M. P. Singh // IEEE Internet Computing. — 2017. — Vol. 21, no. 2. — P. 86—90.

263. *Schaffer, K. B.* Expanding continuous authentication with mobile devices [Текст] / K. B. Schaffer // Computer. — 2015. — Vol. 48, no. 11. — P. 92—95.

264. *De Fuentes, J. M.* Secure and usable userin-a-context continuous authentication in smartphones leveraging non-assisted sensors [Текст] / J. M. De Fuentes, L. Gonzalez-Manzano, A. Ribagorda // Sensors. — 2018. — Vol. 18, no. 4. — P. 12—19.

265. *Dahia, G.* Continuous authentication using biometrics: An advanced review [Текст] / G. Dahia, L. Jesus, P. S. M. // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. — 2020. — Vol. 10, no. 4. — e1365.

266. Digital Psychological Platform for Mass Web-Surveys [Текст] / E. Nikulchev [et al.] // Data. — 2020. — Vol. 5, no. 95. — P. 1—16.

267. User's reaction time for improvement of security and access control in web services [Текст] / S. Magomedov [et al.] // Applied Science. — 2021. — Vol. 11, no. 6. — P. 2561.

268. *Shikhaliev, A. P.* GLR, Rao, and Wald Tests for Distributed Parametric Detection in Subspace Interference [Текст] / A. P. Shikhaliev, B. Himed // IEEE Transactions on Signal Processing. — 2023. — Vol. 71. — P. 388—400.

269. ScriptingRT: A Software Library for Collecting Response Latencies in Online Studies of Cognition [Текст] / T. Schubert [et al.] // PloS one. — 2013. — Vol. 8. — P. 1—12.

270. *McGraw, K. O.* The Integrity of Web-Delivered Experiments: Can You Trust the Data? [Текст] / K. O. McGraw, M. D. Tew, J. E. Williams // Psychological Science. — 2000. — Vol. 11. — P. 502—506.

271. *Steenbergen, H. van.* Promises and pitfalls of Web-based experimentation in the advance of replicable psychological science: A reply to Plant [Текст] / H. van Steenbergen, B. R. Bocanegra // Behavior Research Methods. — 2016. — Vol. 48. — P. 1713—1717.

272. *Sarita, J. R.* Performance on the traditional and the touch screen, tablet versions of the Corsi Block and the Tower of Hanoi tasks [Текст] / J. R. Sarita, B. Gayle // Computers in Human Behavior. — 2016. — Vol. 60. — P. 29—34.

273. Web Application Resource Requirements Estimation Based on the Workload Latent Features [Текст] / A. Erradi [et al.] // IEEE Transactions on Services Computing. — 2021. — Vol. 14, no. 6. — P. 1638—1649.

274. Switching away: Exploring on-device media multitasking in web surveys [Текст] / J. K. Hohne [et al.] // Computers in Human Behavior. — 2020. — Vol. 111. — P. 1—11.

275. *Toninelli, D.* How Mobile Device Screen Size Affects Data Collected in Web Surveys [Текст] / D. Toninelli, M. Revilla // Advances in Questionnaire Design, Development, Evaluation and Testing. — 2019. — P. 349—373.

276. Инструменты статистической обработки результатов онлайн тестирования студентов [Текст] / Ш. Г. Магомедов [и др.] // International Journal of Open Information Technologies. — 2023. — Т. 11, № 5. — С. 94—99.

277. Real-time big data processing for anomaly detection: A Survey [Текст] / A. Habeeb [et al.] // International Journal of Information Management. — 2019. — Vol. 45. — P. 289—307.

278. *Chetverikov, A.* Online versus offline: The Web as a medium for response time data collection [Текст] / A. Chetverikov, P. Upravitelev // Behavior research methods. — 2016. — Vol. 48. — P. 1086—1099.

279. Контроль вовлеченности в интерактивное взаимодействие пользователя образовательных веб-сервисов на основе анализа реакций [Текст] / Ш. Г. Магомедов [и др.] // Современные информационные технологии и ИТ-образование. — 2023. — № 16. — С. 489—497.

280. A light weight smartphone based human activity recognition system with high accuracy [Текст] / M. O. Gani [et al.] // Journal of Network and Computer Applications. — 2019. — Vol. 141. — P. 59—72.

281. Engagement assessment for the educational web-service based on largest Lyapunov exponent calculation for user reaction time series [Текст] / S. Magomedov [et al.] // Education Sciences. — 2023. — Vol. 13, no. 2. — P. 1—12.

