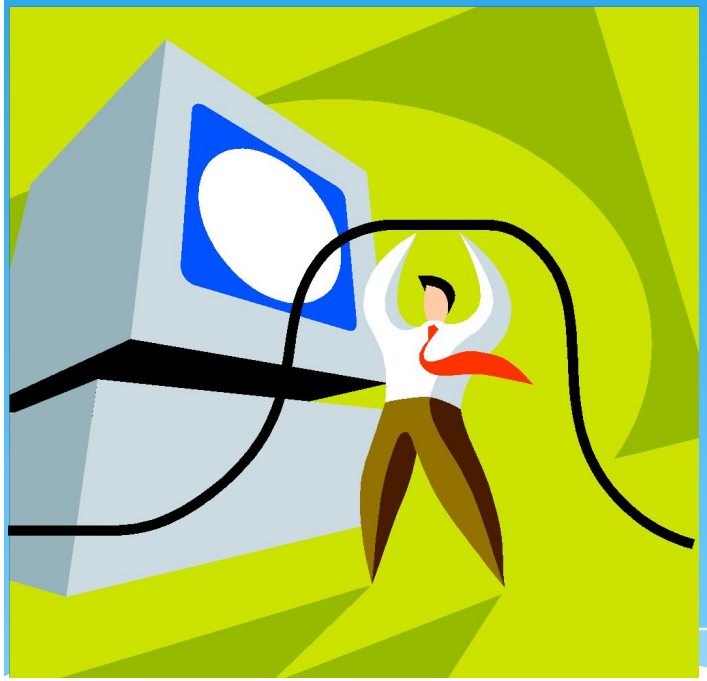
# Как все было плохо, но стало хорошо: опыт успеха



Автоматизация задачи управления правами пользователей SAP с помощью Microsoft FIM

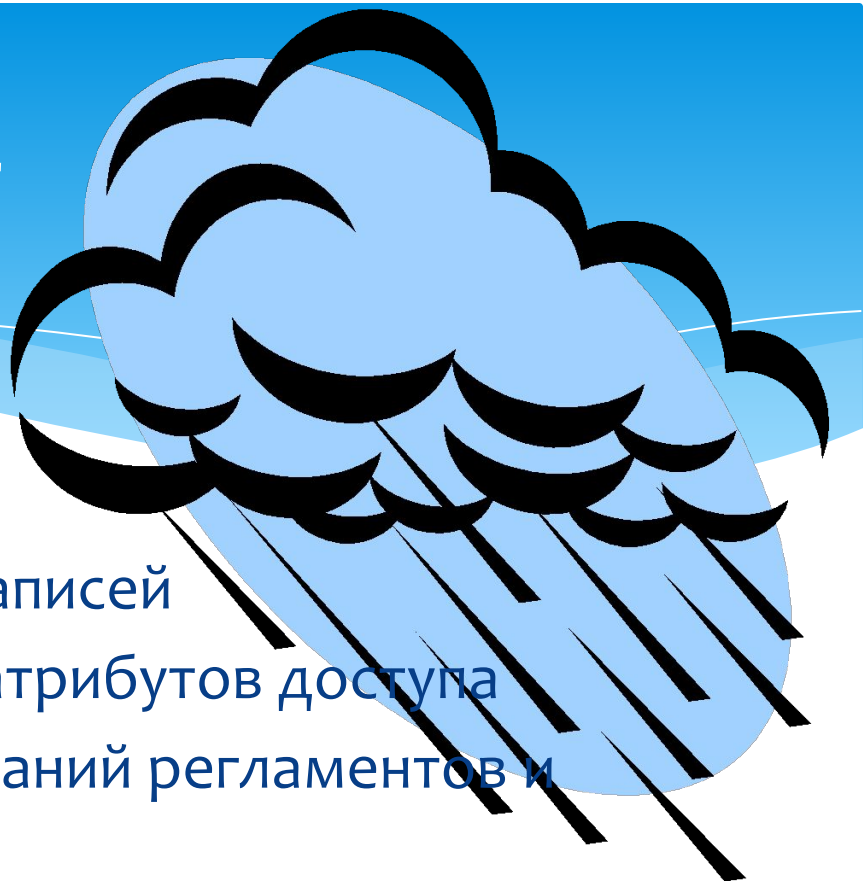
АйТи

# О чем речь


Прием на работу
Отпуск
Команди-
ровка
Больнич-
ный
Измене-
ние
данных
Перевод
Увольнение

