

# Большие данные — большая ответственность.

Опыт защиты от утечек в аналитических системах

Алексей Артемов

<https://www.linkedin.com/in/aartemov/>

# Предпосылки к выступлению

Sept 16 (Reuters) [redacted] said it was investigating a cybersecurity incident after report of a network breach that forced the company to shut several internal communications and engineering systems.

On Friday, [redacted] said it had no evidence that the incident involved access to sensitive user data such as trip histories and that internal software tools that the company had taken after the hack were coming back online.

VC.ru

**[redacted] подтвердил утечку личных данных клиентов ...**

Ритейлер сообщил, что обнаружил утечку личных данных клиентов и сотрудников. Сейчас [redacted] проводит расследование и устраняет последствия атаки...

VC.ru

**[redacted] заподозрили в утечке данных: в сети ...**

[redacted] заподозрили в утечке данных: в сети распространяют информацию о продаже данных клиентов и продавцов.

3DNews

**Сервис [redacted] сообщил об утечке данных пользователей**

В заявлении компании указывается, что утечка произошла из-за недобросовестных действий одного из её сотрудников. Источник изображения: [redacted]

1 Mar 2022

**В сети появилась интерактивная карта с утекшими данными [redacted]**

На карте появились данные из [redacted] и других источников. На сайте с утечками...

# План

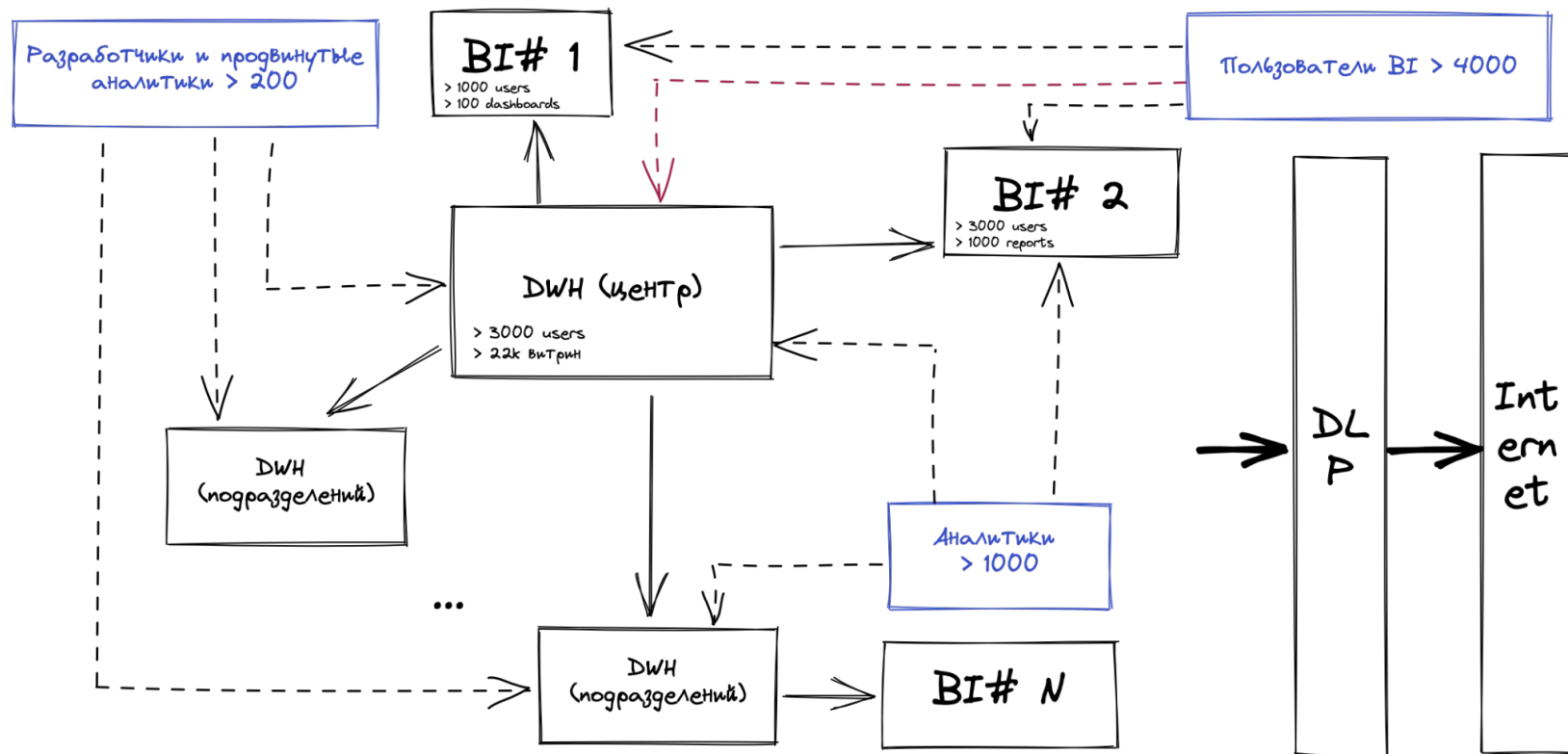
- Задача
- Исходная ситуация
- Вызовы
- Определение приоритетов
- Реализация
- Выученные уроки

