

## СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ И ПРАВАМИ ДОСТУПА SATORI

М.В. СТЕРЖАНОВ

*Белорусский государственный университет информатики и радиоэлектроники  
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь  
accept@bk.by*

Система централизованного управления учетными записями и правами доступа – механизм, обеспечивающий синхронизацию, распространение и централизованное управление правами и учетными записями пользователей в гетерогенных информационных системах и приложениях предприятия на основе единого централизованного представления учетных данных. В работе описываются требования, архитектура, технологии реализации предлагаемой системы Satori.

*Ключевые слова:* централизованное управление доступом, управление учетными записями, корпоративное программное обеспечение.

При создании единого информационного пространства современного предприятия одной из наиболее сложных проблем является управление правами доступа к приложениям и сервисам внутрикорпоративной сети. Для управления доступом к сервисам разных типов приходится использовать несколько разных систем управления и выполнять большое число операций, что создает большую нагрузку на администраторов. Согласно исследованию, проведенному Gartner в 2010 году, управление учетными данными и правами доступа занимает первое место в первой пятерке приоритетов безопасности, в список которых входят межсетевое экранирование, предотвращение вторжений, предотвращение утечки данных и антивирусное обеспечение.

В сетях крупных организаций, с большим количеством сервисов и пользователей, многообразие технологий приводит к повышению сложности процесса управления доступом. Сервисы разных типов, использующие разные технологии управления доступом, требуют создания инфраструктуры управления: репозитория правил разграничения доступа, системы управления доступом и т.п. Большое количество сервисов разных типов приводит к большому количеству инфраструктур управления доступом, которые нужно создавать и поддерживать. Часть информации в таких инфраструктурах дублируется и требует синхронизации при изменениях.

Для упрощения процесса управления доступом необходимо выполнить интеграцию систем управления доступом к сервисам, использующим различные технологии управления доступом.

Система Satori должна удовлетворять следующим требованиям: интероперабельность (управление доступом к сервисам разных типов); масштабируемость (возможность добавления новых сервисов при их появлении); гибкость управления доступом (возможность сочетания нескольких популярных методов управления доступом); простота в использовании и администрировании.

В настоящее время распространены три подхода к интеграции информационных систем, обеспечивающие различные уровни интероперабельности [1]:

- 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.

Нами проектируется система централизованного управления учетными записями и правами доступа Satori, назначением которой является автоматизация процедуры управления доступом пользователей к ресурсам предприятия. Кроме того, система будет обеспечивать для разрабатываемого и поддерживаемого корпоративного программного обеспечения потребности в создании ролей и назначении прав пользователей, что освобождает ИТ-отдел предприятия от решения этих задач в каждом отдельном приложении.

Система Satori взаимодействует с тремя группами пользователей:

1. Сотрудники предприятия. Рядовым пользователям система Satori предоставляет портал самообслуживания, с помощью которого они могут проводить простые операции по управлению доступом к ИТ-ресурсам и настройке своего профиля.

2. Администраторы системы. Основной задачей администратора является управление пользователями и выполнение контроля корректности функционирования системы.

3. Внешние программы. Сторонние сервисы обращаются к системе Satori для управления доступом пользователей.

Архитектура комплекса Satori будет состоять из нескольких логически обособленных уровней:

- Поддержка репозитория правил разграничения доступа;
- Реализация прикладной логики управления доступом;
- Взаимодействие с внешними клиентами (сервисами, пользователями).

Планируется обеспечить поддержку работы с системой как через Web интерфейс, так и посредством командной строки.

Система Satori имеет распределенную архитектуру. Для реализации клиентской части системы используется технология ExtJS. К серверным приложениям относятся компоненты, отвечающие для обработку и переадресацию запросов к БД и внутреннюю логику. Для реализации данных компонент был выбран язык Java. В качестве СУБД планируется использовать продукт Oracle 11g.

Результатом внедрения системы Satori будет являться наличие единого имени и пароля у каждого пользователя для входа во все информационные ресурсы предприятия. Единая процедура управления правами имеет большие возможности по автоматизации процесса управления и поддержания данных в актуальном состоянии. Практическая значимость предлагаемой системы Satori заключается в повышении уровня управляемости и защищенности информационных систем предприятия, повышении производительности труда администраторов.

#### Список литературы

1. Управление учетными записями и правами доступа [Электронный ресурс]. – Режим доступа: <http://usscltd.tmweb.ru/services/22/71/?read-all=Y>. – дата доступа: 23.01.2014.

2. *Созыкин А.В.* Семантическая интеграция управления доступом к сервисам : дис... к-та тех. наук. – Пермь, 2008. – 107 с.