На правах рукописи

Созыкин Андрей Владимирович

СЕМАНТИЧЕСКАЯ ИНТЕГРАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ К СЕРВИСАМ

Специальность 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Пермь – 2008

Работа выполнена в Институте механики сплошных сред Уральского отделения Российской академии наук (ИМСС УрО РАН)

Научный руководитель: кандидат технических наук
Масич Григорий Федорович

Официальные оппоненты: доктор технических наук, профессор
Сухов Андрей Михайлович

кандидат физико-математических наук
Филиппов Виктор Иванович

Ведущая организация: Пермский Государственный Технический Университет

Защита состоится ___ декабря 2008 года в _____ часов на заседании диссертационного совета Д002.073.01 при Институте проблем информатики РАН по адресу: 119333, Москва, ул. Вавилова, д.44, кор.2.

С диссертацией можно ознакомиться в библиотеке Института проблем информатики РАН

Отзывы в одном экземпляре, с заверенной подписью, просим направлять по адресу: 119333, Москва, ул. Вавилова, д.44, кор.2, в диссертационный Совет.

Автореферат разослан «___» ноября 2008 г.

Ученый секретарь диссертационного совета Д002.073.01
доктор технических наук, профессор

С.Н.Гринченко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Современные научные и коммерческие организации строят корпоративные сети, предоставляющие сотрудникам сервисы разных типов: сетевые (электронная почта, доступ в Интернет), вычислительные (кластеры, многопроцессорные серверы), информационные (справочные системы, порталы, системы управления предприятием, прикладные научные системы). В таких сетях повышенное внимание уделяется управлению доступом к сервисам в целях обеспечения безопасности и удобства работы.

В крупных сетях с большим количеством сервисов и пользователей управление доступом к сервисам связано с рядом проблем. Управление является трудоемкой задачей, создающей большую нагрузку на администраторов и предъявляющей высокие требования к их квалификации. Для управления доступом к сервисам разных типов приходится использовать несколько разных систем управления и выполнять большое число операций. Сервисы разных типов используют отдельные репозитории правил разграничения доступа, часть информации в которых дублируется и требует синхронизации при изменении. Пользователям работать с сервисами неудобно из-за большого количества идентификаторов и паролей, требуемых для разрешения доступа к сервисам. Безопасность работы с сервисами находится на низком уровне: пользователи выбирают простые пароли, которые легко подобрать, сложные пароли записывают, нетрудно реализуются атаки социальных инженеров.

Актуальной является задача повышения эффективности процесса управления доступом и увеличения удобства работы с сервисами путем интеграции механизмов управления доступом к сервисам разных типов. Интеграция осложняется тем, что сервисы используют различные протоколы управления доступом: RADIUS, KERBEROS, LDAP, SAML, WS-Security и др. Для хранения правил разграничения доступа применяются различные репозитории: текстовые файлы, XML, реляционные СУБД, каталоги LDAP. В последнее время все большей популярностью пользуются интегрированные системы, позволяющие управлять доступом к сервисам разных типов, независимо от деталей взаимодействия. При этом расхождения в базовых семантических моделях этих систем приводят к проблемам интероперабельности и существенно ограничивают круг поддерживаемых сервисов.

В данной работе предложена формальная основа для интеграции механизмов управления доступом к сервисам разных типов на основе семантического похода и разработан комплекс программ для интеграции управления доступом к сервисам разных типов. Данный комплекс обеспечивает хранение правил разграничения доступа, реализацию процедур защиты информации (идентификация, аутентификация и авторизация), предоставляет единую систему управления правилами разграничения доступа для всех сервисов, используемых в организации, независимо от их типа.

Целью диссертационной работы является повышение эффективности процесса управления доступом к сервисам за счет интеграции механизмов управления доступом к сервисам разных типов (информационным, сетевым и вычислительным). В работе исследованы и решены следующие **задачи**:

1. Исследование и сравнительный анализ существующих подходов к управлению доступом к сервисам с точки зрения возможности интеграции процессов управления доступом к сервисам разных типов.
2. Разработка методики семантической интеграции управления доступом к сервисам разных типов.
3. Построение семантической модели системы управления доступом к сервисам.
4. Создание средств описания правил разграничения доступа в формальном виде.
5. Разработка комплекса программ, интегрирующего управление доступом к сервисам разных типов.

6. Исследование эффективности применения семантической интеграции управления доступом к сервисам в сетях научных организаций.

Объект исследования: процесс управления доступом к сервисам.

Предмет исследования: интеграция управления доступом к сервисам разных типов.

Научая новизна. В диссертационной работе получены следующие новые результаты:

– Применен семантический подход для интеграции управления доступом к сервисам разных типов, что позволило значительно расширить интероперабельность. Разработана методика интеграции управления доступом к сервисам на основе семантического подхода.

– Предложена унифицированная онтологическая модель, определяющая базовые понятия и операции управления доступом к сервисам. Модель делает возможной интеграцию управления доступом к сервисам разных типов, использующих различные модели, методы и технологии управления доступом на основе семантического подхода.

– Разработана алгебраическая запись правил разграничения доступа, представляющая собой формальную запись понятий разработанной онтологической модели. Алгебраическая запись позволяет в формальном виде описывать правила разграничения доступа с использованием различных методов управления доступом.

– Реализован комплекс программ управления доступом к сервисам на основе разработанных технологий.

Положения, выносимые на защиту:

1. Методика семантической интеграции управлении доступом к сервисам, позволяющая значительно расширить круг поддерживаемых сервисов и методов управления доступом.

