# Big Data

## для предотвращения потерь в ритейле

Дмитрий Мананников

# Инциденты

Причина и основа существования «безопасности» как функции. И единственная вещь на которую функция влияет. И единственная «переменная»  изменение которой коррелирует с множеством «переменных» в функции. С бюджетом, стратегией, техническими или организационными нормами, зарплатами и количеством работников и прочими (всеми) другими.


Существует ли какой либо другой драйвер для безопасности кроме инцидентов?

1

# Все лучшие практики крутятся единицы инцидента

# «Золотые» инциденты

Если мы повторяем полный цикл действий для каждого инцидента, то это требует огромное количество ресурсов.

Поэтому понятие «инцидент» сужается…

# «Злые» инциденты

Если мы повторяем полный цикл действий для каждого инцидента, то это требует наказаний.

«У каждого инцидента есть фамилия»

Поэтому понятие «инцидент» еще более сужается…

# «Бестолковые» инциденты

Если мы постоянно сокращаем количество (и как следствие частоту) инцидентов, то мы не можем исправить  причину его возникновения

# Во что превращается процесс управления инцидентами?

Слишком много, пусть сами разбираются

Тут нет умысла, просто ошибка

Это не системно, нет смысла исправлять причину

Ура! Наконец-то нормальный инцидент

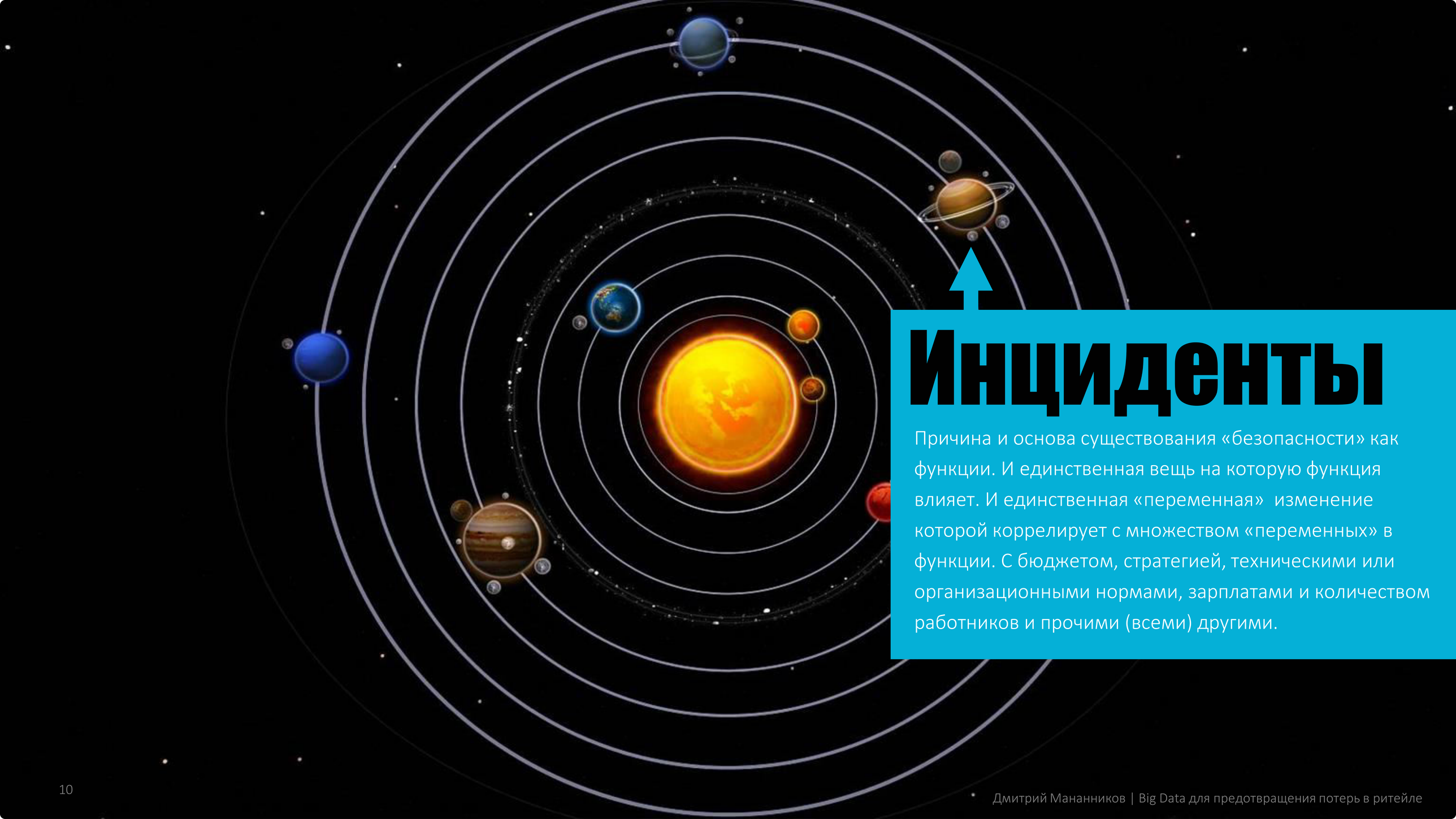
Слишком много, пусть сами разбираются