282. *Магомедов, Ш. Г.* Обеспечение безопасности открытых проектов Python: проблема оценки потенциально разрушительного функционала [Текст] / Ш. Г. Магомедов, С. А. Раковский // International Journal of Open Information Technologies. — 2023. — Т. 11, № 10. — С. 113—118.

283. *Nikulchev, E.* Technology stack selection model for software design of digital platforms [Текст] / E. Nikulchev, D. Ilin, A. Gusev // Mathematics. — 2021. — Vol. 9, no. 4. — P. 1—13.

284. *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. — Vol. 11, no. 11. — P. 4718.

285. *Борисов, А. В.* Имитационное моделирование распределенной экспертно-информационной системы [Текст] / А. В. Борисов // Известия Института инженерной физики. — 2008. — Т. 4, № 10. — С. 30—33.

286. *Босов, А. В.* Модели оптимизации функционирования информационного веб-портала [Текст] / А. В. Босов, А. В. Борисов // Труды Института системного анализа Российской академии наук. — 2009. — Т. 45. — С. 107—133.

287. *Шелухин, О. И.* Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями [Текст] /

О. И. Шелухин, А. А. Антонян // T-Comm-Телекоммуникации и Транспорт. — 2014. — Т. 8, № 6. — С. 61—64.

288. *Шелухин, О. И.* Фрактальные характеристики сетевых атак [Текст] / О. И. Шелухин, А. В. Долгова // Материалы XIII международной отраслевой научно-технической конференции "Технологии информационного общества". — 2019. — С. 405—409.

289. *Nikulchev, E.* Study of chaos in the traffic of computer networks [Текст] / E. Nikulchev, E. Pluzhnik // International Journal of Advanced Computer Science and Applications. — 2014. — Vol. 5, no. 9. — P. 60—62.

290. *Karpukhin, A.* Simulation of chaotic phenomena in infocommunication systems with the TCP protocol [Текст] / A. Karpukhin, D. Griciv, E. Nikulchev // Journal of Theoretical and Applied Information Technology. — 2018. — Vol. 96, no. 15. — P. 5080—5093.

291. JSON documents processing using situation-oriented databases [Текст] / V. Mironov [et al.] // Acta Polytechnica Hungarica. — 2020. — Vol. 17, no. 8. — P. 29—40.

292. *Петрушин, В. Н.* Адаптивно-вероятностная модель прогнозирования временных рядов [Текст] / В. Н. Петрушин, Г. О. Рытиков // Известия вузов. Проблемы полиграфии и издательского дела. — 2013. — № 6. — С. 125—140.

293. *Никульчев, Е. В.* Интервальная оценка средних значений случайной величины в условиях неопределенности функции плотности распределения вероятностей [Текст] / Е. В. Никульчев, В. Н. Петрушин, М. В. Ульянов // Известия вузов. Проблемы полиграфии и издательского дела. — 2013. — № 2. — С. 53—59.

294. *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.

295. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный комплекс обнаружения вредоносной активности в корпоративной сети [Текст] / Ш. Г. Магомедов [и др.]. — № 2021614531 ; заявл. 10.03.2021 ; опубл. 25.03.2021, 2021613300 (Рос. Федерация).

296. *Свидетельство о гос. регистрации программы для ЭВМ.* Конфигуратор настройки параметров работы сервера [Текст] / Ш. Г. Магомедов [и др.]. — № 2021664584 ; заявл. 25.08.2021 ; опубл. 09.09.2021, 2021663658 (Рос. Федерация).

297. *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.

298. *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).

299. Low-complexity access control scheme for MEC-based services [Текст] / M. Sepczuk [et al.] // 17th Conference on Computer Science and Intelligence Systems (FedCSIS 2022). — 2022. — P. 673—681.

Список рисунков

Список таблиц

Приложение А

Категории и возможности потенциальных нарушителей

Внешние нарушители, согласно ФСТЭК России, могут быть разделены на следующие категории:

- разведывательные службы государств;
- криминальные структуры;
- конкуренты (конкурирующие организации);
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель может иметь следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры информационной системы, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к информационной системе.

