ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Духана Евгения Изовича
на диссертацию и автореферат диссертации
Магомедова Шамиля Гасангусейновича на тему
«Модели и методы адаптивного риск-ориентированного управления доступом в распределенных информационных системах», представленных на соискание ученой степени доктора технических наук по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертации

На современном этапе развития общества и технологий процесс обучения все больше тяготеет к цифровым дистанционным методам. Это характерно не только для ВУЗов, например, система обучения в ПАО «Ростелеком» охватывает 90000 обучающихся в год по всей стране в рамках полутора тысяч учебных программ. При этом процесс обучения организовывается и контролируется централизованно. Пандемия недавних годов не только показала необходимость, действенность дистанционных технологий, но и их удобство.

Перенос образовательных услуг в цифровую среду — сложный процесс, в котором участвуют в качестве субъектов различные категории обучающихся, приглашенные педагоги, администраторы процесса обучения и системные администраторы, а также контролирующие лица. Объектами доступа являются самые разнообразные ресурсы в виде электронных лекций и учебников, баз данных, интерактивные сервисы, к которым одновременно могут обращаться несколько пользователей, средства оценки качества обучения.

Стремительное увеличение объемов данных, сложность топологии цифровых распределенных систем приводит к росту типовых и возникновению специфических угроз информационной безопасности и предъявляет новые требования к организации управления доступом в них.

Традиционные модели и методы управления доступом используют логику, основанную на жестких правилах, не в полной мере адаптируются к задачам цифровых технологий образования. Предопределенность и статичность политик доступа не позволяют одновременно обеспечивать его оперативность и безопасность, гибко и своевременно реагировать на динамично меняющиеся условия процесса обучения, контент, контингент и требования нормативных правовых актов.

Одним из перспективных направлений решения указанной проблемы является разработка новых моделей и методов динамического адаптивного управления доступом в сложных гетерогенных информационных системах, основанных на риск-ориентированном прозрачном для пользователей

атрибутивном подходе, что определяет актуальность диссертационного исследования Магомедова Ш.Г.

Степень обоснованности научных положений, выводов, рекомендаций, сформулированных в диссертации

Обоснованность научных положений, выводов и рекомендаций, представленных в диссертационной работе, обеспечивается корректным использованием известных математических методов нечеткой логики, математической статистики и методов машинного обучения, адекватностью постановки задач проводимого исследования.

Выстроенная автором логика изложения текста рукописей диссертации и автореферата, структурирование материалов позволяют говорить о высокой аргументированности сформулированных выводов и положений.

Достоверность положений, выводов и рекомендаций, сформулированных в диссертации

Достоверность основных научных результатов диссертации Магомедова Ш.Г. обеспечивается сформированной методологией исследования, результатами анализа современных отечественных и зарубежных научных трудов по исследуемой проблематике, их согласованностью с положениями, сформулированными соискателем, широкой апробацией материалов работы.

Основные научные результаты диссертации отражены в 58 работах, из них 40 статей опубликованы в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, включая 22 статьи в изданиях, входящих в международные цитатно-аналитические базы Scopus и Web of Science; 9 свидетельств о государственной регистрации программы для ЭВМ. Результаты работы также докладывались на 23 конференциях различного уровня, в том числе международных.

Полученные результаты реализованы и внедрены в деятельность: АО «Позитив Текнолоджиз», ООО «Непрерывные технологии», ООО «Лаборатория Наносемантика», АО «Перспективный мониторинг», ФГАНУ «Центр информационных технологий и систем органов исполнительной власти им. А.В. Старовойтова», ФГБОУ ВО Институт кибербезопасности и цифровых технологий РТУ МИРЭА, о чём свидетельствуют соответствующие акты внедрения.

Характеристика структуры и содержания диссертации

Диссертационная работа состоит из введения, пяти глав, заключения, словаря терминов, списка литературы, содержащего 299 источников, 2 приложений, 82 рисунка и 19 таблиц. Объем рукописи составляет 314 страниц.

Во введении обоснована актуальность темы исследования, сформулированы цель и задачи, определены объект, предмет исследования, раскрыта научная новизна, теоретическая и практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

Первая глава посвящена анализу защищенности распределенных информационных систем, используемых методов и моделей управления доступом к таким системам, а также анализу исследований в области оценки риска информационных систем. На основе выявленных недостатков в защищенности распределенных информационных систем сформирована модель угроз и модель нарушителя для угрозы нарушения конфиденциальности информации, обрабатываемой в образовательных вычислительных сервисах, функционирующих на базе распределенных информационных систем. Представлена структура научно-методического аппарата риск-ориентированного атрибутивного управления доступом.