Тут нет умысла, просто ошибка

Это не системно, нет смысла исправлять причину

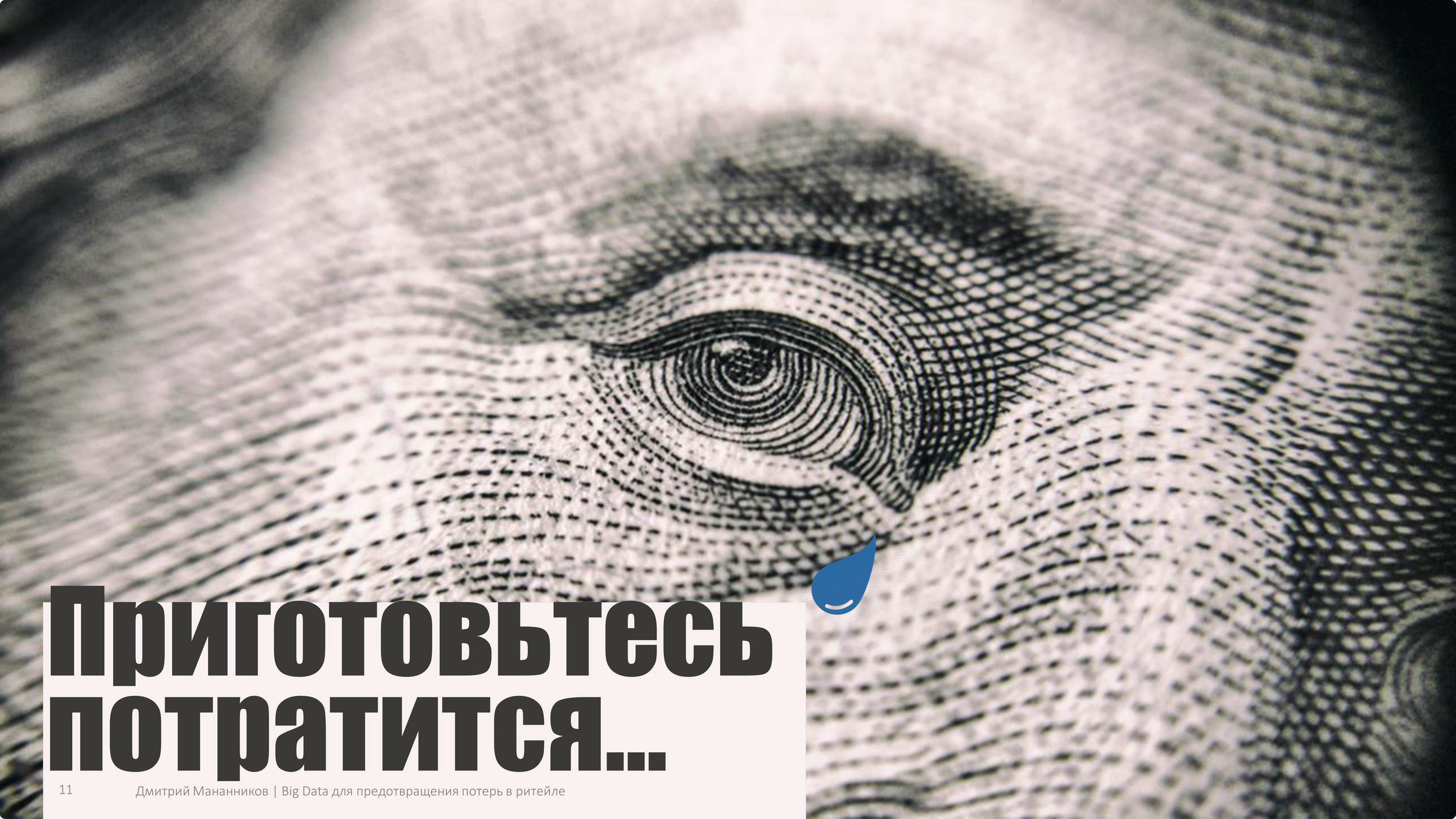
Ура! Наконец-то нормальный инцидент


А поскольку бюджет мы получаем как правило через FUD, то профильный бюджет выделят только на него. А значит..



# Инциденты

Причина и основа существования «безопасности» как функции. И единственная вещь на которую функция влияет. И единственная «переменная»  изменение которой коррелирует с множеством «переменных» в функции. С бюджетом, стратегией, техническими или организационными нормами, зарплатами и количеством работников и прочими (всеми) другими.



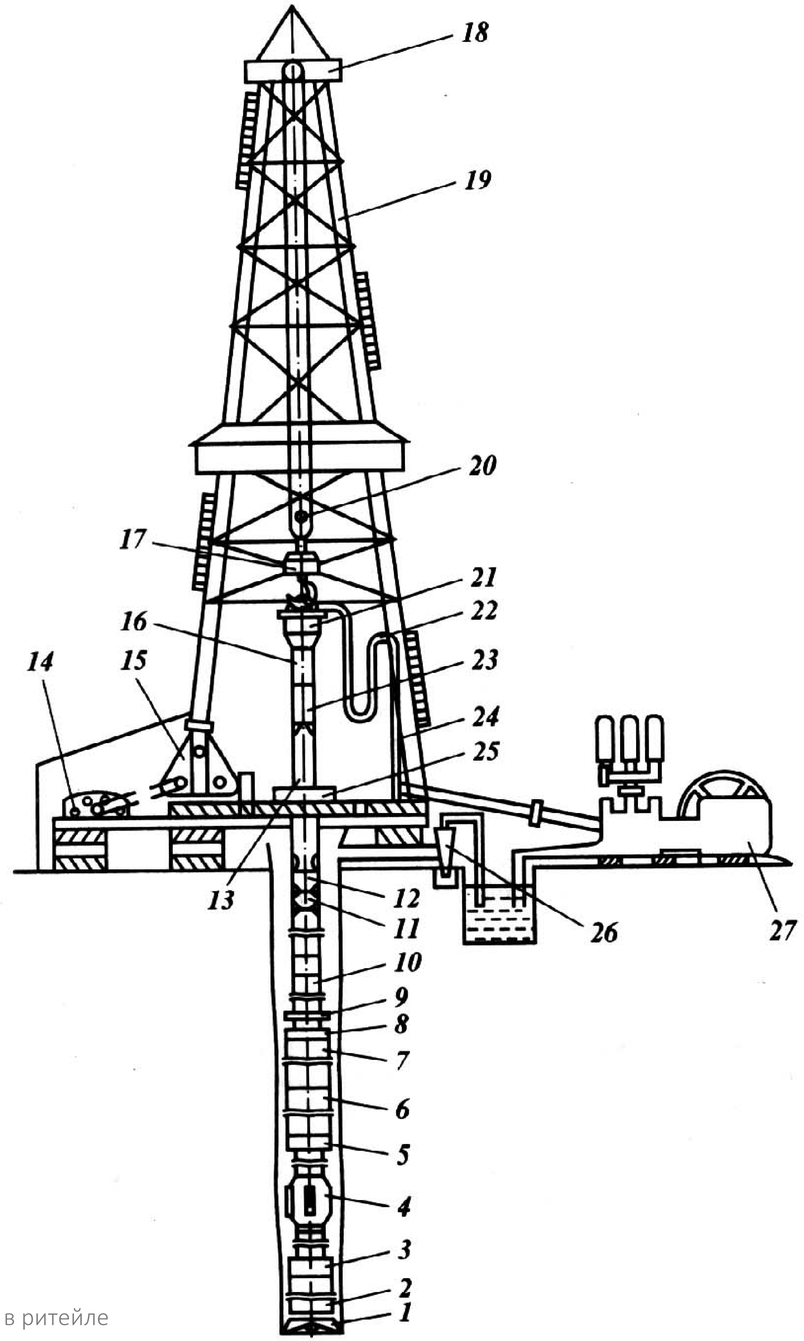
# Приготовьтесь потратится...

