Безопасность как Бизнес-функция

Дмитрий Мананников

Бизнес-консультант

по безопасности

Дмитрий Мананников

Бизнес-консультант по безопасности

Управляю безопасностью в коммерческих компаниях с 2003 года.

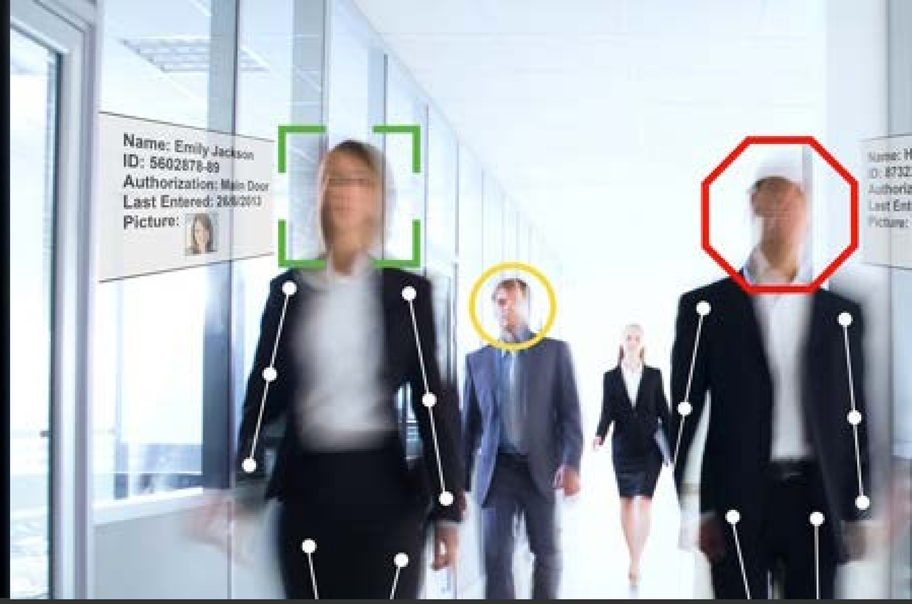
Имею успешный опыт выстраивания процессов безопасности в кредитно-финансовой сфере, энергетике, логистике и ИТ. Методолог. Автор ряда методик оценки эффективности безопасности.

Преподаватель в рамках программ MBA РАНХиГС

О чем данный мастер-класс

Как обеспечивать безопасность

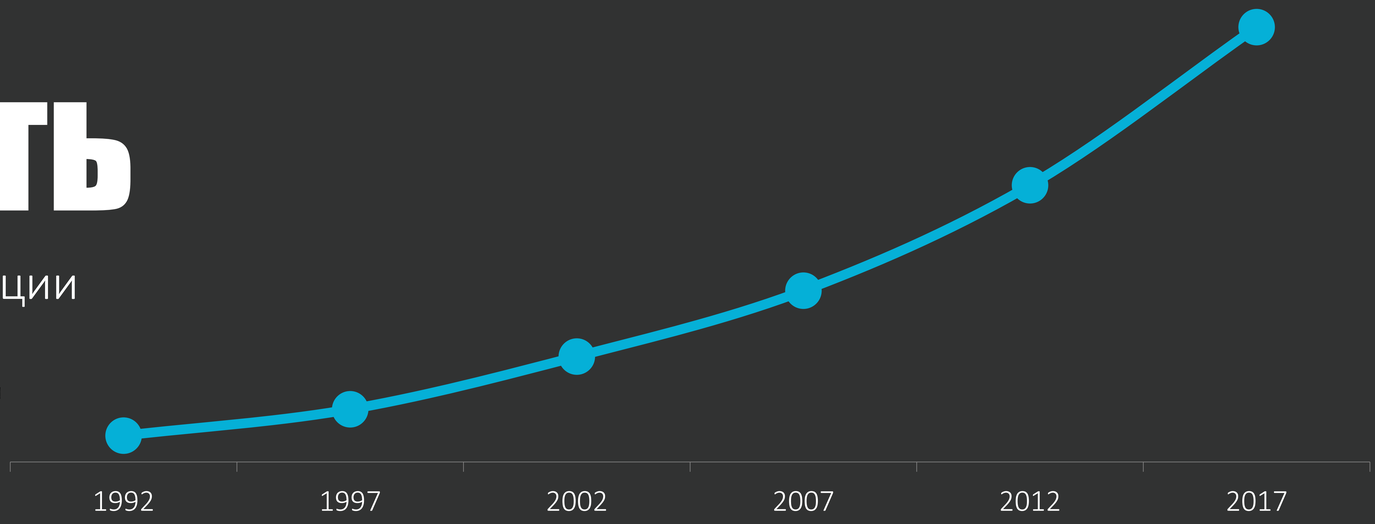
Как определить зачем нужна безопасность бизнесу и как ее органично вписать в бизнес-процессы



Актуальность

Экспоненциальный рост стоимости функции

«Игрушки» стали дороже. За последние 20 лет бюджеты выделяемые на безопасность выросли более чем в 16 раз



Цель мастер-класса

Изменить «точку сборки»

Научится смотреть на безопасность со стороны внутреннего заказчика

Изменить позицию с «Знаю как» на «Знаю зачем»

процесс?
состояние?
потребность?
ощущение?

Что такое безопасность как термин?

Что такое безопасность как часть бизнеса?

Как бизнес видит такую безопасность?

Сколько стоит ИБ для средней компании (1000-1200 сотрудников) в год?

Фонд оплаты труда

	оклад	выплаты	бонус	итого за год
начальник отдела	140 000 ₽	42 000 ₽	280 000 ₽	2 464 000 ₽
ведущий специалист	120 000 ₽	36 000 ₽	240 000 ₽	2 112 000 ₽
специалист	90 000 ₽	27 000 ₽	180 000 ₽	1 584 000 ₽
специалист	90 000 ₽	27 000 ₽	180 000 ₽	1 584 000 ₽
			Итого:	**7 744 000 ₽**

Рабочие места	
аренда 25 кв.м. в офисе B+	425 000 ₽
прочие расходы	192 000 ₽
Итого:	**617 000 ₽**

Минимальные "игрушки"	
антивирус (1000-1200 пользователей)	700 000 ₽
антиспам (1000-1200 пользователей)	800 000 ₽
защита web ресурсов (1-2 ресурса)	500 000 ₽
Итого:	**2 000 000 ₽**

Как бизнес видит безопасность?