Вторая глава содержит описание и основные параметры разработанной риск-ориентированной атрибутивной модели управления доступом в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределительных информационных системах. В разработанной модели управления доступом наряду с атрибутами среды и субъектами доступа в качестве дополнительного атрибута применяется значения риска реализации угроз информационной безопасности.

В третьей главе представлено описание метода количественной оценки рисков реализации угроз информационной безопасности, посредством, которого осуществляется вычисление количественного значения атрибута – риск реализации угроз, разработанной атрибутивной модели управления доступом. Разработанный метод базируется на проведенных исследованиях подходов к адаптированному управлению доступом, интеллектуальных агентах сбора и обработки событий безопасности, а так же аппарате нечеткой логики, позволяющих оценить величину риска реализации угроз информации безопасности при осуществлении доступа к компонентам образовательных вычислительных сервисов распределенных информационных систем. Разработанная атрибутивная модель управления доступом и метод количественной оценки рисков реализации угроз информационной безопасности позволили разработать и реализовать метод непрерывной аутентификации пользователей, учитывающий количественные значения времени реакции пользователей.

Четвертая глава содержит описание и результаты экспериментальных оценок разработанного метода непрерывной аутентификации пользователей на основе их психологических реакций, а именно времени реакции пользователей при осуществлении доступа и взаимодействия

с компонентами образовательных вычислительных сервисов организаций высшего образования, базирующихся на распределительных информационных системах.

Пятая глава содержит результаты количественных оценок затрат производительности разработанных методов и модели управления доступом посредством разработанного метода оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов. Полученные значения позволили обосновать применение разработанного научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков, как в образовательные вычислительные сервисы высшего образования, так и в распределенные информационные системы.

В заключении представлены полученные соискателем результаты исследования, сформулированы выводы, намечены направления дальнейших исследований в области внедрения современных математических методов для риск-ориентированного управления доступом в распределенных информационных системах.

Диссертация соответствует паспорту специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность. Текст диссертации и автореферата написан грамотным языком, в выдержанном научном стиле, не содержит материалов, не относящихся к тематике проводимого исследования. Автореферат с достаточной полнотой отражает содержание диссертации.

Теоретическая значимость диссертационной работы

1. Разработанные модели и методы вносят значительный вклад в теорию информационной безопасности, предлагая новые подходы к управлению доступом и оценке рисков. В частности, риск-ориентированная атрибутивная модель управления доступом интегрирует оценку риска при принятии решений о предоставлении доступа, что расширяет существующие теоретические основы адаптивного управления доступом в условиях динамически изменяющейся среды.

2. Метод количественной оценки рисков на основе анализа событий от агентов дополняет теорию оценки рисков новыми инструментами для своевременной и точной оценки состояния распределенных информационных систем.

3. Метод непрерывной аутентификации на основе психологических реакций пользователей добавляет новый уровень защиты, учитывающий поведенческие и физиологические аспекты, что существенно расширяет теоретические модели аутентификации.

4. Метод оценки эффективности реализации защитных мер посредством анализа затрат ресурсов вносит важный теоретический вклад в понимание баланса между затратами и эффективностью механизмов защиты.

5. Научно-методический аппарат риск-ориентированного атрибутивного управления доступом, основанный на количественном анализе рисков, развивает теоретические подходы к управлению доступом, делая их более гибкими и адаптивными к изменяющимся условиям, что критически важно для повышения устойчивости информационных систем к угрозам.

Практическая значимость диссертационной работы

Практическая значимость результатов Магомедова Ш.Г. заключается в том, что предложенный в диссертации научно-методический аппарат риск-ориентированного атрибутивного управления доступом позволяет совершенствовать механизмы управления доступом, осуществлять оперативный мониторинг состояния распределенных информационных систем на основе анализа рисков с учетом вариативности внешней среды, а также обеспечивать адаптацию политик безопасности управления доступом под изменяющиеся условия среды. Указанные особенности позволяют сделать вывод о том, что предложенные решения вносят значительный вклад в повышение защищенности распределенных информационных систем при обеспечении их высокой доступности для пользователей.

Следует также отметить стремление соискателя к достижению компромисс между рисками и доверием, рисками и гарантированным правомочным доступом пользователей к востребованным ими ресурсам, что также весьма ценно при построении любых информационных систем.

Научная новизна исследования

В диссертации Магомедова Ш.Г. получены следующие основные результаты, обладающие, на мой взгляд, научной новизной.

1. Впервые предложенная риск-ориентированная атрибутивная модель управления доступом учитывает динамическое изменение условий функционирования распределенных информационных систем и использует оценку значения риска для адаптивного управления. Разработанная модель вводит дополнительный атрибут — риск реализации угроз информационной безопасности, в систему управления доступом, что, в свою очередь, обеспечивает возможность повышения защищенности распределенных информационных систем в процессе предоставления пользовательского доступа (п.12. Паспорта специальности).

