На правах рукописи

Магомедов Шамиль Гасангусейнович

Методы и модели построения масштабируемой архитектуры системы контроля доступа к вычислительным сервисам

05.13.15 — Вычислительные машины, комплексы и компьютерные сети

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

доктора технических наук

Москва – 2022

Работа выполнена на кафедре «Интеллектуальные системы информационной безопасности» Федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет» (РТУ МИРЭА)

Научный консультант: доктор военных наук, профессор, профессор кафедры КБ-2 «Прикладные информационные технологии» РТУ МИРЭА
Лось Владимир Павлович

Официальные оппоненты:
Алчинов Александр Иванович
доктор технических наук, профессор, ведущий научный сотрудник Лаборатории 46 Федерального государственного бюджетного учреждения науки Институт проблем управления им. В. А. Трапезникова Российской академии наук
Барахнин Владимир Борисович
доктор технических наук, доцент, ведущий научный сотрудник лаборатории информационных ресурсов Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр информационных и вычислительных технологий»
Козачок Александр Васильевич
доктор технических наук, доцент, сотрудник ФГКВОУ ВО «Академия Федеральной службы охраны Российской Федерации»

Ведущая организация: Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»

Защита состоится 28 сентября 2022 г. в 10 часов 00 минут на заседании диссертационного совета Д 002.073.02 при Федеральном исследовательском центре «Информатика и управление» Российской академии наук, по адресу: 119333, Москва, Вавилова, д. 44, кор. 2.

С диссертацией можно ознакомиться в библиотеке Федерального исследовательского центра «Информатика и управление» Российской академии наук, по адресу: 119333, Москва, Вавилова, д. 44, кор. 2 и на сайте: http://www.frccsc.ru

Автореферат разослан «___» _____ 2022 года

Ученый секретарь диссертационного совета  Р.В. Разумчик

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. В настоящее время все больше государственных, медицинских, банковских, образовательных и прочих услуг переносится в цифровую среду. Активное развитие цифровизации определило ее массовое проникновение во все сферы жизни и деятельности. Экономические отношения и отношения людей с государственными органами принимают форму взаимодействия с вычислительными сервисами по компьютерным сетям. Основным инструментом цифровой среды становятся веб-сервисы (или цифровые порталы, вычислительные сервисы, далее — ВС) или специализированные приложения, подключенные к общедоступным сетям.

В развивающейся цифровой среде разработчики ВС стоят перед разрешением противоречия: с одной стороны — вычислительный сервис должен быть максимально доступен, платформонезависим, удобен и прост в использовании (желательно, например, в «один клик»); с другой — предоставляемые услуги связаны с большим количеством персональных, медицинских, банковских и прочих конфиденциальных данных, защита которых требует значительного дополнительного контроля, верификации пользователя. Для обеспечения защищенного контроля доступа (КД) используются технологии информационной безопасности. Подключение внешних модулей к вычислительному комплексу, обслуживающему ВС, требует учета вычислительных ресурсов, определения точек интеграции компонентов контроля доступа.

Системы КД являются частью информационных систем, обеспечивающих ВС, в тоже время КД представляют собой отдельные компоненты, под управление КД выделяется часть инфраструктуры, виртуальные и физические ресурсы ВК, то есть система КД — это самостоятельный объект со своими задачами проектирования и конфигурирования. Системы КД могут развиваться отдельно от собственно технологий, обеспечивающих предоставление ВС, могут добавляться реализации новых концепций КД, обновляться и изменяться программное, аппаратное обеспечение, не затрагивая основных функциональных возможностей ВС. Все вышесказанное делает актуальной задачу проведения теоретических, экспериментальных, структурных, программно-аппаратных исследований по разработке принципов и решений по построению новых и совершенствованию существующих средств защищенного доступа к ВС на основе построения масштабируемой архитектуры системы КД, обеспечивающих функционирование многопользовательских ВК.

В ВС имеется ряд специфических задач, связанных с КД: передача паролей и средств контроля сторонним лицам; защита от перехвата паролей программными средствами; выявление ситуаций, в которых пользователь, прошедший все способы верификации, оставил систему активной (сознательно или случайно), а другой пользователь стал взаимодействовать с ВС и др., требующие по-

стоянного подтверждения личности пользователя в процессе взаимодействия. В банковских антифрод-системах используется система анализа подозрительных операций; в системах с повышенной конфиденциальностью используются средства, анализирующие поведение пользователя. Включение компонентов анализа поведения пользователя и других потенциальных современных технологий должно быть обеспечено масштабируемостью архитектуры КД.

Таким образом, разработка методов и моделей построения масштабируемой архитектуры контроля доступа к вычислительным сервисам на основе совершенствования существующих средств защиты информации, является актуальной задачей, имеющей важное значение для развития современной защищенной цифровой среды.

Научная проблема. Системы КД к информационным ресурсам развиваются параллельно с самими информационными системами: чем больше функций, разных категорий доступа к данным, тем сложнее становится контроль. Это определяет проблему построения такого организационно-технологического решения, которое позволяло бы наращивать мощности и совершенствование технологий информационной безопасности в рамках общей вычислительной архитектуры и инфраструктуры. Особенно важным контроль доступа является для веб-сервисов, порталов, предоставляющих доступ по компьютерным сетям общего пользования, в этих случаях добавляется необходимость постоянной верификации пользователя, защиты от несанкционированного доступа со стороны субъектов и программных систем. Системы контроля в соответствии с новыми технологиями должны иметь возможность совершенствования КД и системы предупреждения киберугроз. Таким образом, в настоящее время стоит проблема, требующая научных теоретических и экспериментальных исследований по разработке принципов, методов и моделей построения архитектуры контроля доступа к ВС, обеспечивающей интеграцию технологий передачи, хранения, мониторинга, идентификации и аутентификации пользователей и субъектов информационных процессов.

Состояние проблемы. В настоящее время развиваются системы КД, основанные на концепции SIEM (Security information and event management), которая объединяет мониторинг событий в реальном времени и управление информационной безопасностью. Существуют коммерческие решения SIEM-систем: QRadar IBM, Arc Sight HP, Symantec Security Services, FortiSIEM и др. Разработке SIEM-систем, выявлению источников угроз и механизмов их выявления посвящено значительное количество современных исследований: в распределенных системах (И.В. Котенко, И.Б. Саенко, А.В. Степашкина, L. Kufel, L. Coppolino, S. D’Antonio, N. Kheir, M. Frigault и др.); для блокировки вредоносного трафика с устройств IoT (Н.Г. Милославская, B. Al-Duwairi, R. Fahmawi и др.); исследование по интеллектуальной обработке данных из нескольких источников (J. Lee, J. Kim, N. Moukafih, G. Orhanou, S. El Hajji и др.);

по использованию методов классификации событий (J.C. Sancho; A. Caro, A. Walker, J. Svacina, A.S.M. Kayes, R. Kalaria, M. Islam и др.) и многие другие исследования.

Для веб-сервисов одним из способов является использование role-based access control (RBAC), где каждая точка входа связана с набором ролей пользователя. Различные исследовательские группы разработали контекстно-зависимые подходы и структуры управления доступом, которые различаются своими контекстными моделями, моделями политик и возможностями рассуждений. Было предложено несколько моделей управления доступом на основе ролей, включающих в политики динамически изменяющиеся контекстные условия (например, информацию, ориентированную на местоположение пользователя и ресурсы). Подобно пространственному и временному подходам, эти контекстно-зависимые подходы в основном зависят от предметной области и принимают во внимание определенные типы контекстных условий. Контекстно-зависимый подход к управлению доступом на основе ролей был разработан для облегчения управления доступом к ресурсам данных на основе широкого диапазона контекстных условий.

Перспективным направлением многопользовательских сервисов является анализ контроля доступа на основе шаблонов поведения — технологии UBA (анализ поведения пользователей, User behavior analytics). Предложены разные варианты развития UBA: использование интеллектуальных технологий, применение встраиваемых динамических моделей в интернет-приложения (В.В. Миронов и соавт.); ситуационные и прецедентные модели (K. Csaba, H.B. Péter, X. Xi, T. Zhang и др.) и т.п. Современные психологические исследования выявили достоверность данных по исследованию реакций, полученных с использованием веб-интерфейсов с данными, полученными в лабораторных условиях, что позволяет признать целесообразным использование психомоторных реакций.

В настоящее время SIEM и UBA рассматриваются как дополняющие друг друга концепции. При внедрении их в практику выясняется ряд нерешенных задач, связанных с возможностью интеграции вычислительных комплексов, масштабируемости, ресурсоэффективности, точек подключения систем мониторинга, выбора способов и места для хранения вспомогательных данных, направления и анализа потоков данных, и прочих вопросов, относящихся к архитектуре, структуре и технологиям вычислительных комплексов.

Типовая архитектура внедряемых систем КД включает в себя следующие уровни: сетевой; систем хранения; инфраструктуры приложений; систем управления; систем безопасности. Такой подход обеспечивает решение задач безопасности без учета ресурсных затрат и способов обработки данных КД, что затрудняет внедрение. Работы по масштабируемой архитектуре комплексов обес-

печения сетевой безопасности (О.Ю. Гузев, И.В. Чижов) определяют следующий состав: аппаратная платформа, виртуальные машины, программный гипервизор, средства управления вычислительной инфраструктурой, средства управления коммутацией сетевого трафика, средства коммутации сетевого трафика. Однако этот подход нацелен на конкретные технологии реализации анализа сетевого трафика и управления виртуальными ресурсами, не вводя методологические принципы построения архитектуры КД, что не дает возможность учесть совершенствование технологий и масштабируемость.

Таким образом, все вышеперечисленные результаты дают предпосылки для проведения теоретических и экспериментальных исследований по разработке принципов, методов и моделей построения масштабируемой архитектуры КД для обеспечения защищенного доступа к ВС.

Цель исследования: разработка принципов, методов и моделей построения масштабируемой архитектуры контроля управлением доступа, обеспечивающей интеграцию технологий передачи, хранения, мониторинга, идентификации и аутентификации пользователей и субъектов информационных процессов доступа к вычислительным сервисам по компьютерным сетям.

Для реализации цели были поставлены и решены **следующие задачи**:

1. Обзор подходов к построению архитектур и используемых технологий обеспечения разграничения и контроля доступа к ВС.
2. Анализ общих моделей ВС и выявление особенностей интеграции технологий КД.
3. Исследование особенностей архитектуры и технологии построения SIEM и UBA-систем.
4. Формирование комплекса методов и моделей построения многоуровневой масштабируемой архитектуры КД.
5. Разработка методики проектирования инфраструктуры виртуальных ресурсов КД.
6. Разработка метода оценки ресурсных затрат при внедрении технологий КД.
7. Разработка ресурсоэффективного метода КД для анализа поведения пользователей.
8. Разработка методик учета прикладных аспектов при разработке архитектуры КД.

Объектом исследования в диссертации являются программно-аппаратные средства защиты информации в информационных системах, обеспечивающих предоставление вычислительных сервисов по общедоступным компьютерным сетям.

Предметом исследования являются архитектуры, технологии реализации КД, включающие системы идентификации и аутентификации пользователей и

субъектов информационных процессов, связанных с действиями устройств и пользователей при взаимодействии с вычислительными сервисами.

Методология и методы исследования. В работе использованы методологии, методы и модели проектирования архитектуры вычислительных комплексов, проектирования и исследования систем контроля доступа, теории хранения данных, методологии облачных технологий, методы моделирования защищенных распределенных систем; методы планирования экспериментов и статистической обработки экспериментальных данных.

Новизна научных результатов диссертационного исследования заключается в следующем:

1. Сформулированы принципы и модели построения архитектуры системы КД как подсистемы программно-аппаратного вычислительного комплекса, имеющей собственные задачи: сбор, передачу, хранение и обработку данных о действиях пользователей и программных систем, методы, ресурсы и технологии обработки которых независимы от используемых для предоставления ВС. Таким образом, система КД требует собственных вычислительных ресурсов, при этом должны быть соблюдены технико-экономические ограничения. Предложенный подход позволяет сформулировать ряд задач, являющихся типовыми для рассматриваемого класса объектов: определить состав системы сбора данных, содержащих информацию о доступе к ВС; сформировать виртуальную инфраструктуру для обработки данных КД; определить состав и технико-экономические требования к вычислительным ресурсам для компонентов анализа данных системы КД.