10 361 000 ₽

стало безопаснее чем вчера XXX XXX ₽
compliance XXX XXX ₽
лучшие практики XXX XXX ₽
снижены риски XXX XXX ₽
сохранены тайны XXX XXX ₽
консалтинг XXX XXX ₽

Что бизнес получает от безопасности?

Состояние?
Ощущение?

Это почти как СТРАХОВАНИЕ только без возмещения ущерба

В чем основная проблема страхования? В методологии расчета страхового взноса. А точнее в его размере. «Риски» против «Жадности».

OCTAVE
CORAS
CRAMM

«Риски» против «Жадности» работают ли методики оценки рисков безопасности?*

*на самом деле отлично работают, вопрос лишь в том что это внутренний узкоспециализированный инструмент который используется для внутренних целей безопасности и абсолютно бесполезен за ее пределами

Страхование как снижение рисков?

Вполне бы себе работало, если бы бизнес не ставил на одно поле риски операционные и риски безопасности

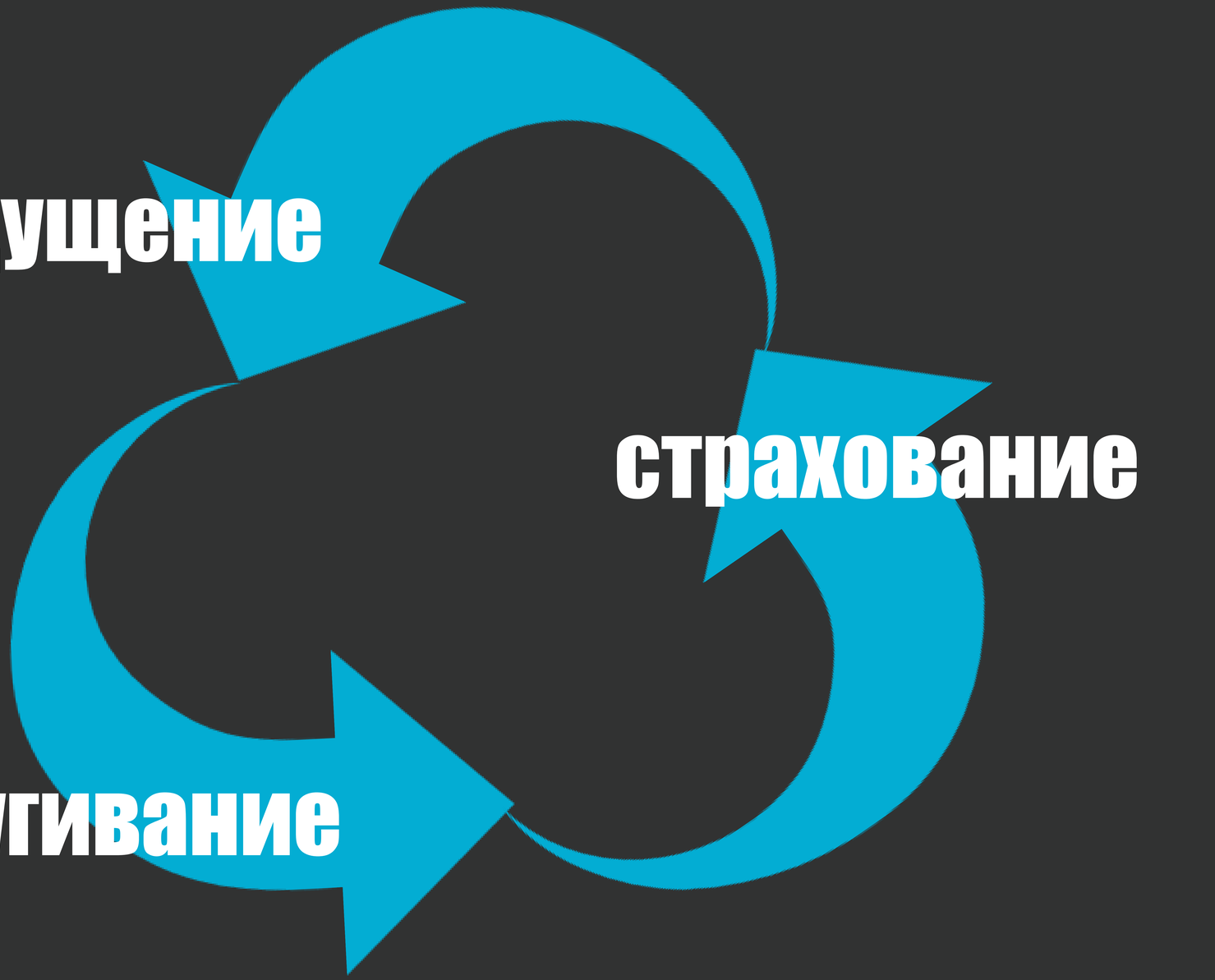
Что двигает страхование?

