МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ»
(МТУСИ)

MINISTRY OF DIGITAL DEVELOPMENT, COMMUNICATIONS AND MASS MEDIA OF THE RUSSIAN FEDERATION

MOSCOW TECHNICAL UNIVERSITY OF COMMUNICATIONS AND INFORMATICS
(MTUCI)

ул. Авиамоторная, д. 8а, Москва, 111024,
www.mtuci.ru; мтуси.рф; e-mail: kanc@mtuci.ru
Телефон (495) 957-77-31; факс (495) 957-77-36
ОГРН 1027700117191; ИНН/КПП 7722000820/772201001; ОКПО 01179952;
ОКВЭД 85.22, 46.19, 58.19, 61.10, 68.32, 72.19, 85.21, 85.23, 85.42.9, 71.20, 33.13, 26.60 ; ОКТМО 45388000

31.08. 2022 № 2413/02-17

На № _____ от _____

«УТВЕРЖДАЮ»
Проректор по научной работе МТУСИ
д.т.н., профессор
_____ Ю.Л. Леохин
«29» августа 2022 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертационною работу Магомедова Шамиля Гасангусейновича «Методы и модели построения масштабируемой архитектуры системы контроля доступа к вычислительным сервисам», представленную на соискание ученой степени доктора технических наук по специальности 05.13.15 – Вычислительные машины, комплексы и компьютерные сети

1. Оценка актуальности темы диссертации

В современных условиях интернет-сервисы получают все большое распространение в различных организациях, что создает дополнительные возможности и условия для несанкционированного вмешательства в их работу. Естественное повышение требований к обеспечению надежности и безопасности информационных и компьютерных систем приводит к совершенствованию функций контроля доступа (КД). В то же время их реализация требует дополнительных вычислительных ресурсов и может существенно замедлять работу основного функционала вычислительного сервиса. Вопросы эффективного построения системы КД к вычислительным и информационным ресурсам предприятий остаются открытыми и актуальными в настоящее время, в связи с постоянным совершенствованием

средств преодоления различными злоумышленниками контроля доступа. Актуальная проблема требует своего научно-обоснованного решения.

Диссертация Магомедова Ш.Г. посвящена разработке и исследованию новых моделей, методов, алгоритмов и методик построения многоуровневых систем КД, обеспечивающих в комплексе защищенный доступ по открытым компьютерным сетям к вычислительным сервисам. При этом система КД рассматривается как самостоятельный ИТ-объект со своими задачами проектирования и конфигурирования, имеющий программно-аппаратные компоненты, занимающие часть инфраструктуры вычислительного комплекса.

В диссертационной работе предложен четырехуровневый подход к построению вычислительной архитектуры КД, сопровождаемый методикой оценки требуемых вычислительных ресурсов для обеспечения качества функционирования веб-сервисов в условиях возможных негативных проникновений. Учтены особенности веб-сервисов: передача паролей и средств контроля сторонним лицам; перехват паролей программными средствами; замена пользователя в ходе сеанса работы с сервисом. ситуации, в которых пользователь, прошедший все способы верификации. Исследования опираются на современные направления развития технологий безопасного контроля доступа Security Information and Event Management (SIEM), User Behavior Analytics (UBA), учитывая их особенности при создании прикладных решений. В качестве полигона для отработки и апробации предложенных подходов и методов КД, в работе выбраны образовательные и медицинские сервисы.

Все перечисленное определяет актуальность, высокую научную и практическую значимость тему настоящего исследования, посвященной разработке многоуровневой масштабируемой архитектуры контроля доступа к сервисам в условиях цифровой среды.

2. Оценка содержания диссертационной работы

Во введении обосновывается актуальность темы диссертации, определены цель, объект, предмет, задачи диссертационного исследования, сформулированы основные положения, выносимые на защиту; раскрыта научная новизна, теоретическая и практическая значимость работы, приведены сведения об апробации и внедрении результатов исследования.