2. Система моделей управления доступом к сервисам, включающая онтологическую модель управления доступом к сервисам и алгебраическую запись правил разграничения доступа. Модели предоставляют основу для интеграции управления доступом к сервисам разных типов: онтология задает общую семантику понятий предметной области управления доступом и операций над ними, общий формальный синтаксис задает алгебраическая запись правил разграничения доступом.

3. Результаты оценки эффективности применения семантической интеграции управления доступом к сервисам в сетях научных организаций.

Практическая ценность. Разработанные модели, методы, технологии и созданный на их основе комплекс программ позволяют интегрировать управление доступом к сервисам разных типов. Работа пользователей с сервисами становится более удобной за счет интеграции учетных записей для доступа ко всем сервисам с возможностью однократной регистрации. Администраторам, отвечающим за управление доступом к сервисам, предоставляет единая, удобная, интуитивно понятная система управления.

Апробация работы. Основные результаты работы докладывались и обсуждались на следующих научных конференциях и семинарах:

– Всероссийская научная конференция «Научный сервис в сети Интернет», Новороссийск, 2002, 2006, 2007.

– 13 Зимняя школа по механике сплошных сред, Пермь, 2003.

– Региональная молодежная конференция «Проблемы теоретической и прикладной математики», Екатеринбург, 2003, 2004.

– Конференция представителей региональных научно-образовательных сетей «RELARN», 2004, 2006, 2007.

– XIV Всероссийская научно-методическая конференция «Телематика’2007» Санкт-Петербург, 2007.

– Международная конференция «Вычислительные и информационные технологии в науке, технике и образовании», Казахстан, Алматы, 2008

Публикации. По теме диссертации опубликовано 17 научных работ, в том числе 2 в изданиях, входящих в список ВАК.

Структура и объём работы. Диссертация состоит из введения, четырех глав, заключения, списка использованных источников, включающего 112 работ, приложения. Работа изложена на 107 страницах, содержит 29 рисунков, 8 таблиц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, описаны решаемые проблемы и задачи.

В первой главе выполнен обзор текущего состояния систем, интегрирующих управления доступом к сервисам разных типов. В первом разделе рассмотрены существующие технологий управления доступом к сервисам. Управление доступом (access control) – это процесс проверки запросов на доступ к сервису с целью определить разрешить или запретить доступ. Большая часть современных систем использует модель управления доступом, предложенную Лампсоном в 1974 г (рис. 1.).

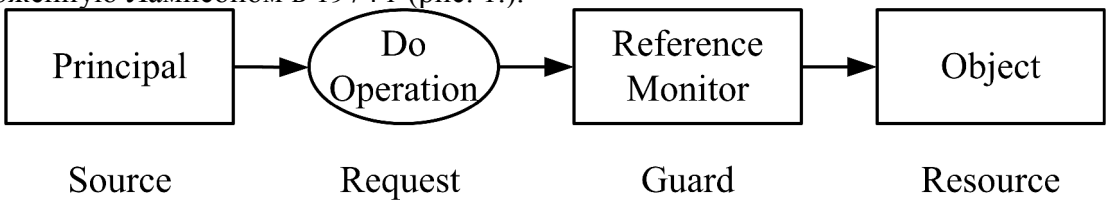

Рис. 1. Модель управления доступом (Лампсон, 1974).

Модель Лампсона включает следующие элементы:

- **Principal** – автор запроса (принципал, иногда называют субъектом).
- **Object** – ресурс, информационный, сетевой или вычислительный.
- **Request** – запрос на выполнение операции с объектом.
- **Reference Monitor –** диспетчер доступа, проверяющий все запросы к объекту и принимающий решение о разрешении или запрещении доступа.

Диспетчер доступа для принятия решения проводит три процедуры защиты информации. Определение источника запроса называется **идентификацией**, подтверждение подлинности источника называется **аутентификацией**, анализ правил разграничения доступа называется **авторизацией**.

В настоящее время существует большое количество реализаций процедур защиты. В работе описаны распространенные методы идентификации и аутентификации: парольная, многофакторная, биометрическая, с использованием криптографии и с нулевой передачей знаний (Фейге, Фиат, Шамир, 1986). Приведен обзор методов управления доступом (авторизации): дискреционного (Лампсон, 1974), мандатного (Белл и Ла Падула, 1975), ролевого (Сандху, 1996), атрибутного (Юан и Тонг, 2005).

Показано, что основной причиной неэффективности процесса управления доступом к сервисам является многообразие технологий управления доступом. Многообразие технологий обеспечивает гибкость процесса управления, но значительно увеличивает сложность и трудоемкость. Для упрощения процесса управления необходима интеграция систем управления доступом к сервисам, использующих различные технологии.

Во втором разделе рассмотрены подходы к интеграции информационных систем, обеспечивающие различные уровни интероперабельности:

- **Синтаксическая** интеграция основывается на использовании согласованных форматов данных;
- **Структурная** интеграция обеспечивает согласование структур данных путем преобразования форматов с применением метаданных;
- **Семантическая** интеграция устанавливает смысловое соответствие между сущностями.

Наиболее полную интероперабельность интегрируемых систем обеспечивает семантическая интеграция. Интеграционные решения, использующие синтаксический и структурный подход являются частными, рассчитанными на определенные системы. Широкое применение таких решений затруднено.