2. Разработана четырехуровневая масштабируемая архитектура системы контроля доступа, интегрируемая в вычислительные комплексы, обеспечивающие защиту взаимодействия пользователей с ВС. Архитектура включает комплекс понятий и свойств системы КД, реализованных в ее элементах, взаимосвязи компонентов, основанных на реализации функций КД. Масштабируемость архитектуры определяется наличием четырех уровней, на каждом из уровней определен специфический класс задач, который может быть реализован разными вариантами технологических решений, что позволяет внедрять различные технологии КД: SIEM, UBA и др.

3. Разработана методика построения облачной инфраструктуры, обеспечивающей решение задач КД. Сформированы принципы решения задач сбора и перенаправления специализированных данных о доступе к ВС, для которых требуется с использованием облачных технологий виртуализировать ресурсы с целью обеспечения параллельного решения задач КД с основными функциями ВС.

4. Разработаны модель и метод анализа затрат вычислительных ресурсов для реализации систем контроля доступа на основе подхода, использующего

имитационные виртуальные стенды в условиях заданных характеристик эксплуатации.

5. Предложен метод контроля доступа на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы. Предложенный метод дополняет и совершенствует существующие методы верификации пользователей при доступе в ВС.

6. Разработаны методики учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов (на примере медицинских и образовательных услуг).

7. Разработаны принципы и информационные модели проектирования архитектуры системы КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза.

Достоверность и обоснованность научных результатов и рекомендаций, приведенных в диссертационной работе, основаны на корректном использовании архитектурных, структурных, логических и программно-аппаратных методов создания систем защиты информации, на применении вычислительно надежных моделей, проведении экспериментальных исследований, а также апробации и обсуждении результатов на международных научных конференциях и семинарах, публикациях результатов в рецензируемых отечественных и международных научных изданиях.

Теоретическая и практическая значимость работы. Результаты работы были использованы при выполнении работ по грантам и договорам:

1) государственный контракт № 087/ГК на выполнение работ (оказание услуг) для государственных нужд «Создание цифровой образовательной среды и разработка (доработка) ЭОР для учителей школ за рубежом», проводимый в рамках Национальной программы «Цифровая экономика Российской Федерации» утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16;

2) соглашение о предоставлении из федерального бюджета субсидии в соответствии с абзацем вторым пункта 1 статьи 78.1 Бюджетного кодекса Российской Федерации (внутренний номер 08-01/Х4354/706) № 075-02-2019-2358 от 20.11.2019, «Проектирование интеграционной платформы непрерывного образования»;

3) соглашение о предоставлении из федерального бюджета субсидии в соответствии с абзацем вторым пункта 1 статьи 78.1 Бюджетного кодекса Российской Федерации (внутренний номер 08-04/Х4354/706) № 075-02-2020-1583 от 06 апреля 2020 года, «Разработка и реализация мер по выделению грантов аспирантам и молодым ученым и проведению научно-образовательных и проект-

ных мероприятий в области информационной безопасности для задач цифровой экономики»;

4) договор № 308ГРНТИС5/42860-3 от 30.10.2018 г по выполнению проекта «Развитие системы поддержки принятия врачебных решений на основе международных баз данных по доказательной медицине и в соответствии с Национальными клиническими рекомендациями и Стандартами оказания медицинской помощи в Российской Федерации, в том числе для наблюдения за больными с профессиональными заболеваниями и с высоким риском их развития и для профилактики и лечения возраст-зависимых патологических процессов и заболеваний».

Результаты работы использованы при разработке веб сервисов и информационных систем в РТУ МИРЭА, Федеральном бюро медико-социальной экспертизы Министерства труда и социальной защиты Российской Федерации, ФГУП «НПО «Техномаш», ООО «Непрерывные технологии», ООО «КПР», ФГУП «НТЦ «Орион», ООО «Лаборатория Наносемантика».

Апробация работы. Основные положения и результаты исследования, составляющие содержание диссертации, докладывались и обсуждались на Futuristic Trends in Networks and Computing Technologies (FTNCT-2020) (Таганрог, 13–15.10.2020); Научно-практической конференции «Цифровые аналитические инструменты и прикладные программы в образовании» (Москва, РАО, 27.10.2020); Big Data & AI Conference 2020 (Москва, 17–18.09.2020); II Всероссийской научно-технической конференции «Состояние и перспективы развития современной науки по направлению «Информационная безопасность» (Анапа, 19–20.03.2020); V региональной научной конференции «Прикладные исследования и технологии» ART2018 (Москва, 15–16.08.2018); XXVII научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт Петербург, 24–27.09.2018); III Всероссийской научно-практической конференции «Информационные технологии в экономике и управлении» (Махачкала, 29–30.11.2018); Межвузовской школе-семинаре «Задачи системного анализа, управления и обработки информации» (Москва, МТИ, 2017, 2019); LXVI Международной научно-практической конференции «Технические науки — от теории к практике» (Новосибирск, 2017); Всероссийской научно-практической конференции «Актуальные проблемы науки и практики в предпринимательстве» (24.03.2017); XX Международной научно-практической конференции «Теории и практика современной науки» (22.03.2017); V Международной научно-практической электронной конференции «Социально-антропологические проблемы информационного общества» (10.03.2017); VI Международной научно-практической электронной конференции «Современные научные исследования: актуальные теории и концепции» (10.04.2017); XV Международной научно-практической конференции «Науч-

ный поиск в современном мире» (31.04.2017); XIII Международной научно-практической конференция «Теоретические и практические проблемы развития современной науки» (31.03.2017).

Основные положения и результаты, выносимые на защиту:

1. Принципы и модели построения архитектуры системы КД, как подсистемы программно-аппаратного вычислительного комплекса, имеющей собственные данные, цели, задачи и технологии реализации, отличные от ВС. Отличие от альтернативных подходов связано с возможностью параллельной разработки, поэтапного внедрения, возможностью замены или расширения элементов системы КД, что можно реализовать, с одной стороны — независимо, с другой — используя требования и условия эксплуатации. Построение КД, разработанного в соответствии с предложенными принципами, позволяет провести обоснованную оценку вычислительных ресурсов, что дает возможность сократить затраты на внедрение КД, обеспечить миграцию на новые технологии, возможность поэтапного внедрения отдельных компонентов КД.

2. Четырехуровневая масштабируемая архитектура системы КД, интегрируемая в вычислительную среду ВС, обеспечивающая защищенный доступ: 1) программно-аппаратный уровень, включающий средства, обеспечивающие КД; 2) уровень виртуальной инфраструктуры обработки данных системы КД; 3) уровень физических ресурсов для обработки данных КД; 4) уровень компонентов анализа данных. Четырехуровневость обеспечивает интуитивно понятную декомпозицию задач, решение которых может быть осуществлено специалистами разных квалификаций, а также совершенствование методов и моделей на каждом уровне независимо от других уровней архитектуры. Архитектура может быть реализована разными вариантами технологических решений.

3. Методика построения облачной инфраструктуры, обеспечивающей решение задач КД. Методика основана на принципе сбора и перенаправления специализированных данных о доступе к ВС, выделении прав защищенного доступа, основанного на выявлении серверных ролей. Облачная инфраструктура, в отличие от иных решений, позволяет обеспечить миграцию системы КД.

4. Метод и модель ресурсного анализа реализации элементов системы КД на основе имитационных исследований. Особенностью метода является повышение эффективности использования логирования сеансов доступа, позволяющее получить экспериментальные оценки скорости обработки, объемов и ширины каналов и др. характеристик ресурсов, требуемых для модулей КД.

5. Новый метод и соответствующая система КД на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы. Предложенный метод дополняет и совершенствует существующие методы верификации пользователей при доступе в ВС. Метод позволяет учитывать персональные реакции

только на основе времени ответа на контрольные вопросы, что позволяет существенно сократить затраты ресурсов для оперативного анализа.

6. Методики учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов на примере медицинских и образовательных услуг. Предложенные методики направлены на сокращение затрат вычислительных ресурсов, обеспечивающих заданный уровень защищенности взаимодействия пользователей с вычислительными сервисами.

7. Разработаны принципы и информационные модели проектирования архитектуры системы КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза в условиях защищенной цифровой образовательной среды. Использование разработанных методов и моделей КД способствует повышению защищенности образовательных ресурсов от несанкционированного доступа.

Соответствие паспорту специальности. Тема исследования и полученные результаты соответствуют областям исследования, изложенным в пунктах 1, 2 и 5 паспорта специальности 05.13.15 – Вычислительные машины, комплексы и компьютерные сети.

Публикации по теме диссертации. Основные результаты диссертационного исследования опубликованы в 51 работе, из них: 14 — в изданиях, включенных в перечень рецензируемых журналов, рекомендованных ВАК по специальности 05.13.15; 20 — индексируемых в Web of Science/Scopus (включая квартиль Q1/Q2); 9 свидетельств о регистрации РИД.

Личный вклад. Все выносимые на защиту результаты получены лично автором. В работах, опубликованных в соавторстве, личный вклад состоит в разработке архитектуры вычислительных комплексов, средств контроля доступа, методик контроля доступа на основе технологий SIEM и UBA.

Структура и объем диссертационной работы. Материалы диссертации изложены на 318 страницах машинописного текста, включают введение, 7 глав, заключение, список литературы (249 источников), приложения. Работа содержит 33 таблицы, 70 рисунков.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

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

В первой главе «**Обзор подходов к построению архитектур и используемых технологий обеспечения контроля доступа к вычислительным сер-**

висам» проведен анализ современных вычислительных инфраструктур, систем и комплексов, обеспечивающих поддержку и контроль доступа в информационной среде цифровых услуг.

В условиях цифровой среды и цифровизации общества современные вычислительные сервисы представляют собой распределенные системы, обеспечивающие взаимодействие с пользователями по компьютерным сетям с использованием веб-интерфейсов или специализированных приложений с доступом к внутренней вычислительной инфраструктуре. ВС в современной цифровой среде имеют ряд общих особенностей: веб-интерфейс, цифровую платформу или приложение с доступом по сети, большое количество пользователей, сложную инфраструктуру хранения данных на внутренних или облачных сервисах, разграничение прав доступа к данным и различные функции, предоставляемые определенным группам пользователей.

В работе, в соответствии с ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 «Системная и программная инженерия. Описание архитектуры» (введен 01.09.2017), под *архитектурой* ВК понимается «комплекс основных понятий, свойств системы в окружающей среде, воплощенной в ее элементах, отношениях и конкретных принципах ее проекта и развития». Согласно стандарту, архитектура характеризуется: набором системных компонентов или элементов; как системные элементы устроены или взаимосвязаны; принципами организации системы или проекта; принципами, управляющими развитием системы в ее жизненном цикле.

Под *масштабируемостью* архитектуры КД понимается возможность увеличения используемых технологических принципов и наращивания дополнительных ресурсов ВК без структурных изменений основных узлов комплекса.

Проведен анализ используемых компонентов, протоколов и стандартов передачи данных, концепций построения защищенных вычислительных архитектур. Рассмотрен структурный подход к проектированию и управлению распределенными вычислительными системами. Выявлены этапы организации и проектирования архитектуры информационных систем.

Рассмотрены SIEM-системы, которые возникли в результате слияния систем SEM и SIM. SEM (Security Event Management) — системы, которые действуют во времени, приближенном к реальному, включают мониторинг событий и генерацию предупреждающих сообщений. SIM (Security Information Management) — системы, которые анализируют накопленную статистическую информацию и фиксируют различные отклонения.

