

# Централизованное управление правами доступа – от целей проекта до его реализации

**Евгений Акимов**

*Заместитель директора*

*Центра Информационной Безопасности*

*eakimov@jet.su*

*Инфосистемы Джет*

*\**

# Содержание

- Центр информационной безопасности Джет
- Цели IdM проекта
  - Управление доступом - большая проблема больших компаний
- Решение Джет
  - Консалтинг по разработке модели доступа и процессов его предоставления
  - Автоматизация и схема работы
- Инициация IdM проекта

- **Центр информационной безопасности Джет**
- Цели IdM проекта
  - Управление доступом - большая проблема больших компаний
- Решение Джет
  - Консалтинг по разработке модели доступа и процессов его предоставления
  - Автоматизация и схема работы
- Инициация IdM проекта

# Центр Информационной Безопасности



Крупнейшее подразделение по ИБ  
среди ИТ интеграторов  
> 130 специалистов  
> 350 проектов за последние 2 года

Отдел консалтинга  
> 20 специалистов  
> 40 проектов

Отдел проектирования  
> 15 специалистов  
> 200 проектов

Отдел сервиса  
> 20  
специалистов  
> 50 контрактов

Группа IdM  
проектов  
> 10 специалистов  
3 крупнейших  
проекта

Группа  
управления  
проектами  
> 10 проджектов

Отдел  
«Дозоров»  
> 300 инсталляций

- *Комплект лицензий (Гостехкомиссии России, ФАПСИ, ФСБ) дает Компании право на выполнение работ по защите информации, в том числе содержащей сведения, составляющие государственную тайну.*

# География проектов ЦИБ



# Заказчики

**МИНИСТЕРСТВА и ВЕДОМСТВА**  
Центральный Банк РФ (более 20 регионов)

ГУВД Москвы  
МВД Азербайджана  
Московское Казначейство...

## БАНКИ

Русский Стандарт  
Сбербанк  
ВнешТоргБанк  
АбсолютБанк  
УРСАБанк  
Росбанк  
СКББанк  
УВТБ  
... всего более 50

## ТЭК и ПРОМЫШЛЕННОСТЬ

Мосэнерго  
Газпром  
ТНК-BP  
Лукойл  
Тенгиз-Шевройл  
Русский Алюминий  
Норникель  
Северсталь...

## ОПЕРАТОРЫ СВЯЗИ

Билайн (Россия и СНГ)

МТС (60 городов)  
Казхотелеком  
МГТС  
Мегафон  
МТТ  
Комкор  
МТУ-Информ  
Совинтел...

## ЗАРУБЕЖНЫЕ КОМПАНИИ

Reebok  
Sony  
ГлобалСтар  
GlobalOne  
АскариБанк...