При реализации угроз безопасности представителями разведки иностранных государств способы их действий будут носить решительный характер и основываться на современных технологиях при высокой квалификации специалистов. Тем не менее, ИС не обрабатывает сведения, составляющие государственную тайну. Характер и объем информации, которую хранит и обрабатывает ИС, не могут быть интересны разведкам иностранных государств, поэтому не будем рассматривать потенциальных нарушителей этого типа.

Самый агрессивный источник внешних угроз – это криминальные структуры. Они способны пойти на открытое нарушение закона, привлекать спе-

циалистов в области защиты информации любыми средствами. Затраты на добычу информации в ИС, с учетом характера и объема информации, хранимой и обрабатываемой в данной ИС, будут экономически не обоснованными, потенциальные нарушители этого типа далее рассматриваться не будут. Так как задачи, решаемые ИС, носят некоммерческий характер, а конкурирующих организаций нет, то потенциальные нарушители данного типа не будут рассматриваться далее.

По методике ФСТЭК России внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа в информационную систему. Категории внутренних нарушителей и их способ доступа и полномочия доступа к информационной системе, а также возможности внутреннего нарушителя:

1. Первая категория:
   - Способ доступа – лица, имеющие санкционированный доступ к информационной системе, но не имеющие доступа к информации. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование информационной системы.
   - Полномочия доступа – лицо этой категории, может иметь доступ к фрагментам информации, содержащейся в информационной системе и распространяющейся по внутренним каналам связи информационной системы; располагать фрагментами информации о топологии информационной системы (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; располагать именами и вести выявление паролей зарегистрированных пользователей; изменять конфигурацию технических средств информационной системы, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам информационной системы.
2. Вторая категория:
   - Способ доступа – зарегистрированные пользователи информационной системы, осуществляющие ограниченный доступ к ресурсам информационной системы с рабочего места.

- Полномочия доступа – лицо этой категории: обладает всеми возможностями лиц первой категории; знает, по меньшей мере, одно легальное имя доступа; обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству информации; располагает конфиденциальными данными, к которым имеет доступ. Его доступ, аутентификация и права по доступу к некоторому подмножеству информации должны регламентироваться соответствующими правилами разграничения доступа.

3. Третья категория:
   - Способ доступа – зарегистрированные пользователи информационной системе, осуществляющие удаленный доступ к информационной системе по локальным и (или) распределенным информационным системам.
   - Полномочия доступа – лицо этой категории: обладает всеми возможностями лиц первой и второй категорий; располагает информацией о топологии информационной системы на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств информационной системы; имеет возможность прямого (физического) доступа к фрагментам технических средств информационной системы.
4. Четвертая категория:
   - Способ доступа – зарегистрированные пользователи информационной системы с полномочиями администратора безопасности сегмента (фрагмента) информационной системы.
   - Полномочия доступа – лицо этой категории: обладает всеми возможностями лиц предыдущих категорий; обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) информационной системы; обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) информационной системы; имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) информационной системы; имеет

доступ ко всем техническим средствам сегмента (фрагмента) информационной системы; обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) информационной системы.

5. Пятая категория:
   - Способ доступа – зарегистрированные пользователи с полномочиями системного администратора информационной системы.
   - Полномочия доступа – лицо этой категории: обладает всеми возможностями лиц предыдущих категорий; обладает полной информацией о системном и прикладном программном обеспечении информационной системы; обладает полной информацией о технических средствах и конфигурации информационной системы; имеет доступ ко всем техническим средствам обработки информации и данным информационной системы; обладает правами конфигурирования и административной настройки технических средств информационной системы. Системный администратор выполняет конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от несанкционированного доступа.
6. Шестая категория:
   - Способ доступа – зарегистрированные пользователи с полномочиями администратора безопасности информационной системы.
   - Полномочия доступа – лицо этой категории: обладает всеми возможностями лиц предыдущих категорий; обладает полной информацией об информационной системе; имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы; не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). Администратор безопасности отвечает за соблюдение правил разграничения

доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

7. Седьмая категория:
   - Способ доступа – программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.
   - Полномочия доступа – лицо этой категории обладает информацией об алгоритмах и программах обработки информации в информационной системе; обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы на стадии ее разработки, внедрения и сопровождения; может располагать любыми фрагментами информации о топологии информационной системы и технических средствах обработки и защиты информации, обрабатываемой в информационной системе.
8. Восьмая категория:
   - Способ доступа – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств в информационной системе.
   - Полномочия доступа – лицо этой категории: обладает возможностями внесения закладок в технические средства информационной системы на стадии их разработки, внедрения и сопровождения; может располагать любыми фрагментами информации о топологии информационной системы и технических средствах обработки и защиты информации в информационной системе.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных организационно-технических мер защиты, в том числе по допуску физических лиц к ИС и контролю порядка проведения работ.