Выявлены наиболее перспективные направления повышения эффективности SIEM-систем: автоматизация реагирования на инциденты, технологии анализа трафика, анализ происходящего на конечных узлах, мониторинг поведения пользователей, использование облачных технологий. Показано, что важным направлением признано добавление к возможностям SIEM инструментов UBA,

таким образом, что SIEM-система выступает в качестве конструктора для сбора данных, а решение UBA строит поведенческие модели.

Рассмотрены прикладные аспекты систем КД в современной цифровой среде — в системах здравоохранения и образования.

Таким образом, сформулированы основные направления исследований и уточнены задачи, решение которых направлено на достижение цели диссертационного исследования.

Во второй главе «**Разработка многоуровневой масштабируемой архитектуры контроля доступа**» сформулированы задача проектирования архитектуры, требования к составу средств КД, разработана четырехуровневая архитектура КД.

Рассмотрена типовая система доступа в ВС, со средствами контроля, идентификации и верификации пользователей (рис. 1).

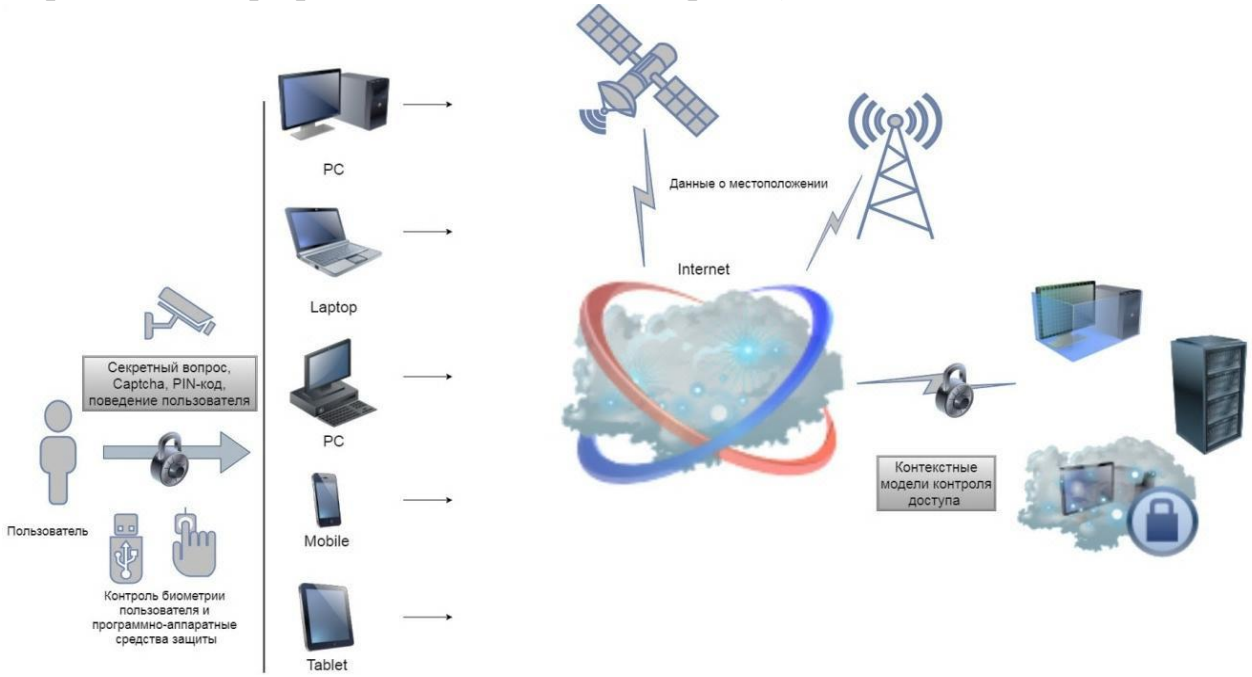


Рис. 1 — Архитектура вычислительного комплекса
с многоуровневым контролем доступа

Предложенная концепция позволяет задачу проектирования архитектуры КД рассматривать как задачу формирования в рамках ВК, предоставляющего ВС, подсистему, включающую комплекс понятий и свойств КД, реализованных в ее элементах, взаимосвязи компонентов, основанных на реализации функций КД. Конкретные задачи заключаются в определении: системы сбора данных; виртуальной инфраструктуры для обработки данных КД; состава требований к вычислительным ресурсам, учитывающих и технико-экономические требования к условиям функционирования; взаимосвязи компонентов анализа данных КД.

Перед системой SIEM ставятся следующие задачи: консолидация и хранение журналов событий от различных источников; предоставление инструментов для анализа событий и разбора инцидентов; корреляция и обработка событий по правилам; инцидент-менеджмент. Рассмотрены типовые схемы и модели SIEM-систем. Схема реализуется с помощью компонентов: агенты (сбор данных из различных источников); серверы-коллекторы (аккумуляция информации, поступившей от агентов); сервер баз данных (хранение информации); сервер анализа информации.

Сформированы принципы построения архитектуры, реализующей SIEM и UBA-технологии. Клиентскими устройствами, с помощью которых пользователи подключаются через общедоступные сети к веб-сервисам, могут быть сетевые компьютеры, портативные компьютеры, карманные компьютеры, смартфоны, умные часы, умные телевизоры, игровые устройства и т. д. Программное обеспечение, интегрированное в состав информационного обеспечения сервисов и управления доступом и обработке данных, реализует следующие функции: фиксирование, передачу и хранение данных о доступе пользователей к вычислительным сервисам; генерацию правил и прогноз значений (оценка вероятных значений) маркеров поведения пользователей в соответствии с заданными политиками защищенного доступа, сравнение полученных показателей с шаблонными персонифицированными значениями. Серверы вместе с системой хранения данных (СХД) подключены к сети. Виртуальные серверы включают в себя диспетчер событий и анализатор. Сервера могут отправлять инциденты безопасности на компоненты анализа на основе идентифицированных характеристик инцидентов безопасности, обнаруженных во время локального анализа с помощью информации безопасности и диспетчера событий

Для эффективности системы обеспечения КД в качестве целевых показателей предлагается использовать стохастические методы — использование величины, равной сумме среднего значения этого фактора и его среднеквадратического отклонения. Данный подход позволяет оценить средние ожидаемые значения оцениваемых характеристик, значение которых должно лежать в диапазоне, заданном технико-экономическими требованиями к условиям функционирования системы, то есть обеспечить гарантированное значение качества обслуживания (Quality of Service, QoS).

Пусть p — оцениваемый параметр системы, имеющий абсолютное измерение; p_1, p_2, …, p_n — набор статистических наблюдений либо экспертных данных по параметру p, где n — число наблюдений. Пусть средние значения $p_{\text{ср}}$ целевого показателя p_i и его экстремальное значение $p_{\text{э}}$ равны соответственно

$$p_{\text{ср}} = \frac{1}{n}\sum_{i=1}^{n} p_i\,,\ \ p_{\text{э}} = \max\{p_i; 1 \le i \le n\}.$$

Вместо $p_{\text{ср}}$ и $p_{\text{э}}$ предлагается использовать значение $p_{\text{г}}$ (соответствующее гарантированному качеству, QoS), которое равно:

$$p_{\text{г}} = p_{\text{ср}} + \sigma_{\text{р}},\ \sigma_p = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i - p_{\text{ср}})^2}. \qquad (*)$$

Для получения относительных целевых показателей оценки, аналогичной (*), можно поступить следующим образом. Пусть имеет место следующая зависимость вероятности $p_{\text{скд}}$ от интенсивности λ_p:

$$p_{\text{скд}} = C(\lambda_p, T)\cdot\exp\{-K(\lambda_p, T)\lambda_p T\},$$

где $C(\lambda_p, T)$ и $K(\lambda_p, T)$ — некоторые ограниченные функции.

Гарантированная оценка для эффективности внедрения средств КД:

$$p_г = \exp\{-K\lambda_{P,г}T\},\quad \lambda_{P,г} = \overline{\lambda_P} + \sigma_\lambda,\ \overline{\lambda_P} = \frac{1}{n}\sum_{i=1}^{n}\lambda_{P,i},\ \sigma_\lambda = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\lambda_{P,i} - \overline{\lambda_P})^2},$$

где $\lambda_{P,г} = \overline{\lambda_P} + \sigma_\lambda$ — соответствующие гарантированные оценки интенсивностей. Отметим, что значения вторых слагаемых σ_λ могут быть увеличены путем введения множителей, больших единицы, то есть использования слагаемых $\mu\sigma_\lambda$, $\mu > 1$ — константа.

Разработана *многоуровневая масштабируемая архитектура контроля доступа пользователей в вычислительном комплексе, обеспечивающем доступ пользователей к веб-сервисам через компьютерные сети*. Выделено 4 уровня: 1) программно-аппаратный уровень ВК, включающий средства, обеспечивающие КД; 2) уровень виртуальной инфраструктуры обработки данных КД; 3) уровень физических ресурсов для обработки данных КД; 4) уровень компонентов анализа данных.

Выделены *уровни архитектуры доступа к данным* при использовании веб-сервисов для доступа к ВК (рис. 2).

Программно-аппаратный уровень ВК включает в себя: аппаратные компоненты (могут включать: мэйнфреймы, серверы, блейд-серверы, устройства хранения, сетевые компоненты); системное и программное обеспечение; а также программно-аппаратное обеспечение клиентского приложения и веб-сервисы, доступные через браузеры клиентских устройств.

Уровень виртуальной вычислительной инфраструктуры обеспечивает взаимодействие виртуальных серверов, виртуальной памяти; виртуальных сетей; виртуальных приложений и операционных систем; виртуальных клиентов, управление сетевым взаимодействием клиентских запросов с ВС.

Уровень физических ресурсов включает: распределение вычислительных ресурсов ВК, которые используются для выполнения задач КД в облачной среде; специализированное ПО; доступ к среде пользователей и системных администраторов; а также управление системой хранения данных.

Уровень компонентов анализа данных КД включает конкретное программно-математическое обеспечение, которое обеспечивает обработку и анализ данных, анализ инцидентов безопасности.

Рис. 2 — Четырехуровневая архитектура КД

Показано, что каждому уровню соответствует свой набор технологий, компонентов, их разработка является отдельными задачами, и, таким образом, ей однозначно соответствуют этапы разработки системы КД: 1) определение состава параметров, которые могут быть получены о действиях пользователей, способы их сбора и передачи; 2) формирование виртуальной вычислительной инфраструктуры, требуемой для решения задач обработки информации КД; 3) оценка параметров вычислительных ресурсов; 4) разработка компонентов анализа информации. Результаты рассмотрения теоретических и прикладных аспектов этих задач изложены в последующих главах работы.

Разработан общий принцип формирования системы КД на аппаратном уровне. Система обработки данных включает в себя структуру связи, которая обеспечивает связь между процессорным блоком, памятью, постоянным хранилищем, блоком коммуникационного оборудования. В системах хранения данных, представляющих собой совокупность серверного оборудования и СХД, содержатся компоненты, реализующие контроль доступа к ВС. В систему КД включены следующие компоненты, требующие вычислительных ресурсов: база инцидентов; диспетчер событий; анализатор инцидентов — программный мо-

дуль, обеспечивающий оперативный контроль доступа на основе анализа событий; модуль сравнения полученных значений параметров доступа и характеристик событий с заданными моделями или пороговыми значениями; текущие значения параметров, характеризующие контроль доступа пользователей, а также возможные варианты перерасчета пороговых значений; сбор статистических данных; база пороговых значений, модуль повторной верификации; модуль статистических характеристик.

В третьей главе «**Облачная инфраструктура обработки данных систем контроля доступа**» рассмотрены вопросы построения уровня облачной инфраструктуры архитектуры КД, изложена методика распределения виртуальных вычислительных ресурсов и сетевое взаимодействие, рассмотрен пример инфраструктуры для КД при сетевом взаимодействии на примере протокола DICOM.

