

PROFIT FINANCE DAY

УПРАВЛЕНИЕ  
БЕЗОПАСНОСТЬЮ ДАННЫХ  
КАК ЧАСТЬ DATA  
GOVERNANCE

И КОТИКИ..



Подумайте об этом:

” **Data Management** – процесс, связанный с накоплением, организацией, запоминанием, обновлением, хранением данных и поиском информации.

“

” **Data Governance** – подход к управлению данными, который определяет данные как основной актив организации и требующий внедрения специфичных ролей процессов и решения для управления данными как ценным активом

“

---

Роли:

**CDO (Chief Data Officer)** – он же директор по данным, нужен для эффективного превращения данных в деньги, отвечает за разработку и реализацию концепции развития корпоративных данных.

**Data Owner** – владелец данных, человек, способный принимать решение и обеспечить их выполнение во всей организации. Владельцы могут быть назначены на уровне сущности (например, записи о клиентах), либо на уровне атрибутов (например, адрес). Несут ответственность за состояние данных как актива.

---

Роли:

**Data Stewards (управляющие данными)** – те, кто будет следить за тем, чтобы политика и стандарты данных выполнялись в повседневной работе, отвечают за заботу о данных как активе.

**Data Custodians (хранители, операторы данных)** – производят технические и бизнес изменения, техническое обслуживание и т.д.

**Data Governance Committee (комитет по управлению данными)**  
– форум, для утверждения политики и стандартов в области данных