# Задача

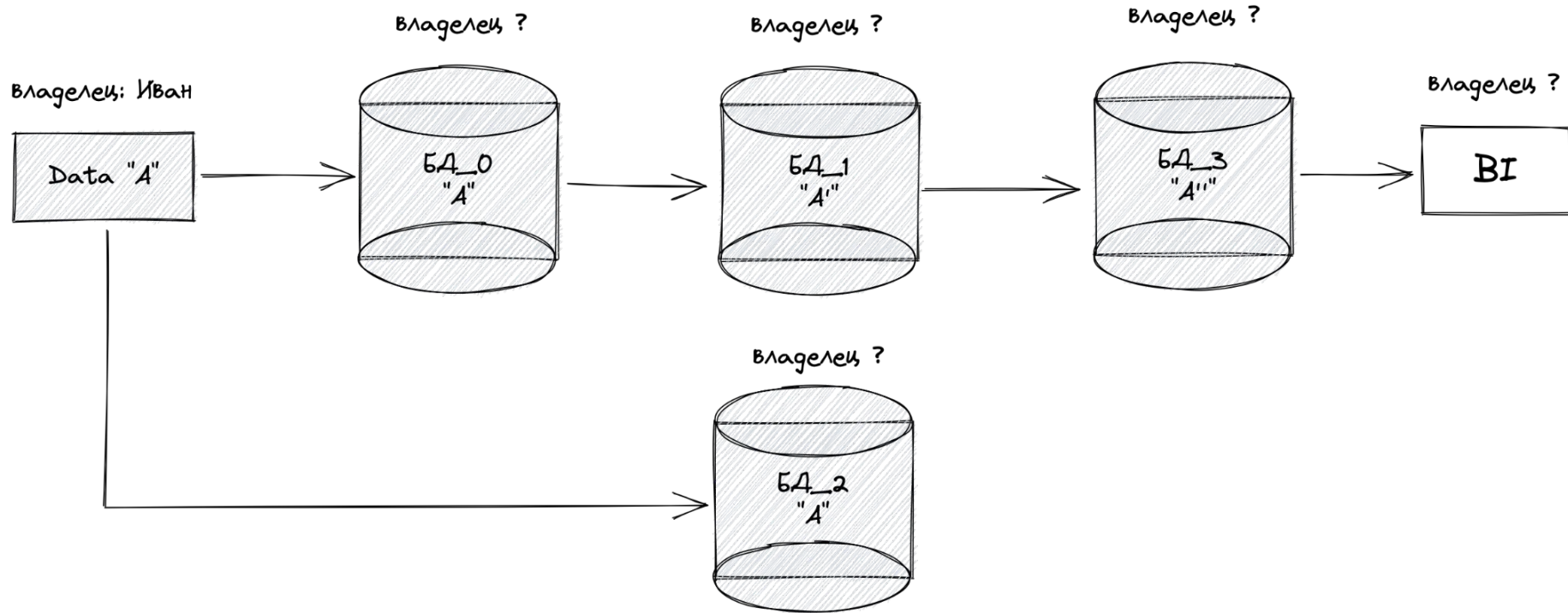
1. Необходимо было ограничить возможность неправомерной передачи данных 3м лицам
2. Не сломать работу компании
3. Сроки - ASAP



# Исходная ситуация



# Вызов 1 - “расползание” данных и ответственности



## Вызов 2 - RLS

RLS (row level security) - это здорово, но:

- а. Нужно знать к каким данным его необходимо применять
- б. Где-то вести привязку УЗ - Ключ справочника
- с. Трудозатраты на внедрение на уже существующей инфраструктуре

UserName	Country	Sales
Fred	USA	10000
Chris	USA	9500
Tom	France	9600
Fred	Spain	9200
Chris	Germany	9000