# Как оно обычно бывает…

# … и чем бесит



- Рутина по заведению учетных записей
- Рутина по ручному изменению атрибутов доступа
- Тенденция к нарушению требований регламентов и правил
- Длительность процедур и объем документооборота
- Влияние человеческого фактора
- Потери рабочего времени

# А можно лучше?

ПРИКАЗ

принять на работу

Сотрудник HR

Ввод данных

Кадровая система

Новый работник

Уведомление

Регистрация и наделение полномочиями

AD

ERP

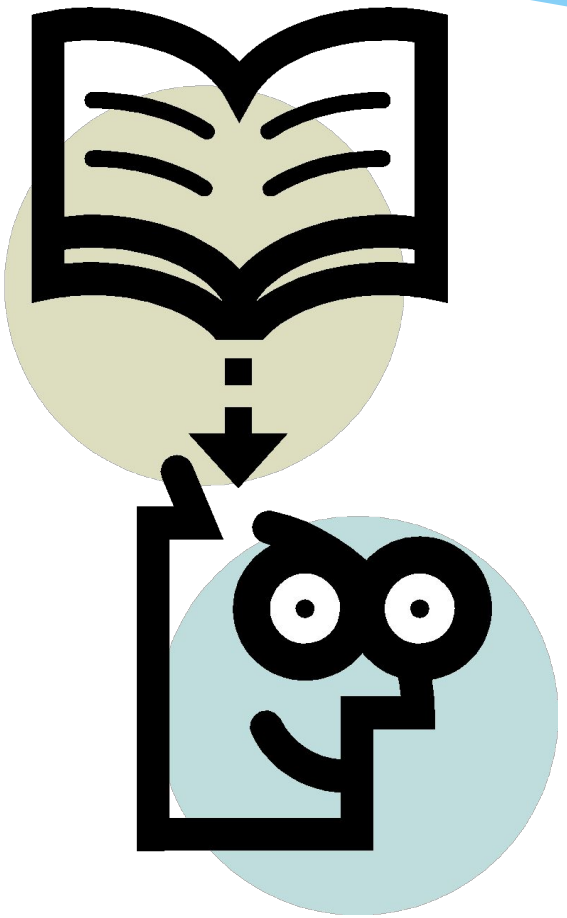
Почта

СКУД

УПАТС

Отчет

# Можно!

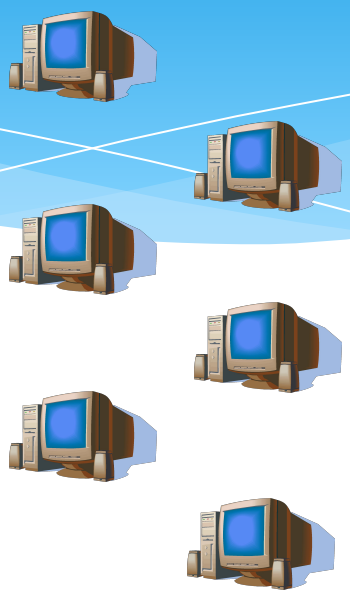


Мы хотим рассказать об опыте реализации проекта построения СУИИ в одной компании (крупный ритейл, много магазинов, 2600 пользователей)

# Было

SAP

AD



- Система управления персоналом SAP HR
- Система управления бизнесом

- Включение в группы безопасности в зависимости от должности
- Управление доступом к ERP-порталу для сотрудников