В настоящее время наиболее популярной технологией семантической интеграции являются онтологии. Онтологии определяют общий словарь предметной области, который может совместно использоваться людьми или информационными системами. Для разработки онтологий существует широкий набор инструментальных средств: язык описания онтологий OWL (Web Ontology Language), являющийся стандартом W3C, среды редактирования онтологий Protégé, Ontolingua, Chimaera, готовые и доступные к использованию онтологии, описывающие различные предметные области.

На основе анализа подходов к интеграции информационных систем делается вывод, что интеграцию систем управления доступом к сервисам необходимо выполнять с помощью семантического подхода, что обеспечит максимальную интероперабельность. В качестве инструментария интеграции целесообразно использовать онтологии.

В третьем разделе выполнен обзор существующих систем интеграции управления доступом к сервисам. Выявлены аналоги трех типов: системы централизованного управления, системы федеративной идентификации, системы интегрированного управления. Оценка наиболее близких аналогов приведена в табл. 1.

Таблица 1. Оценка существующих систем интеграции управления доступом

Название	Интероперабельность	Функциональные возможности	Методы управления доступом	Схема распространения	Область применения	Всего
Системы централизованного управления						
AAA	1	6	1	10	5	23
LDAP	1	6	1	10	5	23
KERBEROS	1	6	1	10	5	23
A-Select	1	6	1	10	5	23
SAML	1	7	1	10	5	24
Системы федеративной идентификации						
Liberty	4	7	7	8	5	31
WS-Federation	3	7	7	5	5	27
OpenID	2	5	5	8	3	23
Windows CardSpace	2	5	6	5	3	21
Системы интегрированного управления						
IBM Tivoli Identity Manager	5	10	10	5	10	40
Sun Identity Manager	**5**	**10**	**10**	**10**	**10**	**45**
Oracle Identity Manager	5	10	10	5	10	40
Novell Identity Manager	5	9	8	5	10	37
Microsoft Identity Intergation Server	5	9	8	5	10	37

Анализ позволил выбрать прототип – Sun Identity Manager. Основным недостатком прототипа и других аналогов является низкая интероперабельность. Это объясняется применением синтаксической (системы централизованного управления и федеративной идентификации) и структурной (системы интегрированного управления) интеграции. В результате задача интеграции механизмов управления доступом к сервисам разных типов с использованием

существующих систем затруднена. Расширить интероперабельность можно с помощью семантической интеграции, для чего необходимо разработать четкую семантическую модель управления доступом к сервисам.

В четвертом разделе выполнен обзор существующих онтологий в области управления доступом к сервисам. Выявлены аналоги трех типов: онтологии для управления доступом к конкретным информационным системам, онтологии для различных методов управления доступом, и онтологии верхнего уровня. Оценка наиболее близких онтологий с точки зрения возможности применения для интеграции управления доступом к сервисам разных типов приведена в табл. 2.

На основе результатов оценки в качестве прототипа была выбрана онтология BWW (Bunge, Wand and Weber ontology). Недостатком онтологии BWW является слишком высокий уровень абстракции: онтология описывает информационные системы в целом, без учета особенностей конкретных информационных систем. Необходимо выполнить адаптацию онтологии BWW к предметной области управления доступом к сервисам разных типов с учетом существующих Российских и международных стандартов и распространенных методов управления доступом.

Таблица 2. Оценка онтологий в предметной области управления доступом

Онтология	Широта применения	Ориентация на информационные системы	Практическое использование	Всего
Онтологии для управления доступом к конкретным информационным системам				
HL7	1	10	1	12
LSDIS	1	10	1	12
Access-eGov	1	10	1	12
Онтологии для методов управления доступом к сервисам				
Access Control Lists ontology	3	10	3	16
Role base access control ontology	3	10	3	16
Attribute base access control ontology	3	10	2	15
Rule base access control ontology	3	10	2	15
Context aware access control ontology	2	10	1	13
Онтологии верхнего уровня				
Cys	10	1	10	21
SUMO	10	2	9	21
GOL	8	2	6	16
BWW	**6**	**10**	**8**	**24**
DOLCE	7	8	8	23

Вторая глава посвящена семантической интеграции управления доступом к сервисам разных типов.

В первом разделе представлены анализ и критика прототипа. Схема прототипа и предлагаемого решения приведена на рис. 2.

Основным недостатком прототипа является низкая интероперабельность, вызванная использованием структурной интеграции. Для увеличения интероперабельности предлагается использовать семантическую интеграцию: разработать семантическую модель в виде онтологии, ввести блок согласования семантики в адаптеры сервисов, модифицировать схему дан-

ных и блоки хранения правил разграничения доступа, ПО управления доступом и консоль управления доступом.