Предлагается структура уровня виртуальных вычислительных сервисов КД, включающая сетевой фильтр для проверки подлинности данных и легальности пользовательского поведения, обеспечивающий возможность анализа наборов архивных данных и входящих потоков больших данных, и управления предупреждениями. Использование облачной инфраструктуры обеспечивает горизонтальную масштабируемость и отказоустойчивость.

Сформулированные базовые принципы и технологии, на основе которых предлагается строить второй уровень архитектуры КД.

1) Применение технологий виртуализации сетевых функций.

2) Выделение серверных ролей виртуальным ресурсам.

3) Масштабирование виртуальной инфраструктуры как ее свойство.

4) Универсальность модели облачной инфраструктуры по отношению к серверному оборудованию.

Разработана *методика построения облачной инфраструктуры* для систем КД:

1. Определение состава и потока данных КД.
2. Выделение серверных ролей виртуальных машин (ВМ).
3. Выбор ПО, реализующего функции серверных ролей.
4. Определение состава ВМ, обеспечивающих решение задач КД.
5. Разработка информационной модели обмена данных между ВМ.
6. Разработка облачной инфраструктуры.
7. Конфигурирование инфраструктуры.
8. Экспериментальная оценка ресурсной эффективности.

В качестве примера уровня виртуальных ресурсов рассмотрены сетевые функции анализа трафика, передаваемого с использованием протокола DICOM, который применяется в системе здравоохранения, а также трафика, передаваемого по протоколу HTTP, и предназначенного для UBA.

Рассмотрены ряды данных с периодически отправляемыми в архив отчетами, которые генерируются клиентскими устройствами и мобильными приложениями. Аппаратные средства предоставляют данные по запросу программного обеспечения, которое обычно выполняет периодические запросы и отправляет данные в облако. КД направлен, как на отслеживание заведомо искаженных данных, так и данных, полученных с нарушением свойств периодичности.

Разработаны информационная модель и инфраструктура виртуальных вычислительных ресурсов с использованием модели корректности периодичности, целостности содержимого в архиве DICOM, легальности пользовательского поведения. Все модули проверки целостности данных для разных модальностей и модули проверки легальности пользовательского поведения реализованы в отдельных компонентах. Все они должны быть развернуты во множестве экземпляров для обеспечения высокой доступности.

Функционирование аналитических компонентов можно обеспечить в среде виртуальных машин, что поможет улучшить отказоустойчивость за счет механизмов миграции виртуальных машин (ВМ), активизируемых при отказе физических серверов, а также уменьшить накладные расходы, связанные с администрированием серверных систем. Распределение компонентов по виртуальным машинам приведено в табл. 1 и 2, описывающих серверные роли, выполняемые ВМ. Функционирование всех ВМ предполагается под управлением ОС Linux x64, выбор конкретного дистрибутива определяется рекомендациями разработчиков развертываемого ПО.

Таблица 1 — Серверные роли виртуальных машин (кластер для проверки корректности содержимого в архиве DICOM)

Имя ВМ	Серверная роль ВМ	Компоненты ПО	Описание ВМ
dicomsrv	DICOM Archive	dcm4che	Архив DICOM, содержащий медицинские данные
dicomdb	DICOM Archive Database	PostgreSQL	База данных архива DICOM, необходимая для его функционирования
tcpfront	TCP Interceptor Frontend	Linux (libpcap)	Входящий трафик, предназначенный для PACS, просматривается на TCPInterceptorFrontend и направляется для анализа на узлы LegalityAnalysisBackend с балансировкой по алгоритму round-robin
laback1, …, labackM	Legality Analysis Backend	DICOMAnalyzer RGAnalyzer MRAnalyzer ECGAnalyzer	Содержит компонент анализа содержимого файлов DICOM (DICOMAnalyzer), а также плагины проверки корректности для каждой модальности (RG, MR, ECG)

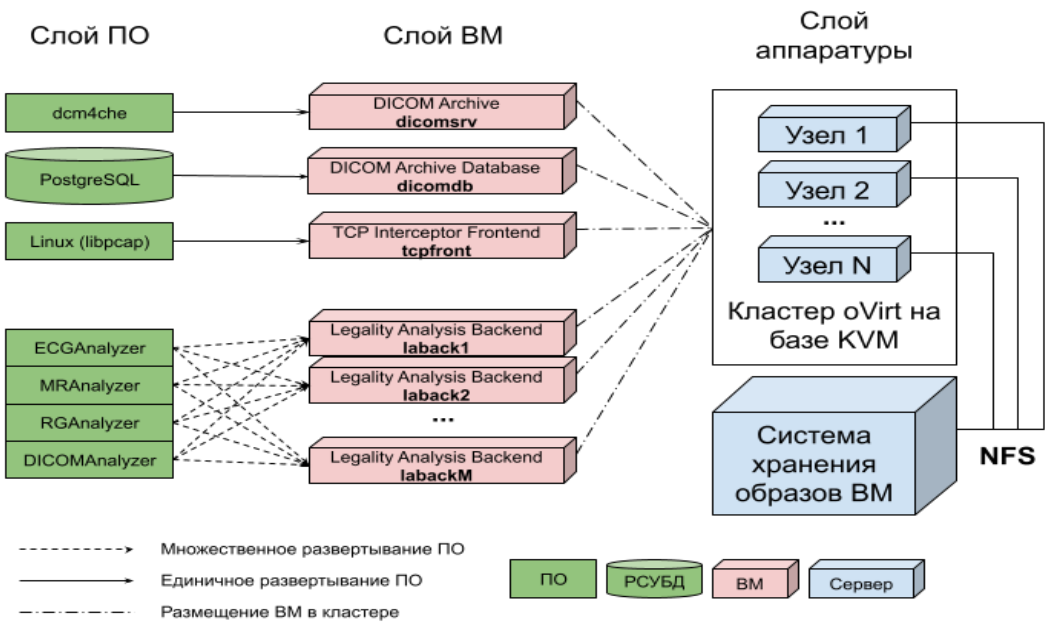
Таблица 2 — Серверные роли виртуальных машин
(кластер для проверки корректности пользовательского поведения)

Имя ВМ	Серверная роль ВМ	Компоненты ПО	Описание ВМ
websrv	Web Server	ApplicationServer	Сервер приложений.
journal0	Journal Backend (primary)	rsyslog	Журнал пользовательских действий. Отказоустойчивость обеспечивается наличием первичного и вторичного экземпляров rsyslog. При отказе первичного экземпляра данные направляются на вторичный. При возвращении в строй первичного экземпляра он вновь начинает принимать данные
journal1	Journal Backend (secondary)	rsyslog	
httpfront	HTTP Interceptor Frontend	mitmproxy	Входящий трафик, предназначенный для сервера приложений, просматривается на узле HTTPInterceptorFrontend и направляется для анализа на узлы BehaviorAnalysisBackend с балансировкой по алгоритму round-robin
baback1, …, babackM	Behavior Analysis Backend	HTTPAnalyzer MRAnalyzer CTAnalyzer AnesthetistAnalyzer	Содержит компонент анализа поведения пользователей (HTTPAnalyzer), а также плагины проверки корректности пользовательского поведения для различных сценариев (CT, MR, Anesthetist)

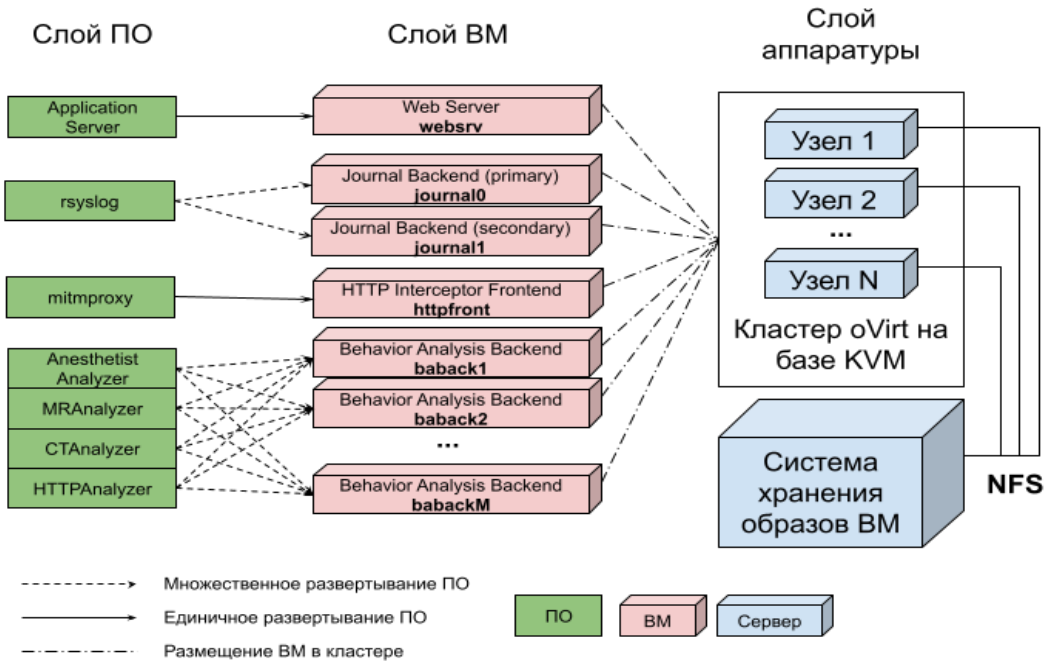
На рис. 3 представлена разработанная инфраструктура проверки целостности архива DICOM (рис. 3а) и UBA (рис. 3б) с учетом слоя виртуализации. Отказоустойчивость кластеров обеспечивается за счет множественности экземпляров серверных ролей Legality Analysis Backend и Behavior Analysis Backend.

Разработана *методика анализа трафика* на узлах Legality Analysys Backend и Behavior Analysis Backend с помощью подключаемых модулей (плагинов). Разработана архитектура анализатора, реализующая следующие функции: анализ пакетов DICOM; предоставление данных аналитическим компонентам; управление конфигурацией и обеспечение функции проверки соответствия для компонента анализа медицинских изображений.

Разработанные инфраструктуры позволяют расширять функциональность на уровне рабочей среды анализа данных поддержкой новых методов анализа медицинских изображений и пользовательского поведения для различных модальностей и врачебных специализаций соответственно. Разработана информационная модель компонентов анализа медицинских изображений. Предложена кластерная модель вычислительной архитектуры анализатора содержимого в архиве DICOM, предназначенная для перехвата DICOM-трафика и автономного анализа поступающих в PACS файлов.



а) облачная инфраструктура проверки целостности архива DICOM



б) облачная инфраструктур UBA

Рис. 3 — Примеры облачной инфраструктура для КД в системах здравоохранения

Для оценки ресурсных затрат на облачные ресурсы и другие компоненты требуется разработка специализированной методики, которой посвящена следующая глава.

В четвертой главе «**Метод оценки вычислительных ресурсов для компонентов системы контроля доступа»** предложен метод экспериментального оценивания, требуемого для резервирования количества вычислительных ресурсов при проектировании системы КД.

Сформулирована *задача оценки ресурсной эффективности* компонентов архитектуры КД. Пусть заданы технико-экономические характеристики функционирования ВК, представляющие собой набор заданных желаемых диапазонов значений при заданном уровне обслуживания QoS, и планируемую форму и интенсивность запросов к ВС. Тогда для пользовательских запросов X к ВС и для компонента Z_k с допустимыми технико-экономическими характеристиками архитектуры V может быть оценено:

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

где R_i — n-мерный вектор измеряемых вычислительных ресурсов; отображение Φ такое, что по наблюдаемому процессу X, параметры R_i измеримы.