К первой категории внутренних нарушителей ИС относятся: обслуживающий персонал организации (сторожа, вахтеры), работники инженерно-технических и административно-хозяйственных служб организации.

Ко второй категории внутренних нарушителей ИС относятся сотрудники иных организаций, являющиеся зарегистрированными пользователями ИС, который имеют ограниченный доступ к информационным ресурсам ИС с рабочего места в соответствии со своими должностями.

Третья категория внутренних нарушителей ИС – это сотрудники организаций, являющиеся зарегистрированными пользователями ИС, которые имеют удаленный доступ к информационным ресурсам ИС в рамках своих полномочий.

Четвертая категория внутренних нарушителей информационной системы к ИС не применима в виду отсутствия зарегистрированных пользователей информационной системы с полномочиями администратора безопасности сегмента (фрагмента) информационной системы.

К пятой категории внутренних нарушителей ИС относятся зарегистрированные пользователи с полномочиями системного администратора информационной системы.

К шестой категории внутренних нарушителей ИС относятся зарегистрированные пользователи с полномочиями администратора безопасности информационной системы.

К седьмой категории внутренних нарушителей ИС относятся программисты-разработчики программного обеспечения, входящего в состав информационной системы и лица, обеспечивающие его сопровождение на защищаемом объекте.

К восьмой категории внутренних нарушителей ИС относятся работники РТУ МИРЭА, обеспечивающие поставку, сопровождение и ремонт технических средств информационной системы.

Приложение Б

Порядок работы разработанной системы, реализующей научно-методический аппарат риск-ориентированного атрибутивного управления

Разработанная система, реализующая научно-методический аппарат риск-ориентированного атрибутивного управления, способна отслеживать активность пользователей и создает отчеты о поведении пользователей и производительности системы.

Порядок работы приложения:

1. Пользователь открывает веб-приложение в браузере и видит форму для ввода данных.
2. Пользователь вводит необходимую информацию и нажимает кнопку "Отправить". JavaScript отправляет асинхронный запрос на Flask-сервер через AJAX для обработки введенных данных.
3. Сервер Flask принимает запрос и обрабатывает данные, которые конвертируются в JSON который будет обработан политикой.
4. Запрос пользователя (листинг Б.1) сохраняется в логах с дополнительной меткой времени для последующего доступа и анализа.
5. Сервер применяет политики управления доступом на основе ABAC, определяющие, имеет ли пользователь право на доступ к этим данным.

Для примера выделим две политики:

– политика для высокого риска, которая явно запрещает удаление при высоком риске;
– политика для низкого риска, которая разрешает основные операции в базе данных на низком риске.

В зависимости от текущего риска системы будет применена одна из политик. Особенность риск-ориентированной модели в том что показатель риска используется как атрибут для политики и является динамическим, то есть рассчитывается в реальном времени. Таким образом при грамотной настройке политик можно запрещать или разрешать определенные действия в зависимости от текущего риска. Что позволит в случае выявления анома-

лий пользователя или конкретных инцидентов информационной безопасности уменьшить последствия или полностью остановить действия злоумышленника.

6 Запрос пользователя сохраняется в логах с дополнительной меткой времени для последующего доступа и анализа.

Листинг Б.1: Пример запроса пользователя:

```
{"subject":
        {"id": "",
                "attributes":
                {"role": "Teacher",
                        "device_type": "Personal Laptop",
                        "connection_type": "VPN"}},
        "resource":
        {"id": "",
                "attributes":
                {"service": "Science"}},
        "action":
        {"id": "",
                "attributes": {
                        "method": "Write"}},
        "context":
        {"risk": "Low"}}

{"subject": {
                "id": "",
                "attributes": {
                        "role": "Teacher",
                        "device_type": "Personal Laptop",
                        "connection_type": "VPN"}},
        "resource": {
                "id": "",
                "attributes": {
                        "service": "Science"}},
        "action": {
                "id": "",
                "attributes": {
                        "method": "Write"}},
        "context": {
                "risk": "Low"}
}
```

Разработанное приложение может быть интегрировано в различные системы и сервисы. В качестве демонстрационного примера была использована система электронного обучения и тестирования Moodle. Интеграция может проводиться следующим образом:

– в качестве отдельного плагина;

– как модификация уже существующих плагинов.