# 1 DRILL DOWN

Инциденты, они нужны нам все!

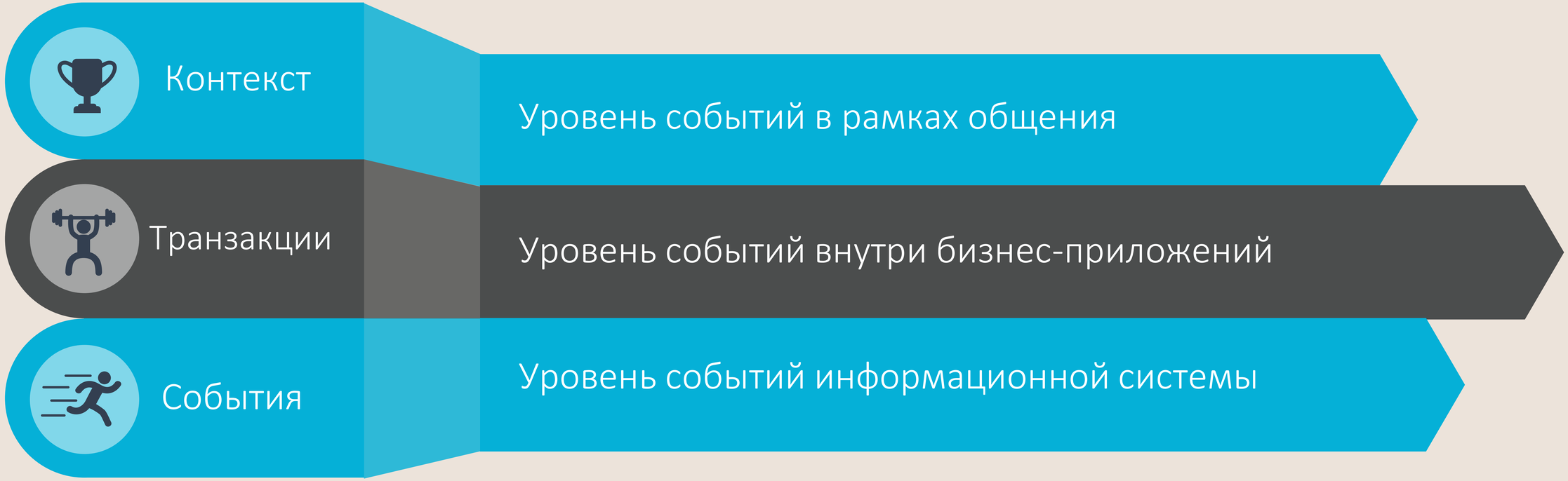
Не нужно его сужать понятие, наоборот необходимо максимально его расширить

**инцидент информационной безопасности -** абсолютно все что «пошло не так»



# Информационные слои

в которых живут инциденты



# DATA MINING

## 2

Очистка\сортировка данных о инцидентах

После того как информация о инцидентах начинает собираться, нужно научится и приводить ее в однообразную форму, для того что бы делать выводы на совокупных данных

# Локирование инцидентов

для всех инцидентов нам интересны следующие элементы

## бизнес-логика

Почему это проблема?