FUD

Fear, uncertainty and doubt

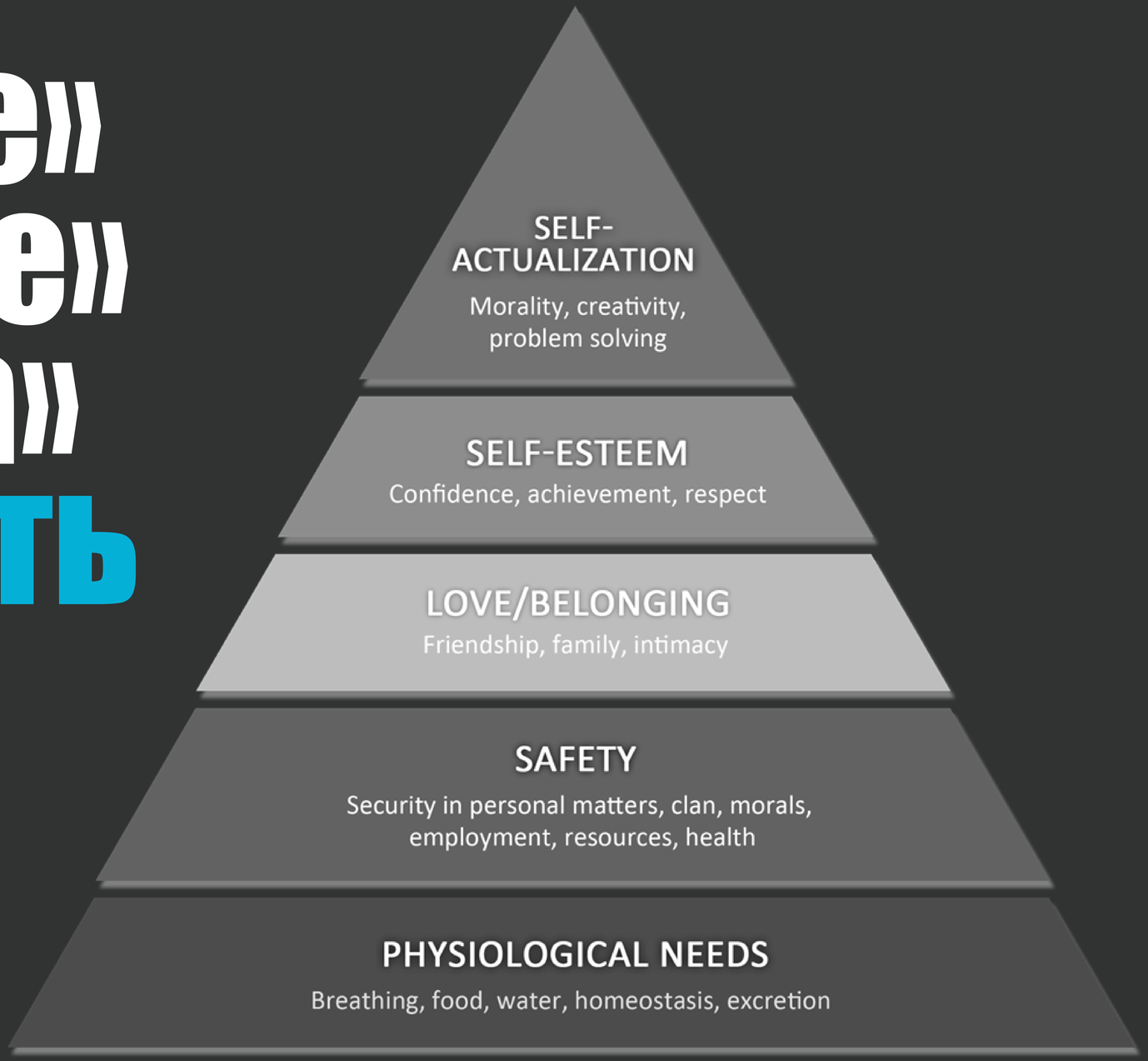
(акроним от англ. — «Страх, неуверенность и сомнение») — тактика психологической манипуляции, применяемая в маркетинге и пропаганде вообще, заключающаяся в подаче сведений о чем-либо (в частности, продукте или организации) таким образом, чтобы посеять у аудитории неуверенность и сомнение в его качествах и таким образом вызвать страх перед ним. При этом может использоваться клевета, голословные утверждения и намеки. Может применяться как для антирекламы, так и для рекламы, сея страх перед неопределенным кругом альтернативных решений. Является частным случаем апелляции к страху.

Все это приводит к порочной практике пустых затрат.
Когда все крутится ради ощущения основанного на нагнетании обстановки но поделенного на жадность.
Неплохая модель.
Так работает например рынок фармацевтики. Или страхования жизни. Единственная беда в том что фактические риски растут несоизмеримо. ИТ критически проникает в бизнес процессы.