Для тестовой реализации был выбран второй вариант. Была проведена модификация плагина Database, который позволяет в пределах Moodle создать SQL базу данных и форму точки доступа для пользователей. Суть интеграции заключается в проверке каждой операции удаления, добавления и изменения файлов на предмет соответствия заданным политикам Py-ABAC. Проверка осуществляется посредством POST запросов на сервер Flask. Добавлена функция sendPostRequest в двух вариациях для реализации Delete и Write операций. Для определенных участков кода в которых реализованы нужный функционал добавлена дополнительная проверка которая посредством POST запроса к веб сервису на Flask проверят действие на соответствии политикам.

В момент, когда идет попытка создать, изменить или удалить запись отсылается POST запрос, который принимает Flask веб сервис, после обработки запроса возвращается логическая переменная, которая разрешает или запрещает выполнение операции (рис. Б.1). Данные об операции заносятся в лог файл веб сервиса Flask. Данные проверки можно встроить в любой участок PHP кода исходного плагина или использовать при разработки своего. В каталоге данного плагина были модифицированы следующие файлы: edit.php, lib.php, locallib.php, view.php.

При нажатии на соответствующую кнопку на веб сайте на веб сервис Flask приходит Json следующего содержания, представленного на рисунке Б.2.

Далее данные из этого JSON используются для формирования другого JSON, который идет на проверку. Риск, использующийся в процессе принятия решения, поступает посредством отдельного Request запроса на другой веб-сервис, который рассчитывает риск системы на основе анализа логов. После проверки создается запись в логах о транзакции и возвращается ответ в Moodle (рис. Б.3).

В соответствии с политиками в одном из курсов необходимо создать базу данных Science (рис. Б.4). Вне рамок курса у пользователя необходимо задать

роль в контексте всей системы, но текущая реализация получает роли на уровне контекста курсов.