All records in table

UserName	Country	Sales
Fred	USA	10000
Fred	Spain	9200

Fred's login




UserName	Country	Sales
Chris	USA	9500
Chris	Germany	9000

Chris's login

# Вызов 3 - RBAC & ABAC

## RBAC (role based access control):

- a. Требуется регулярной актуализации
- b. Потенциально большое кол-во ролей для управления
- c. Доступ на уровне объектов системы

 Sales	 Finance	 Engineering
<input checked="" type="checkbox"/> <b>Customer Database</b>	Customer Database	Customer Database
Payroll	<input checked="" type="checkbox"/> <b>Payroll</b>	Payroll
Codebase	Codebase	<input checked="" type="checkbox"/> <b>Codebase</b>

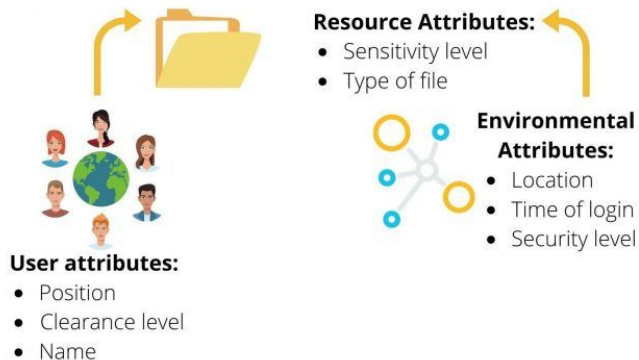


# Вызов 3 - RBAC & ABAC

## ABAC (attribute based access control):

- a. Нет повсеместной поддержки со стороны технических систем
- b. Очень гибкий подход, позволяет детально управлять доступом
- c. Может использоваться как абстракция над RBAC & RLS

### Attribute-Based Access Control



## Вызов 4 - DLP

DLP система анализирует и перехватывает трафик компании для выявления конфиденциальной информации и, при необходимости, блокировки передачи данных.

Базовый принцип работы DLP систем – это фильтрация контента при отправке за периметр организации или в облако.

# Вызов 5 разное понимание критичности данных

Персональные данные - это самое важное



# Вызов 5 разное понимание критичности данных

Забыли, что компания публичная



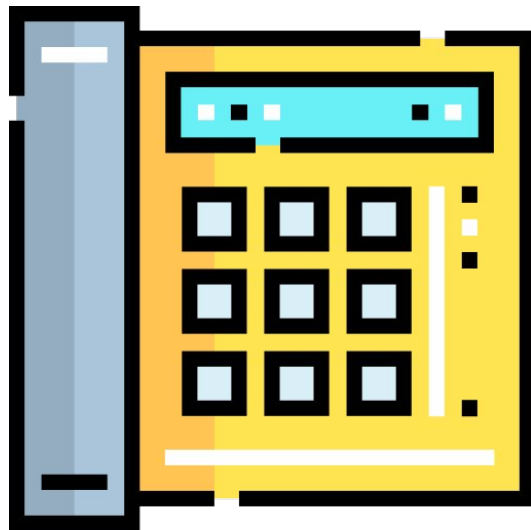
# Вызов 5 разное понимание критичности данных

А вдруг в логах найдут IP адреса или может там будут пароли



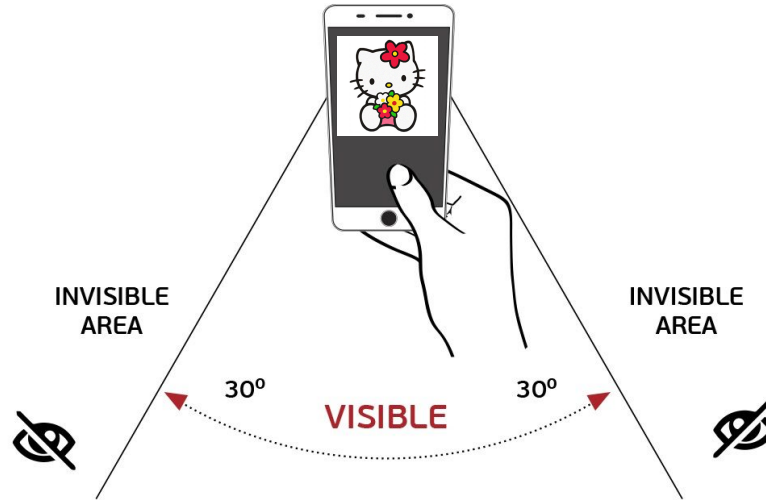
# Вызов 5 разное понимание критичности данных

