ИБ
ДЛЯ БИЗНЕСА
А НЕ РЕГУЛЯТОРА

Николай Казанцев

Начальник отдела ИБ
ООО «НТФФ «ПОЛИСАН»

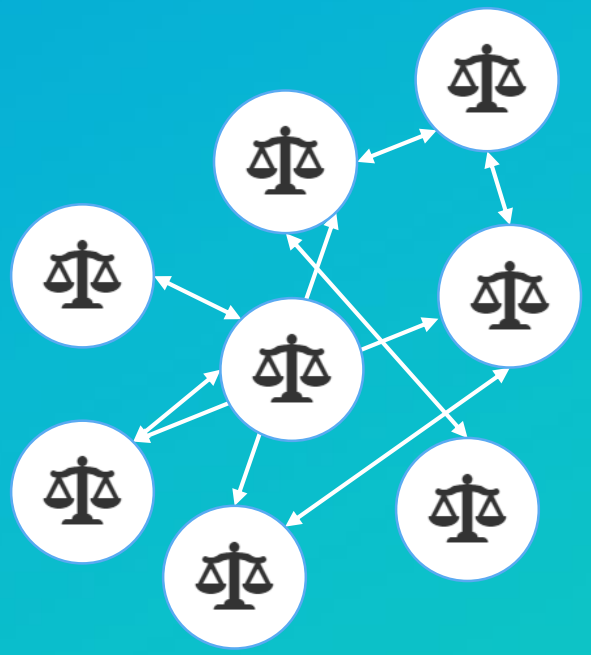
О КОМПАНИИ

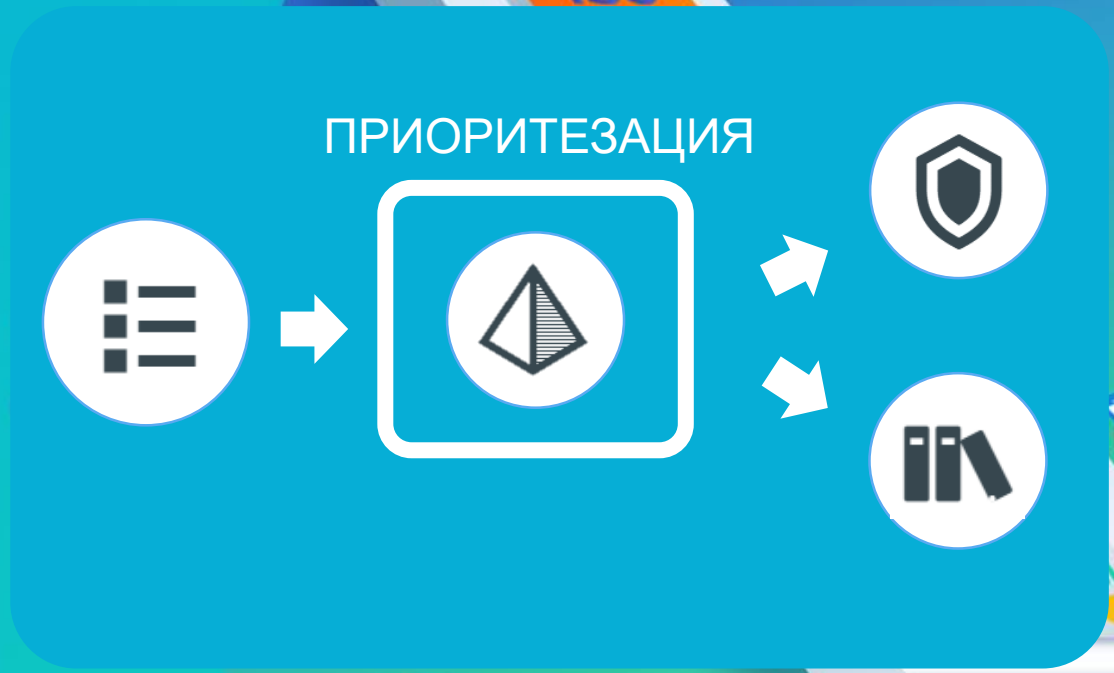
Полисан

Заводов	2
Работников	1300
ИБ	4

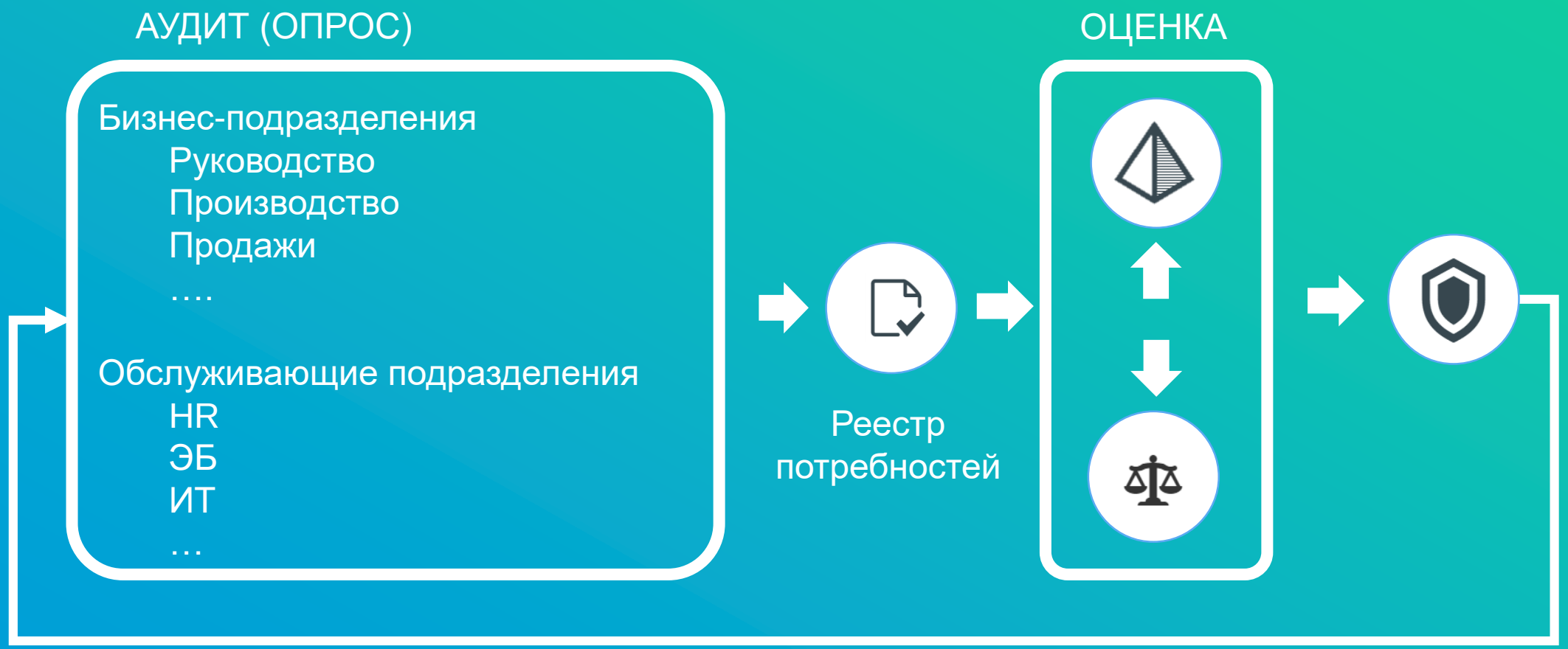
ОБЛАСТЬ ОТВЕТСТВЕННОСТИ

ТРЕБОВАНИЯ





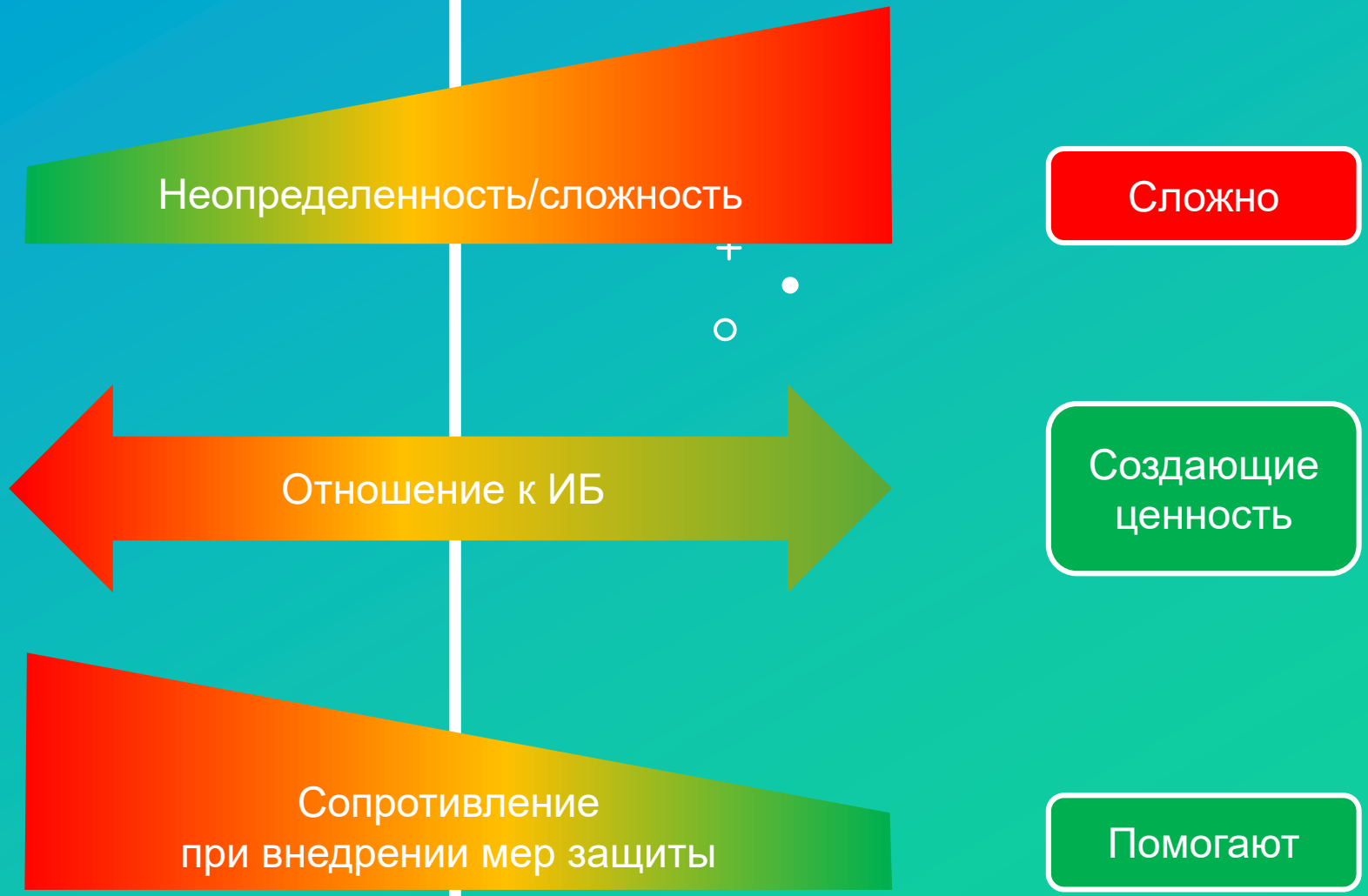
ПОТРЕБНОСТИ БИЗНЕСА



Ежегодно + по инициативе подразделений

ТРЕБОВАНИЯ

ПОТРЕБНОСТИ



РИСКИ?

Сочетание вероятности события и его последствий

ГОСТ Р 51901.1-2002

Влияние неопределенности на цели

ISO/IEC 27000:2018

Риск ~ ущерб

Методика оценки угроз ФСТЭК от 05.02.2021

Потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации.

ГОСТ ИСО/МЭК 27000-2012

Вероятность того, что угрозы будут реализовываться с использованием уязвимостей информационных активов или групп информационных активов и, тем самым, наносить ущерб организации

ISO/IEC 27000:2018

Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов. Определяется как сочетание вероятности события и его последствий.

ГОСТ Р ИСО/МЭК 13335-1-2006

Вероятность причинения ущерба сети электросвязи или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в сети электросвязи.