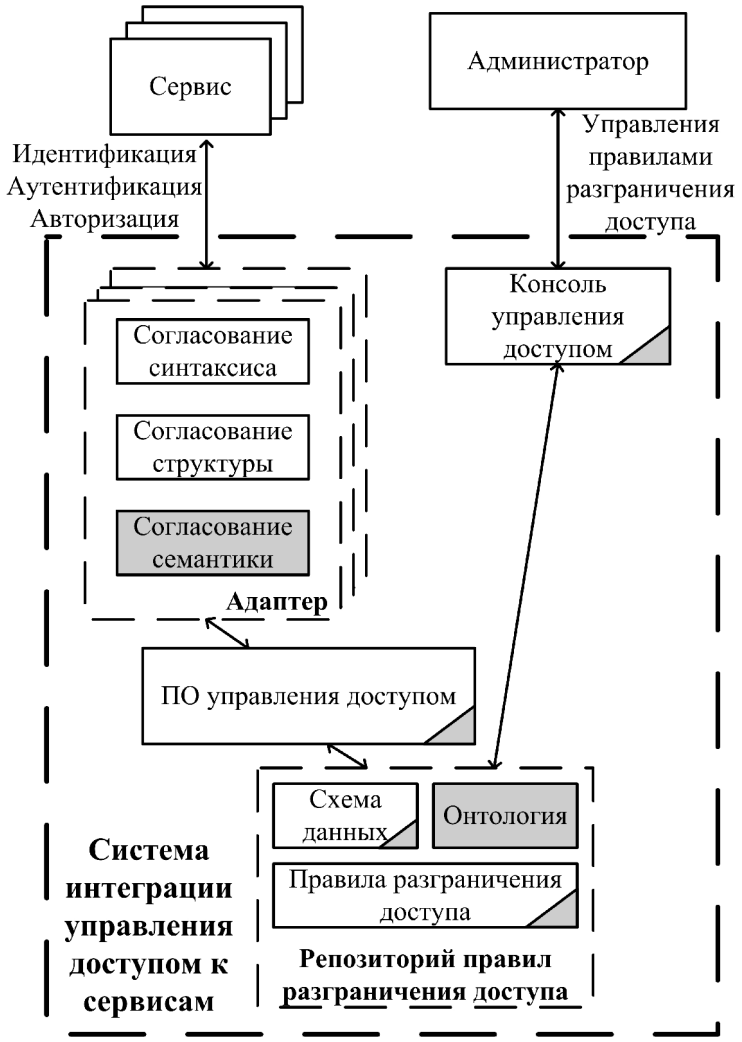

Рис. 2. Прототип и предлагаемое решение (новые блоки закрашены, развитые отмечены уголком)

Во втором разделе предложена методика интеграции управления доступом к сервисам разных типов на основе семантического подхода. Методика заключается в выполнении следующих шагов:

1. Задать множество сервисов S, которые подлежат интеграции.
2. Задать множество моделей M, используемых для управления доступом к сервисам из множества S.
3. Задать множество репозиториев правил разграничения доступа R, которые подлежат интеграции.
4. Задать множество протоколов управления доступом P, которые используются сервисами из множества S.
5. Разработать унифицированную модель управления доступом M_0. Модель включает семантическое описание базовых понятий и операций систем управления доступом (представленное в виде онтологии) и синтаксис записи правил разграничения доступа с использованием данной семантики.
6. Определить отображение моделей управления доступом $m_i \in M$ в унифицированную модель M_0: $F: m_i \rightarrow M_0 | m_i \in M$.

7. Создать консолидированный репозиторий правил разграничения доступа R_0, использующий унифицированную модель M_0.

8. Разработать адаптеры AR, обеспечивающие перенос данных из репозиториев $r_i \in R$ в консолидированный репозиторий R_0.

9. Создать программное обеспечение управления доступом, реализующее процедуры защиты информации с использованием правил разграничения доступа в консолидированном репозитории R_0.

10. Разработать адаптеры AS протоколов управления доступом $p_i \in P$, обеспечивающие взаимодействие сервисов $s_i \in S$ с ПО управления доступом, для выполнения процедур защиты информации с использованием протокола $p_i \in P$.

11. Настроить сервисы $s_i \in S$ для взаимодействия с ПО управления доступом с помощью адаптеров $a_i \in AS$ по протоколам $p_i \in P$.

12. Разработать консоль управления правилами разграничения доступа в консолидированном репозитории R_0.

Структурная схема системы семантической интеграции управления доступом к сервисам разных типов, получаемой с помощью предлагаемой методики, показана на рис. 3.

Рис. 3. Структурная схема системы семантической интеграции управления доступом к сервисам

Особенность предлагаемого метода интеграции управления доступом к сервисам разных типов заключается в применении семантического подхода к интеграции, обеспечивающее большую интероперабельность, по сравнению с используемыми в настоящее время синтаксическим и структурным подходами. Построенная с применением данного метода система обеспечит интеграцию более широкого круга сервисов и использование большего количества методов управления доступом.

В **третьей главе** представлена разработанная система моделей управления доступом к сервисам. В соответствии с методикой интеграции управления доступом к сервисам, предложенной во второй главе, система моделей состоит из двух частей:

– Семантическая модель, описывающая базовые понятия и операции предметной области управления доступом к сервисам.

– Алгебраическая модель, определяющая синтаксис записи правил разграничения доступа.

В первом разделе представлена семантическая модель управления доступом к сервисам. Модель представлена в виде онтологии управления доступом к сервисам на основе онтологии верхнего уровня BWW.

Основные сущности разработанной онтологии управления доступом показаны на UML-диаграмме на рис. 4. В верхней части диаграммы представлены базовые понятия онтологии BWW, в нижней их сужение на предметную область управления доступом к сервисам.