Номера телефонов - это секретно



# Вызов 5 разное понимание критичности данных

Среди нас враги

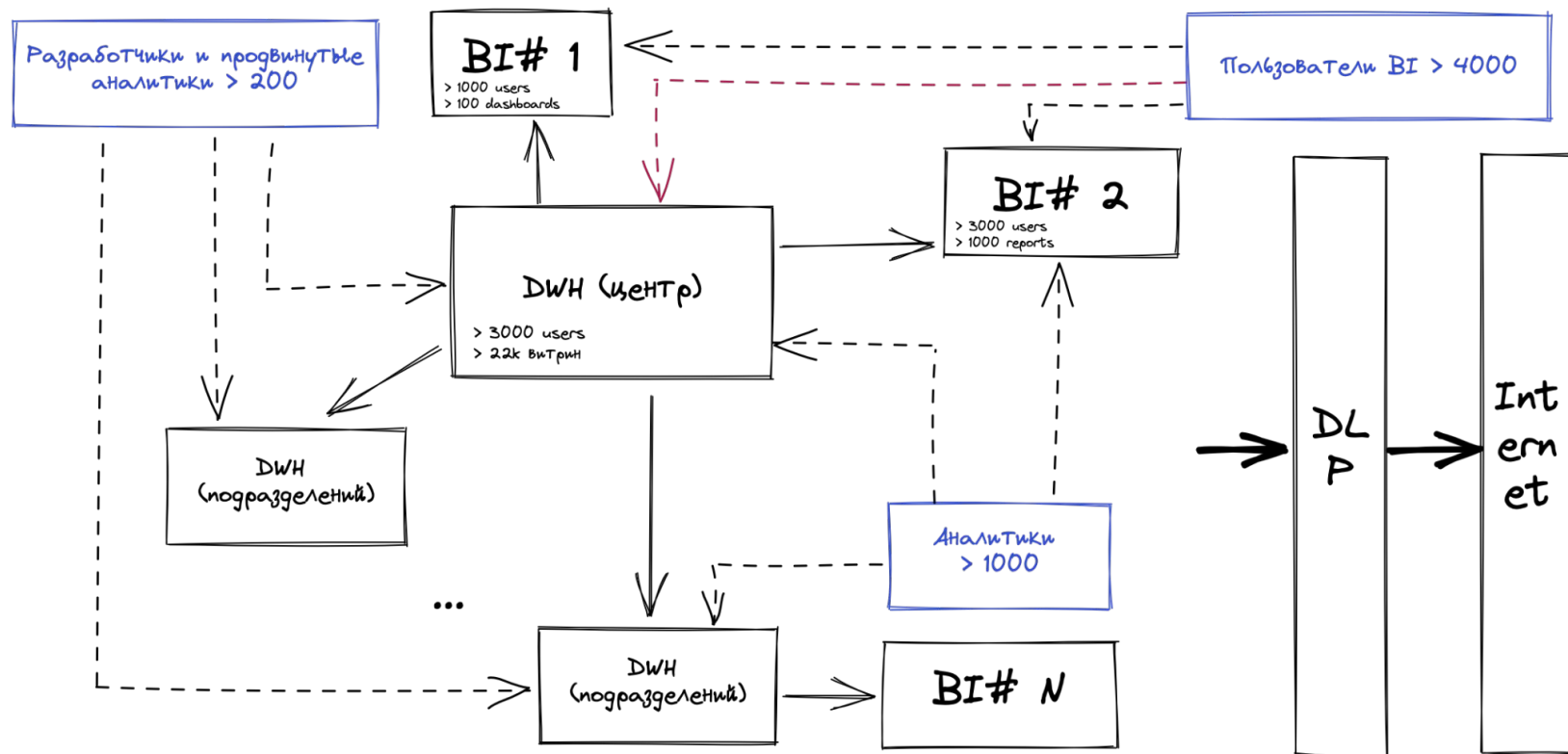


# ВЫЗОВЫ - ИТОГО

1. “расползание” данных и ответственности
2. RLS (row level security)
3. RBAC (role based access control)
4. DLP - false\positive
5. Разное понимание критичности данных