ГОСТ Р 52448-2005

РИСК

Реализация угрозы через использование уязвимости в активе

СМК и общие методики:

Последствия + Угроза / Опасность + Причина

МЫ:

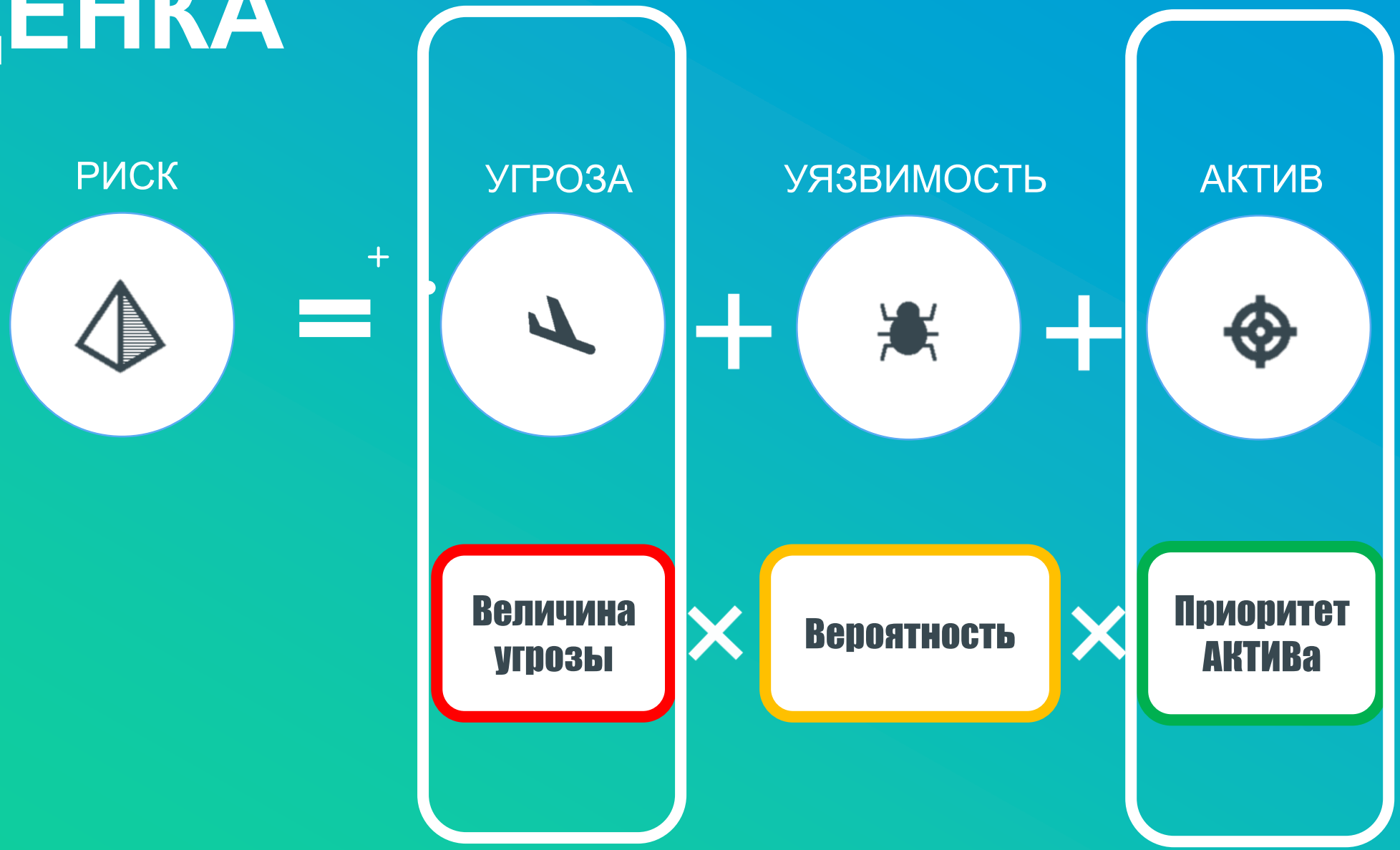
Угроза + Уязвимость + Актив

МУ ФСТЭК:

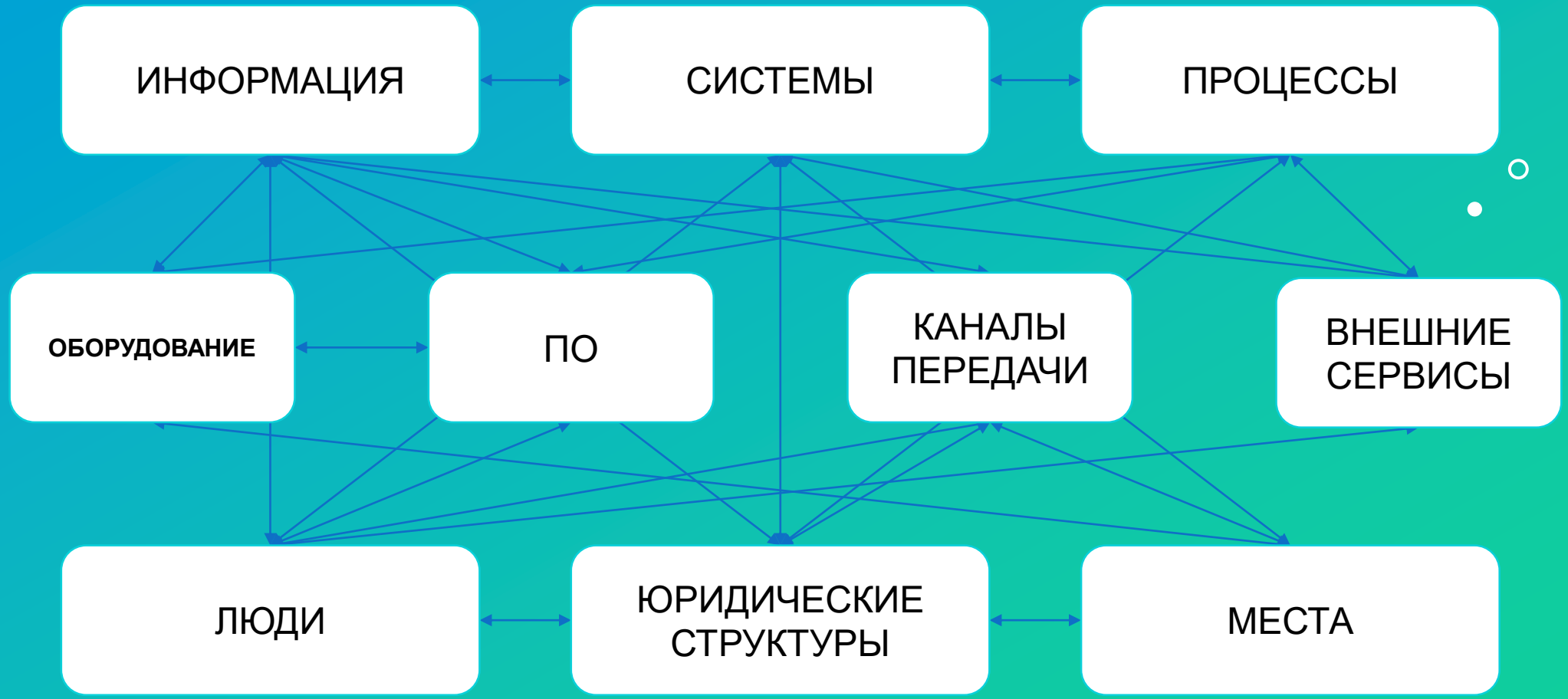
Риск (ущерб) + Негативное последствие + Угроза + Объект воздействия + Интерфейс + Способ реализации