В первой главе проведен анализ современных вычислительных инфраструктур, систем и комплексов, обеспечивающих поддержку и контроль доступа в информационной среде цифровых услуг.

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

Во второй главе сформулирована задача проектирования архитектуры контроля доступа, даны требования к составу средств контроля доступа; разработана четырехуровневая архитектура контроля доступа в условиях заданных технико-экономических характеристик к вычислительному комплексу, предоставляющему веб-сервисы в цифровой среде. Для оценки эффективности системы обеспечения контроля доступа предложено использовать стохастические методы, которые позволяют определять ожидаемые значения характеристик, значение которых должно обеспечить гарантированное значение качества обслуживания.

В третьей главе рассмотрены вопросы построения уровня облачной инфраструктуры архитектуры КД, представлена методика распределения виртуальных вычислительных ресурсов и сетевого взаимодействия. Разработана информационная модель корректности периодичности и целостности содержимого в архиве протокола DICOM (Digital Imaging and Communications in Medicine). Для повышения отказоустойчивости предлагается включение аналитических компонентов в среду виртуальных машин. Разработана архитектура устройства, реализующего функции анализа пакетов DICOM; предоставление данных аналитическим компонентам; управление конфигурацией и обеспечение функции проверки соответствия для медицинских изображений.

В четвертой главе предложена методика экспериментального оценивания количества вычислительных ресурсов, требуемого для резервирования при проектировании системы КД. Дана постановка задачи оценки ресурсной эффективности компонентов архитектуры КД. Разработанная методика основана на подходе, использующем виртуальные стенды. Проведенные экспериментальные исследования позволили оценить влияние действий пользователей на загрузку процессора сервера.

В пятой главе предложен метод КД на основе использования психологических реакций, которые могут быть измерены на основе работы с интерфейсами. Разработанный метод основан на гипотезе наличия индивидуальной зависимости времени реакции пользователей на ответы на заданные вопросы при работе с элементами интерфейса и возможности определения на этой основе индивидуальных психомоторных реакций. Показано, что реализация разработанного метода не приводит к значимому

увеличению объемов передаваемых данных и не замедляет работу клиентского приложения.

В шестой главе рассмотрены вопросы обеспечения безопасного КД к объектам инфраструктуры медицинского учреждения. Дан анализ особенностей инфраструктуры и систем сервисов учреждений здравоохранения. Выявлены уязвимые места и сценарии доступа в сетях и хранилищах медицинских данных. Разработана методика учета прикладных аспектов внедрения многоуровневого КД для предоставления медицинских услуг, в том числе предложены средства оценки производительности используемых и планируемых к приобретению кластерных конфигураций.

В седьмой главе исследованы особенности внедрения КД в образовательные сервисы. Рассмотрены вопросы реализации предложенной четырехуровневой архитектуры контроля доступа. Разработана методика учета прикладных аспектов внедрения многоуровневого КД в архитектуру специализированных вычислительных комплексов в учреждениях высшего образования. Разработанный механизм особенно актуален в формате дистанционного обучения и повышения его надежности .

В заключении автором подведены итоги диссертационного исследования, представлены основные результаты и выводы.

Текст диссертационной работы написан на технически грамотном языке, основные ее положения аргументированы, изложены логично и последовательно.

Полученные Магомедовым Ш.Г. научные и практические результаты направлены на решение актуальных и востребованных задач теории и практики построения масштабируемой архитектуры контроля доступа, обеспечивающей интеграцию технологий передачи, хранения, управления, мониторинга и анализа действий пользователей в вычислительных комплексах, предоставляющие веб-сервисы в условиях цифровой среды с использованием общедоступных компьютерных сетей.

3. Научная новизна

Следующие результаты, представленные в диссертации, теоретически обоснованы и имеют признаки научной новизны:

1. Научная концепция построения архитектуры КД как отдельной подсистемы вычислительного комплекса, предоставляющего веб-сервис, имеющей собственные цели, задачи и технологии реализации, что определяет ее относительную автономность и универсальность.