Обеспечение

Сопровождение,  
стаффинг, аутсорсинг

Обследование,  
аудит, оценка рисков

Управление процессом  
Доступа IdM

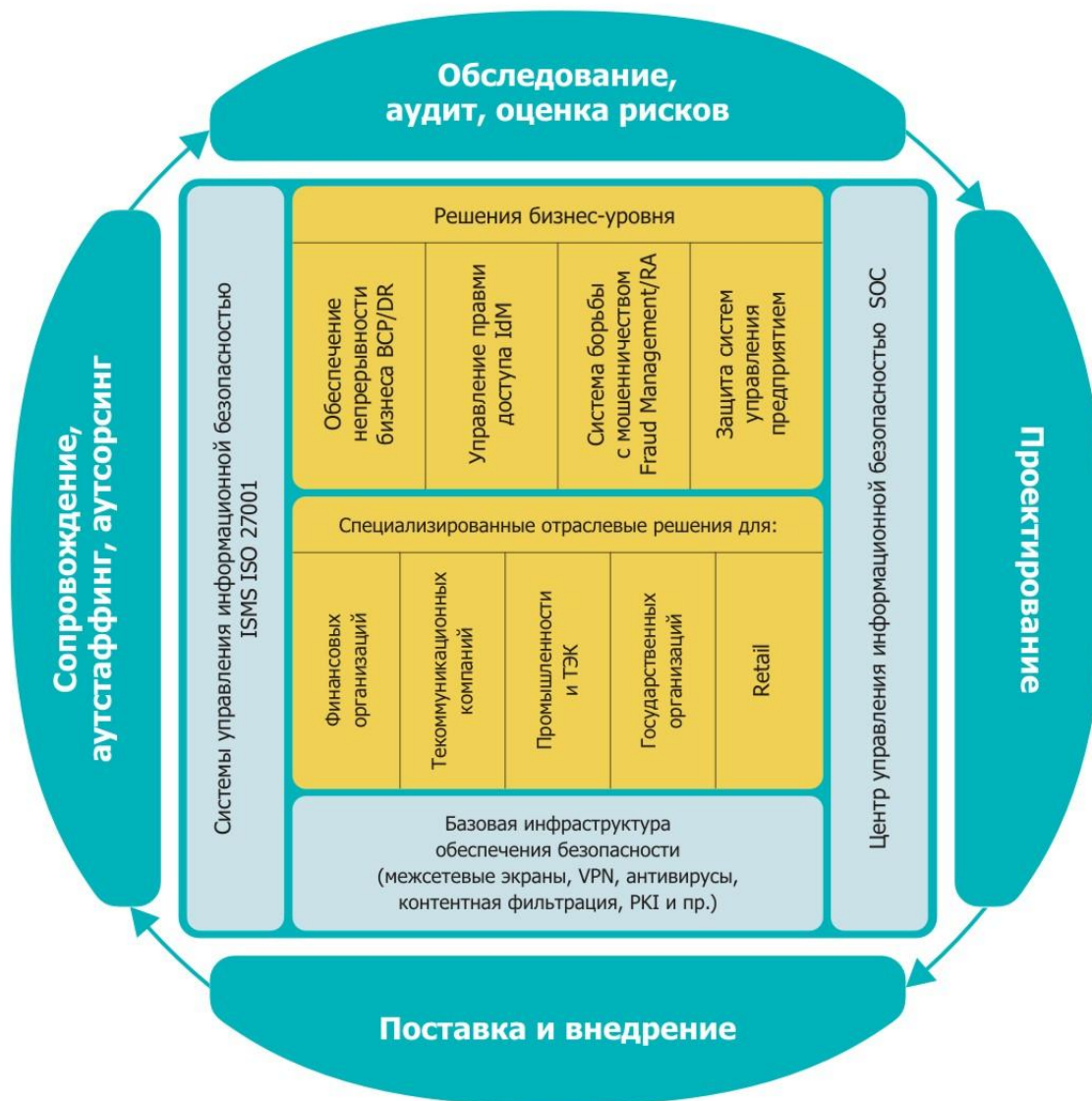
Система борьбы  
с мошенничеством  
Fraud Management