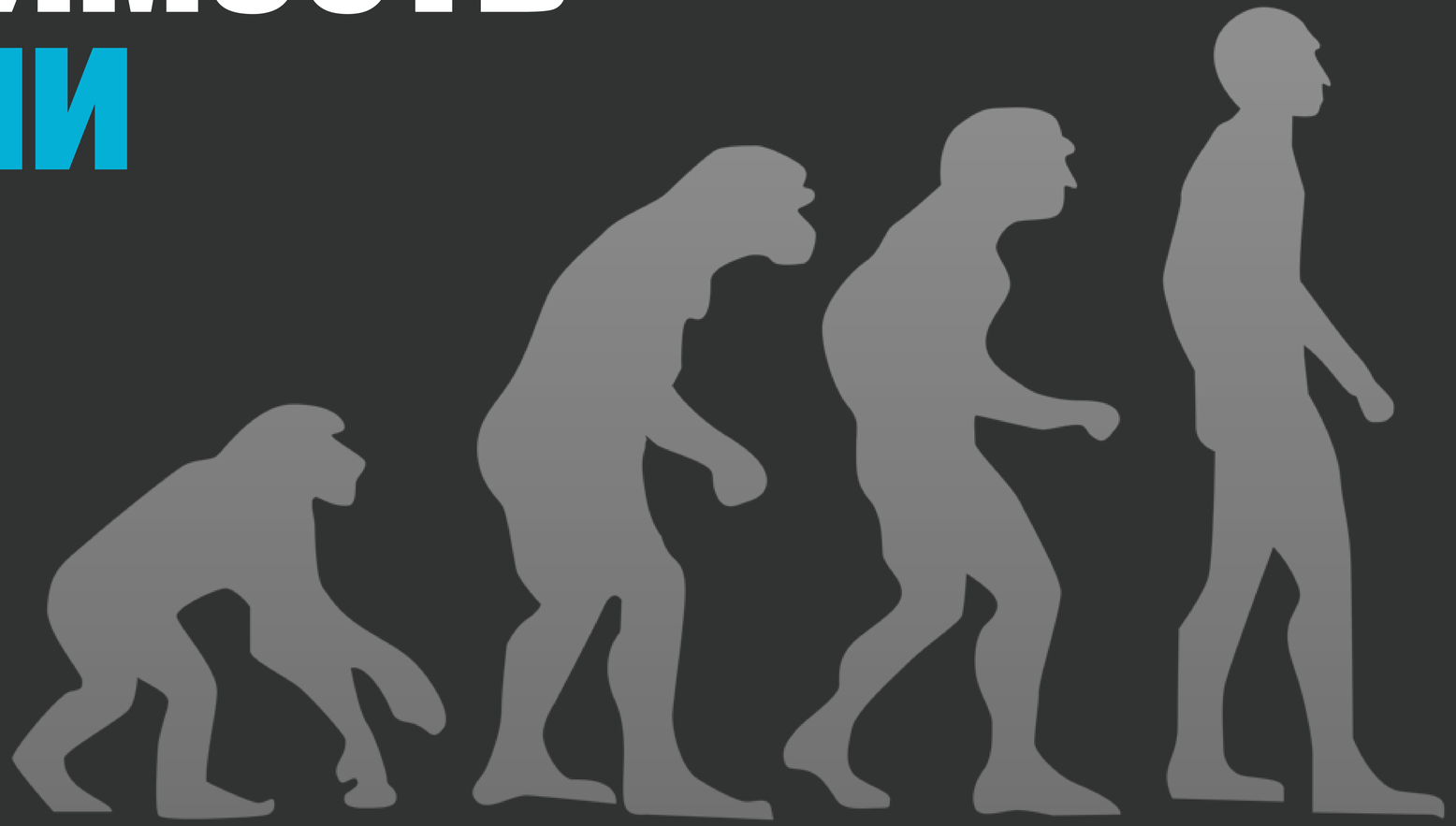
«состояние»
«ощущение»
«страховка»
потребность бизнеса?

...или же это просто потребности менеджера как конкретной личности? Средство для достижения персональных целей человека?



Необходимость эволюции

как необходимый фактор
в контексте постоянно растущих угроз



«потребность» «ощущение» «состояние» функция

например

Gartner®

говорит об этом уже несколько лет

Бизнес как система

процессы

совокупность различных видов деятельности

функции

совокупность однородных видов деятельности

виды деятельности

Функции безопасности

Возмещение потерь
минимизация ущерба
по наступившим инцидентам

Увеличение выручки
создание дополнительных
свойств безопасности для
выпускаемых продуктов

Сокращение потерь
минимизация общего количества и
снижение среднепорогового
значения стоимости инцидентов

Управление стоимостью функции
повышение эффективности
бизнес-процессов функции безопасности

Вектора деятельности функции безопасности

внутренние сервисы

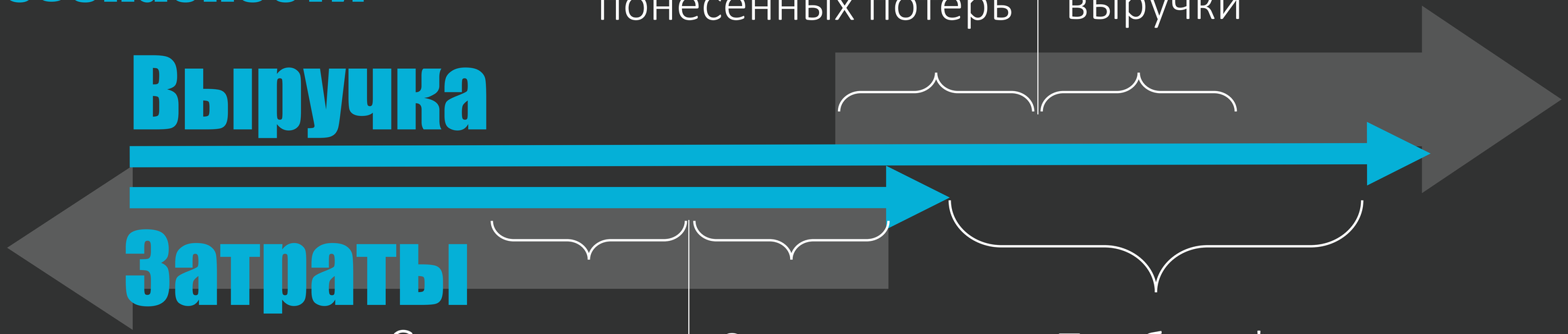
минимизация ущерба
по наступившим инцидентам

Возмещение
понесенных потерь

внешние сервисы

создание дополнительных
свойств продуктов

Увеличение
выручки



Сокращение
потерь

минимизация общего количества и снижение среднепорогового
значения стоимости инцидентов безопасности

внутренние сервисы
compliance

Стоимость
функции

повышение эффективности
бизнес-процессов функции

управление
бюджетом

Прибыль*

*если за основную цель компании
взята прибыль

Внутренние сервисы

Антивирусная защита
как сервис обеспечивающий работоспособность пользователей

1

Антиспам
как сервис снижающий нагрузку на пользователя

2

Защита от DDoS атак
как сервис обеспечивающий доступность сайта

3

WAF
как сервис обеспечивающий работоспособность сайта

4

Контроль кода
как сервис обеспечивающий сокращение времени простоя при «откатах» билдов

5

IDM
как сервис сокращения времени на заведение нового пользователя.

6

SIEM
как сервис сокращающий время реакции на инцидент

7

Доступность «зарабатывающей» инфраструктуры 99% с заданными параметрами качества

Первое правило комплаенса

Необходимо соблюдать максимум требований минимумом усилий

Второе правило комплаенса

Всегда необходимо соблюдать максимум требований минимумом усилий

Основной парадокс состоит в том, что нормы комплаенса это способ защиты государственных интересов, а не интересов бизнеса. В результате этого, нормы комплаенса становятся неким дополнительным «налогом»

Compliance

Комплаенс (англ. compliance — согласие, соответствие; происходит от глагола to comply — исполнять) — буквально означает действие в соответствии с запросом или указанием; повиновение.