В каком процессе?

В каком из блоков процесса?

Как повлияло на процесс?

Как повлияло на другие процессы

## люди, техника и время

Где эта проблема?

Кто источник(роль\имя)?

Кто пострадавший (роль\имя)?

Где проблема в железе?

Где проблема в системе?

Когда она произошла?

## регламенты

Вопреки чему эта проблема?

Нарушенные инструкции?

Нарушенные регламенты?

Обойдённые правила?

# Анализ данных

Теперь когда у нас есть огромное количество однородной информации, мы можем начать делать выводы

# Разделение по уровням

Все инциденты равны, но некоторые инциденты равнее других.

## safety

Инциденты которые по отдельности не «страшны», но в совокупности дают эффект, достаточный для инвестиций на коррекцию

«декостылизация»

## security

Классические инциденты ИБ «как мы любим».

Приводящие к значительным ресурсным потерям.

Требующие полного «классического» цикла

## operations

Инциденты живущие в рамках операционных «проблем».

Быстро решаемые. По совокупности потерь не тянущие даже на «костыли»

# Во что теперь превращается процесс управления инцидентами?

Мы знаем обо всех инцидентах

Их влияние на бизнес

Системно исправляем причины

Акцентируем свои усилия только на важном

# 4

# USE THE FORCE Of STATISTICS

## ФОРКАСТЫ КОРРЕЛЯЦИИ ПРЕДИКТЫ

вот это вот все...

# БИЗНЕС БЕНЕФИТЫ

Что данный подход дает в бизнес контексте

01

## ОШИБКИ БИЗНЕС-АРХИТЕКТУРЫ

Фактически, статистика собираемая таким способом начнет показывать «бутылочные горлышки» в рамках существующих бизнес-процессов. И явится триггером для их реинжиниринга

02

## КАЧЕСТВО ПРОЦЕССА\ПРОДУКТА

Инцидент (их совокупность) становится параметром для оценки качества процессов продуктов, которое можно учитывать при дизайне (помните - security by design?)

03

## ПЕРФОМИНГ ПРОЦЕССОВ

Инцидент становится исчисляемым количественным параметром влияя на который мы получаем влияние на основной бизнес-показатель самого процесса

04

## БЕНЧМАРКИНГ

Инциденты становятся одним из бенчмарков для внутренней оценки одинаковых процессов проходящих на разных площадках

# БЕНЕФИТЫ БЕЗОПАСНОСТИ

Что данный подход дает в контексте функции

01

## РАСШИРЕНИЕ ГОРИЗОНТА

Не нужно ждать хакеров и читать «страшную аналитику» для поиска своей полезности. Такой подход позволяет найти ее в повседневной операционке

02

## КОРРЕКЦИЮ ПРАВИЛ

Много инцидентов с нарушением одних и тех же правил – прямой показатель того что правило не работает и его нужно менять.

03

## ОБОСНОВАНИЕ БЮДЖЕТА

Совокупное влияние на операционные показатели позволит получить обоснование для существенной доли бюджета на средства защиты или мероприятия

04

## ПРЕДИКТИВНОСТЬ

Возможность выявлять «пиковые» инциденты в стадии их формирования, даже если до этого не было никакого негативного опыта

# [x] ВАЖНО!!!

# НЕ ВСЕГДА ЕСТЬ ПРИЧИННО-СЛЕДСТВЕННАЯ СВЯЗЬ

# Спасибо за внимание!

# Возможно есть вопросы?

dmitriy.manannikov

dmitriy@manannikov.ru