# Исходная ситуация - итогов



# Определение приоритетов

Понять какие данные защищать → список систем подлежащих защите



# Определение приоритетов

Как защищать → оценка трудозатрат



# Реализация

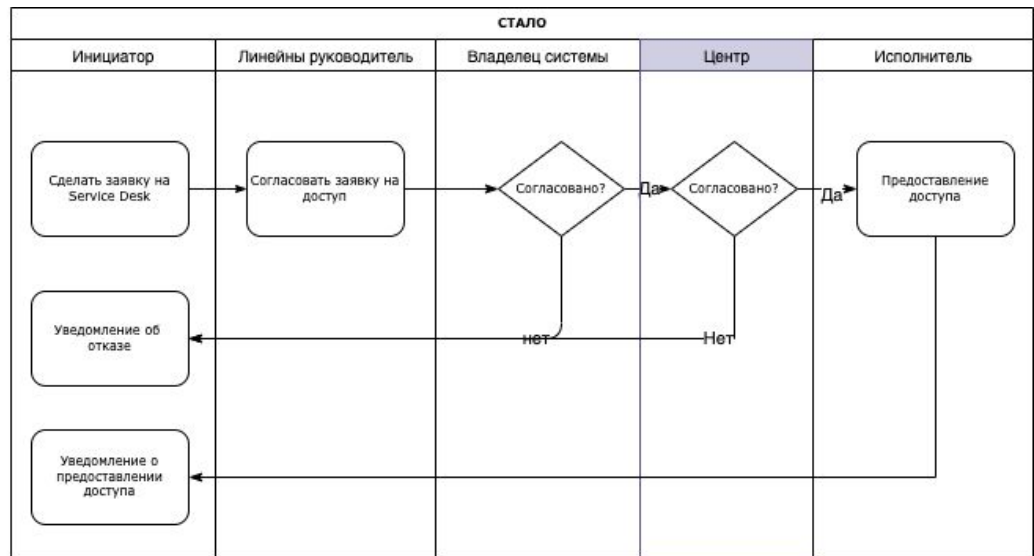
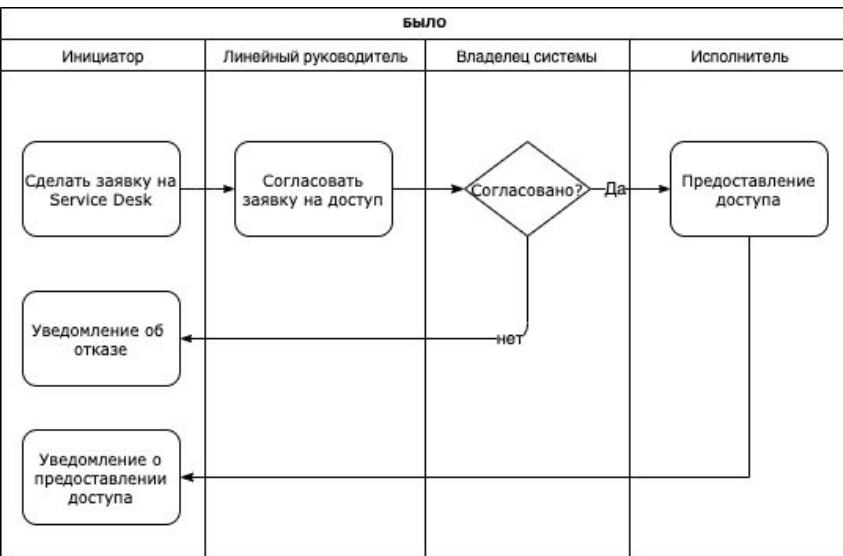
# Реализация - организационная