Проектирование

внедрение  
предприятия

Поставка и внедрение

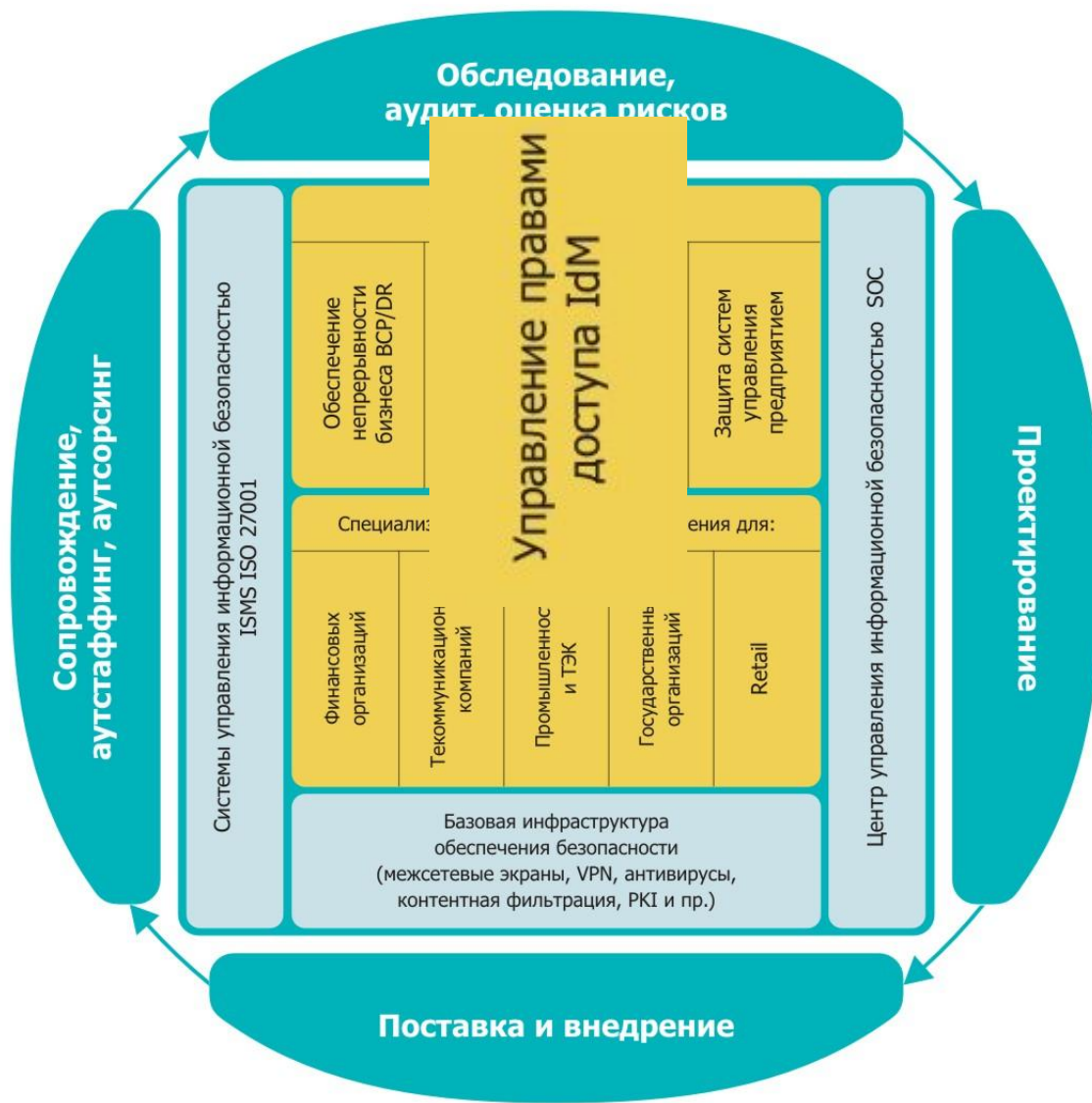
# Спектр решений ЦИБ Джет





- Центр информационной безопасности Джет
- **Цели IdM проекта**
  - Управление доступом - большая проблема больших компаний
- Решение Джет
  - Консалтинг по разработке модели доступа и процессов его предоставления
  - Автоматизация и схема работы
- Инициация IdM проекта

# Спектр решений ЦИБ Джет



# «Традиционное» управление доступом



Ошибки

запрос

Изучение  
роли и  
правил  
доступа

Создание/  
изменение  
учетной  
записи

Отложенные  
запросы

Сложный  
аудит

Утверждение  
начальством

Передача в  
ИТ отдел

Много  
запросов

Утверждение  
администратором  
ресурса

Неполная  
информация



## Если организация не большая...

- Заявки не частые
- ИТ систем мало
- Пользователей сотни
- Принцип доступа – «всем все, а для бухгалтерии – еще и свой файловый сервер»



**...то серьезных проблем нет**

# Но в крупной организации

- Непонятно кому к чему нужен доступ
  - Либо много доступа
  - Либо недостаточно
- «Бумажные» заявки идут долго (и теряются)
  - Задержки в полноценной работе
  - Высокие трудозатраты
- Инциденты очень сложно расследовать
  - Трудоемко
  - А иногда и невозможно