ОЦЕНКА

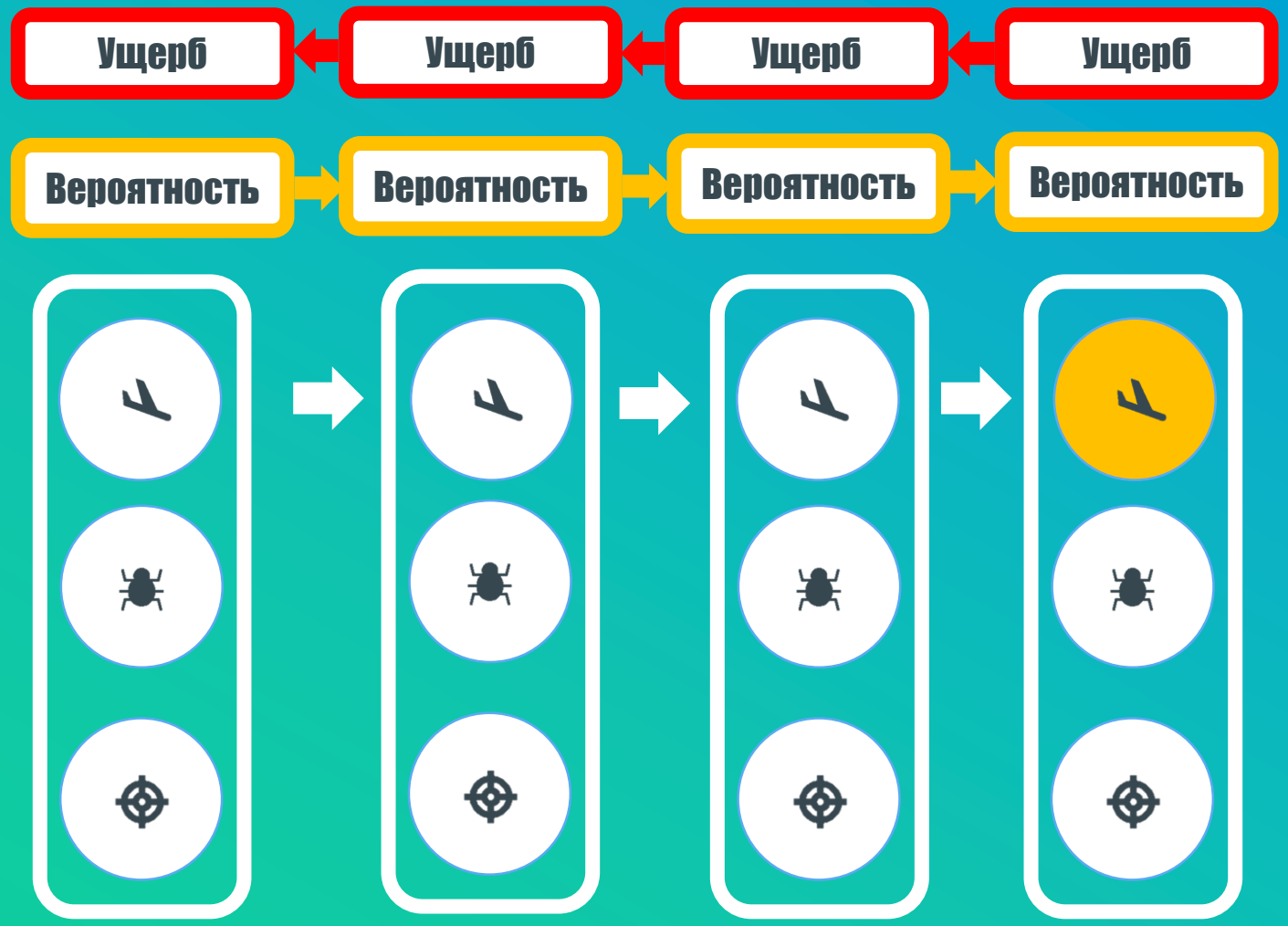
КАК СЧИТАТЬ РИСКИ



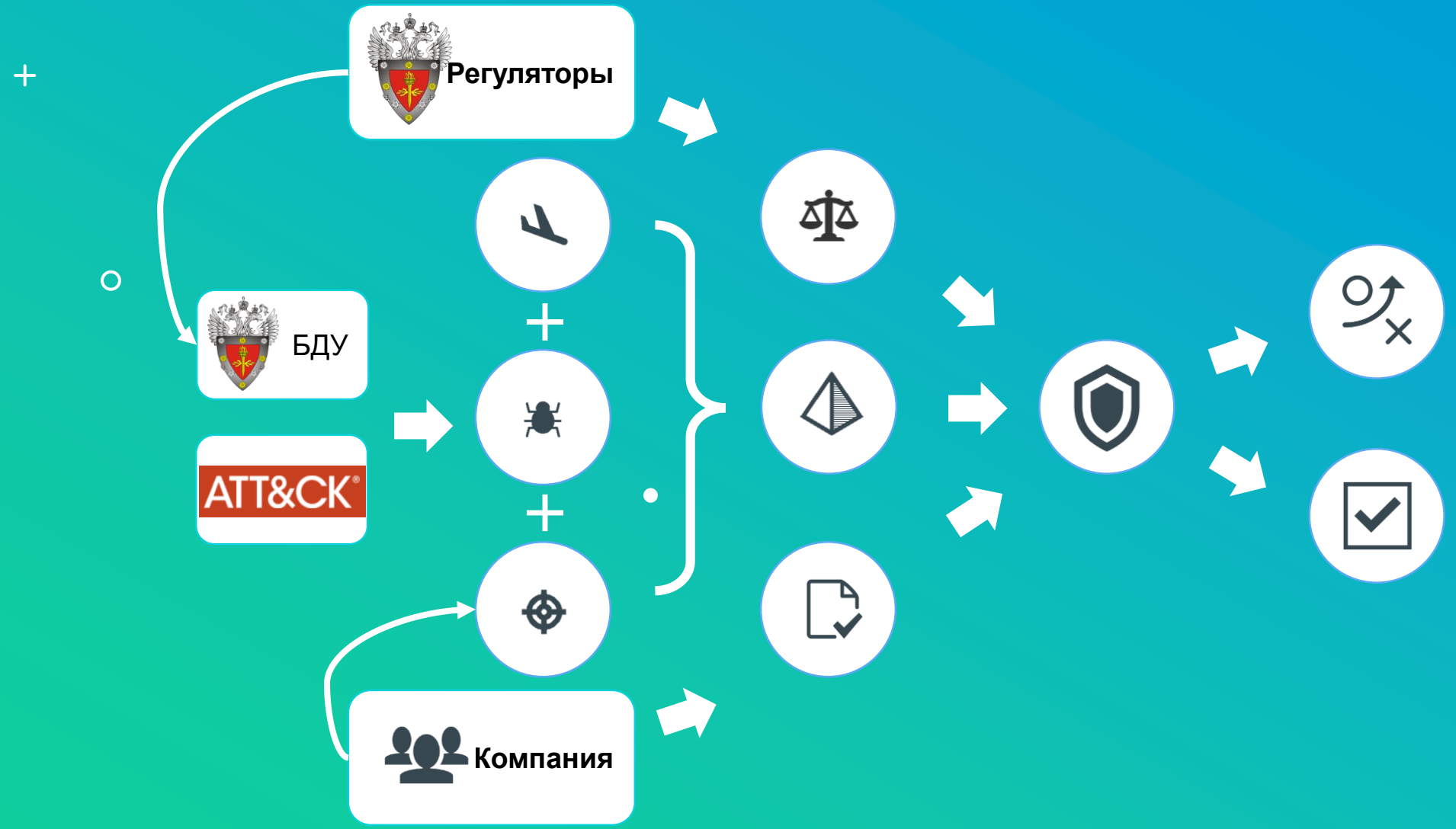
АКТИВЫ


ИНФОРМАЦИЯ
СИСТЕМЫ
ПРОЦЕССЫ
ОБОРУДОВАНИЕ
ПО
КАНАЛЫ ПЕРЕДАЧИ
ВНЕШНИЕ СЕРВИСЫ
ЛЮДИ
ЮРИДИЧЕСКИЕ СТРУКТУРЫ
МЕСТА

ЦЕПОЧКА УГРОЗ



ОБЩАЯ СХЕМА



ЗАЩИТНЫЕ МЕРЫ

ЗАДАЧА

1. СНИЖАТЬ **РИСКИ** информационной безопасности
2. ИСПОЛНЯТЬ **ТРЕБОВАНИЯ** регуляторов и стандартов
3. ЗАКРЫВАТЬ **ПОТРЕБНОСТИ** заинтересованных сторон внутри компании

ПРИНЦИПЫ

1. **РАССТАВИТЬ ПРИОРИТЕТЫ**
   между 3 подходами исходя из специфики вашей организации
2. **ИСКАТЬ ПЕРЕСЕЧЕНИЯ**
   в требованиях регуляторов, потребностях бизнеса и актуальных рисках
3. **ВЕСТИ РЕЕСТР МЕР**
   отражающий всю активность службы ИБ в связке с регуляторикой, запросами бизнеса и рисками