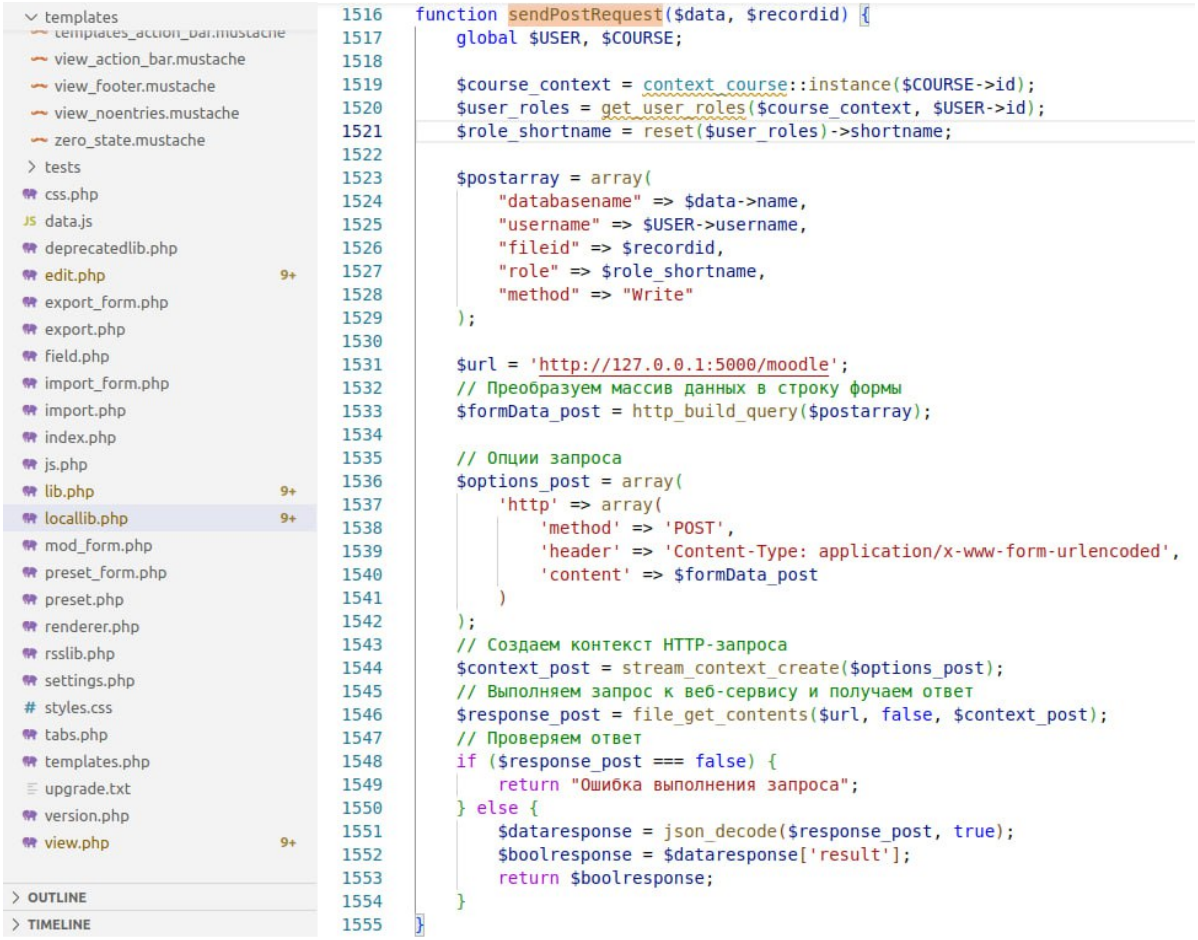


Рисунок Б.1 — Внедрение проверки веб сервиса Flask в участок PHP кода

```
127.0.0.1 - - [27/Apr/2024 23:19:47] "POST /moodle HTTP/1.1" 200 -
Поле 'databasename': 'Science'
Поле 'amp;username': 'admin'
Поле 'amp;fileid': '0'
Поле 'amp;role': 'student'
Поле 'amp;method': 'Write'
127.0.0.1 - - [27/Apr/2024 23:19:51] "POST /moodle HTTP/1.1" 200 -
Поле 'databasename': 'Science'
Поле 'amp;username': 'admin'
Поле 'amp;fileid': '0'
Поле 'amp;role': 'student'
Поле 'amp;method': 'Write'
127.0.0.1 - - [27/Apr/2024 23:19:58] "POST /moodle HTTP/1.1" 200 -
Поле 'databasename': 'Science'
Поле 'amp;username': 'admin'
Поле 'amp;fileid': '0'
Поле 'amp;role': 'student'
Поле 'amp;method': 'Write'
```

Рисунок Б.2 — Сформированный файл JSON веб сервисом Flask

```
71  student,Personal Laptop,VPN,Science,Write,High,None,False,1713809468
72  student,Personal Laptop,VPN,Science,Write,High,None,False,1714245882
73  student,Personal Laptop,VPN,Science,Write,Low,None,True,1714245903
74  student,Personal Laptop,VPN,Science,Delete,Low,204,True,1714245908
75  student,Personal Laptop,VPN,Science,Write,High,None,False,1714246039
76  student,Personal Laptop,VPN,Science,Write,High,None,False,1714246042
77  student,Personal Laptop,VPN,Science,Write,High,0,False,1714246922
78  student,Personal Laptop,VPN,Science,Write,High,0,False,1714246943
79  student,Personal Laptop,VPN,Science,Write,High,0,False,1714246963
80  student,Personal Laptop,VPN,Science,Delete,High,202,False,1714247522
81  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249092
82  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249147
83  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249187
84  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249191
85  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249198
86  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249201
87  student,Personal Laptop,VPN,Science,Write,High,0,False,1714249375
88  student,Personal Laptop,VPN,Science,Delete,High,202,False,1714249617
89
```