# Сложные, но нужные вопросы



Клиенты



Сотрудники



Партнеры



Web-сервисы

~~Кто к чему имеет доступ?~~

~~Как внедрять новые сервисы?~~

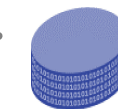
~~Как создавать отчеты по правам?~~

~~Как проводить аудит?~~

~~Как всем этим управлять?~~



Каталоги



Базы данных



Приложения



Унаследованные системы

## Проблемы и последствия

- Ущерб от несанкционированного доступа к информации
- Ущерб от не расследованных инцидентов
- Затраты на администрирование
- Потери от простоя пользователей
- Потери от неполноценной работы пользователей
- Затраты на «мертвые» лицензии



- Центр информационной безопасности Джет
- Цели IdM проекта
  - Управление доступом - большая проблема больших компаний
- **Решение Джет**
  - Консалтинг по разработке модели доступа и процессов его предоставления
  - Автоматизация и схема работы
- Инициация IdM проекта



# Решение Джет

Вместо раздельного ведения учетных записей в ИТ системах – централизованное управление правами доступа



# Содержание

- Центр информационной безопасности Джет
- Цели IdM проекта
  - Управление доступом - большая проблема больших компаний
- **Решение Джет**
  - **Консалтинг по разработке модели доступа и процессов его предоставления**
  - Автоматизация и схема работы
- Инициация IdM проекта

# От «матричного» доступа...

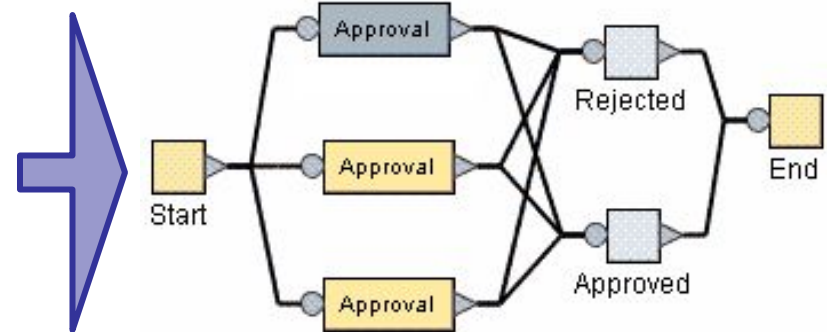
Подр.	Персона	e-mail	Файл сервер 1	ERP	Web	CRM	Файл сервер 2	System Z
Фин департамент	Иванов	+	+	+	+	-	-	+
	Сидоров	+	+	-	+	-	-	-
Логистика	Петров	+	-	+	+	-	+	-
	Кузнецов	+	-	-	+	+	+	-
	Иванов 2	+	-	-	+	-	+	-
***		***	***	***	***	***	***	***
10 000-й		+	-	-	-	-	+	-

# ... к ролевой модели

Подр.	Роль	e-mail	Файл сервер 1	ERP	Web	CRM	Файл сервер 2	System Z
Фин департамент	Экономист	+	+	+	+	-	-	+
	Бухгалтер	+	+	-	+	-	-	-
Логистика	Нач. отдела	+	-	+	+	-	+	-
	Специалист 1	+	-	-	+	+	+	-
	Специалист 2	+	-	-	+	-	+	-
***		***	***	***	***	***	***	***
Практикант		+	-	-	-	-	+	-