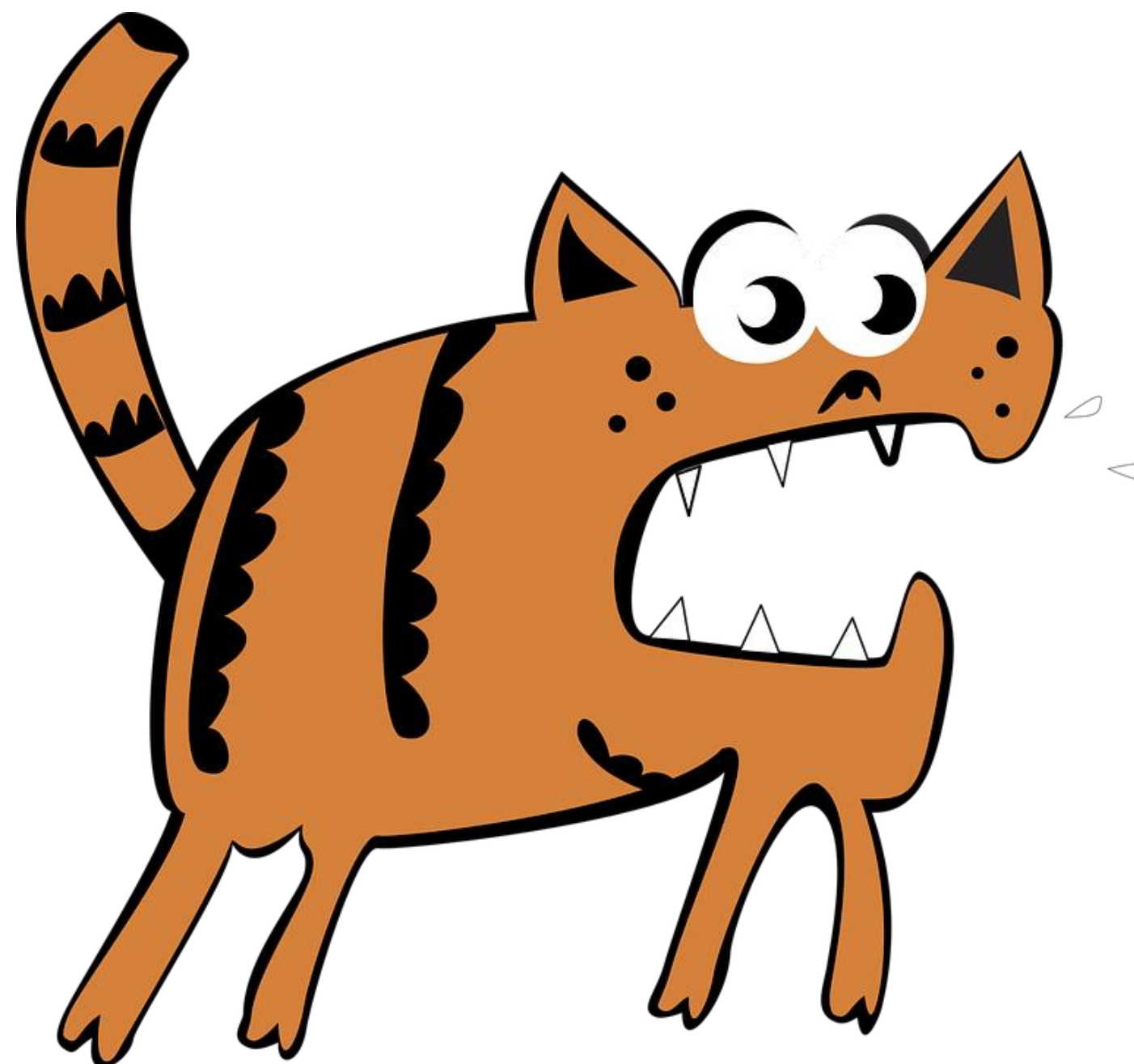
---

Есть ещё:

## **Data Governance Team**

- менеджер
  - архитектор
  - аналитик
  - стратег
  - комплаенс-офицер
-

**ДАННЫЕ -  
ЧТО  
ЭТО за  
странный  
предмет?**



# Проблема №1

**Вот они есть, а  
вот их уже ...  
больше?**

**или данных  
много не  
бывает?**

---

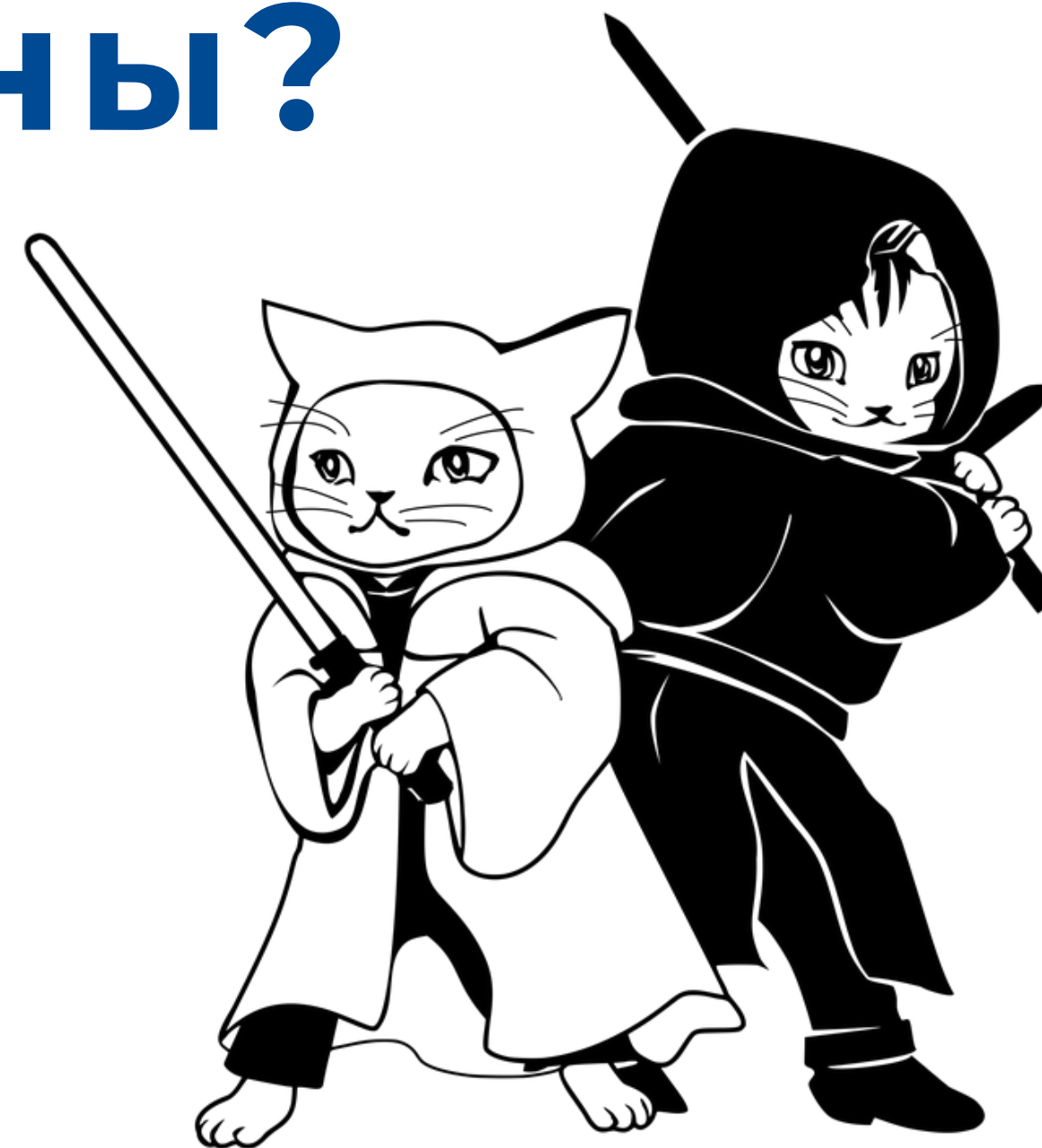






# Проблема №2

**Все ли данные  
одинаково  
полезны?**



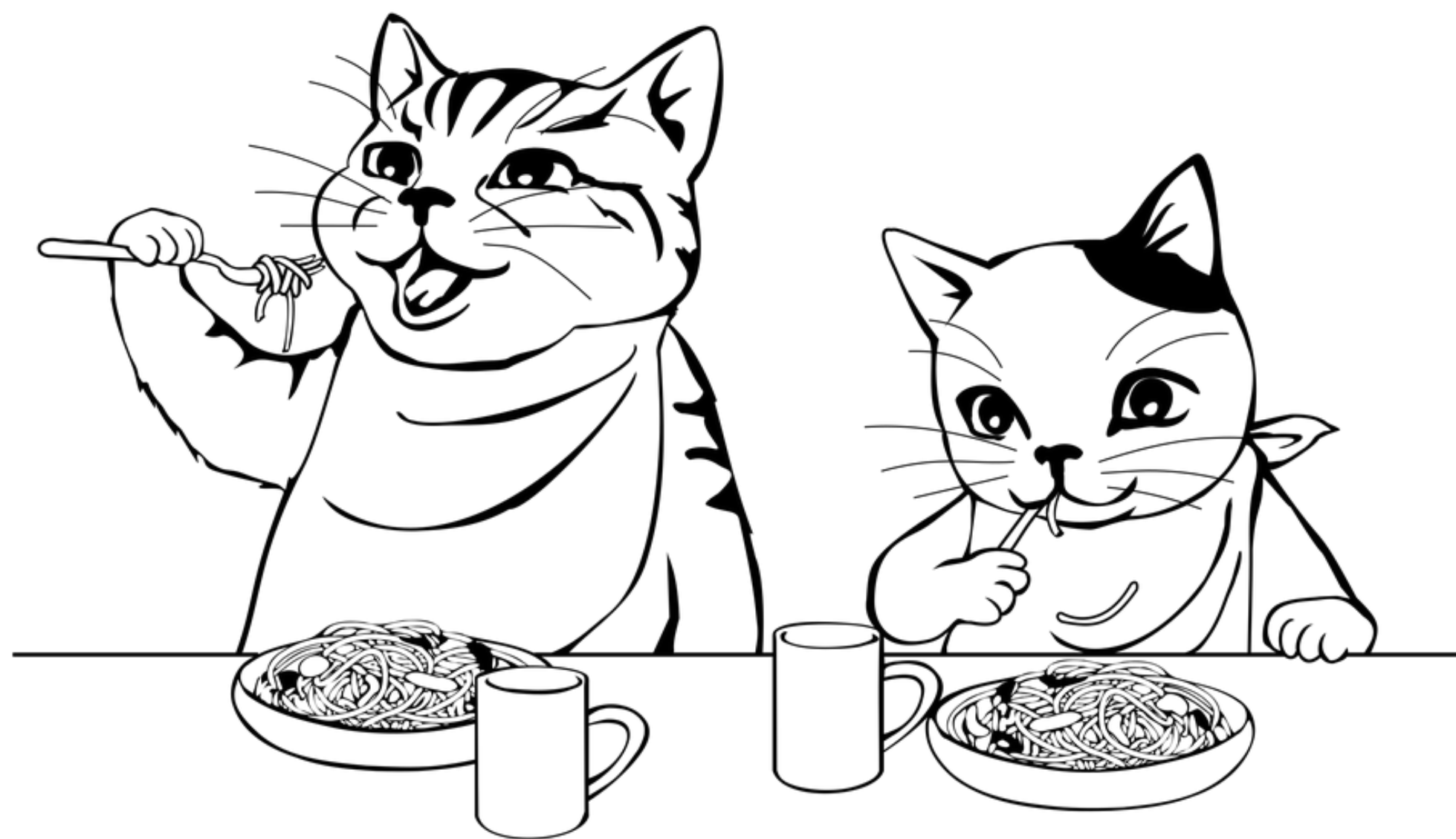
# Проблема №3

**Данных много,  
я один!**



# Проблема №4

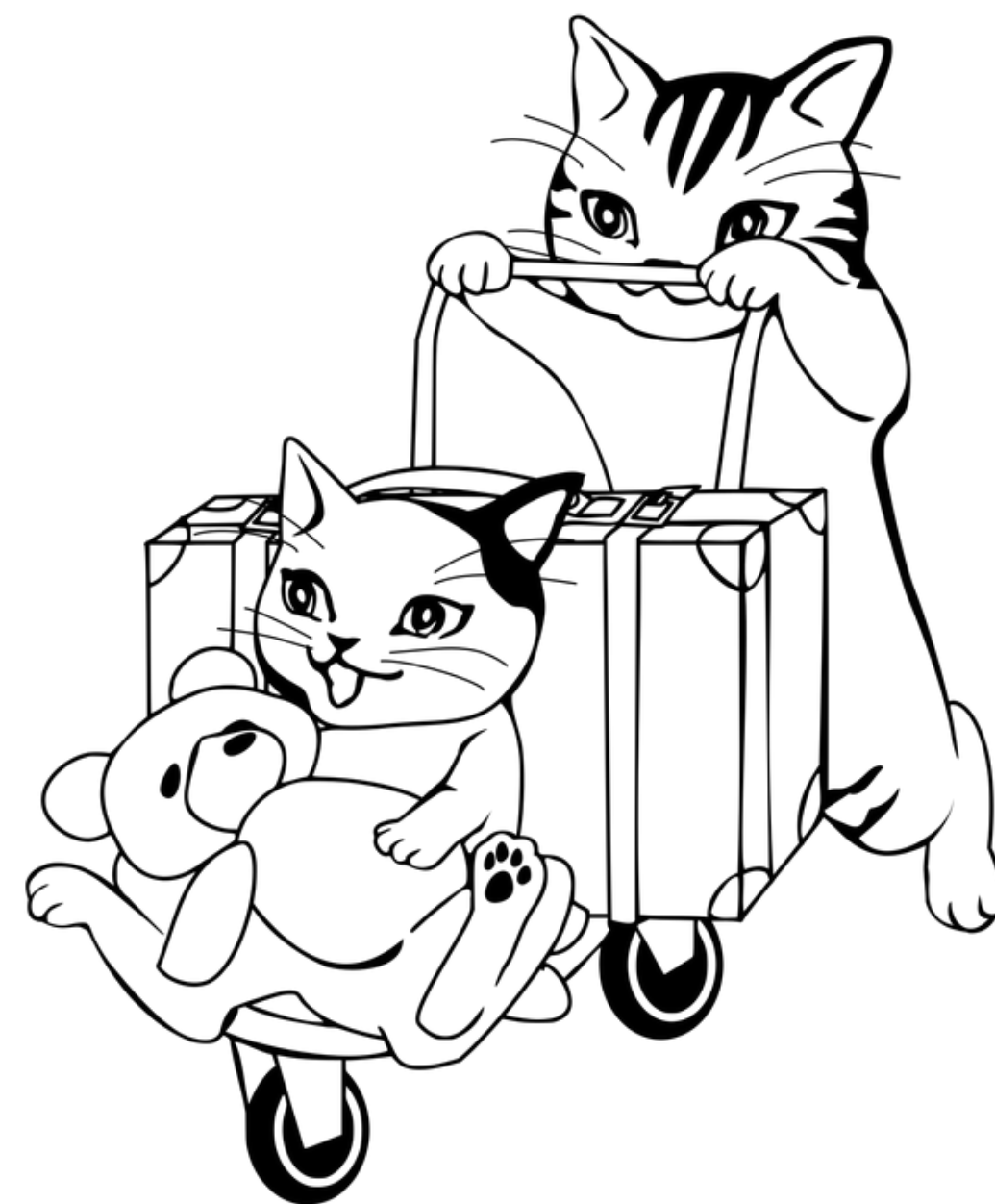
## Данные - прожёры





# Проблема №5

## Данные - непоседы



# Цели защиты данных

---

Для чего мы работаем?



Обеспечение  
конфиденциальности



Обеспечение  
надлежащего доступа



Обеспечение  
целостности

# МЕТОДЫ ЗАЩИТЫ

---

DLP, UDCS

ENCRYPTION  
RMS

IDM, PAM

HASHING  
E-SIGNATURE



ДОРОГО, ДОЛГО,  
МНОГО РЕСУРСОВ  
НЕ ГАРАНТИРУЕТ  
ЭФФЕКТИВНОСТИ



# ЧТО ЖЕ ДЕЛАТЬ?

---

1

**Выстроить процессы**

2

**Оптимизировать данные и их жизненный цикл**

3

**Идентифицировать данные, определить владельца**

4

**Оценить риски**

**Внедрить контроли**

**СПАСИБО  
ЗА ВНИМАНИЕ**

---