# Проблемы ИТ-директора

* Недовольство бизнес-подразделений простоями новых сотрудников
* Недовольство бизнес-подразделений и сотрудников ошибками в данных о пользователях
* Недовольство бизнес-подразделений задержками при внесении изменений
* «Сиротские» учетные записи
* Отсутствие четких регламентов обработки учетных записей пользователей
* Высокие административные издержки

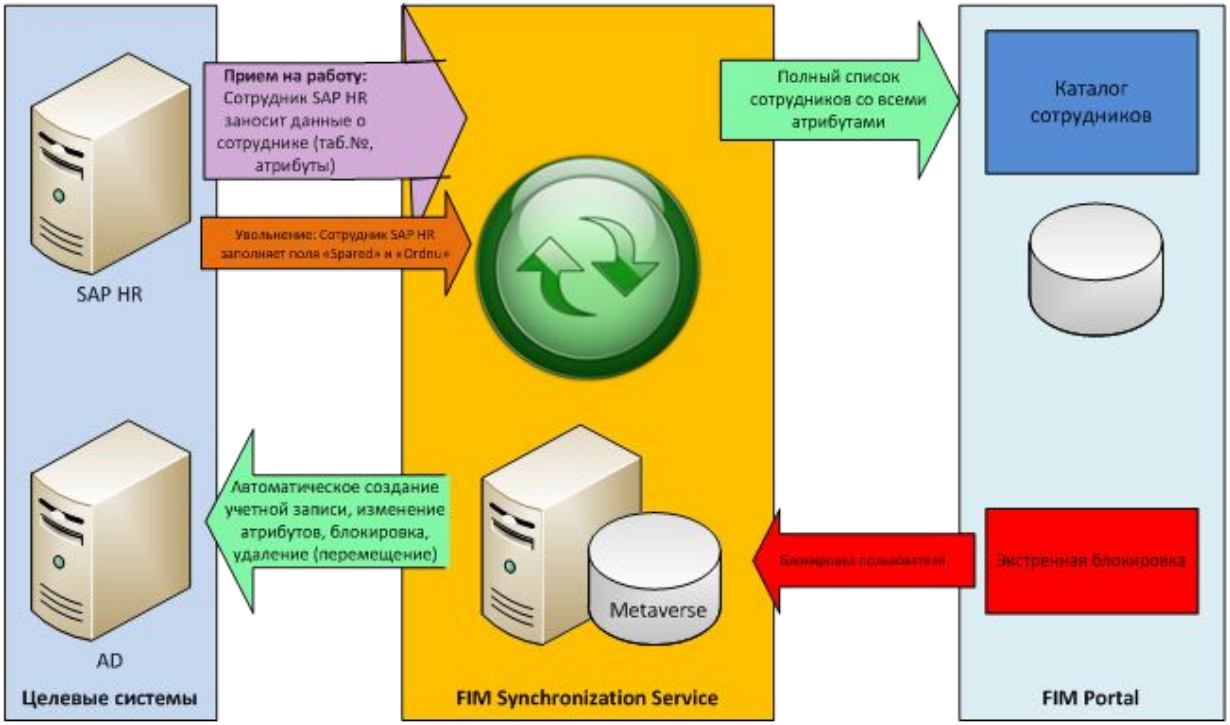
# Постановка задачи

* Автоматизация процессов управления учетными записями пользователей
* Централизованное управление доступом
* Синхронизация данных о пользователях между SAP и AD
* Назначение ролей пользователей на основании должностей
* Журналирование
* Масштабируемость

# Сделали

* Анализ бизнес-процессов
* Выработка регламентов создания, удаления (блокирования) и модификации учетных записей в связанных источниках данных применительно к СУИИ
* Внедрение программного комплекса на базе
  - Windows Server 2008 Standard/Enterprise Edition - ОС, в среде которой выполняются службы FIM
  - Microsoft SQL Server 2008, Standard или Enterprise Edition – служебные базы данных FIM
  - Windows Sharepoint Services 3.0.
  - Microsoft Forefront Identity Manager 2010 - сервер FIM
  - .Net Framework 3.0.