Отображение Ф в условиях виртуальности ресурсов может быть получено путем построения экспериментального стенда по технологии «инфраструктура как код», т. е. получено в результате натурных испытаний конфигурации Z_k при имитационном моделировании входного потока X. Иными словами, отображение Ф 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 X может быть использовано имитационное моделирование. В ряде работ (А.В. Борисов, А.В. Босов, А.В. Иванов и др.), посвященных построению математических моделей процессов 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 исследований, связанное с генерацией хаотического сигнала (О.И. Шелухин, Е.В. Никульчев, А.В. Карпухин и др.), имитирующего протокол TCP/IP. Для оценки ресурсов нет необходимости строить точные прогнозные модели процессов, поскольку искомые значение запасов вычислительных ресурсов зависят только от диапазона и интенсивности процессов, что может быть реализовано имитационным моделированием случайной величины с заданной функцией распределения. В случае, если технико-экономические характеристики не сужают сильно канал, целесообразно использовать бета- или гамма-распределение, для узких каналов — распределение с «тяжелыми хвостами».

Разработана *метод анализа затрат вычислительных ресурсов* для реализации систем контроля доступа на основе подхода, использующего виртуальные стенды, обеспечивающие имитационную среду использования ВК на каждом уровне КД. 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 контроля доступа.

6. В случае решения задачи выбора вариантов реализации средств КД, выбор вариантов, имеющих меньшие ресурсные затраты.

7. Формирование архитектуры вычислительного комплекса с учетом полученных значений затрат вычислительных ресурсов.

Рассмотрены вопросы технологической реализации методики. Рассмотрим, например задачу оценки вычислительных затрат при записи событий в БД при работе с веб-сервисами по компьютерным сетям, с логированием действий пользователей. Предполагается, что запись действий пользователей будет осуществляться в журнал событий. Для каждого устройства предлагается вести свою запись журнала действий. Для проведения экспериментальных исследований будем использовать следующие данные: объем исходного файла с данными составляет 450 МБ; файл содержит записи в слабоструктурированном формате JSON.

Перед началом эксперимента создаются три виртуальные машины (ВМ) (Client, Server, Database) с заданными характеристиками. Для повторных экспериментов, если они были созданы ранее, существующие ВМ предварительно удаляются, чтобы обеспечить чистоту эксперимента между повторениями. Структура экспериментального стенда приведена в табл. 3 и на рис. 4.

Таблица 3 — Параметры виртуальных машин

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

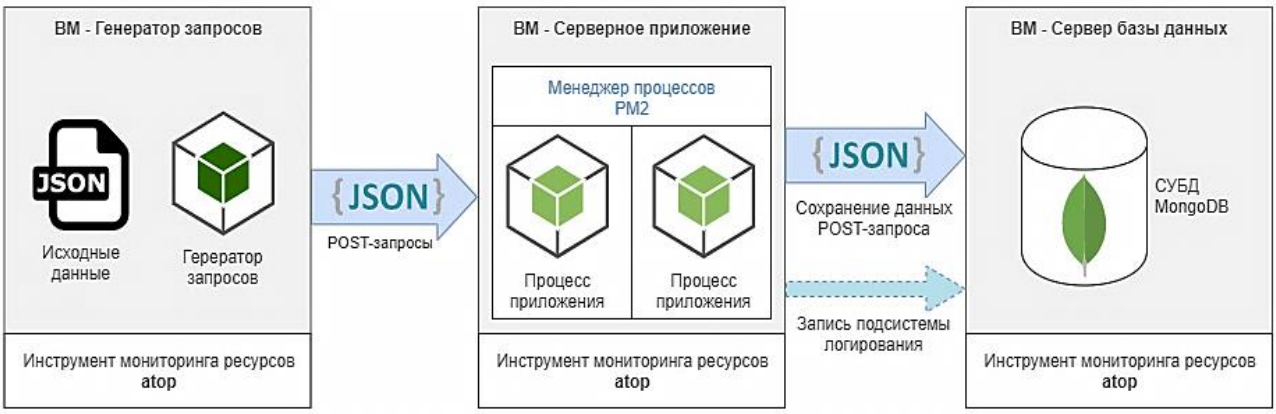


Рис. 4 — Схема эксперимента

После создания ВМ, установки и запуска серверного ПО и СУБД начинается сам эксперимент. Исходные данные загружаются в оперативную память ВМ Client. После их полной загрузки начинается отправка данных с заданными параметрами. Результаты вычислительного эксперимента приведены в табл. 4.

Таблица 4 — Показатели ресурсных затрат на логирование действий пользователей

Ресурсный показатель	Значение без использования логирования	Значение с использованием логирования	Разница в %
ЦПУ ВМ client	8.4982	8.2170	3.3
ЦПУ ВМ server	19.7109	22.23014	12.7
ЦПУ ВМ Database	2.8590	4.3716	52.9
Память ВМ client	1296828.1859	1295666.4060	0.08
Память ВМ server	41345.7973	39147.0563	5.32
Память ВМ Database	340911.1149	341359.7882	0.13

Таким образом, для рассматриваемого примера экспериментально установлено, что использование логирования действий пользователей существенно влияет только на загрузку процессора сервера (рис. 5) и сервера базы данных (рис. 6), незначительно увеличивает загрузку памяти сервера.

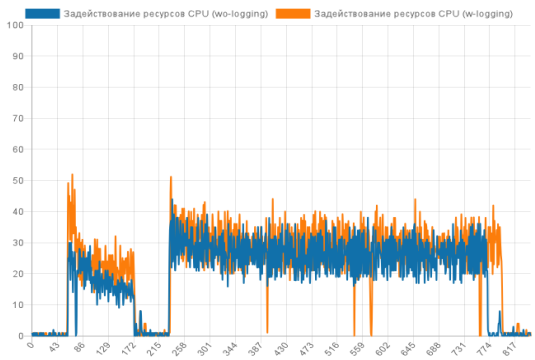


Рис. 5 — Используемые ресурсы СПУ ВМ Server, %

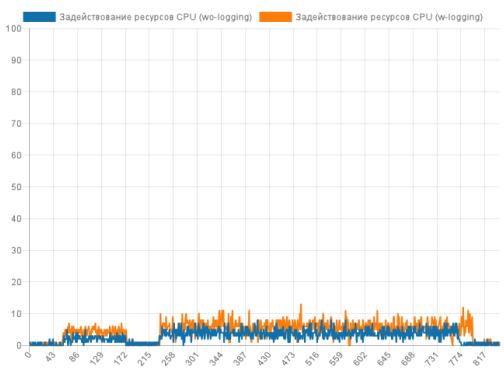


Рис. 6 — Используемые ресурсы ЦПУ ВМ Mongodb, %

Полученные оценки на основе имитационных экспериментальных исследований позволяют получить значение ресурсов вычислительного комплекса, требуемого для логирование данных контроля доступа.

В пятой главе «**Совершенствование контроля доступа на основе использования реакций пользователей при работе с элементами интерфейса»** предложен метод контроля доступа на основе использования психологических реакций, которые могут быть измерены на основе работы с интерфейсами. Метод экспериментально проверен на выборке.

Существуют подходы к контролю доступа, связанные с анализом всех параметров действий пользователя (движение мыши, среднее время между нажатием клавиши мыши и началом движения курсора, скорость набора текста и др.). Подобные исследования носят ограниченный характер — для многопользовательских систем получение, передача, хранение и обработка всех движений курсора мыши вычислительно затратны, зависят от используемого оборудования, версий программного обеспечения. Современные психологические исследования (J. Kim, U. Gabriel, P. Gygax, S. 2019; Anrijs, K. Ponnet, L. De Marez 2020) выявили достоверность данных по исследованию реакций, полученных с использованием веб-интерфейсов с данными, полученными в лабораторных условиях. Эти результаты психологов дают основание для разработки информационной технологии построения архитектуры многоуровневого КД, 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).

Разработан *метод контроля доступа на основе анализа реакций пользователей*. Метод основан на гипотезе, подтвержденной экспериментальными исследованиями. Исследования проводились с помощью цифровой платформы DigitalPsyTools Российской академии образования. Система является одновременно цифровой платформой с веб-интерфейсом и инструментом психодиагностики, используемой для популяционных исследований в системе образования. В ВС в элементы интерфейса встроены платформонезависимые функции оценки когнитивных реакций.

Гипотеза заключалась в том, что время реакции на разные ответы с разными элементами интерфейса является индивидуальным. 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.

В ходе проведения массового опроса был проведен эксперимент, на выборке 23 102 чел. Оценивалось время реакции респондентов на 3 простых анкетных вопроса, при этом учитывалось только время реакции, вне зависимости от самого ответа. 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 23 102. Записи, содержащие пустые ответы или время реакции менее 2 секунд, были удалены из набора данных. Остальные 22 357 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 рис. 7. Анализ гистограмм на основе методов психометрики подтверждает корректность психологического исследования.

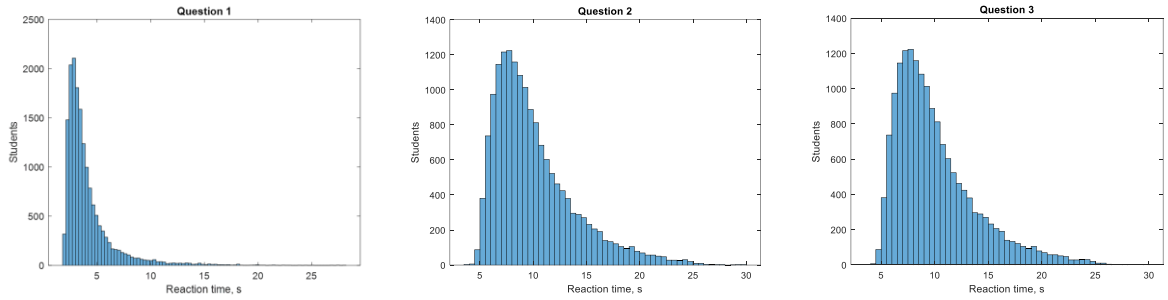


Рис. 7 — Гистограммы нормализованного времени реакции пользователей при ответе на вопросы 1–3.

Для качественной оценки отклонений времени реакции введена шкала, делящая отклонения на 4 квартиля в порядке возрастания. Таким образом, у каждого из 22 357 студентов была упорядоченная триада типа (1, 2, 4), представляющая их относительно отклонений времени реакции на вопросы 1–3. Границы квартилей показаны в табл. 5.

Таблица 5 — 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	0.0081	1
Вопрос 3				
Нижняя граница	0	0.0075	0.011	0.014
Верхняя граница	0.0074	0.0109	0.013	1

Количественный анализ данных отклонений времени реакции показал достоверную корреляцию между отклонениями при ответах на вопросы 1–3. Коэффициенты корреляции представлены в табл. 6.

Таблица 6 — Коэффициенты корреляции отклонений времени реакции на вопросы 1–3 (аргументы 1–3 обозначают номер вопроса)

R (1,2)	**R (1,3)**	**R (2,3)**
0.9298	0.8039	0.8376

В ходе качественного анализа было обнаружено, что 17 002 или 76% респондентов 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. Выявлено, что зависимости могут быть построены, что демонстрирует допустимость построения достоверных прогнозных значений реакций пользователей. Это имеет важное значение для рассматриваемой задачи КД. 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 КД может сравнить прогнозируемое значение с полученным. Для прогнозирования реакций были проверены возможности построения регрессионных зависимостей, проведен тест Вальда. Тест показал, что значимыми могут быть простые модели, то есть проверка и расчет прогноза не потребуют значительного количества вычислительных ресурсов для сбора и передачи данных.

На основе гипотез и проверенных экспериментальных исследования можно сформулировать метод контроля доступа, основанный на реакциях пользователей. Метод состоит в следующем:

1. В интерфейс ВС встраивается, или периодически возникает 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. Сравниваются полученными значения с прогнозными.

4. Если полученный экспериментальный результат входит в состав другого квартиля от ожидаемого значения, то запускаются механизмы идентификации пользователя, требующие персонального подтверждения.

5. Если результаты совпадают (попадают в один квартиль), то пользователь считается верифицированным.

Для ВС предлагается в системы КД и верификации встроить вспомогательные индикаторы использования элементов интерфейса — время реакции (ВР) 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.

Реализация разработанного метода существенно не увеличивает объемы передаваемых данных и не замедляет работу клиентского приложения.