Убедили подразделения, что цель сохранить эффективность работы сотрудников



# Реализация - организационная

## Централизован процесс предоставления доступа

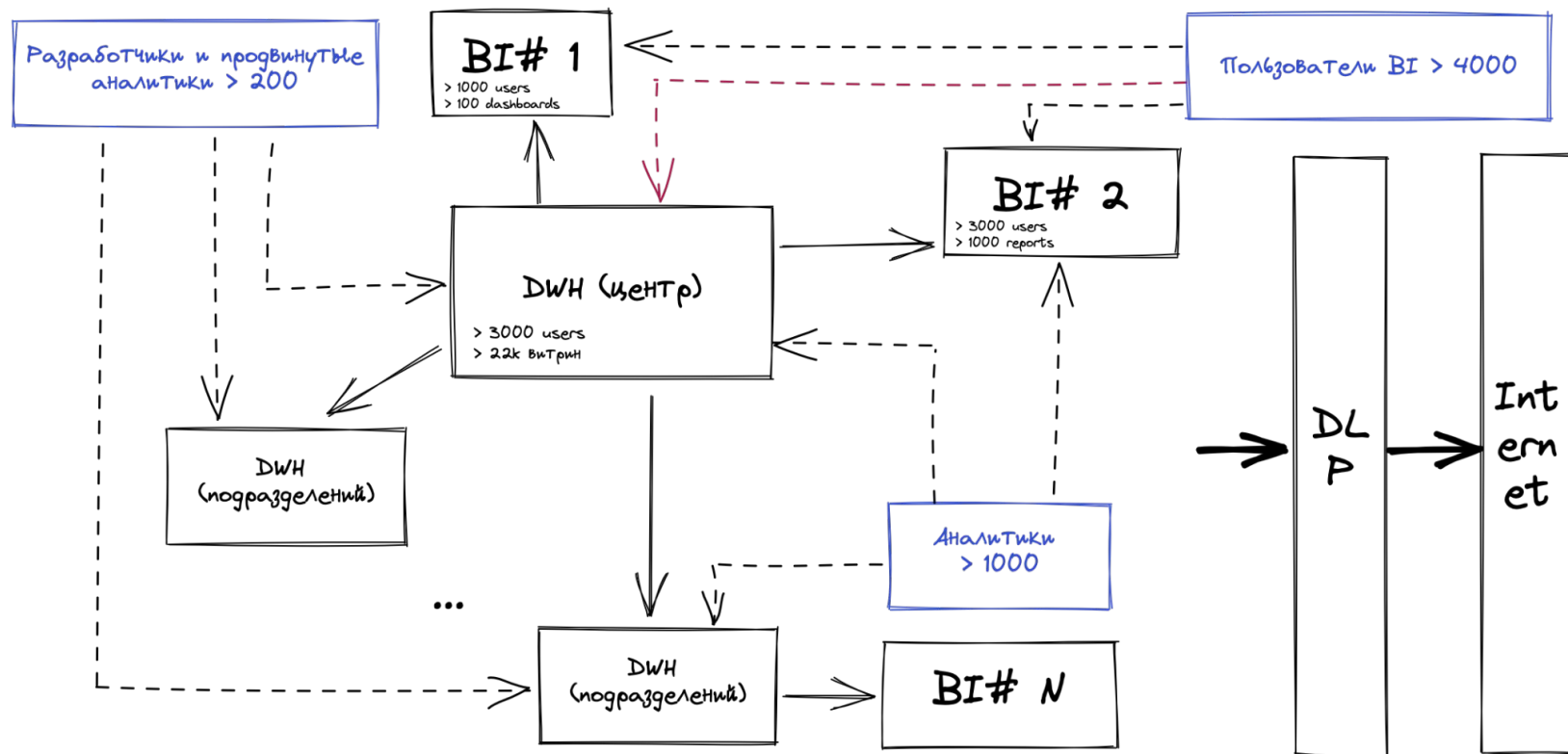


