ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Котенко Игоря Витальевича на диссертационную работу Магомедова Шамиля Гасангусейновича на тему «Модели и методы адаптивного риск-ориентированного управления доступом в распределенных информационных системах», представленной на соискание ученой степени доктора технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Актуальность темы диссертации

Современные распределенные информационные системы характеризуются высокой сложностью, масштабируемостью и интенсивным взаимодействием между пользователями и компонентами системы. В то же время количество кибератак и сложность угроз продолжают стремительно расти, что требует разработки более гибких и эффективных механизмов управления доступом. Традиционные модели управления доступом, ориентированные на статические правила, не всегда способны обеспечить должный уровень безопасности в условиях постоянной динамики угроз и контекстных факторов.

Адаптивные риск-ориентированные подходы, позволяющие учитывать контекст взаимодействия, изменчивость внешних и внутренних условий, а также анализировать вероятность реализации угроз, приобретают особую значимость. Такие методы позволяют оперативно принимать решения о предоставлении доступа, минимизируя риски нарушения информационной безопасности и оптимизируя ресурсы системы.

Актуальность исследования определяется необходимостью создания новых моделей и методов управления доступом, которые интегрируют анализ рисков в реальном времени, обеспечивают гибкость политик безопасности и их адаптацию к текущей ситуации. Это особенно важно для обеспечения защищенности критически важных данных и инфраструктуры в распределенных системах, что имеет ключевое значение для широкого спектра отраслей, включая финансовый сектор, здравоохранение, телекоммуникации и государственное управление.

При этом решение задачи по разработке адаптивных риск-ориентированных моделей управления доступом, позволяющих учитывать динамически изменяющиеся атрибуты доступа и среды в распределенных информационных системах, является актуальным направлением исследований.

Научная новизна полученных результатов

Диссертационное исследование направлено на разработку и реализацию мер по обеспечению конфиденциальности и целостности информации, обрабатываемой в распределенных информационных системах, посредством развития теоретических аспектов и практического применения разработанных методов, моделей, алгоритмов и средств управления доступом и обеспечения информационной безопасности при осуществлении взаимодействия пользователей с компонентами распределенных информационных систем. При этом, получены следующие результаты, характеризующиеся научной новизной:

1. Разработана риск-ориентированная атрибутивная модель управления доступом, включающая оценку риска при принятии решений о предоставлении доступа и позволяющая адаптивно реагировать на изменения условий доступа, обеспечивая гибкость в управлении правами пользователей в распределенных информационных системам с высоким уровнем динамичности.

2. Предложен метод количественной оценки рисков реализации угроз информационной безопасности, основанный на анализе событий, сформированных интеллектуальными агентами, позволяющий как оперативно идентифицировать потенциальные угрозы, так и проводить детализированный анализ факторов, влияющих на уровень риска.

3. Разработан метод непрерывной аутентификации пользователей на основе их психологических реакций, включающий анализ физиологических и поведенческих характеристик пользователей, которые позволяют повысить состояние защищенности распределительных информационных систем посредством снижения вероятности реализации пользователями несанкционированного доступа к компонентам системы.

4. Предложен метод оценки эффективности реализованных защитных мер, основанный на анализе затрат ресурсов, позволяющий осуществлять обнаружение фактов избыточного потребления ресурсов механизмами защиты информации в распределенных информационных системах, оптимизировать последующее потребление ресурсов и повысить эффективность применяемых защитных мер.

5. Разработан научно-методический аппарат риск-ориентированного атрибутивного управления доступом, основанный на количественном анализе рисков в условиях динамически изменяющихся атрибутов доступа и среды в распределенных информационных системах, обеспечивающий адаптивное управление доступом, учитывая текущее состояние атрибутов доступа и внешние условия функционирования распределенных информационных систем и пользователей, осуществляющих доступ.