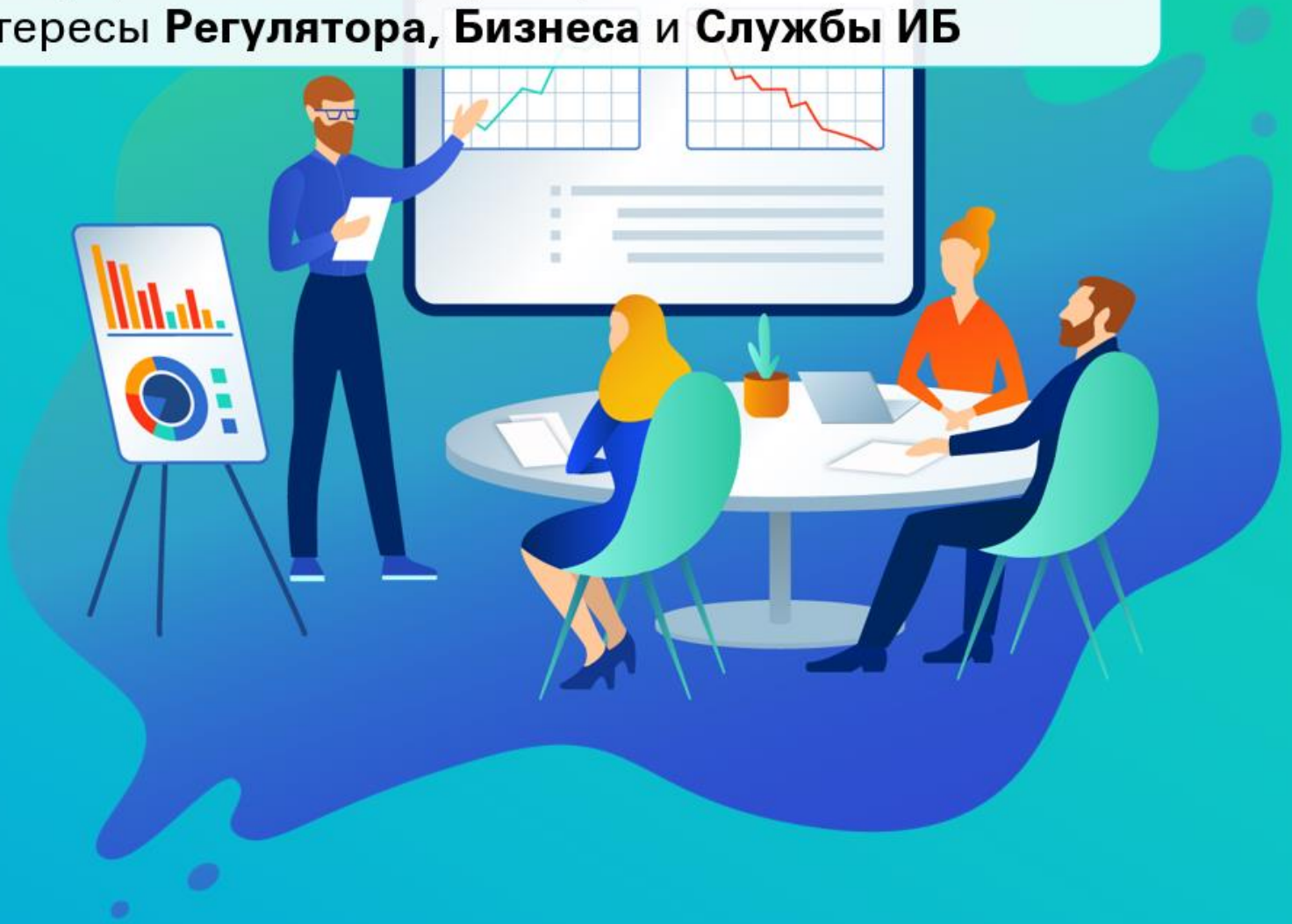
PROFIT

Нормализованная система управления информационной безопасностью соблюдающая интересы **Регулятора, Бизнеса** и **Службы ИБ**

ОПТИМИЗАЦИЯ РЕСУРСОВ

ОБЩИЙ ЯЗЫК С БИЗНЕСОМ

ОБОСНОВАНИЕ АКТИВНОСТИ



СПАСИБО ЗА ВНИМАНИЕ

Николай Казанцев

+7 906 255 2009

t.me/**NicKazantsev**