Внешние сервисы

Внешние сервисы безопасности направленны на создание дополнительных свойств выпускаемого компанией продукта.

И влияют на его конкурентные свойства, а следовательно и на выручку от его реализации

Например защита данных вывела компанию Blackberry в лидеры корпоративного рынка и сделала в 2009 году самой быстрорастущей компанией в мире с ростом дохода на 84 % за три года несмотря на глобальную рецессию. За десять лет компания продала 50 миллионов смартфонов, что сделало BlackBerry вторым по популярности смартфоном в мире.

Управление бюджетом

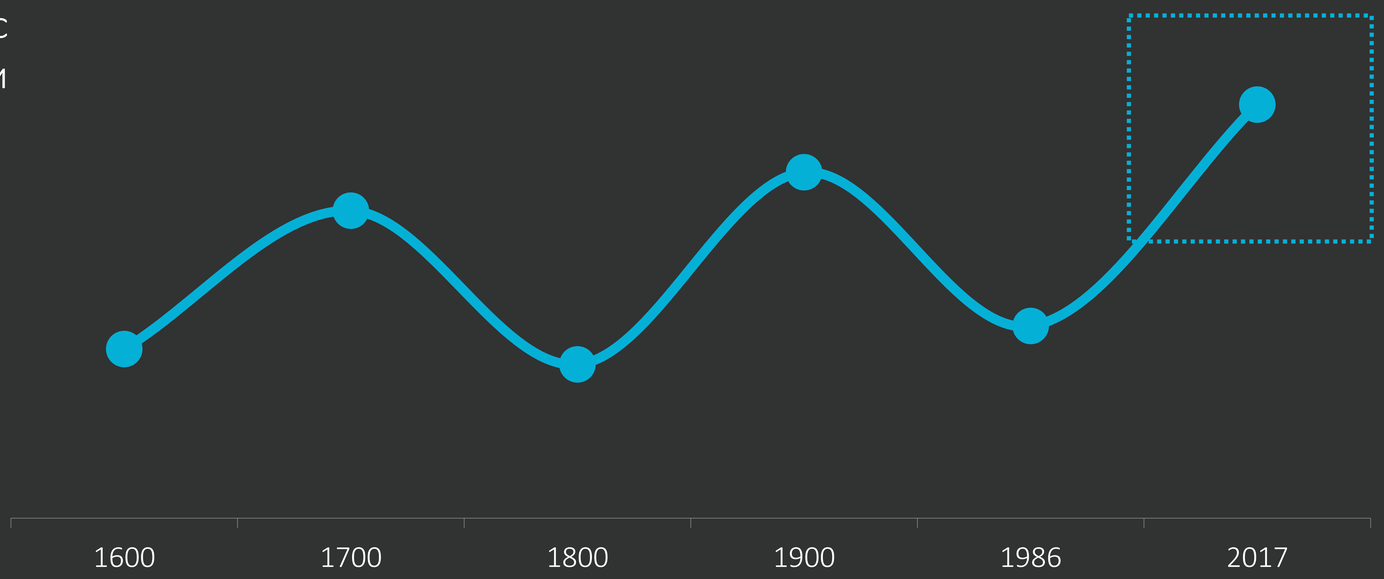
Нахождение точки баланса затрат на безопасность и эффекта от этой функции. Отдавая бюджет в управление бизнес ждет обеспечение эффективности, оптимизацию, воплощение закона Парето и т.д.

ОСТ ИНДСКАЯ КОМПАНИЯ

сформулировала основные виды и инструменты функции безопасности в 1600 г.

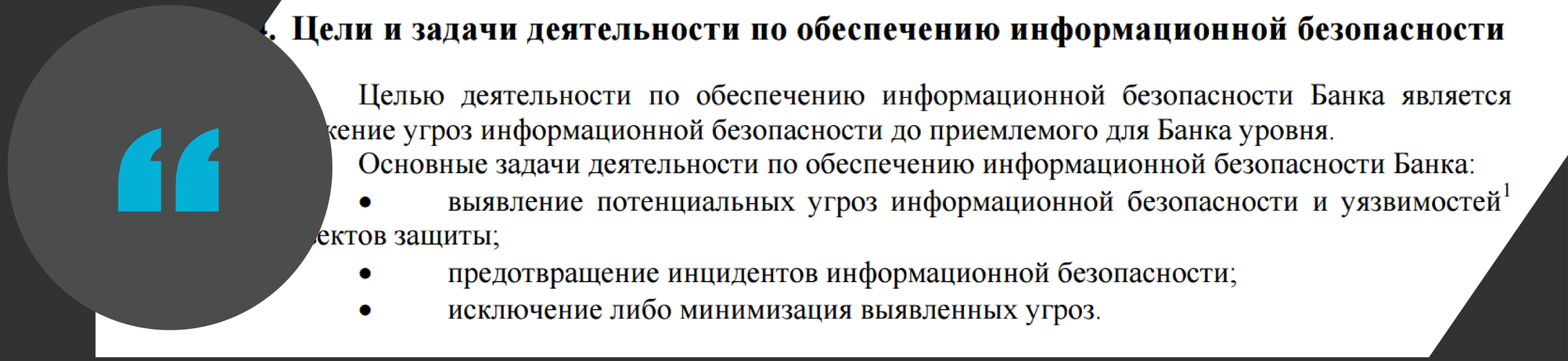
Востребованность функции

Пики приходятся на высоко-рисковые эпохи, сейчас у нас одна из таких эпох из-за развития технологий и пока мы движемся к пику - востребованность будет очень высокой. При этом возникает парадокс потребности и того что предлагают безопасники "страховщики"



* График разумеется очень и очень условный, исключительно для наглядности

Что написано в вашей стратегии безопасности*?