# Как это устроено: схема



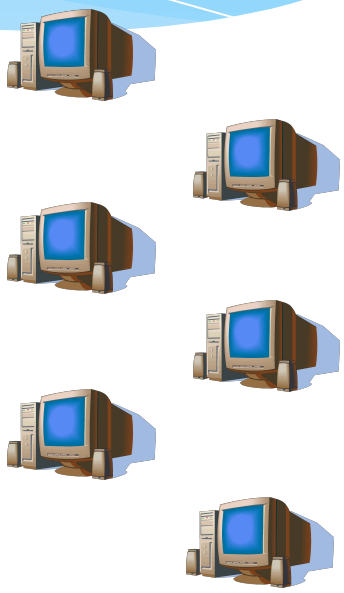
# Ряд особенностей

* Формализованные правила формирования учетных записей пользователей
* Формализованные таблицы синхронизации атрибутов данных
* Первичное связывание: загрузка уже имеющихся учетных записей сотрудников в SAP HR в базу данных СУИИ с последующим сопоставлением и проверкой соответствия атрибутов учетных записей
* Формализация ролевая матрица доступа

# Стало

SAP

AD



**Автоматизированные сценарии функционирования:**

* **Прием нового сотрудника на работу**
* **Изменение атрибутов учетной записи**
* **Увольнение сотрудника**

**Сценарии функционирования СУИИ с участием пользователей:**

* **Экстренная (ручная) блокировка доступа**
* **Отмена блокировки доступа**
* **Получение отчетности**

# Админ в отпуске вторую неделю????

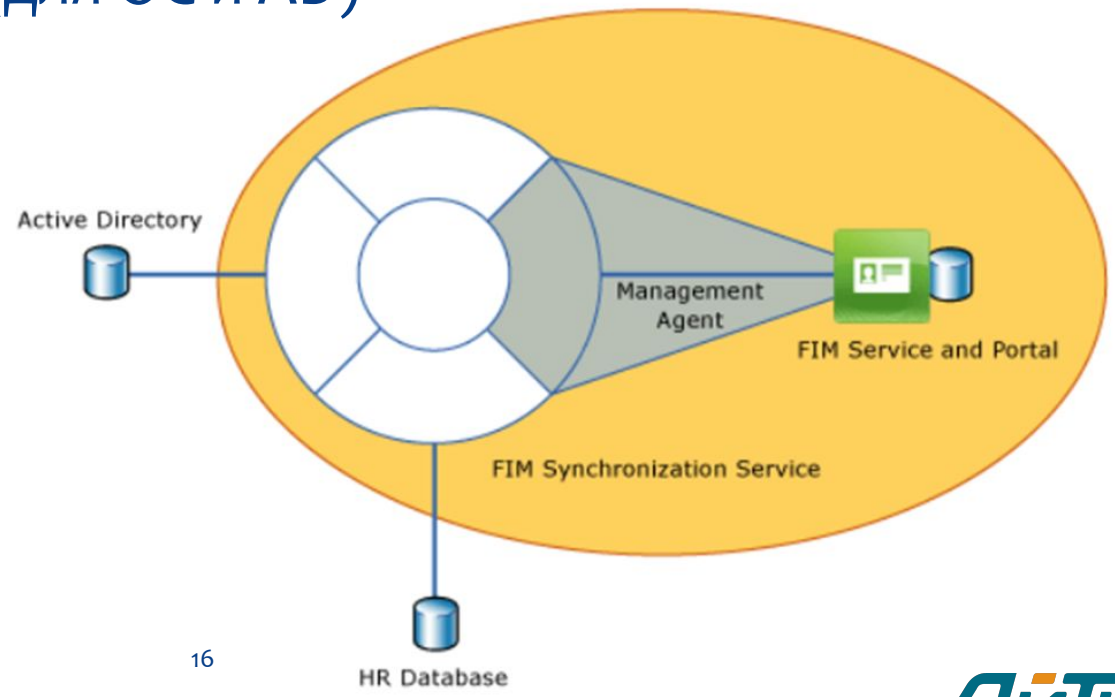
* Автоматизированы основные процессы управления УЗ в ключевых приложениях
* Минимизировано влияние «человеческого фактора»
* Внедрены формальные правила управления УЗ
* Достоверная отчетность
* Опробован подход и заложен базис под дальнейшую автоматизацию