# Реализация - организационная

Аудит существующих доступов и регулярный мониторинг доступов

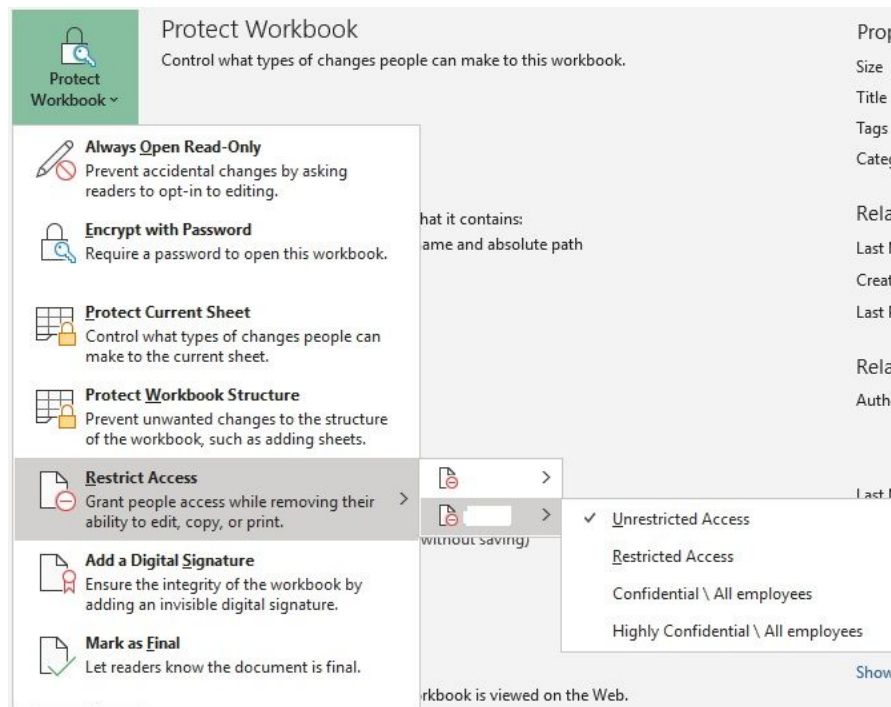
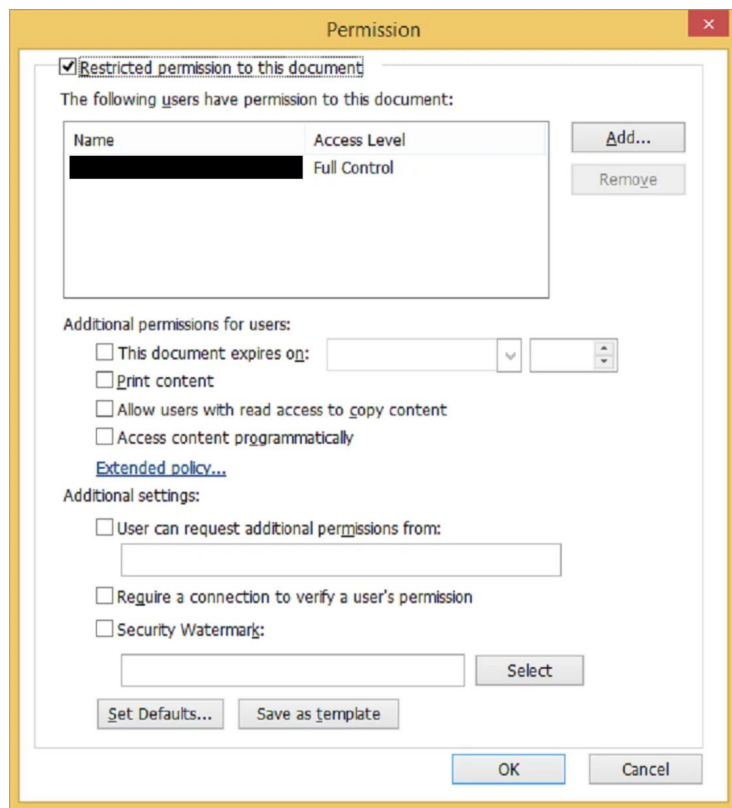