. Цели и задачи деятельности по обеспечению информационной безопасности

Целью деятельности по обеспечению информационной безопасности Банка является
жение угроз информационной безопасности до приемлемого для Банка уровня.

Основные задачи деятельности по обеспечению информационной безопасности Банка:

- выявление потенциальных угроз информационной безопасности и уязвимостей[1]
ектов защиты;
- предотвращение инцидентов информационной безопасности;
- исключение либо минимизация выявленных угроз.

*на самом деле сгодится любой верхнеуровневый документ определяющий вашу деятельность

Зачем?

Хочу поставить мировой рекорд

Хочу проверить силу воли

Хочу улучшить свое здоровье

Какая цель?

Пробежать 100 м за 9.8 секунд

Пробежать 21,1 км за 2 часа

Пробегать по 10 км 3 раза в неделю в течении 2-х лет

Вы бегаете?

Зачем?

Защитить персональные данные

Защитить коммерческую тайну

Защитить компанию от атак хакеров

Какая цель?

????

????

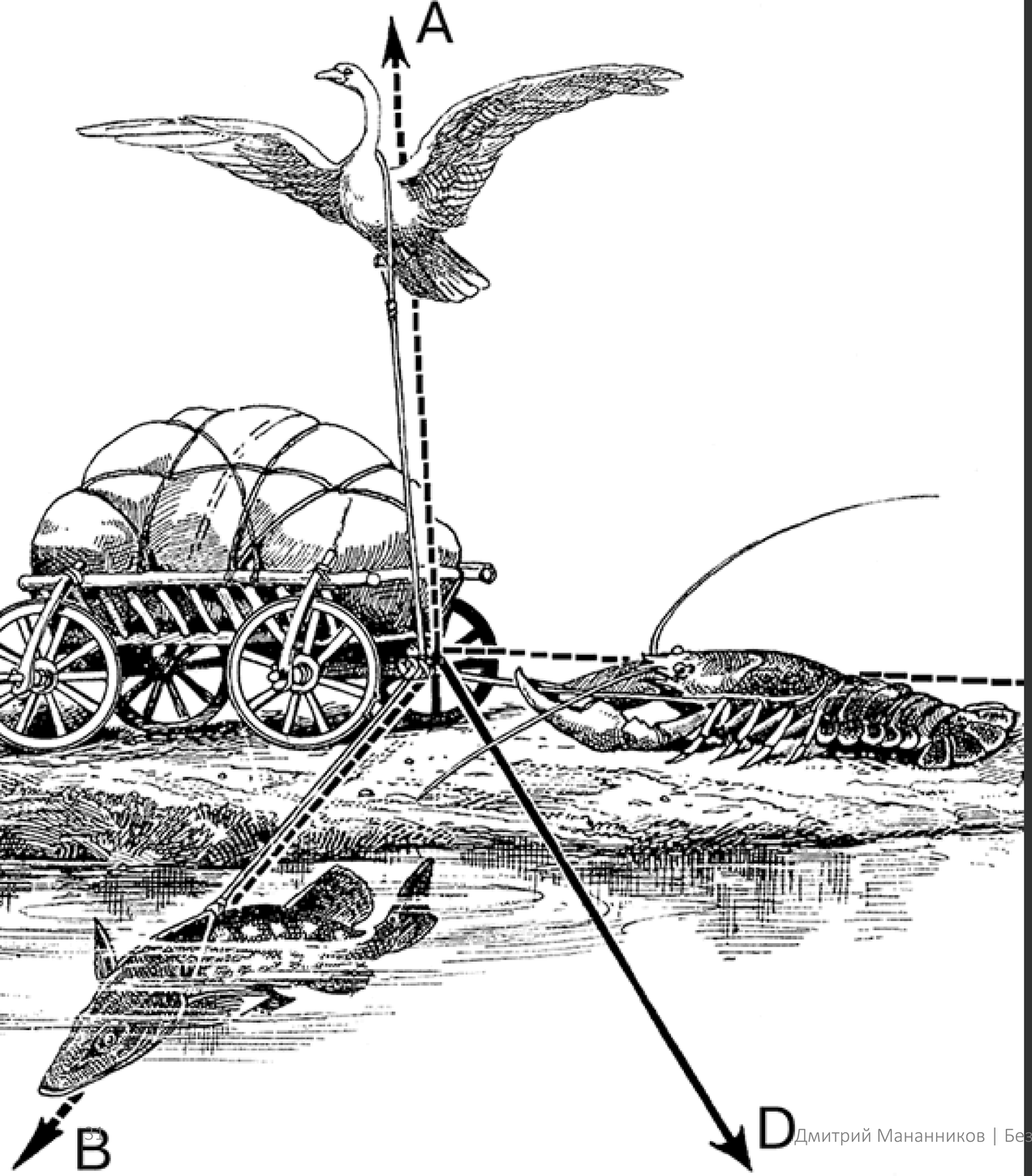
????

????

Обеспечиваете безопасность?

Субъекты бизнеса и их цели

Цель – это не просто некая мечта, а будущее, представленное в виде конкретного желаемого результата, который мы для себя сознательно выбрали и установили и планируем достигнуть к определенному моменту времени в каком-либо следующем периоде деятельности.



Может ли бизнес достигать несколько целей?

«Когда в товарищах согласья нет,
На лад их дело не пойдет,
И выйдет из него не дело, только мука.»

И.А. Крылов

Бизнес всегда определяет единую цель

EBITDA?
ВЫРУЧКА?
МАРЖА?

«Основной целью деятельности Общества является получение прибыли Обществом путем ....»