# Об опыте эксплуатации

* Налицо экономия трудозатрат (создание/удаление учетных записей, восстановление паролей)
* Нет ошибок в данных
* За полгода эксплуатации сбоев нет
* Принято решение о дальнейшем развитии проекта
* Тиражирование в регионы

# Почему именно FIM

* Дешевое лицензирование
* Отлично работает
* «Родная» технология (для ОС и AD)
* Гибкость интеграции



# Возможности по интеграции

| Тип систем | Примеры |
|---|---|
| Сетевые операционные системы и службы каталогов | Active Directory<br>Active Directory Application Mode<br>Microsoft Windows NT<br>IBM Tivoli Directory Server<br>Novell eDirectory<br>SunONE/iPlanet Directory<br>OpenLDAP |
| Почтовые системы | Lotus Notes и Domino<br>Microsoft Exchange 5.5, 2000, 2003 и 2007 |
| Мейнфреймы | IBM Resource Access Control Facility<br>Computer Associates eTrust ACF2<br>Computer Associates eTrust Top Secret |
| Прикладные системы | SAP<br>PeopleSoft<br>ERP<br>Системы, использующие XML и DSML |
| Базы данных | Microsoft SQL Server<br>Oracle, Informix<br>dBase<br>IBM DB2 |
| Системы, основанные на доступе к файлам | DSMLv2<br>LDIF<br>CSV<br>Файлы с разделителем<br>Файлы с фиксированным размером полей<br>Файлы, содержащие пары атрибут-значение. |

Стандартная поставка FIM содержит обширный набор управляющих агентов для различных систем (хранилищ данных)

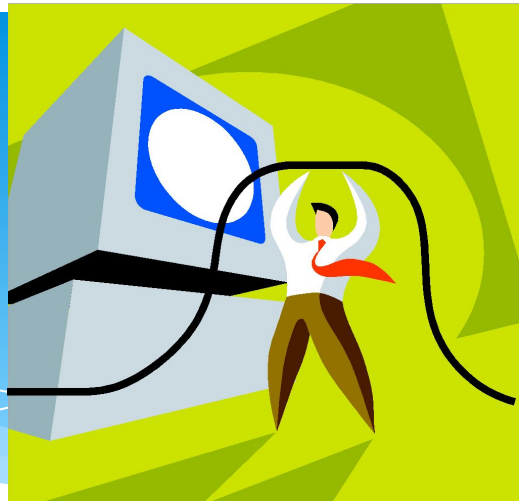
# А что, если?..

* Доверенный источник данных
* Регламенты управления учетными записями
* Нормализация кадровой базы
* Первичное связывание
* Правила именования
* Матрица ролевого доступа

# А вот это – попробуйте!

* Обследование
* Бизнес-процессы
* Макет (пилот) на Вашем ландшафте
* Затраты ~1000 тыс. руб. (без лицензий)
* Принятие решения о целесообразности развития

# Резюмируем



* IdM на базе Microsoft FIM успешно работает с SAP
* Автоматизированы основные операции управления УЗ
* Наведен порядок с имеющимися учетными записями
* Решены отдельные задачи ИБ
* Оптимальная цена «старта»

# Спасибо за внимание!

**Бежан Александр Валерьевич**

Директор по развитию бизнеса Microsoft компании АйТи

E-mail: ABezhan@it.ru

**Компания АйТи**

115280, г. Москва, ул. Ленинская Слобода, д. 19, стр. 6, (БЦ «Омега-Плаза»)

Тел.: +7 (495) 974-79-79, 974-79-80

Факс: +7 (495) 974-79-90