Рисунок Б.3 — Пример создания лог-файла о транзакции

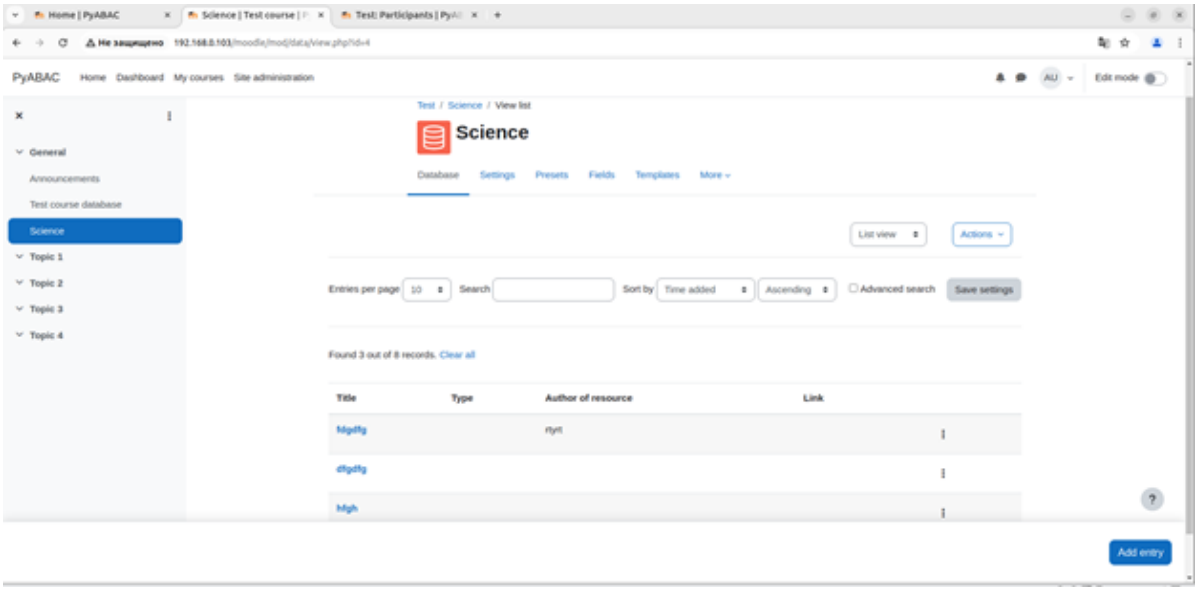


Рисунок Б.4 — Пример создания базы данных Science

В базе данных создано некоторое количество записей. Текущий риск системы высокий. На момент создания скриншотов риск задается статически, но после реализации сервиса расчета риска он будет передаваться в реальном времени посредством POST запросов. На рисунке Б.5 код Python который обрабатывает запросы со стороны веб сервиса управления доступом.

Текущий пользователь это Admin User. Для корректной обработки политик требуется задавать роли во вкладке курса "Participants" (рис. Б.6).

Исходя из того, что текущая роль у пользователя – студент, ему запрещено как изменять, так и удалять файлы в базе данных. Попытка сохранить эту запись приведет к срабатыванию разработанной системы (рис. Б.7).

```python
@app.route('/moodle', methods=['POST'])  # Маршрут для обработки данных из формы
def moodle_form():
    if request.method == 'POST':
        # Запись в дебаг лог.
        with open('temp_data.txt', mode='w', newline='') as file:
            exit = []
            for key, value in request.form.items():
                print(f"Поле '{key}': '{value}'")
                exit.append(f"Поле '{key}': '{value}'")
            json.dump(request.form, file)
        #
        role = str(request.form.get('amp;role'))
        device_type = "Personal Laptop"
        connection_type = "VPN"
        service = str(request.form.get('databasename'))
        method = str(request.form.get('amp;method'))
        file_id = str(request.form.get('amp;fileid'))
        risk = "High"
        decision = policy_handler.policy_proc(role, device_type, connection_type, service, method, risk)

        list_to_log = [role,device_type,connection_type,service,method,risk,file_id,str(decision[0])]
        policy_handler.logger(list_to_log) # Функция отправления записи в лог

        return jsonify({'result': decision[0]})
```

Рисунок Б.5 — Программный код, обрабатывающий запросы со стороны веб сервиса управления доступом