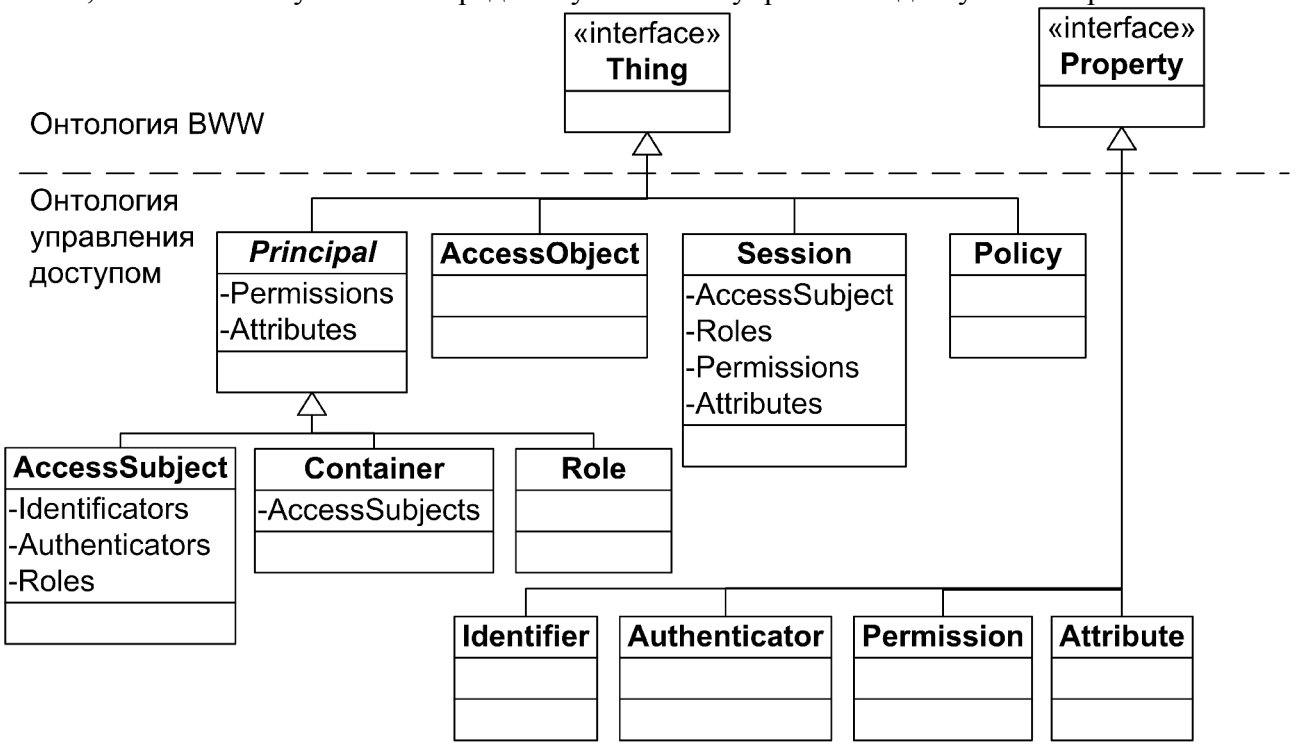

Рис. 4. Структура системы управления доступом к сервисам

Основными классами сущностей являются:

– **AccessObject** – объект, управление доступом к которому ведется.

– **Principal** – сущность, наделенная правами доступа и атрибутами. Principal – абстрактный класс, который не может иметь экземпляров. Класс имеет три наследника: **AccessSubject** (субъект доступа)**, Container** (контейнер) и **Role** (роль). Субъект доступа представляет собой персону, программу или систему, взаимодействующую с объектом доступа. Контейнеры и роли введены для упрощения процесса управления.

– **Session** – сессия, возникающая при обращении субъекта к объекту.

– **Policy** – совокупность правил разграничения доступа.

Основными свойствами являются:

– **Identifier** – уникальный признак объекта.

– **Authenticator** – аутентификатор, позволяющий подтвердить подлинность объекта.

– **Permission** – права доступа субъекта к объекту. Онтология не накладывает никаких ограничений на семантику и синтаксис прав доступа. Анализ прав и принятие решения о разрешении или запрещении доступа – это задача каждого конкретного сервиса. За счет этого обеспечивается возможность широкого применения.

– **Attribute** – атрибут, может содержать различную информацию. Как и в случае с правами доступа, на семантику и синтаксис атрибутов не накладывается никаких ограничений.

Кроме определения основных классов и атрибутов, онтология задает состояния, правила изменения состояний, события системы управления доступом. Работа содержит подробное описание онтологии.

Во втором разделе вводится алгебраическая запись правил разграничения доступа к сервисам, которая предоставляет формальный синтаксис для записи правил разграничения доступа к сервисам с использованием семантики предложенной онтологии.

Определено несколько уровней алгебраической записи с разными выразительными возможностями. Базовый уровень содержит основные компоненты, необходимые для управления доступом к сервисам. Первый уровень позволяет использовать контейнеры, второй – ролевое управление доступом, а третий обеспечивает возможность делегирования полномочий управления доступом к сервисам. Компоненты алгебраической записи более высокого уровня включают все компоненты записи уровней ниже.

Базовый уровень алгебраической записи правил разграничения доступ включает (рис. 5.):

– Множества *U, I, A, P*, *V, S (*субъектов, идентификаторов, аутентификаторов, прав доступа, атрибутов и сессий соответственно).

– *user:* $I \rightarrow U$ – функция, отображающая каждый идентификатор i_j в единственный субъект доступа $user(i_j)$.

– $K(i_u) = \left\{ i_j \middle| user(i_j) = u \right\}$ – классы эквивалентности идентификаторов i_u, задающие разбиение множества идентификаторов I на подмножества идентификаторов, принадлежащих одному субъекту u.

– *id:* $A \rightarrow I$ – функция, отображающая каждый аутентификатор a_j в единственный идентификатор $id(a_j)$.

