**Основные результаты проекта РФФИ 18-07-01369 за 2019 год**

В 2019 году исследования проводились в рамках второго этапа Проекта – этапа разработки моделей, методов и алгоритмов оценки, оптимизации, верификации и реконфигурации политик разграничения доступа к информации в облачных инфраструктурах (ОИ) критически важных информационных систем (КВИС). На этом этапе были получены следующие основные результаты.

1. Разработаны **модели, методы и алгоритмы оценки качества политик разграничения доступа в ОИ КВИС**. При этом в качестве исходных данных учитывались требуемая и результирующая схемы разграничения доступа. Если требуемая схема разграничения доступа задается лицом, принимающим решения, то результирующая схема образуется на основании правил, свойственных выбранной модели контроля доступа. Результатом решения задачи является значение обобщенного показателя, отражающего схожесть между требуемой и результирующей схемами.

Исследования по оценке качества политик разграничения доступа были ориентированы на модель разграничения доступа, основанную на атрибутах (Attribute-Based Access Control, ABAC), которая считается наиболее перспективной для применения в ОИ. В качестве оцениваемых показателей были выбраны точность, целостность и доступность политик разграничения доступа.

Для оценки точности предложена универсальная модель представления политик, которая использует матрицу доступа. Каждая ячейка в этой матрице соответствует множеству прав доступа, которые субъект доступа может выполнять над объектом, полагая, что выполняются условия некоторых политик доступа. Показателем точности является мера близости двух матриц доступа, соответствующих существующей политике и желаемой схеме разграничения доступа.

В качестве показателя целостности предлагается учитывать взвешенную структурную сложность политик разграничения доступа. Эта сложность определяется на основе анализа сложности универсальной модели представления политик. При этом учитываются весовые коэффициенты логических условий и операций, присутствующих в правилах, составляющих политики разграничения доступа.

Полученные результаты по оценке качества политик разграничения доступа в ОИ КВИС были успешно апробированы в следующих прикладных задачах: построение доверенной среды для разграничения доступа к информации в ОИ, формирование концептуальных основ обеспечения информационной безопасности в системе распределенных ситуационных центров, сравнительная оценка реализации моделей обработки данных в веб-приложениях, оценка качества принципиально новой модели визуального контроля доступа, основанной на треугольных матрицах.

2. Разработаны **модели и алгоритмы оптимизации политик разграничения доступа в ОИ КВИС на основе технологии искусственного интеллекта**, ориентированные как на перспективную модель доступа ABAC, так и на наиболее распространенную в настоящее время в существующих ОИ ролевую модель (Role-Based Access Control, RBAC).

Для оптимизации политик ABAC в ОИ КВИС разработаны модель и алгоритм, основанные на глубоком обучении. При этом был реализован подход, который позволяет вывести правила разграничения доступа из существующих записей регистрации (логов). При построении модели глубокого обучения были использованы различные искусственные нейронные сети, в частности, ограниченные машины Больцмана, вычисляющие меру подобия для кластеризации правил-кандидатов.

Для оптимизации политик RBAC в ОИ КВИС разработаны модель и алгоритм оптимизации единых схем разграничения доступа в ОИ в различных режимах их формирования. Для этих целей были предложены различные критерии оптимизации, используемые в различных режимах: минимальное количество ролей для режима первоначального проектирования и минимальные схемные изменения для режима реконфигурации.

Для оптимизации политик сетевого разграничения доступа в ОИ КВИС на основе технологии VLAN разработаны модели и алгоритмы, в которых изыскиваются виртуальные роли для сетевых хостов и происходит объединение хостов в кластеры по этим ролям. Как было показано, при достаточно большой размерности ОИ КВИС такая модель разграничения доступа обеспечивает более высокие показатели качества формируемых политик сетевого разграничения доступа, чем другие известные подходы.

3. Разработаны **модели и алгоритмы верификации и обеспечения непротиворечивости политик разграничения доступа в ОИ КВИС на основе технологии искусственного интеллекта.** Разработанная модель обеспечения непротиворечивости политик разграничения доступа основана на логических формулах первого порядка и состоит из множества состояний, системы переходов между состояниями и индикаторной функции, помечающей истинные свойства в каждом состоянии. При этом используются следующие правила: множество состояний есть множество всех оценок над множеством переменных; для любой пары состояний отношение перехода соблюдается в том и только в том случае, когда соответствующая ему логическая формула становится истинной; каждое атомарное высказывание представляет собой присваивание переменным значений из некоторого домена.

Модель обеспечения непротиворечивости используется в разработанном алгоритме верификации политик разграничения доступа в ОИ КВИС. Алгоритм осуществляет построение модели обеспечения непротиворечивости политик в виде конечного автомата. На языке темпоральной логики формируется спецификация проверяемой системы, задающяя условия отсутствия аномалий. Далее следуют вычисление модели с помощью программного средства верификации (верификатора), обработка результатов верификации и оценка их соответствия требованиям эффективности.

Разработанные модель и алгоритм верификации реализованы в программном средстве верификации политик ABAC, использующем верификатор UPPAAL. На это программное средство получено свидетельство о государственной регистрации программы для ЭВМ.

4. Разработаны **модели и алгоритмы выявления условий проведения и непосредственного выполнения реконфигурации политик разграничения доступа в ОИ КВИС на основе технологии искусственного интеллекта,** ориентированные на обе модели разграничения доступа, применяющиеся в ОИ – RBAC и ABAC.

В случае использования модели RBAC задача выявления условий проведения и непосредственного выполнения реконфигурации политик разграничения доступа заключается в переходу от существующей схемы доступа к новой, обусловленной появившимися изменениями в полномочиях пользователей, с минимальными вычислительными издержками. Для условий проведения достаточно частых последовательных реконфигураций политик разграничения доступа разработаны модель и алгоритм, позволяющие обосновать необходимость выполнения полного перепроектирования единых схем разграничения доступа в ОИ КВИС.

В случае использования модели ABAC для решения задачи выявления условий проведения и непосредственного выполнения реконфигурации политик разграничения доступа предлагается подход, основанный на анализе правил разграничения доступа с помощью методов глубокого обучения и нечетких ситуационных сетей.

В предложенной модели глубокого обучения используется составная искусственная нейронная сеть, состоящая из многослойного персептрона и автоэнкодера. Показано, что такая нейросетевая конструкция позволяет достаточно эффективно диагностировать компьютерные инциденты различной природы, включая инциденты, связанные с изменениями правил в модели ABAC.

В разработанном подходе к оперативному принятию решений по изменению правил разграничения доступа, основанном на применении нечетких ситуационных сетей, осуществляется представление текущего состояния политики разграничения доступа в виде множества взаимосвязанных нечетких ситуаций, а решение о необходимости реконфигурации политики принимается по результатам проведения нечеткого логического вывода, основанного на известном методе Мамдани.