Устав ООО «Какоетоназвание»

4. Цели и задачи деятельности по обеспечению информационной безопасности

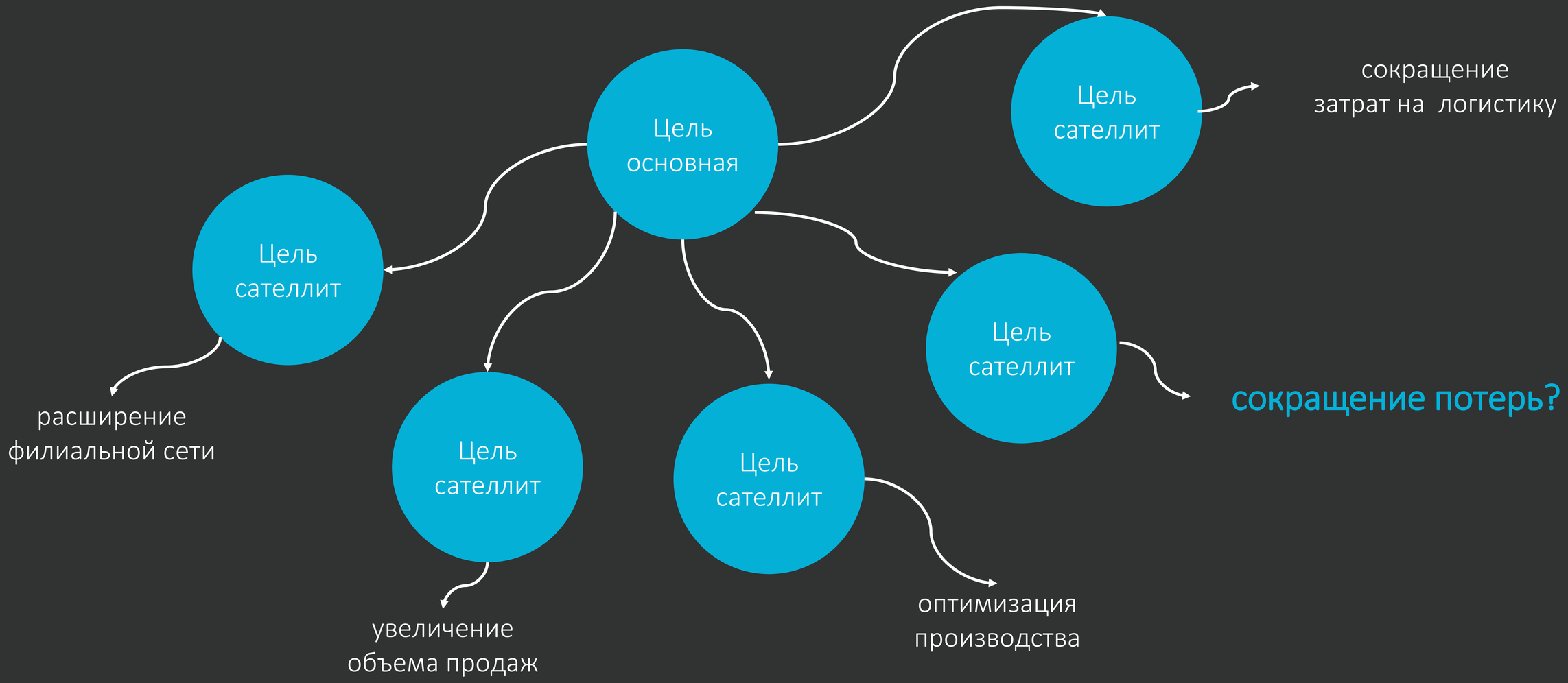
Целью деятельности по обеспечению информационной безопасности Банка является снижение угроз информационной безопасности до приемлемого для Банка уровня.

Основные задачи деятельности по обеспечению информационной безопасности Банка:

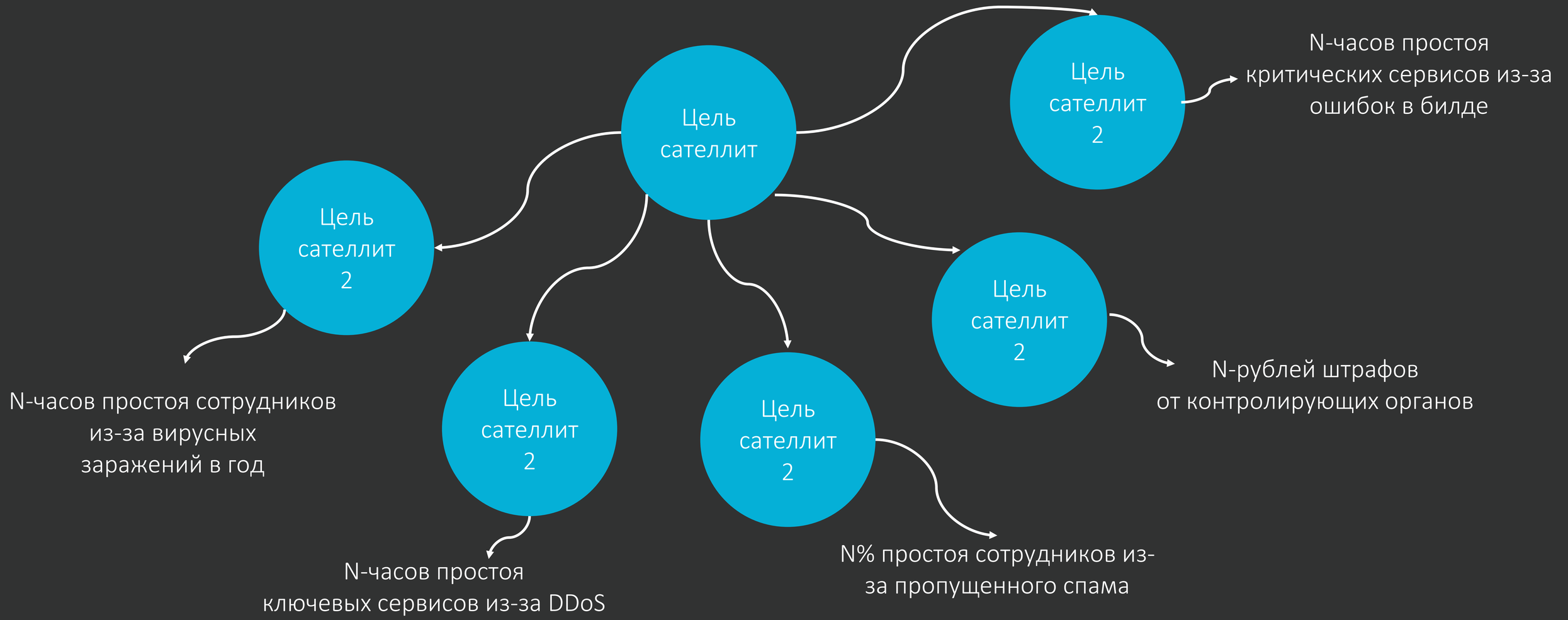
- выявление потенциальных угроз информационной безопасности и уязвимостей[1] объектов защиты;
- предотвращение инцидентов информационной безопасности;
- исключение либо минимизация выявленных угроз.