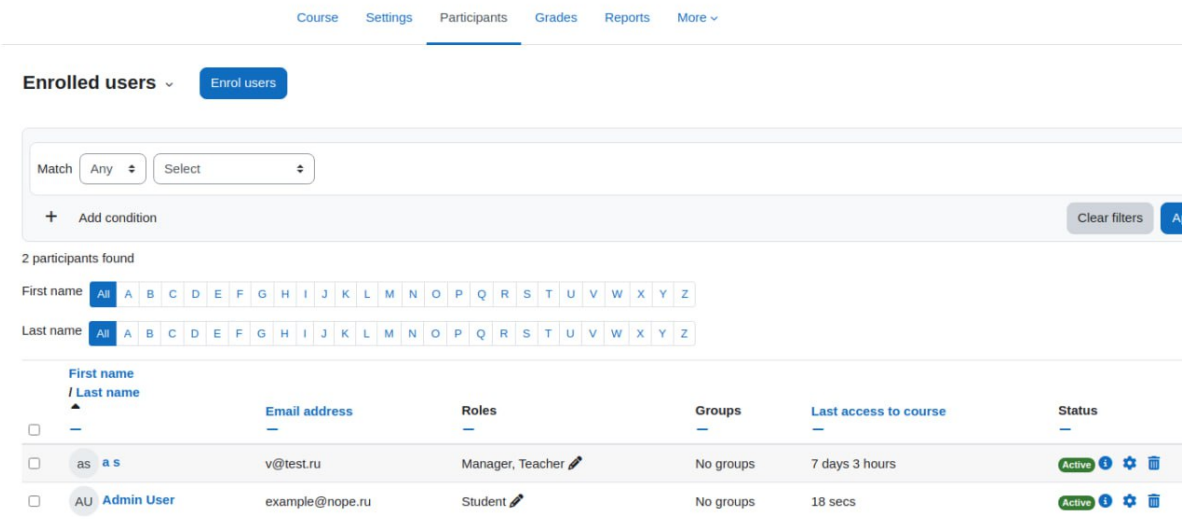


Рисунок Б.6 — Пример задания роли пользователю во вкладке курса

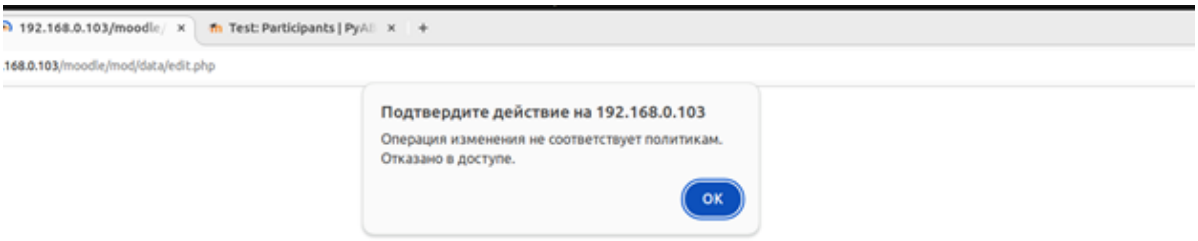


Рисунок Б.7 — Блокирование внесения несанкционированных изменений

При попытке удалить запись также появится окно схожего содержания (рис. Б.8).

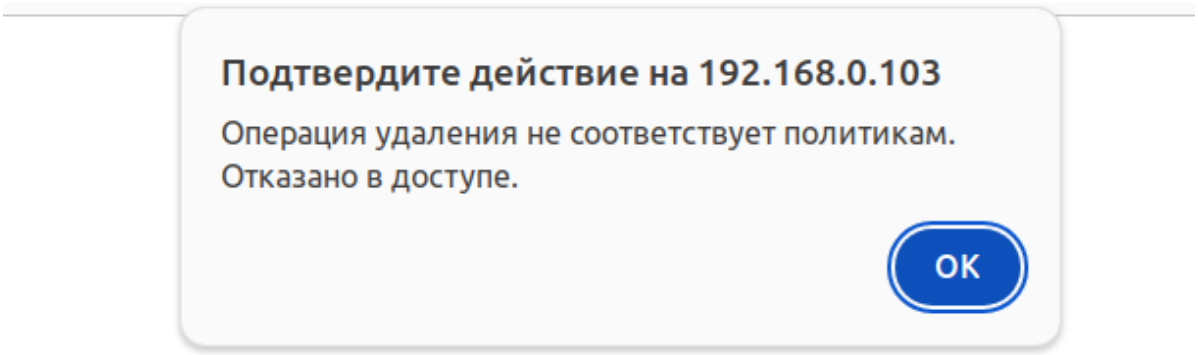


Рисунок Б.8 — Блокирование удаления выполненных действий

В этот момент на стороне Moodle функция sendPostRequest отправляет запрос на веб сервис политик (рис. Б.9).

```
$boolresponse = sendPostRequest1($data, $delete);
if ($boolresponse) {
    if (data_delete_record($delete, $data, $course->id, $cm->id)) {
        echo $OUTPUT->notification(get_string('recorddeleted','data'), 'notifysuccess');
    }
} else {
    echo '<script>alert("Операция удаления не соответствует политикам. Отказано в доступе.");</script>';
}
else {   // Print a confirmation page
```

Рисунок Б.9 — Отчет о блокировании запрещенных действий