Основные результаты проекта РФФИ 18-07-01369 за 2018 год

В 2018 году исследования проводились в рамках первого этапа Проекта – этапа системного анализа и концептуального моделирования систем разграничения доступа к информации в облачных инфраструктурах (ОИ) критически важных информационных систем (КВИС). На этом этапе были получены следующие основные результаты.

1. Проведен **анализ состояния дел в предметной области проекта, в том числе существующих моделей, технологий и средств разграничения доступа к информации в ОИ и применения для их разработки технологии искусственного интеллекта.** Результаты анализа позволили сформулировать следующие выводы. Во-первых, облачные ОИ обладают существенными структурными и функциональными особенностями, выделяющие их в отдельный класс информационно-телекоммуникационных систем, в которых реализуется разграничение доступа к информации. Во-вторых, вычислительный процесс в ОИ может быть реализован в соответствии с тремя основными моделями предоставления услуг: «программное обеспечение как сервис» (SaaS), «платформа как сервис» (PaaS) и «инфраструктура как сервис» (IaaS). Модель IaaS становится наиболее распространенной, однако она является наиболее сложной в разграничении доступа. В-третьих, для ОИ справедливо резкое увеличение угроз реализации программно-информационных воздействий (компьютерных атак). К числу наиболее известных классов атак на ОИ относятся атаки типа «отказа в обслуживании», инъекции вредоносной услуги, атаки через вредоносную виртуальную машину и другие. Наконец, в настоящее время используется несколько базовых моделей разграничения доступа к ресурсам ОИ. Наибольшей популярностью обладает ролевая модель (RBAC). Дискреционная (DAC) и мандатная (MAC) считаются устаревающими, т.к. их возможности обеспечиваются моделью RBAC. Атрибутивная модель (ABAC) является менее распространенной, чем RBAC, однако обладает более гибкими возможностями, поэтому считается более перспективной. Модель ABAC выделяет атрибуты объектов, действий, субъектов и условий доступа. При применении этой модели значения атрибутов сравниваются с политикой безопасности, и принимается соответствующее решение о предоставлении доступа. Несмотря на то, что традиционная модель RBAC в большинстве случаев вполне подходит для решения задач разграничения доступа в ОИ, в перспективе, при приобретении моделью ABAC достаточного практического распространения, следует переходить на эту новую модель.

2. Сформирована **общая формальная постановка задачи обеспечения требуемого разграничения доступа в ОИ КВИС**. Для этой цели определен состав исходных данных, критерии формирования единой системы разграничения доступа в ОИ, и ограничения. Исходные данные задачи составляют: множество пользователей; множество ресурсов; множество полномочий; требуемая политика разграничения доступа пользователей к ресурсам. Роль ограничений играют функциональные ограничения, определяемые используемыми моделями предоставления услуг в ОИ, стратегиями использования ресурсов, а также используемой моделью разграничения доступа. Критерии задачи определяют степень соблюдения единой системой разграничения доступа ОИ правил требуемой политики разграничения доступа. Для этой цели введены понятия «требуемой» и «реальной» схемы (конфигурации) разграничения доступа и определена мера (показатель) схожести этих схем. Для модели RBAC требуемая схема определяется матрицей «пользователи – полномочия», а реальная схема образуется в результате булева матричного произведения X*Y, где X – матрица «пользователи – роли», а Y – матрица «роли – полномочия». Для модели ABAC требуемая и реальная схемы определяются системами логических выражений (правил), определяющих возможность доступа пользователей к атрибутам ресурсов. Установлено, что оптимизационные задачи по разграничению доступа в ОИ относятся к числу NP-полных. Поэтому для поиска их рациональных решений предложено использовать биоинспирированные методы оптимизации (генетические алгоритмы), а также комбинирование методов машинного обучения. В качестве первичных методов машинного обучения применялись: дерево решений, метод опорных векторов, мультиномиальный наивный байесовский классификатор, метод случайного леса, логистическая регрессия.

Основные положения предложенного подхода по комбинированию методов машинного обучения были опубликованы в журнале “IEEE Access” рейтинга Q1 базы Scopus.

3. Разработана **система показателей и критериев оценки качества политик разграничения доступа для различных моделей управления доступом, применяемых в ОИ КВИС**. При этом полагалось, что оценка качества политик разграничения доступа в ОИ необходима для выявления необходимости принятия контрмер по противодействию атакам на систему разграничения доступа и определения условий начала выполнения реконфигурация политик разграничения доступа. Из этого сделан вывод, что мера близости требуемой и реальной схем является одним из основных показателей качества политики разграничения доступа. Другими показателями являются различные структурные параметры схемы разграничения доступа, например, количество ролей (для модели RBAC), общее количество связей в схеме (для ABAC), количество структурных изменений, необходимых для перехода к новой схеме в случае ее реконфигурации, и т.д. Для формирования критериев оценки политик разграничения доступа, которые могли бы носить универсальный характер и быть применимыми к любым моделям разграничения доступа, предложен подход, основанный на учете показателей конфиденциальности и доступности контролируемых ресурсов. При реконфигурации политик разграничения доступа к ОИ предложено использовать критерий минимизации затрат администрирования, необходимых на переход от текущей схемы к новой схеме разграничения доступа. Основные положения предложенного подхода опубликованы в коллективной монографии “Nature-Inspired Cyber Security and Resiliency: Fundamentals, Techniques and Application”.

4. Разработана **концептуальная модель процесса разграничения доступа к информации в ОИ КВИС**, которая задает описание этого процесса на высшем уровне представления. Модель состоит из следующих компонентов: функционального, понятийно-терминологического, критериального и верификационного. Функциональный компонент определяет основные функции системы разграничения доступа, к числу которых относятся: оценка схем разграничения доступа, верификация политик разграничения доступа, принятие решений на изменение схем доступа и оптимизация этих схем. Функция принятия решений определяет необходимость изменения схем в режимах первоначального проектирования и реконфигурирования. Оптимизация схем доступа позволяет устранить избыточность в схемах в соответствии с заранее выбранными критериями. Для реализации последних двух функций предложен подход, основанный на использовании усовершенствованных генетических алгоритмов. Результаты опубликованы в журнале “ACM Transactions on Reconfigurable Technology and Systems (TRETS)”, имеющего рейтинг Q2 в базе Scopus. Понятийно-терминологический компонент включает новые понятия (схожесть и расхождение между текущими и требуемыми схемами доступа, прямые и непрямые отображения между элементами схем доступа и др.) Критериальный компонент определяет совокупность постановок задач по формированию схем разграничения доступа, в которых используются критерии минимального количества ролей, минимального количества связей, минимального расхождения между схемами, минимальных затрат и другие. В основу построения верификационного компонента были положены модели и алгоритмы, реализующие многоагентную нечеткую классификацию с использованием иерархических нечетких ситуационных сетей и нечеткого логического вывода согласно механизму Мамдани.

5 Дополнительно были проведены исследования в области разработки **аналитических моделей реализации атак и мер противодействия, преобразовании стохастических сетей**. Были построены аналитические модели для наиболее часто встречающихся атак на ОИ КВИС, в частности, атак отказа в обслуживании, сканирования и др. Основные положения предложенного подхода к разработке аналитических моделей атак были опубликованы в коллективной монографии издательства Springer “Cyber Resilience of Systems and Networks. Risk, Systems and Decisions”. Полученные результаты позволили внести в план исследований следующего года разработку моделей и методов, основанных на использовании и преобразовании нечетких стохастических сетей.