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

Обоснованность и достоверность научных результатов проведенных исследований, обеспечивается корректностью использованного математического и теоретического аппарата. Выводы автора логично вытекают из проведенных исследований, обосновываются результатами проведенных в рамках диссертационного исследования экспериментов, а также подтверждаются апробацией полученных результатов на конференциях различного уровня и публикациями в рецензируемых научных изданиях. Рекомендации по практической реализации предложенных решений подробно изложены и обоснованы. Кроме того, рассмотрены сценарии применения и приведены рекомендации по внедрению разработанного научно-методического аппарата в образовательные вычислительные сервисы организаций высшего образования.

Достоверность положений, выводов и рекомендаций, сформулированных в диссертации

Основные научные результаты диссертации опубликованы 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. Получено 9 свидетельств о государственной регистрации программы для ЭВМ.

Теоретическая значимость результатов диссертации

Значимость результатов диссертации заключается в том, новый научно-методический аппарат, имеющий существенное значение для развития методов, моделей, алгоритмов и программных средств управления доступом и обеспечения информационной безопасности в распределенных информационных системах, впервые представлен в виде совокупности модели и методов риск-ориентированного атрибутивного управления доступом, включающей риск-ориентированную атрибутивную модель управления доступом, метод количественной оценки рисков реализации угроз информационной безопасности, метод непрерывной аутентификации, метод оценки эффективности реализации защитных мер и научно-методический аппарат управления доступом.

Практическая значимость результатов диссертации

Практическая значимость результатов диссертации заключается в том, что новый научно-методический аппарат риск-ориентированного атрибутивного управления

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

Полученные результаты внедрены в деятельность Института кибербезопасности и цифровых технологий РТУ МИРЭА, реализованы в проекте Ampire РТУ МИРЭА, а также применены для оценки защищенности распределенных информационных систем в ООО «Непрерывные технологии» и «Лаборатория Наносемантика», ФГАНУ «Центр информационных технологий и систем органов исполнительной власти им. А.В. Старовойтова», а также в АО «Перспективный мониторинг».

Оценка содержания диссертации и её оформления

Диссертация имеет четкую структуру, оформлена в соответствии с требованием ГОСТ Р 7.0.11–2011, соответствует положениям паспорта специальности 2.3.6. Методы и системы защиты информации, информационная безопасность. При этом диссертация содержит 314 страниц текста, 82 рисунка и 19 таблиц, состоит из введения, пяти глав, заключения, списка литературы, содержащего 299 наименований и двух приложений.

В первой главе проведен анализ исследований в области управления доступом в распределенных информационных системах: рассмотрена актуальность совершенствования существующих подходов к управлению доступом на основе исследования защищенности распределенных информационных систем и их компонент, разработана модель угроз и модель нарушителя для угрозы нарушения конфиденциальности и осуществления несанкционированного доступа к компонентам распределенных информационных систем и базирующихся на них образовательных вычислительных сервисов. Полученные результаты позволили сформировать цели и задачи исследования, в рамках реализации которой представлена структура разрабатываемого научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков.

Во второй главе представлены результаты первого положения, выносимого на защиту в виде разработанной риск-ориентированной атрибутивной модели управления доступом, основанной на анализе состояния изменяющихся условий среды и учете получаемых оценок значений риска. Для разработки и реализации модели проведено

сравнительное исследование в области моделей управления доступом, позволившее обосновать применение атрибутивной модели управления доступа и применения в качестве дополнительного атрибута значение риска. В ходе реализации разработанной модели управления доступом сформированы атрибуты доступа, учитывающие оценки значения риска, на основе разработанной модели для образовательных вычислительных сервисов организаций высшего образования, функционирующих на базе распределенных информационных систем.