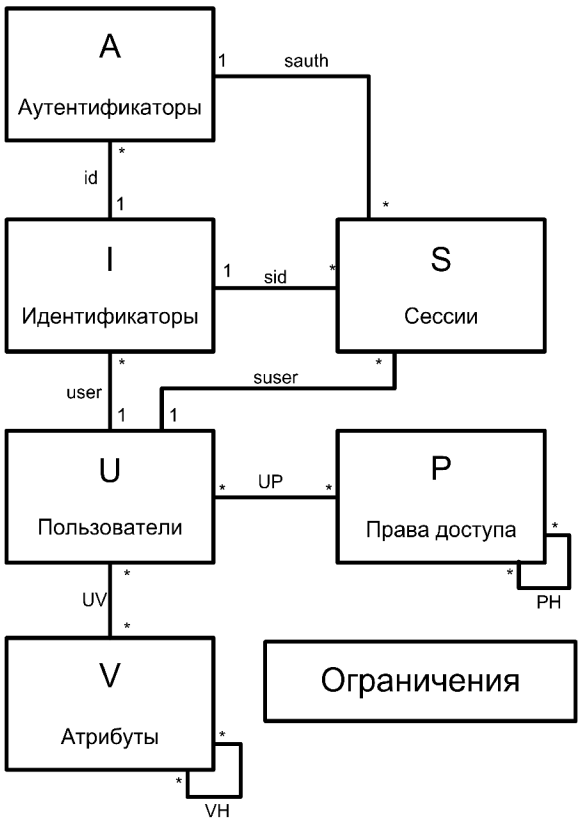

Рис. 5. Алгебраическое представление правил разграничения доступа к сервисам (базовый уровень)

– $UP \subseteq U \times P$ – отношение, задающее соответствие между субъектами и правами доступа.

– $UV \subseteq U \times V$ – отношение, задающее соответствие между субъектами и атрибутами.

– $suser: S \to U$ – функция, отображающая каждую сессию s_j в единственный субъект $suser(s_j)$.

– $sid: S \to I$ – функция, отображающая каждую сессию s_j в единственный идентификатор $sid(s_j)$.

– $sauth: S \to A$ – функция, отображающая каждую сессию s_j в единственный аутентификатор $sauth(s_j)$.

– $PH \subseteq P \times P$ – частичный порядок на множестве прав доступа P, называемый иерархией прав доступа и обозначаемый $\geq$.

– $VH \subseteq V \times V$ – частичный порядок на множестве атрибутов V, называемый иерархией атрибутов и обозначаемый $\geq$.

– $perm: U \to 2^P$ – функция, ставящая в соответствие субъекту u_j множество прав доступа $perm(u_j) \subseteq \{p | (\exists p' \geq p) \text{ и } ((u_j, p') \in UP)\}$

– $attr: U \to 2^V$ – функция, ставящая в соответствие субъекту u_j множество атрибутов $attr(u_j) \subseteq \{v | (\exists v' \geq v) \text{ и } ((u_j, v') \in UC)\}$

– Множество ограничений, определяющих, какие сочетания компонентов модели являются допустимыми. Разрешены только допустимые компоненты. ■

Предложенная система моделей используется в качестве унифицированной модели управления доступом в методике семантической интеграции, разработанной во второй главе, и служит основой для интеграции систем управления доступом к сервисам, использующих различные модели, методы и технологии.

В **четвертой главе** описано практическое применение семантической интеграции управления доступом к сервисам разных типов.

В первом разделе представлен разработанный комплекс программ по управлению доступом к сервисам. Логическая архитектура комплекса программ показана на рис. 6 и состоит из трех уровней:

– **Уровень технических служб** отвечает за взаимодействие с репозиториями правил разграничения доступа $r_i \in R$, обеспечивает создание консолидированного репозитория правил разграничения доступа R_0.

– **Уровень приложений** реализует прикладную логику управления доступом: процедуры защиты информации, управление сессиями и т.д.

– **Уровень представления** обеспечивает взаимодействие комплекса с внешним миром: сервисами, администраторами, пользователями и внешними информационными системами.

Комплекс реализован с использованием бесплатно распространяемого программного обеспечения. Консолидированный репозиторий правил разграничения доступа построен на основе LDAP-каталога Sun Java System Directory Server. Адаптеры протоколов идентификации реализованы с использованием ПО FreeRADIUS, OpenSSO, Samba. Система управления построена на основе Sun Java System Delegated Administrator, функциональность которого расширена для возможности управления доступом к сервисам разных типов. Система управления предоставляет два типа интерфейса: Web и командную строку. Распределение полномочий между администраторами реализовано с помощью делегирования на двух уровнях: администратор с полным доступом и администратор организации. Комплекс работает под управлением ОС Solaris. Надежность работы комплекса обеспечивается с помощью структурного резервирования.