2. Метод количественной оценки рисков реализации угроз информационной безопасности базируется на интеллектуальных агентах, использующих методы машинного обучения для анализа событий безопасности в распределенных информационных системах и количественной оценки рисков. Разработанный метод использует функционал нечеткой логики и математической статистики, что позволяет обеспечить точность результатов и адаптивность реализации в условиях изменяющихся угроз (п.8. Паспорта специальности).

3. Метод непрерывной аутентификации на основе психологических реакций позволяет учитывать индивидуальные особенности пользователей и использовать их как дополнительный фактор аутентификации в процессе предоставления доступа к компонентам распределительных информационных систем (п.12. Паспорта специальности).

4. Впервые предложен метод анализа затрат ресурсов для оценки эффективности защитных мер, направленный на выявление избыточного потребления ресурсов, применяемыми механизмами защиты информации распределенных информационных систем, что позволяет повысить эффективность работы предложенных средств обеспечения безопасности (п.2. Паспорта специальности).

Замечания и вопросы по диссертации

Положительно оценивая диссертацию в целом, следует выделить ряд дискуссионных положений, недостатков и замечаний.

1. В первой главе работы проведен очень тщательный анализ предметной сферы, который позволил соискателю обосновать структуру разрабатываемого научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков. В тоже время предложенный аппарат представлен описательно, в виде набора сущностей. На взгляд рецензента, в разделе 1.5 диссертации следовало представить его в виде схемы со связями между составными частями.

2. При формулировании атрибутов диссертационного исследования не указаны ограничения, поэтому не понятно сколь применимы научные результаты и рекомендации для других образовательных организаций, других разнородных и распределенных информационных систем.

3. В разделе 2.2.2 «Атрибуты безопасности управления доступом в образовательных вычислительных сервисах организаций высшего образования» выделено «несколько категорий атрибутов» и сервисов, которые «могут быть применены в процессе построения риск-ориентированной атрибутивной модели управления доступом». Анализа достаточности и неизбыточности перечня атрибутов и сервисов не приводится.

Тоже касается перечня «интеллектуальных агентов», включенных в метод количественной оценки рисков реализации угроз информационной безопасности с использованием нечеткой логики (раздел 3.4).

4. В разделе 3.4.3 «Метод оценки риска на основе нечетких правил» (стр. 153) приведена таблица правил вычисления нечетких логических выражений. Таблица содержит 15 комбинаций выходных значений агентов, тогда как таких вариантов может быть 81.

5. Ряд рисунков, содержащих результаты функционирования разработанных соискателем программ, в том числе скриншоты (например, рис. 3.23, рис. 5.18 – рис. 5.20) без комментариев, которых недостает в тексте рукописи, трудно трактовать.

6. В разделе 4.3 не приведен анализ различимости конкретных пользователей. Можно ли различать каждого из 2300 пользователей друг от друга, по каким параметрам и с какой достоверностью? Это же касается предложений, выдвинутых соискателем в разделе 5.3.1.

На защите соискателю предлагается более подробно осветить следующие вопросы:

– какое место в разработанном им научно-методическом аппарате занимает кластеризация журналов событий безопасности, поступающих от агентов (раздел 3.5.1)?

– каким образом «Результаты экспериментальных исследований с реальными данными демонстрируют эффективность и состоятельность разработанного метода, позволяющего оперативно обрабатывать события …» (выводы к главе 3 , стр.177)?

– какие дополнительные требования предъявляются к уровню подготовки пользователей образовательного вычислительного сервиса?

Заключение

Диссертационное исследование Магомедова Шамиля Гасангусейновича на тему «Модели и методы адаптивного риск-ориентированного управления доступом в распределенных информационных системах», представленное на соискание ученой степени доктора технических наук, является законченной научно-квалификационной работой, выполненной на высоком уровне.

Автореферат диссертации Магомедова Ш.Г. соответствует тексту диссертации, отражает ее основное содержание. Диссертация и автореферат соответствуют пунктам Паспорта специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность.

По результатам диссертационного исследования автором опубликовано достаточное количество научных работ. Диссертационная работа удовлетворяет требованиям п. 9–14 Положения о присуждении ученых степеней в УрФУ, а ее автор, Магомедов Шамиль Гасангусейнович,

заслуживает присуждения степени доктора технических наук по специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
доктор технических наук, профессор,
военнослужащий в/ч 69617 Е.И. Духан
Тел.: +7-922-218-22-62
Адрес электронной почты: ev.duhan@yandex.ru
620082, г. Екатеринбург, Сибирский тракт, 11 км

Подпись Духана Евгения Изовича заверяю:
сотрудник отдела кадров и воспитательной работы
в/ч 69617 Т.В. Жаворонкова

«18» февраля 2025 г.