# Реализация - техническая

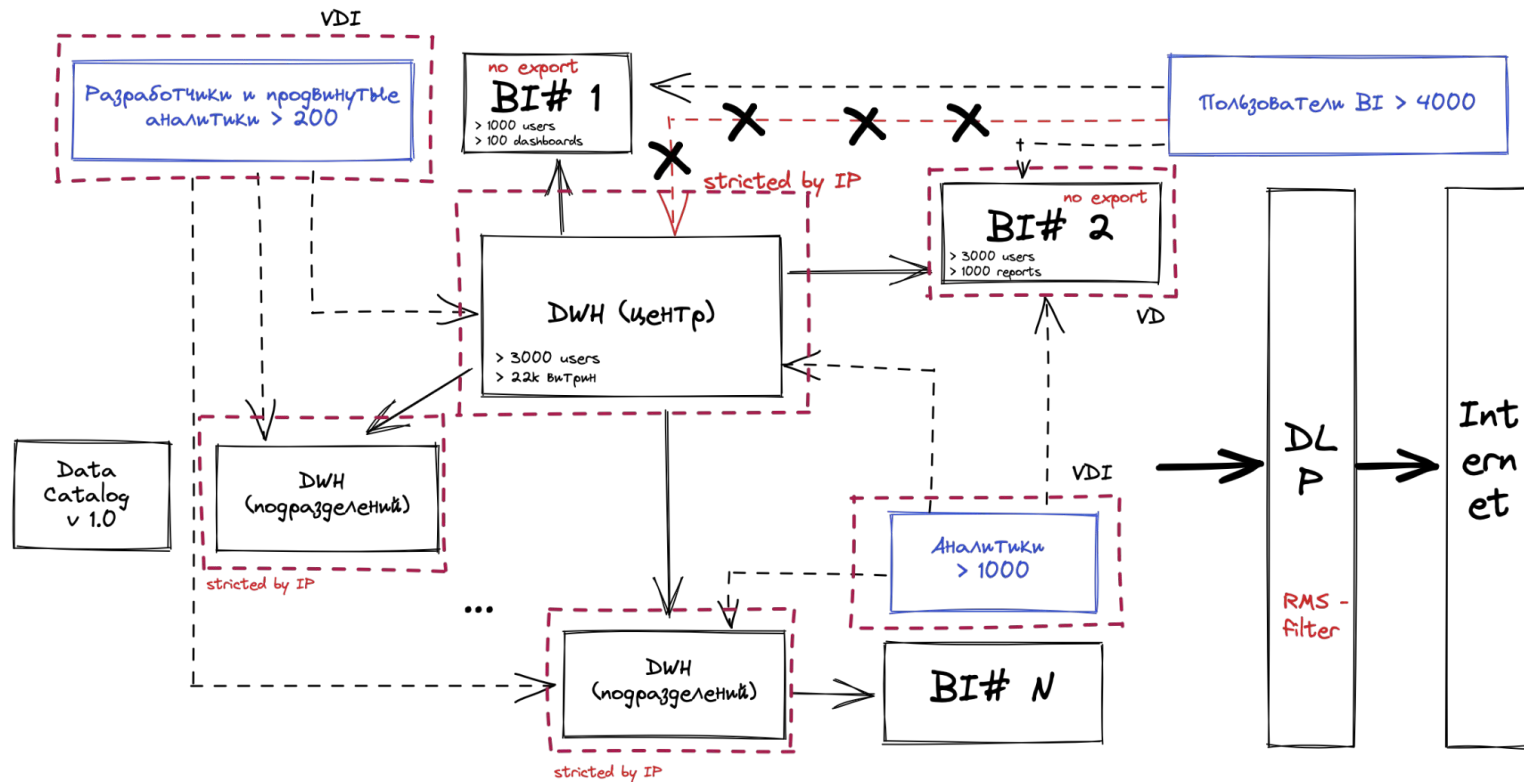




# Реализация - техническая. RMS



# Реализация - техническая



# Выученные уроки

# Выученные уроки

Эффективное функционирование компании и ее сотрудников - это важнейший приоритет



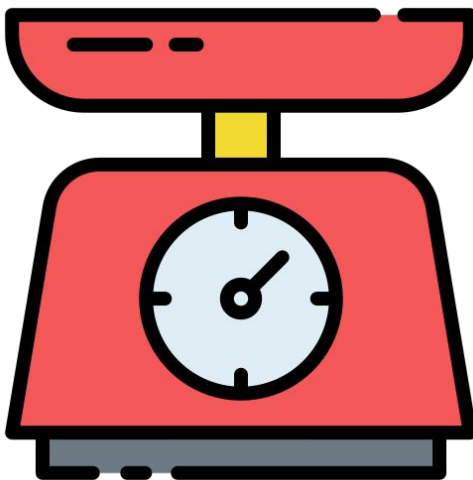
# Выученные уроки

При определении уровня конфиденциальности данных - не полагайтесь слепо на существующие политики



# Выученные уроки

Если не знаете как оценить критичность данных - сходите в профильные подразделения



# Выученные уроки

Проводите регулярный аудит доступов



# Выученные уроки

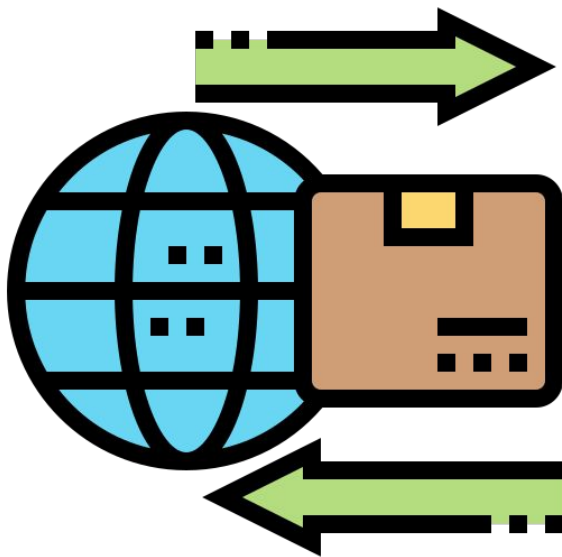
Имейте актуальный Data Catalog данных\отчетов\выгрузок\... Проводите регулярную сверку фактически существующих таблиц\витрин\отчетов\... с тем, что у вас в Data Catalog





# Выученные уроки

Используйте инструменты представления данных, которые позволяют запретить экспорт и копирование данных



# Выученные уроки

Проводите обучение сотрудников