2. Четырехуровневая масштабируемая архитектура КД, интегрируемая в вычислительные комплексы, обеспечивающая в комплексе наиболее полное защищенное взаимодействие пользователей с вычислительными сервисами. На каждом из уровней определен специфический класс задач, который может быть реализован разными вариантами технологических решений с применением технологий КД: SIEM, UBA и др.

3. Комплекс новых научно-обоснованных методик, обеспечивающих: построение облачной инфраструктуры для решения задач КД.

4. Модель и метод анализа затрат вычислительных ресурсов для реализации систем контроля доступ на основе имитационных виртуальных стендов

5. Новый метод и соответствующая UBA-технология построения подсистемы КД на основе вопросно-ответного анализа психологических реакций, основанные на подтвержденной научной гипотезе о наличии индивидуальной реакции пользователя при взаимодействии с элементами интерфейса.

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

4. Значимость для науки и практики полученных результатов

Теоретическая значимость результатов диссертационной работы для развития предметной области заключается в разработке комплекса новых научно-обоснованных методов и технологий, предназначенных для решения проблемы безопасности информационных и компьютерных систем на основе многоуровневой масштабируемой системы контроля доступа.

Практическая значимость работы заключается в быстрой переносимости разработанных алгоритмов и программно-аппаратного обеспечения в различные прикладные области, что подтверждено на примерах создания и внедрения проектов в медицинскую и образовательную сферу.

5. Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна

Научные положения и результаты диссертационной работы основаны на теоретических выкладках, сопровождены ссылками на публикации в

авторитетных научных изданиях, подтверждены экспериментальными исследованиями на основе программных реализаций.

Выводы, и рекомендации, выполненные по главам и в заключении, изложены логично и обоснованно. Они следуют из сравнительного анализа подученных в диссертации результатов и современных результатов отечественных и зарубежных ученых по исследуемой проблеме. Магомедов Ш.Г. обосновал при этом собственную позицию на исследуемую проблему.

Достоверность выводов и результатов подтверждается корректным использованием математических методов и моделей, проведением адекватных теоретических и экспериментальных исследований, согласованием теоретических результатов с результатами экспериментов, положительной апробацией результатов на конференциях и семинарах, их непротиворечивостью с результатами, полученными другими авторами.

Основные научные результаты, представленные в п.3 настоящего отзыва и выносимые на защиту, получены автором самостоятельно.

Результаты 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 базах Web of Science / Scopus (включая квартили Q1 / Q2).

Получено 9 свидетельств о регистрации ПО.

В работах, опубликованных в соавторстве, Магомедову Ш.Г. принадлежат результаты по разработке архитектуры вычислительных комплексов, средств контроля доступа, методик контроля доступа на основе технологий SIEM и UBA.

В целом обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертации, достоверность и научная новизна полученных результатов не вызывают сомнений.

6. Рекомендации по использованию результатов и выводов диссертации

Целесообразно продолжить теоретическую и практическую работу по совершенствованию средств КД в рамках предложенного направления, их широкому внедрению в существующие и вновь создаваемые системы контроля доступа к веб-сервисам.

Рекомендуется использовать результаты диссертации при разработке информационного обеспечения веб-платформ учреждений высшего

образования и учреждений здравоохранения, а также продолжить работу в направлении повышения универсальности методов с целью их применению на промышленных предприятиях, использующих различные протоколы передачи данных.

Рекомендуется использовать результаты диссертации при проектировании и модификаций вычислительных комплексов в центрах обработки данных, предоставляющих защищенный доступ к веб-сервисам.

Результаты могут быть внедрены в информационно-технологические решения цифровой среды в научных организациях, высших учебных заведениях, коммерческих компаниях, государственных и специальных службах.

7. Замечания по работе

1. В диссертации рассматривается и анализируется протокол DICOM применительно к контролю доступа в медицинских учреждениях. В то же время, не указано, могут ли разработанные методы использоваться для иных протоколов и стандартов передачи данных, что существенно бы расширило границы применения результатов.