# Консалтинг – процессы согласования

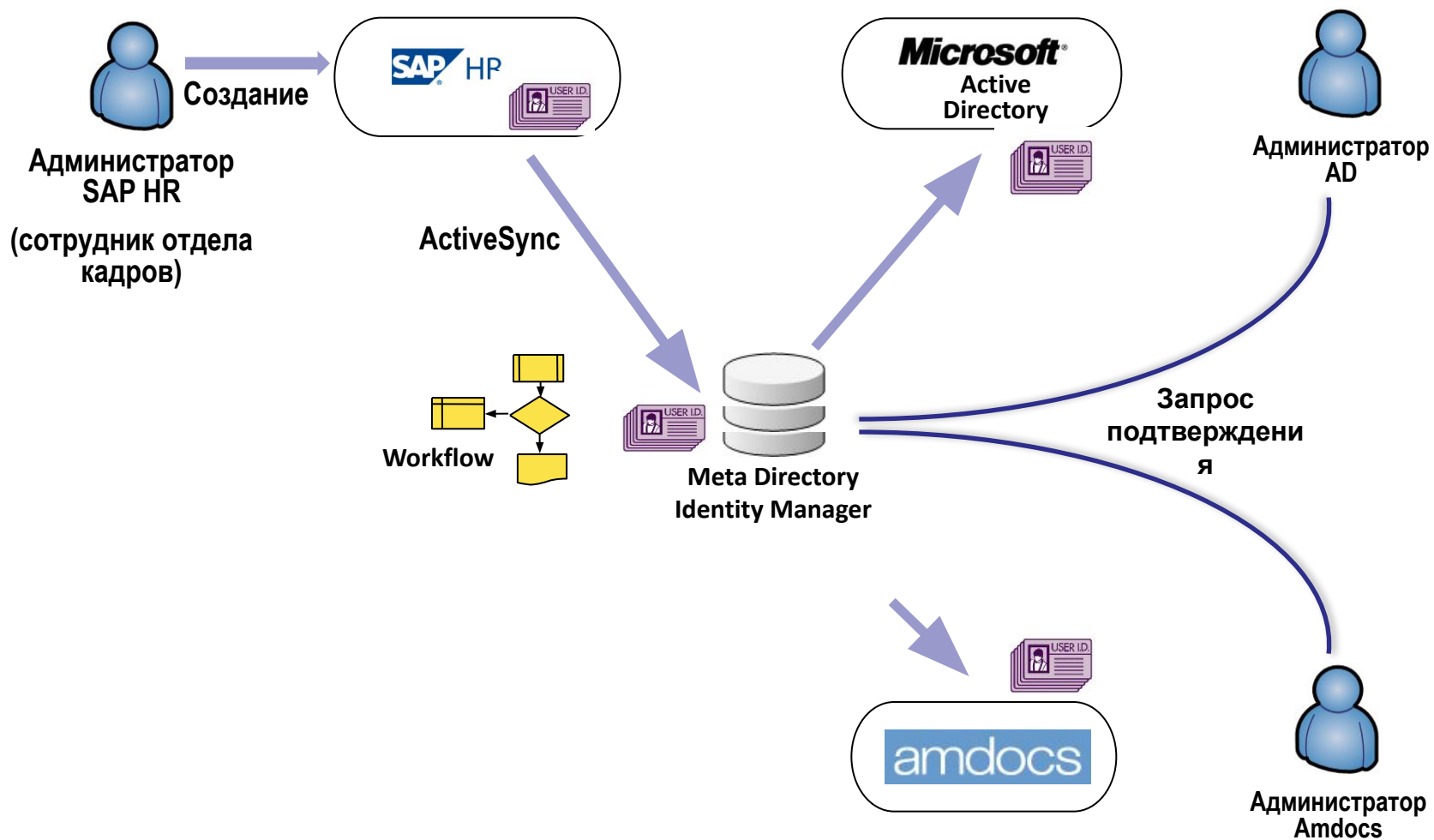
- На основе обследования организационной структуры



# Содержание

- Центр информационной безопасности Джет
- Цели IdM проекта
  - Управление доступом - большая проблема больших компаний
- **Решение Джет**
  - Консалтинг по разработке модели доступа и процессов его предоставления
  - **Автоматизация и схема работы**
- Инициация IdM проекта