В третьей главе описан разработанный метод количественной оценки рисков реализации угроз информационной безопасности. Разработанный метод оценки базируется на анализе событий, создаваемых агентами информационной системы. В качестве агентов выступают разработанные компоненты подсистемы сбора информации о событиях безопасности, полученные посредством анализа наблюдения за действиями пользователей, объектов и субъектов образовательных вычислительных сервисов, функционирующих на базе распределенных информационных систем. Для количественной оценки значения риска применяется математический аппарат теории нечеткой логики. Экспериментальная оценка разработанного метода оценки рисков осуществлена на функционирующей системе дистанционного образования РТУ МИРЭА, что позволило обосновать возможность реализации предложенных решений в распределенных информационных системах.

Четвертая глава содержит разработанный метод непрерывной аутентификации пользователей, основанный на психофизиологических реакциях пользователей, к компонентам образовательных вычислительных сервисов, функционирующих на базе распределительных информационных систем. В процессе обоснования выбранного аутентификационного признака — время реакции пользователей, осуществлены экспериментальные исследования психофизиологических реакций пользователей. Полученные результаты экспериментов позволили практически реализовать и оценить результаты внедрения разработанного метода непрерывной аутентификации, основанного на психологических реакциях пользователей в образовательные вычислительные сервисы РТУ МИРЭА, что, в свою очередь, позволяет использовать предложенные решения в распределительных информационных системах.

В пятой главе приведен разработанный научно-методический аппарат риск-ориентированного атрибутивного управления доступом, основанный на риск-ориентированной атрибутивной модели управления доступом, методе количественной оценки рисков реализации угроз информационной безопасности и методе непрерывной аутентификации пользователей. Для оценки реализации предложенных мер защиты

посредством внедрения разработанного научно-методического аппарата сформирован метод оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов. Полученные значения экспериментальной оценки эффективности разработанного научно-методического аппарата риск-ориентированного атрибутивного управления доступом позволили сделать вывод о достижении цели исследования.

Замечания и вопросы по работе

Вместе с этим следует отметить некоторые замечания и вопросы по содержанию диссертации и автореферата:

1. В диссертации не в полной мере приведены сведения о проведении количественно-качественной оценки представленного комплекса, также подробно не описаны аналоги похожих программно-аппаратных комплексов.
2. Не в полной мере доказана обоснованность представленного метода синтеза массивов данных, что может привести к некорректности при их использовании.
3. В модели угроз безопасности для образовательных вычислительных сервисов не представлены конкретные угрозы безопасности информации из банка данных ФСТЭК России и реализуемые ими последствия нарушения целостности, конфиденциальности и доступности.
4. Агрегирующая система мониторинга агентов использует показатели степени доверия агентов и уровней их критичности, которые не полной мере описаны в работе.
5. В процессе кластеризации событий, поступающих от агентов, применяется искусственная нейронная сеть с архитектурой автокодировщика, при этом другие архитектуры нейронных сетей в работе не рассматриваются.
6. Не представлены результаты верификации разработанной модели управления доступом методом проверки моделей на основе перебора различных комбинаций атрибутов доступа.

Сделанные замечания имеют дискуссионный характер и не снижают научной ценности работы.

Заключение по работе

Диссертационная работа изложена грамотным научно-техническим языком, в полной мере отвечает требованиям по актуальности, научной новизне, практической значимости, личному вкладу автора, отражению результатов в публикациях, а также полностью соответствует п. 9-14 Положения о присуждении ученых степеней в УрФУ. Автор диссертации Магомедов Шамиль Гасангусейнович заслуживает присуждения

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

Официальный оппонент:

Доктор технических наук, профессор,
заслуженный деятель науки Российской Федерации,
главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности,
Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН)

Тел.: +7 (812) 328 26 42
e-mail: ivkote1@mail.ru
Адрес: 199178, г. Санкт-Петербург, 14 линия В.О., д. 39

Котенко Игорь Витальевич

Подпись руки Котенко И.В. заверяю
Заместитель начальника отдела кадров СПб ФИЦ РАН
И.В.
«03» февраля 2025 г.