В шестой главе «**Построение многоуровневой архитектуры вычислительных комплексов для обеспечения контроля доступа к сервисам здравоохранения**» рассмотрены прикладные аспекты внедрения результатов в учреждениях здравоохранения.

Рассмотрены особенности вычислительной инфраструктуры и систем сервисов учреждений здравоохранения. Рассмотрены и проанализированы типы устройств, способы и виды хранения данных, принятые протоколы и системы обмена данных в медицинских организациях. Выявлены уязвимые места и сценарии КД в сетях и хранилищах медицинских данных.

Разработана методика учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов в учреждениях здравоохранения для предоставления медицинских услуг.

Разработанная архитектура призвана обеспечить интеграцию проверки медицинских данных, аналитики поведения пользователей для проверки деятельности медицинских специалистов. Практический эффект разработки и внедрения заключается в повышении защищенности и КД к конфиденциальным медицинским изображениям.

На рис. 8 проиллюстрировано место сетевых анализаторов (кластеров) в архитектуре ВК учреждения здравоохранения.

Предложенная архитектура не накладывает ограничений на количество аналитических бэкендов в кластере, поэтому с точки зрения горизонтальной масштабируемости может считаться надежнее существующих коммерческих решений. Однако перехватывающие фронтенд-серверы могут считаться единой точкой отказа. Для повышения надежности они могут иметь резервного «двойника». В их кластеризации с балансировкой нагрузки по TCP-соединениям нет необходимости, поскольку первичная обработка трафика является легковесной и не задействует локальные файловые системы для хранения каких-либо промежуточных данных. Предложена архитектура системы, готовой к обработке больших данных при автономной проверке корректности медицинских записей в архивах DICOM.

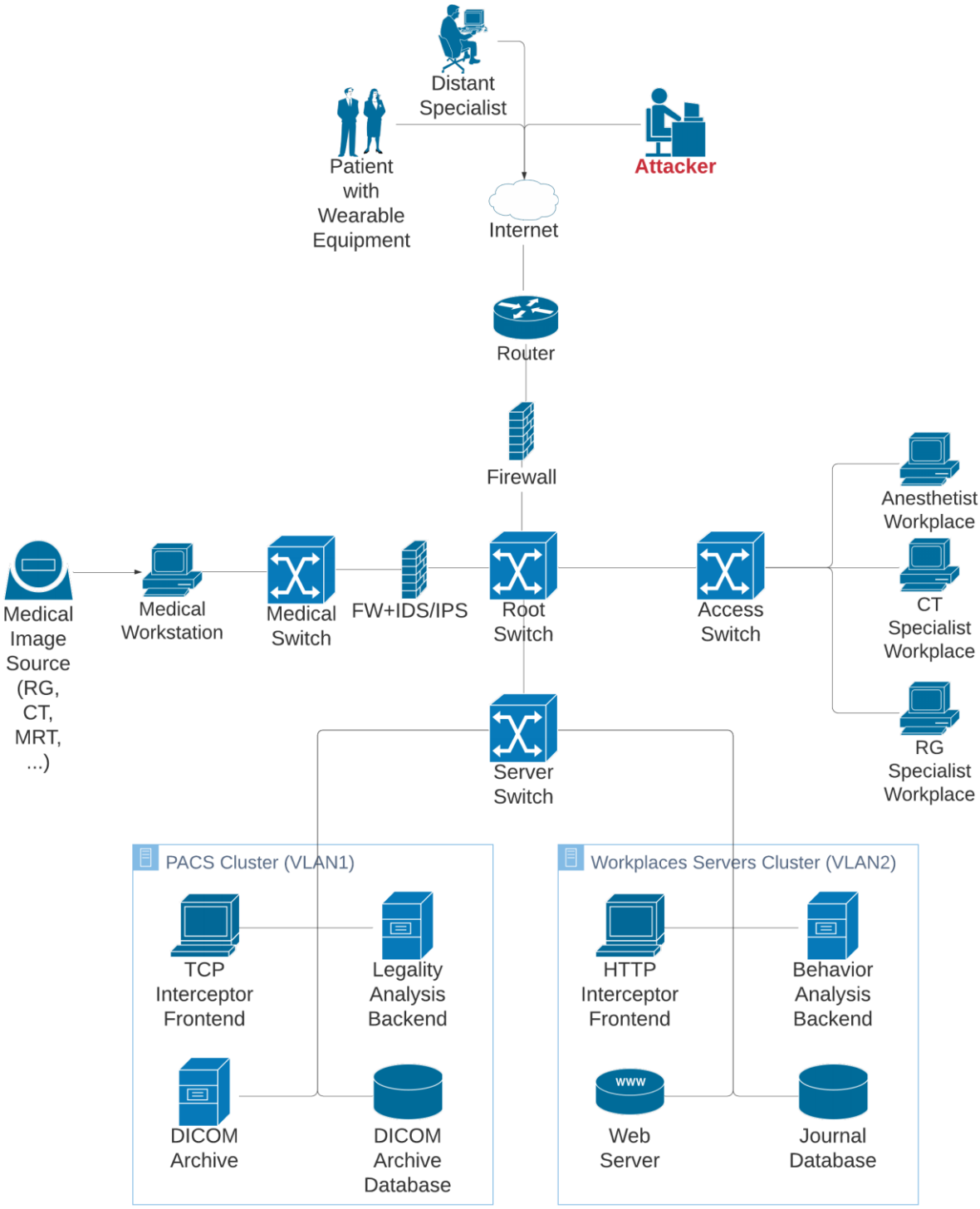


Рис. 8 — Вычислительная инфраструктура ВК с КД для учреждений здравоохранения

Функционирование компонентов можно обеспечить в среде виртуальных машин, что поможет улучшить отказоустойчивость за счет механизмов миграции ВМ, активизируемых при отказе физических серверов, а также уменьшить накладные расходы, связанные с администрированием серверных систем. На рис. 9 проиллюстрирована схема развертывания виртуальных машин.

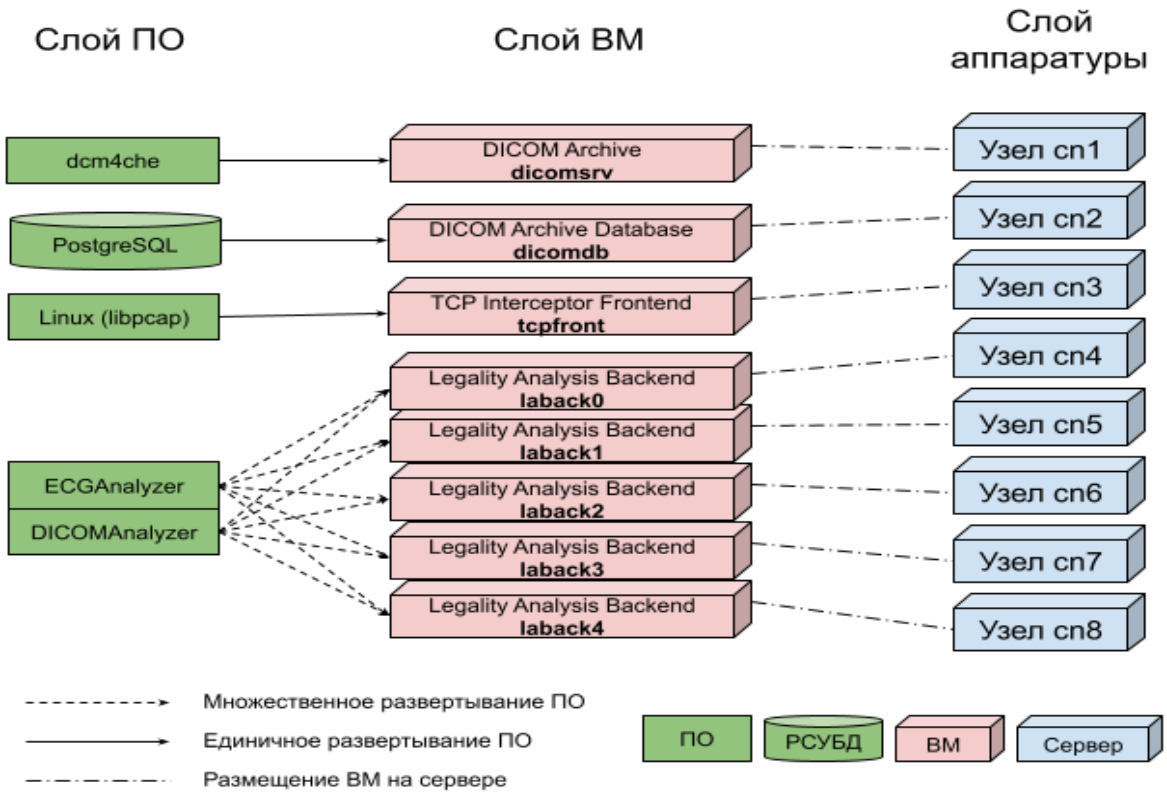


Рис. 9 — Размещение виртуальных машин и программного обеспечения

Экспериментальные исследования проводилось под следующей нагрузкой: на вход машины tcpfront подавались запросы на прием фрагмента ЭКГ со случайным интервалом длительностью от 0 до 625 мс (ГСЧ работает согласно равномерному распределению). Общее количество запросов равно 200. Размер фрагмента ЭКГ — 1.25Мб. Общее время работы системы для обслуживания всех принятых запросов составило 61 с. Нагрузка на виртуальные машины измерялась как при включенных компонентах защиты, так и при выключенных. В табл. 7 приведен коэффициент снижения нагрузки на ресурсы ВМ в условиях отсутствия аналитических компонентов.

Таблица 7 — Коэффициент снижения нагрузки на ресурсы ВМ dicomsrv и dicomdb

ВМ	Средняя загрузка CPU. раз	Средняя загрузка RAM. раз	Средняя загрузка сети. входящий канал. раз	Средняя загрузка сети. исходящий канал. раз	Средняя загрузка диска. раз
dicomsrv	1.96	1.05	1.35	2.77	1.56
dicomdb	1.98	1.02	1.83	1.80	1.95

Почти двукратная разница в загрузке процессоров объясняется двухкратным уменьшением количества запросов в DICOM архив. Значительно изменилась нагрузка на исходящий канал dicomsrv — остались только служебные данные, передаваемые по протоколу DICOM для обеспечения записи в архив

DICOM. Также заметно снижение нагрузки на диск — теперь отсутствует обслуживание операции чтения из архива DICOM.

Разработанный экспериментальный фреймворк и предложенный подход к тестированию применимы для оценки производительности как существующих кластерных конфигураций, так и планируемых, поскольку для оценки доступны ресурсы, потребляемые каждым из компонентов в отдельности.

В седьмой главе «**Построение многоуровневой архитектуры вычислительных комплексов для обеспечения контроля доступа к сервисам учреждений высшего образования»** рассмотрены прикладные аспекты внедрения полученных в работе результатов в ВК, обеспечивающие образовательные услуги в вузе.

Разработаны принципы и информационные модели проектирования архитектуры КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза

Помимо парольной защиты и классических методов (таких как двухфакторная аутентификация и сетевые списки доступа (ACL)) предложено внедрить систему анализа поведения пользователей. Предложенная архитектура не накладывает ограничений на количество аналитических бэкендов в кластере. Однако перехватывающие фронтенд-серверы могут считаться единой точкой отказа. Для повышения надежности они могут иметь резервного «двойника». В их кластеризации с балансировкой нагрузки по TCP-соединениям нет необходимости, поскольку первичная обработка трафика является легковесной и не задействует локальные файловые системы для хранения каких-либо промежуточных данных. Предложена архитектура системы, готовой к обработке больших данных при автономной проверке корректности пользовательского поведения. На рис. 10 приведена структура ВК вуза с многоуровневым КД, реализующая разработанную четырехуровневую архитектуру.

Функционирование компонентов можно обеспечить в среде виртуальных машин, что поможет улучшить отказоустойчивость за счет механизмов миграции ВМ, активизируемых при отказе физических серверов, а также уменьшить накладные расходы, связанные с администрированием серверных систем.