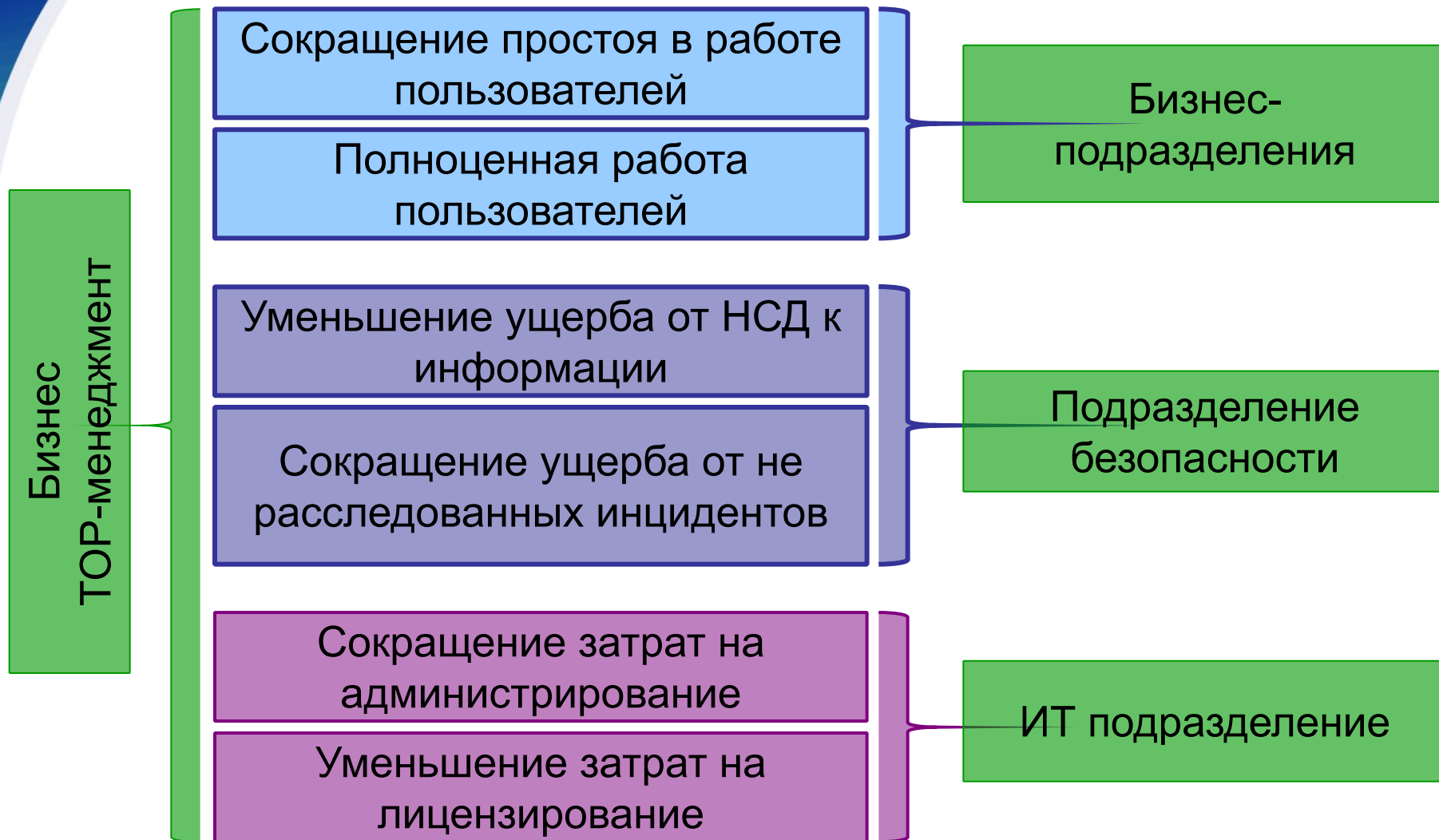
# Схема работы IdM системы



- Центр информационной безопасности Джет
- Цели IdM проекта
  - Управление доступом - большая проблема больших компаний
- Решение Джет
  - Консалтинг по разработке модели доступа и процессов его предоставления
  - Автоматизация и схема работы
- **Инициация IdM проекта**