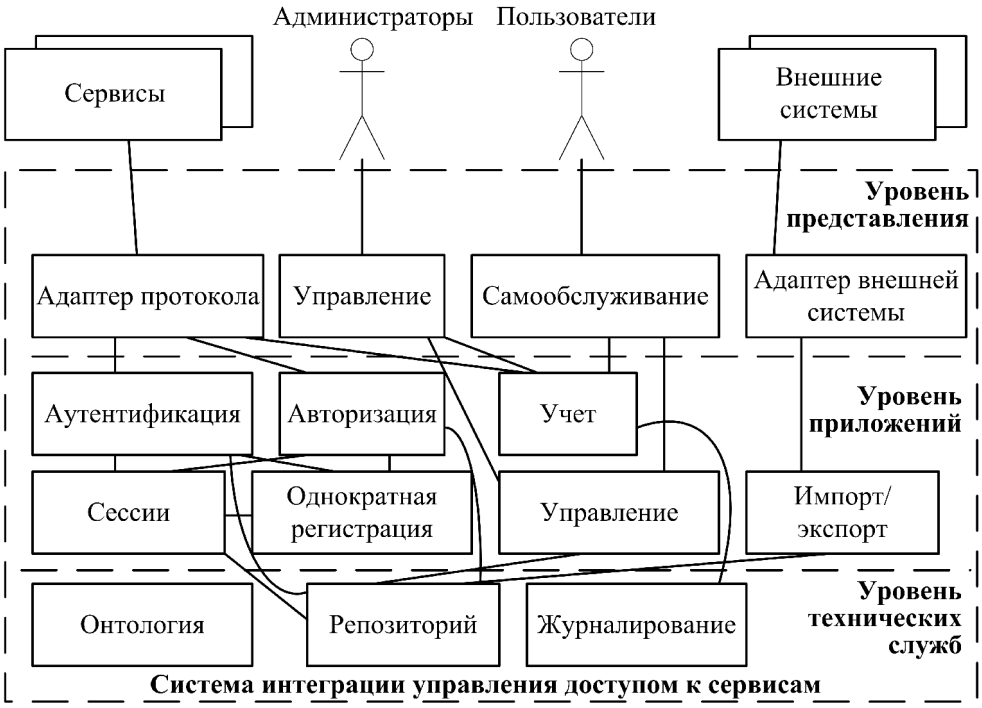

Рис. 6. Архитектура комплекса программ по управлению доступом к сервисам

Во втором разделе описано применение разработанной методики и комплекса программ для интеграции управления доступом к сервисам корпоративной сети Пермского Научного центра Уральского отделения Российской Академии наук (ПНЦ), которая объединяет четыре академических института и Президиум.

Комплекс программ применяется для управления доступом к следующим сервисам ПНЦ:

– Шлюз доступа в Интернет, точки беспроводного доступа Wi-Fi, модемные пулы (аналоговый и ISDN) по протоколу RADIUS.

– Портал ПНЦ и система Web-отчетов статистики использования сервисов с помощью средств J2EE.

– Вычислительный кластер МВС-1000/16, почтовый и файловые серверы UNIX, система хранения документов по протоколу LDAP.

В третьем разделе проведен анализ эффективности использования семантической интеграции управления доступом к сервисам. Для этой цели был проведен ряд экспериментов с системой, внедренной в сети ПНЦ. Анализ эффективности показал, что интеграция управления доступом к сервисам разных типов на основе семантического подхода повышает удобство использования сервисов корпоративной сети и снижает затраты на управление доступом к сервисам.

Удобство использования сервисов повышается за счет единого идентификатора и пароля. Количество необходимых для работы идентификаторов сократилось с 10 (соответствует количеству сервисов, подключенных к системе управления доступом) до одного. Сокращение количества идентификаторов также привело к уменьшению количества запросов в службу поддержки по восстановлению забытых паролей и консультаций по порядку доступа к сервисам на 60%.

Проведен сравнительный анализ временных характеристик процесса управления доступом к сервисам с использование системы интегрированного управления и без нее. Результаты сравнительного анализа представлены в табл. 3.

Таблица 3.

Результаты сравнительного анализа временных затрат в ходе управления доступом к сервисам

Операция	С помощью традиционных систем управления доступом, мин.	С помощью системы интегрированного управления, мин.
Создание учетной записи	15-30	3-5
Изменение учетной записи	5-10	2-3
Удаление учетной записи	15-30	3-5
Назначение прав доступа	10-15	4-10
Изменение прав доступа	5-10	1-2

Время, сэкономленное при управлении доступом с использованием системы интегрированного управления, может составлять до 80% от обычного времени работы с применением существующих систем управления доступом за счет сокращения количества ручных операций.

Интеграция управления доступом к сервисам разных типов позволила снизить требования к администраторам за счет предоставления единой интуитивной понятной системы управления с Web-интерфейсом.

Внедрение системы семантической интеграции управления доступом позволило повысить эффективность управления доступом к сервисам за счет повышения удобства работы пользователей с сервисами, сокращения временных затрат на управление доступом и снижения требований к администраторам.

В заключении приведены основные результаты диссертационной работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Выполнено исследование подходов к управлению доступом к сервисам. Показано, что причиной низкой эффективности процесса управления доступом является многообразие методов и технологий управления доступом. Возможности существующих систем интеграции управления доступом ограниченны из-за использования синтаксического или структурного подходов к интеграции. Для расширения возможностей существующих систем предлагается применить семантическую интеграцию.
2. Предложена методика интеграции управления доступом к сервисам разных типов на основе семантического подхода. Методика обеспечивает повышение интероперабельности: значительно расширяет круг поддерживаемых сервисов и методов управления доступом.
3. Предложена онтология управления доступом к сервисам. Онтология определяет семантику базовых понятий и операций предметной области управления доступом к сервисам и служит основой для семантической интеграции механизмов управления доступом к сервисам разных типов, использующим различные модели, методы и технологии управления доступом.
4. Разработана алгебраическая запись правил разграничения доступа к сервисам, позволяющая описывать правила разграничения доступа в формальном виде с использованием разных методов управления доступом.
5. Реализован комплекс программ управления доступом на основе разработанных технологий.
6. Комплекс программ успешно применен для интеграции управления доступом к сервисам ПНЦ. Исследование эффективности использования системы показало, что интеграция управления доступом повышает удобство использования сервисов корпоративной сети, сокращает временные затраты на управление доступом и снижает требования к администраторам.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. *Созыкин А.В.* Модели и методы создания интегрированной инфраструктуры управления доступом к сервисам // Системы управления и информационные технологии, 2007, №4.1(30). - С. 191-195.