На рис. 11 проиллюстрирована схема развертывания виртуальных машин.

Экспериментальные исследования проводилось следующим образом: на вход машины front подавались HTTP-запросы для Moodle со случайным интервалом длительностью от 0 до 100 мс (ГСЧ работает согласно равномерному распределению). Общее количество запросов равно 1200. Общее время работы системы для обслуживания всех принятых запросов составило 61 с. В табл. 8 приведена средняя загрузка ресурсов на всех восьми виртуальных машинах.

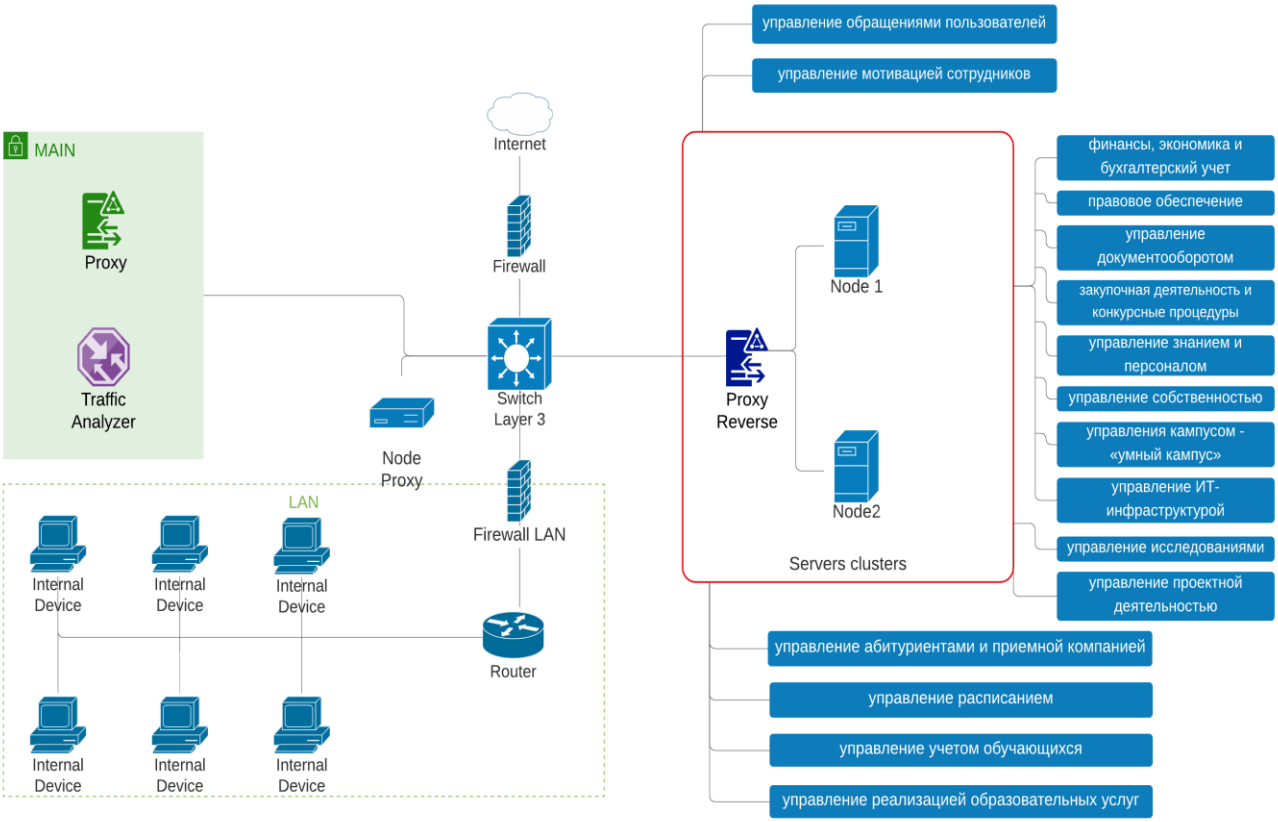


Рис. 10 — Архитектура вузовских сервисов с КД

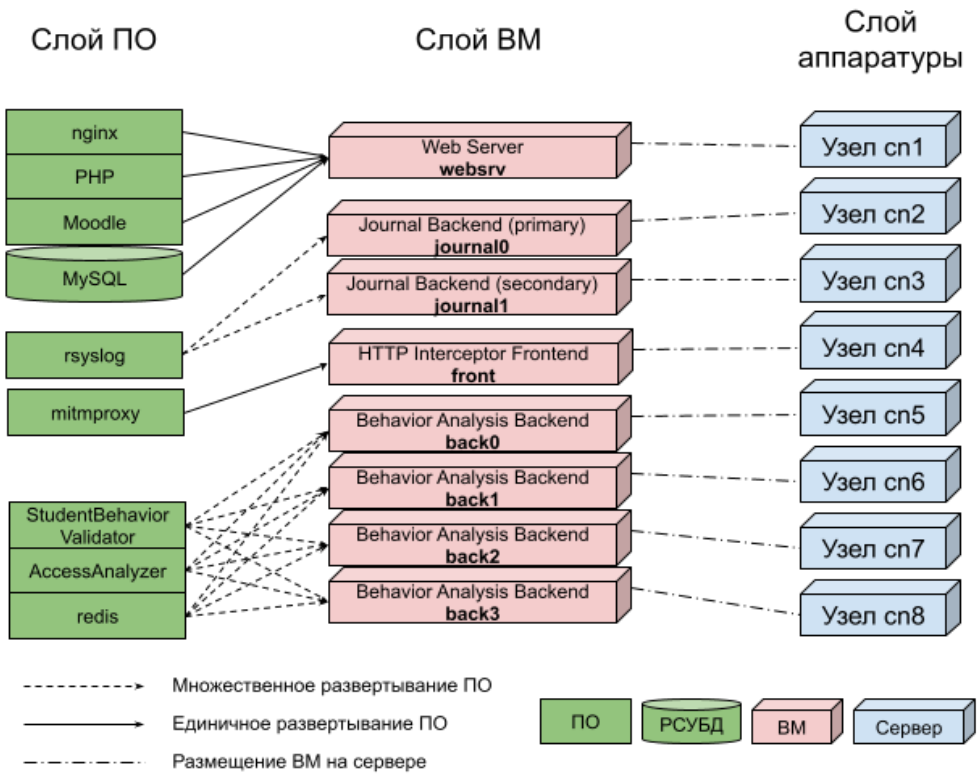


Рис. 11 — Размещение виртуальных машин и программного обеспечения

Таблица 8 — Средняя загрузка ресурсов на виртуальных машинах

ВМ	Средняя загрузка CPU. %	Средняя загрузка RAM. %	Средняя загрузка сети. входящий канал. %	Средняя загрузка сети. исходящий канал. %	Средняя загрузка диска. %
websrv	29.83	15.43	2.25	5.18	11.62
journal0	28.03	33.95	10.22	10.56	10.53
journal1	0.86	11.19	0.85	1.00	0.94
front	19.15	14.03	7.30	4.34	6.86
back0	9.50	7.80	3.59	3.03	2.41
back1	9.04	7.58	3.66	3.16	2.46
back2	9.24	7.71	3.50	3.16	2.23
back3	9.34	7.68	3.63	2.69	2.14

Из табл. 8 видно, что тестовый аналитический кластер может быть оптимизирован путем уменьшения объема оперативной памяти, выдаваемой виртуальным машинам. Нагрузку на процессоры можно оценить как среднюю. запас для обработки всплесков количества запросов остается. Однако при добавлении в будущем новых аналитических плагинов, которые могут быть более ресурсоемки, потребность в свободных ресурсах ВМ может только возрасти.

Разработанный экспериментальный фреймворк и предложенный подход к тестированию применимы для оценки производительности как существующих кластерных конфигураций, так и планируемых.

Описанные в шестой и седьмой главах примеры построения архитектур для медицинских и образовательных вычислительных сервисов, образуют последовательность действий, которая формирует *методику учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов*.

Разработаны *принципы и информационные модели проектирования архитектуры системы КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза* в условиях защищенной цифровой образовательной среды с использованием инструментов UBA. Использование разработанных методов моделей КД способствует повышению защищенности образовательных ресурсов от несанкционированного доступа, возможности для списывания, подлога, а также саботажа учебной работы. Проверка индивидуальных особенностей студентов позволяет снизить вероятность таких нарушений. Результаты внедрения показывают эффективность предложенных решений.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Разработаны принципы, методы и модели построения четырехуровневой масштабируемой архитектуры контроля доступа. обеспечивающая реализацию технологий передачи. хранения. управления. мониторинга и анализа действий пользователей и устройств в вычислительных комплексах. предоставляющих веб-сервисы с учетом оценки ресурсной эффективности систем КД и технико-экономических характеристик заданных условий функционирования.

В ходе выполнения исследований получены следующие основные результаты.

1. Проведен обзор подходов к построению архитектур и используемых технологий обеспечения контроля доступа к вычислительным сервисам, позволивший выделить актуальные задачи, перспективные подходы к их решению, определить направление исследований с целью повышения эффективности контроля доступа к ВС.

2. Сформулирована задача построения архитектуры КД как подсистемы, обеспечивающей собственные, отличные от ВС: сбор, передачу, хранение и обработку данных о действиях пользователей. Решение позволяет сформулировать задачи, являющихся типовыми для обеспечения информационной безопасности; определить состав и требуемые ресурсы для компонентов анализа данных КД.

3. Разработана четырехуровневая масштабируемая архитектура контроля доступа, интегрируемая в вычислительные комплексы, обеспечивающие взаимодействие пользователей с ВС через компьютерные сети. Архитектура позволяет оценивать эффективность. разрабатывать и внедрять разные варианты технологических решений КД: SIEM. UBA.

4. Разработана методика построения облачной инфраструктуры. обеспечивающей решение задач КД. Приведены примеры построения для SIEM и UBA со специализированным протоколом DICOM.

5. Разработан метод анализа затрат вычислительных ресурсов на основе подхода. использующего имитационные виртуальные стенды в условиях заданных технико-экономических характеристик эксплуатации. Метод и соответствующая модель позволяют решать задачу выбора технических реализаций.

6. Предложен метод КД на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса с учетом времени ответа на контрольные вопросы. Проведенные экспериментальные исследования на большой выборке позволили подтвердить достоверность измеряемых данных и получить нормированные значения для трех вопросов об уровне образования.

7. Разработаны методики учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычисли-

тельных комплексов в учреждения здравоохранения и вузы. Предложена архитектура программных средств, реализующих SIEM и UBA решения.

8. Разработаны принципы и информационные модели проектирования архитектуры КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза с учетом инструментов UBA.

9. Результаты внедрены в учреждения образования и учреждения здравоохранения. Полученные результаты внедрения свидетельствуют об эффективности научных и практических результатов диссертации.

ОСНОВНЫЕ РАБОТЫ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Магомедов Ш. Г. Архитектура вычислительного комплекса для веб-сервисов и порталов с многоуровневым контролем доступа по общедоступным сетям // *International Journal of Open Information Technologies.* 2021. Vol. 9. № 3. С. 36–43.
2. Магомедов Ш. Г., Колясников П. В., Никульчев Е. В. Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей // *Российский технологический журнал*. 2020. Т. 8. № 6. С. 34–46. [1)]
3. Магомедов Ш. Г. Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения // *Cloud of Science*. 2020. Т. 7. № 3. С. 685–704.
4. Магомедов Ш. Г. Архитектура информационной системы для проверки подлинности медицинских данных в архиве DICOM // *International Journal of Open Information Technologies*. 2020. Т. 8. № 10. С. 84–89.
5. Ильин Д. Ю., Колясников П. В., Лаптев Н. В., *Магомедов Ш.Г.*, Алексеенко А. С., Никульчев Е. В. Архитектура вычислительного комплекса цифровой платформы DigitalPsyTools междисциплинарных исследований в системе образования // *Cloud of Science*. 2020. Т. 7. № 4. С. 936–949.[2)]
6. Магомедов Ш. Г. Проектирование микропроцессорных устройств. разработанных для систем контроля и управления доступом // *Cloud of Science*. 2019. Т. 6. № 4. С. 752–761.
7. Изергин Д. А., Еремеев М. А., Магомедов Ш. Г., Смирнов С. И. Оценка уровня информационной безопасности мобильной операционной системы android // *Российский технологический журнал*. 2019. Т. 7. № 6. С. 44–55.[3)]

[1)] Личный вклад соискателя состоит в разработке метода UBA на основе анализа реакций пользователей и архитектуры ВК.
[2)] Личный вклад соискателя в разработке архитектуры архитектур ВК с системой КД.
[3)] Личный вклад в разработке принципов построения систем КД.