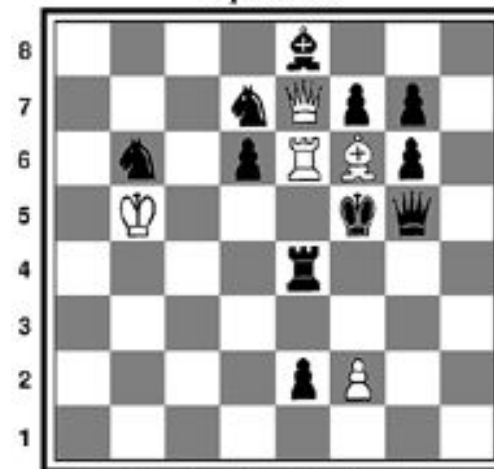
# Цели и заинтересованные подразделения



# Получение поддержки

- Первоначальная инициатива
  - ИТ или
  - ИБ
- Поддержка смежного подразделения
  - ИБ или
  - ИТ
- Поддержка наиболее заинтересованных бизнес-подразделений
  - коммерческие подразделения
  - HR
- Совместный выход на TOP-менеджмент

Задание № 12Т.  
Кооперативный мат в 2 хода;  
4 решения



Белые: Кр**f5**, Ф**e7**, Л**e6**, С**f6**, н.  
f**2** (5).  
Черные: Кр**f5**, Ф**g5**, Л**e4**, С**e8**,  
К**b6**, К**d7**, пп. d**6**, e**2**, f**7**, g**6**, g**7** (11).

# ROI - аргумент для бизнеса

- ИТ составляющая
  - Производительность help-desk
  - Затраты на лицензирование
  - Эффективность управления учетными записями
- Бизнес составляющая
  - Сокращение времени простоя
  - Трудоемкость согласования
  - Затраты на внешний аудит
  - Юридические взыскания
- ИБ составляющая
  - Снижение рисков/ущерба НСД
  - Затраты на внутренний аудит

36	ИТОГО бизнес-эффект за 3 года	\$1 336 924,42
37	Стоимость решения Identity Management	
38	1 Стоимость аппаратного обеспечения	\$55 000,00
39	2 Стоимость ПО IdM	\$520 000,00
40	Количество сотрудников организации, имеющих доступ к ИТ	6 000
41	Количество типов коннекторов к целевым системам	2
42	3 Работы по проектированию и установке	\$600 000,00
43	4 Поддержка (% стоимости ПО)	
44	5 Администрирование IdM	
45	ИТОГО стоимость решения IdM	\$1 181 002,00
46	Поток наличности (Cash flow)	-\$1 175 000,00
47	Прибыль накопленным итогом	-\$1 175 000,00
48		
49	Срок окупаемости (Break-even) (лет)	3,6
50	ROI (Return on investments)	41%

# Примеры проектов: ТНК-ВР, УралСиб и ЯмбургГазДобыча

- 22 000 пользователей
  - Управляемые системы:
    - SAP HR
    - SAP R3
    - BOSS KADROVIK
    - ICS
    - Microsoft Active Directory;
    - Microsoft Exchange Server 2003;
    - Microsoft DFS
    - Парус
    - 1C
    - Hyperion
    - MI GFO
- 9 000 пользователей
  - Управляемые системы:
    - Microsoft Active Directory;
    - Novell eDirectory;
    - Lotus;
    - SAP HR
- 4 000 пользователей
  - Управляемые системы:
    - Microsoft AD;
    - Microsoft Exchange;
    - ЕИС «Кадры»;
    - SAP R/3.



# Итого

- Экспертиза Джет по ИБ
- Цель
- Решение
- Инициализация и бизнес-эффект
- Опыт Джет по IdM



# Ваши вопросы?

**Централизованное  
управление правами  
доступа – от целей проекта  
до его реализации**

***Евгений Акимов***

*Заместитель начальника*

*Центра Информационной Безопасности*

*eakimov@jet.su*



***Спасибо за внимание!***