2. *Созыкин А.В., Масич Г.Ф., Бездушный А.Н., Бобров А.В., Босов А.В.*, Масич А.Г. Онтология управления доступом к сервисам // Наукоемкие технологии, №11, 2008, с.34-43.

В других изданиях

1. *Бездушный А.Н., Масич А.Г., Масич Г.Ф., Созыкин А.В., Серебряков В.А.* Интеграция сервисов управления объектами сети с информационными ресурсами посредством службы каталогов LDAP // Труды Всероссийской научной конференции “Научный сервис в сети Интернет” (23-28 сентября 2002г., Новороссийск). – М.: Изд-во МГУ, 2002. - с.119-122

2. *Алексеев А.Н., Масич А.Г., Масич Г.Ф., Созыкин А.В.* Использование метакаталогов для создания справочной системы научного института. // Тез. докл. 13 Зимней школы по механике сплошных сред, Пермь, 2003, с.15

3. *Алексеев А.Н., Масич А.Г., Масич Г.Ф., Созыкин А.В.* О некоторых аспектах разработки метакаталога для справочной системы научного института // Труды 34-й Региональной молодежной конференции «Проблемы теоретической и прикладной математики», Екатеринбург, 2003.

4. *Масич А.Г., Масич Г.Ф., Созыкин А.В.* Использование каталога LDAP для управления данными о пользователях сервисами корпоративной сети научного центра РАН // Труды 35-й Региональной молодежной конференции «Проблемы теоретической и прикладной математики», Екатеринбург, УрО РАН, 2004,- с.323-327

5. *Масич А.Г., Масич Г.Ф., Созыкин А.В.* Аспекты развития и управления в корпоративной сети Пермского научного центра УрО РАН // Тез. докл. XI конференции представителей региональных научно-образовательных сетей «RELARN-2004», Самара, 2004, - с. 51-55

6. *Созыкин А.В., Масич Г.Ф., Масич А.Г., Бездушный А.Н*. Вопросы интеграции управления идентификацией пользователей сетевых, вычислительных и информационных сервисов. // Журнал «Электронные библиотеки», том 7, выпуск 2. М.: Институт развития информационного общества, 2004.

7. *Масич А.Г., Масич Г.Ф., Созыкин А.В.* Организация распределенного каталога корпоративной сети. // Информационные управляющие системы: Сборник научных трудов ПГТУ, - Пермь, 2004. - с. 279-283

8. *Масич Г.Ф., Алексеев А.Н., Бобров А.В.*, *Созыкин А.В., Чугунов Д.П*. Использование технологии ИСИР при построении корпоративного портала // Информационные и математические технологии в науке, технике и образовании: Труды X Байкальской Всероссийской конференции «Информационные и математические технологии в науке, технике и образовании». Часть I. - Иркутск: ИСЭМ СО РАН, 2005. - С. 12-18.

9. *Созыкин А.В., Масич Г.Ф., Масич А.Г., Бобров А.В.* Архитектура консолидированного хранилища данных о пользователях и сервисах корпоративной сети. // Материалы XIII конференций представителей региональных научно-образовательных сетей «RELARN-2006». Сборник тезисов докладов – Барнаул: Изд-во АлтГТУ, 2006 – С.69-73.

10. *Масич Г.Ф., Созыкин А.В., Бобров А.В.* Модель системы управления доступом к сервисам корпоративной сети // Научный сервис в сети Интернет: технологии параллельного программирования: Труды Всероссийской научной конференции – М.: Изд-во МГУ, 2006. – С.221-223.

11. *Созыкин А.В., Масич Г.Ф.* Использование централизованного управления идентификацией пользователей в Пермском научном центре УрО РАН. // Материалы XIV конференции представителей региональных научно-образовательных сетей «RELARN-2007». Сборник тезисов докладов – Нижний Новгород, 2007 – С.42-48.

12. *Масич Г.Ф., Созыкин А.В., Бобров А.В.*. Использование системы PAM (Pluggable Authentication Modules) для реализации однократной регистрации пользователей UNIX-серверов. // Труды XIV Всероссийской научно-методической конференции Телематика'2007 – СПб.: Редакционно-издательский отдел СПбГИТМО, 2007. – С.385-387.

13. *Созыкин А.В., Масич Г.Ф., Бобров А.В.* Интеграция управления идентификацией пользователей научных сервисов // Научный сервис в сети Интернет: многоядерный компьютерный мир:15 лет РФФИ: Труды Всероссийской научной конференции (24-29 сентября 2007 г., г. Новороссийск) – М.: изд-во МГУ, 2007. - с. 323-328.

14. *Созыкин А.В. Масич Г.Ф. Бобров А.В.* Формальная модель управления доступом к сервисам // Журнал «Информационные технологии моделирования и управления» - Воронеж: изд-во "Научная книга", ISSN 1813-9744, 2007, № 7. – с. 841-849.

15. Sozykin A.V., Masich G.F. Integrated access control infrastructure for network of Perm Research Center of the UrB of RAS // International Conference: Computational and Informational Technologies in Science, Engineering and Education (CTMM-2008) Almaty, Kazakhstan, September 10 — September 14, 2008. – http://www.nsc.ru/ws/show_abstract.dhtml?en+186+13669

Личный вклад автора в работах с соавторами заключается в разработке методики семантической интеграции управления доступом к сервисам разных типов, создании онтологии управления доступом к сервисам, разработке алгебраического представления правил разграничения доступа, описания реализации предложенных технологий в виде комплекса программ.