8. Магомедов Ш. Г., Лебедев А. С. Система автоматического распараллеливания линейных программ для машин с общей и распределенной памятью // *Российский технологический журнал*. 2019. Т. 7. № 5. С. 7–19.[4)]

9. Магомедов Ш. Г., Шамхалов Ф. И. Особенности использования микропроцессорных устройств в системах контроля доступа // *Промышленные АСУ и контроллеры*. 2018. № 3. С. 16–19.[2)]

10. Магомедов Ш. Г. Построение системы обмена закрытыми данными в вычислительных сетях на основе использования систем счисления остаточных классов // *Промышленные АСУ и контроллеры*. 2017. № 1. С. 42–46.

11. Магомедов Ш. Г. Выбор оптимального варианта совершенствования системы защиты информации // *Промышленные АСУ и контроллеры*. 2017. № 3. С. 47–51.

12. Магомедов Ш. Г. Оценка степени влияния сопутствующих факторов на показатели информационной безопасности // *Российский технологический журнал*. 2017. Т. 5. № 2. С. 47–56.

13. Лось В. П., Росс Г. В., Магомедов Ш. Г. Мультиагентный подход для защиты данных в информационном тумане // *Промышленные АСУ и контроллеры*. 2017. № 6. С. 47–50. [3)]

14. Исмаилов Ш. М. А., *Магомедов Ш.Г.* Алгоритмы и структуры преобразования числовых данных из позиционной системы счисления в систему остаточных классов // *Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление.* 2008. № 5 (65). С. 159–169.[5)]

15. *Магомедов Ш. Г.* Формирование состава типовых макроопераций для систем разграничения и контроля доступа // *Информация и безопасность*. 2018. Т. 21. № 1. С. 118–123.

16. Магомедов Ш. Г. Классификация рубежей доступа и связанных с ними факторов влияния в системе контроля доступа // *Вестник Астраханского государственного технического университета. Серия: Управление. вычислительная техника и информатика.* 2018. № 1. С. 62–70.

17. Лось В. П., Тышук Е. Д., Магомедов Ш. Г. Место контроля доступа в системах обеспечения информационной безопасности объектов обработки данных // *Информация и безопасность*. 2017. Т. 20. № 3. С. 356–361. [3)]

18. Магомедов Ш. Г., Шуршев В. Ф., Попов Г. А., Дорохов А. Ф., Руденко М. Ф. Построение моделей описания рисков охранных действий по

[4)] Личный вклад соискателя состоит в разработке методик контроля доступа на уровне виртуализации и разработке архитекторы ВК.

[5)] Личный вклад соискателя состоит в организации КД на уровне данных.

защите внешних периметров организации // *Вестник Астраханского государственного технического университета. Серия: Управление. вычислительная техника и информатика*. 2017. № 3. С. 31–39. [2)]

19. Магомедов Ш. Г., Колотилов Ю. В. Системный анализ процесса разграничения доступа при дискреционной политике управления // *Вестник Астраханского государственного технического университета. Серия: Управление. вычислительная техника и информатика*. 2017. № 4. С. 39–44. [2)]
20. Магомедов Ш. Г., Морозова Т. Ю., Акимов Д. А. Обеспечение безопасности передачи данных в вычислительных сетях на основе использования систем остаточных классов // *Проблемы информационной безопасности. Компьютерные системы*. 2016. № 3. С. 43-47. [2)]
21. Магомедов Ш. Г. Математическое моделирование охранных действий на объекте защиты // *Вестник Астраханского государственного технического университета. Серия: Управление. вычислительная техника и информатика*. 2016. № 1. С. 70–80.
22. Мустафаев А. Г., Магомедов Ш. Г., Савинова А. М., Мустафаев А. Г. Управление технологическим процессом формирования структур интегральных элементов // *Вестник Астраханского государственного технического университета. Серия: Управление. вычислительная техника и информатика*. 2012. № 2. С. 56-61. [2)]
23. Nikulchev E., Ilin D., Kolyasnikov P., Magomedov S., Alexeenko A., Kosenkov A. N., Sokolov A., Malykh A., Ismatullina V., Malykh S. Isolated Sandbox Environment Architecture for Running Cognitive Psychological Experiments in Web Platforms // *Future Internet*. 2021. Vol. 13. No. 10. P. 245.[1)]
24. Magomedov S., Gusev A., Ilin D., Nikulchev E. Used the Time of User Reactions to Improve Security and Control Access To Web Services // *Applied Science*. 2021. Vol. 11. No. 5. P. 2561. [1)]
25. Magomedov S., Ilin D., Nikulchev E. Resource Analysis of the Log Files Storage Based on Simulation Models in a Virtual Environment. // *Applied Science*. 2021. Vol. 11. No. 11. P. 4718. [4)]
26. Magomedov S., Lebedev A. Protected network architecture for ensuring consistency of 2 medical data through validation of user behavior and DICOM 3 archive integrity // *Applied Science*. 2021. Vol. 11. No. 5. P. 2072. [4)]
27. Magomedov S., Ilin D., Silaeva A., Nikulchev E. Dataset of User Reactions When Filling Out Web Questionnaires // *Data*. 2020. Vol. 5. No. 4. P. 108. 1–7. [1)]

28. Nikulchev E., Ilin D., Silaeva A., Kolyasnikov P., Belov V., Runtov A., Pushkin P., Laptev N., Alexeenko A., Magomedov S., Kosenkov A., Zakharov. I., Ismatullina. V., Malykh. S. Digital Psychological Platform for Mass Web-Surveys // *Data*. 2020. V. 5. No. 4. P. 95. 1–16. [4)]

29. Magomedov S. Software for analyzing security for healthcare organizations // *Communications in Computer and Information Science*. 2021. Vol. 1395. P. 181–189.

30. Magomedov S. G., Lebedev A. S. Automatic parallelization of affine programs for distributed memory systems // *Communications in Computer and Information Science*. 2021. Vol. 1396. P. 91–101. [4)]

31. Magomedov S. A system for off-line validation of medical data in DICOM archive // *Journal of Physics: Conference Series*. 2021. Vol. 1727. P. 012011.

32. Otsokov S. A., Magomedov S. G. Using of redundant signed-digit numeral system for accelerating and improving the accuracy of computer floating-point calculations. // *International Journal of Advanced Computer Science and Applications*. 2020. Vol. 11. No. 9. P. 357–363.[5)]

33. Otsokov S. A., Magomedov S. G. On the possibility of implementing high-precision calculations in residue numeral system // *International Journal of Advanced Computer Science and Applications*. 2019. Vol. 10. No. 11. C. 9–13. [5)]

34. Magomedov S.G., Los V.P. Forming the composition of functions and instructions of microprocessor devices for access control systems // *Automatic Control and Computer Sciences*. 2019. Vol. 53. No. 8. P. 883–888. [3)]

35. Magomedov S. G. Increasing the efficiency of microprocessors in an access control systems // *International Journal of Engineering and Technology* (*UAE*). 2018. Vol. 7. No. 4.36. P. 80–83.

36. Magomedov S., Pavelyev S., Ivanova I., Dobrotvorsky A., Khrestina M., Yusubaliev T. Anomaly detection with machine learning and graph databases in fraud management. *International Journal of Advanced Computer Science and Applications*. 2018. Vol. 9. No. 11. P. 33–38.[6)]

37. Magomedov S. G., Dobrotvorsky A. S., Khrestina M .P., Pavelyev S. A., Yusubaliev T. R. Application of artificial intelligence technologies for the monitoring of transactions in aml-systems using the example of the developed classification algorithm // *International Journal of Engineering and Technology* (*UAE*). 2018. Vol. 7. No. 4.36. P. 76–79.[6)]

[6)] Личный вклад соискателя состоит в разработке архитектуры на уровне приложений.

38. Magomedov S. G. The technology of secure dataprocessing in production systems based on the use of special microcontrollers // *International Journal of Engineering and Technology* (*UAE*). 2018. Vol. 7. No. 4.36. P. 84–87.

39. Mikliaev E. M., Antonova I. I., Nikonov V. V., Magomedov S. G. An approach to emergency situation forecasting in the field of road maintenance based on big data analysis // *International Journal of Engineering and Technology (UAE)*. 2018. Vol. 7. No. 4.36. P. 88–91. [5)]

40. Voit A., Stankus A., Magomedov S., Ivanova I. Big data processing for full-text search and visualization with elasticsearch // *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8. No. 12. P. 76–83. [5)]

41. Magomedov S. Organization of Secured Data Transfer in Computers Using Sign-Value Notation // *ITM Web of Conference*. 2017. Vol. 10. P. 04004.

42. Popov G., Magomedov S. Comparative analysis of various methods treatment expert assessments // *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8. No. 5. P. 35–39. [3)]

Свидетельства о государственной регистрации программы для ЭВМ

43. Смирнов С. И., Прибылов И. А., *Магомедов Ш .Г.*, Изергин Д. А. Программный комплекс обнаружения вредоносной активности в корпоративной сети / Свидетельство о регистрации программы для ЭВМ 2021614531. 25.03.2021. [6)]

44. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М. И., Татарканов А. А. Конфигуратор настройки параметров работы сервера / Свидетельство о регистрации программы для ЭВМ 2021664584. 09.09.2021. [6)]

45. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М. И., Татарканов А. А Программный модуль интеллектуального анализа потоковых видеоданных на основе методов машинного обучения / Свидетельство о регистрации программы для ЭВМ 2021664913. 15.09.2021. [6)]

46. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М. И., Татарканов А. А Многофункциональная программная платформа видеоаналитики / Свидетельство о регистрации программы для ЭВМ 2021664454. 07.09.2021. [6)]

47. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М. И., Татарканов А. А Программный модуль интеллектуального автоматизированного поиска ситуационных событий в

видеопотоке / Свидетельство о регистрации программы для ЭВМ 2021664645. 10.09.2021. Заявка № 2021663707 от 25.08.2021. [6)]

48. Магомедов Ш. Г., Кашкин Е. В., Муравьев В. В., Назаренко М. А., Новиков А. С., Горобец А. И., Миськов Д. В. База данных системы управления закупками и проектами для построения контрольных карт Шухарта индивидуальных значений по 30 измерениям с целью определения наличия особых точек за пределами границ статистической управляемости (150 вариантов) / Свидетельство о регистрации базы данных RU 2019620701. 29.04.2019. Заявка № 2019620565 от 16.04.2019. [6)]
49. Магомедов Ш. Г., Лебедев А. С., Смирнов П. А. Модуль генерации участков с болезненными признаками на маммографических изображениях / Свидетельство о регистрации программы для ЭВМ RU 2021614527. 25.03.2021. [6)]
50. Мустафаев А. Г., Магомедов Ш. Г., Ирзаев Г. Х. Программа для определения сходства семантических сетей / Свидетельство о регистрации программы для ЭВМ RU 2015617768. 22.07.2015. Заявка № 2015614331 от 25.05.2015. [6)]
51. Мустафаев А. Г., Магомедов Ш. Г. Система управления версиями / Свидетельство о регистрации программы для ЭВМ RU 2015618491. 11.08.2015. Заявка № 2015615233 от 16.06.2015. [6)]