2. В работе приведен анализ действий пользователя информационной системы на основе формы опроса. Из постановки не ясно, на основе каких правил были выбраны анализируемые параметры и на сколько они универсальны для работы других систем.

3. Поскольку в диссертационной работе затронуты вопросы контроля доступа, требующие распознавания нештатных ситуаций, в том числе анализа действий пользователей сети, то применяемый в работе математический аппарат следовало расширить за счет использования классификаторов и методов машинного обучения.

4. Работа существенно выиграла бы, если бы было приведено описание общей структуры разработанного программного обеспечения и его основных количественных характеристик, оценки которых важны для пользователей при выборе и практической реализации предлагаемой многоуровневой системы контроля доступа.

5. Следовало уделить большее внимания качеству оформления рисунков и поясняющих текстов к ним, так в диссертации на фоне относительно крупных структурных схем часто используются непропорционально мелкие шрифты, что затрудняет чтение и восприятие представленного материала.

Указанные замечания не влияют на общую положительную оценку результатов диссертационной работы.

8. Заключение по работе

Диссертация Магомедова Ш.Г. является завершенной научно-исследовательской работой. Она обладает необходимым внутренним единством, логично и обоснованно приводящем к достижению сформулированной цели. Структура и содержание работы, состоящей из введения, описания глав, заключения, библиографического списка и приложения, дают полное представление о выполненных исследованиях и полученных результатах. Оформление диссертации отвечает требованиям к работам, рекомендуемым к открытой печати.

В автореферате представлены основные результаты, полученные в диссертации, дано краткое изложение содержания всех ее разделов, отражена актуальность работы, ее цель, научная новизна, практическая ценность, реализация результатов и их апробация.

Диссертация соответствует паспорту научной специальности 05.13.15 «Вычислительные машины, комплексы и компьютерные сети», а именно: п.1. Разработка научных основ создания вычислительных машин, комплексов и компьютерных сетей, исследования общих свойств и принципов функционирования вычислительных машин, комплексов и компьютерных сетей; п.2. Теоретический анализ и экспериментальное исследование функционирования вычислительных машин, комплексов и компьютерных сетей с целью улучшения их технико-экономических и эксплуатационных характеристик; п.5. Разработка научных методов и алгоритмов создания структур и топологий компьютерных сетей, сетевых протоколов и служб передачи данных в компьютерных сетях, взаимодействия компьютерных сетей, построенных с использованием различных телекоммуникационных технологий, мобильных и специальных компьютерных сетей, защиты компьютерных сетей и приложений.

Диссертация «Методы и модели построения масштабируемой архитектуры системы контроля доступа к вычислительным сервисам» является законченной научно-квалификационной работой, в которой автором проведены новые исследования, разработаны принципы, методы и модели построения архитектуры контроля доступа к вычислительным сервисам , обеспечивающей безопасную интеграцию технологий в вычислительных комплексах, хранение, мониторинг, идентификацию и аутентификацию

пользователей и субъектов информационных процессов, совокупность которых можно квалифицировать как научное достижение.

Диссертация отвечает требованиям п. 9 Положения ВАК РФ о порядке присуждения ученых степеней, а ее автор, Магомедов Шамиль Гасангусейнович, заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.15 – Вычислительные машины, комплексы и компьютерные сети.

Диссертационная работа рассмотрена и обсуждена на заседании кафедры «Безопасность телекоммуникаций» МТУСИ (присутствовало 8 человек, протокол № 8 от 29 августа 2022 года).

Заведующий кафедрой
«Безопасность телекоммуникаций»,
доктор военных наук, профессор А.Н. Кубанков

«29» августа 2022г

Сведения о ведущей организации:
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (МТУСИ), 111024, г. Москва, улица Авиамоторная, дом 8а, mtuci@mtuci.ru, +7 (495) 957-77-31