В вашем случае цель безопасности совпадает с целью бизнеса?

Основная цель - увеличение прибыли



Цель сателлит - сокращение потерь



Управление по целям

процесс согласования целей внутри организации таким образом, что руководство компании и сотрудники разделяют цели и понимают, что они означают для организации.

Термин «Управление по целям» впервые был введён и популяризирован Питером Друкером

в 1954 году в книге «The Practice of Management».

*на картинке не Друкер а Джеферсон, просто что бы убедится что вы читаете текст на слайдах

S.M.A.R.T.

Specific - специфичные для организации
Measurable - измеримы
Achievable - достижимы, реалистичны
Result-oriented - ориентированы на результат, не на усилия
Time-based - ограничены во времени

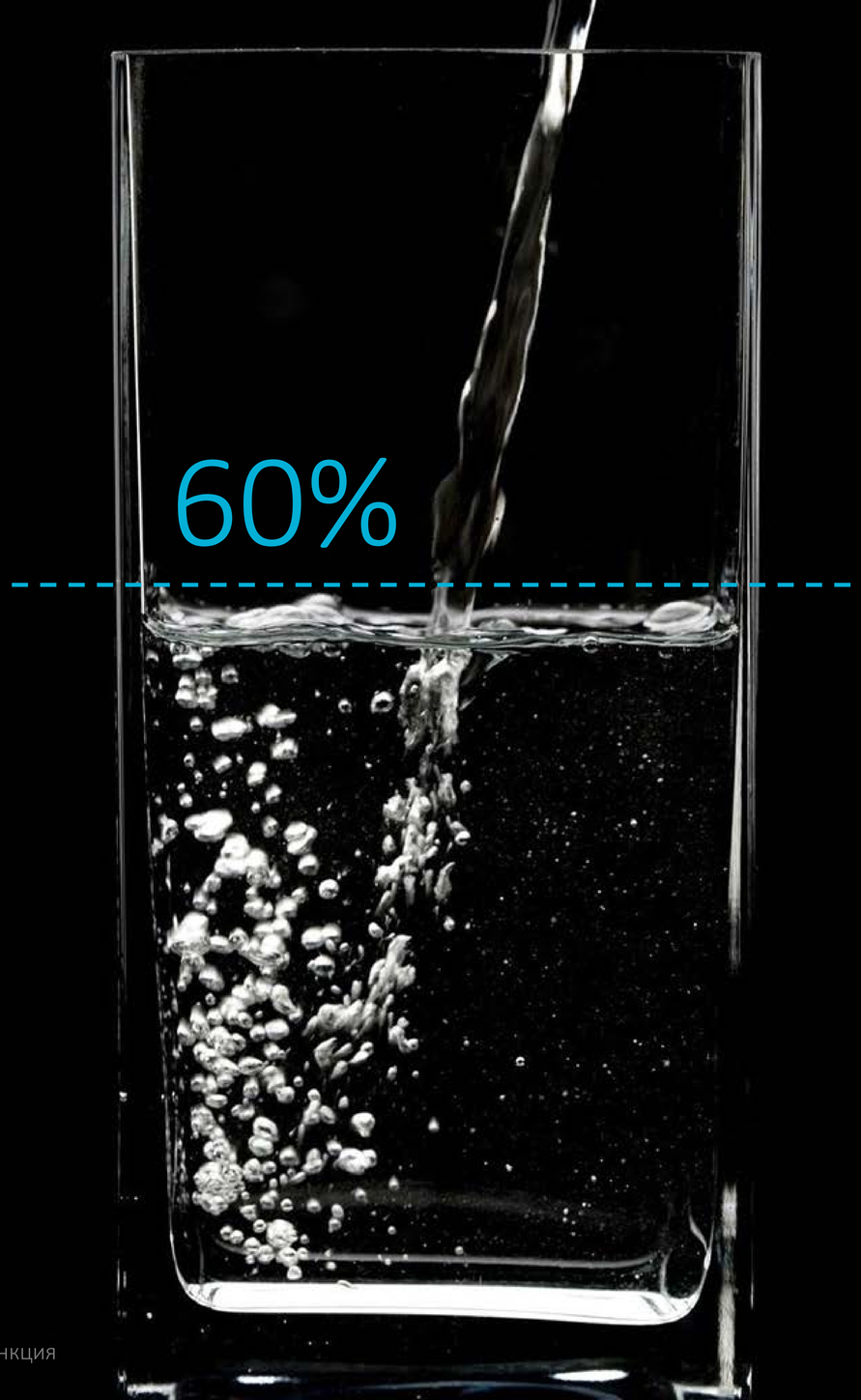
Может ли быть целью желание «стать лидером рынка»? или «обеспечение безопасности компании»

Цели носящие качественный характер неизмеримы. Перевод их в количественное выражение означает установление числа единиц в которых будет измеряться результат

Единицы из которых будут состоять наша цель – есть показатель.
Показатель - величина, позволяющая судить о состоянии объекта.

Например – «снижение логистических расходов на 20% относительно прошлого периода» или «снизить логистические расходы до 10 000 рублей на тонну перевозимого груза»

Цель без показателя – просто предмет результата который нужно получить
Показатель без цели – просто число, не имеющее смысла



«простых» шагов

На этом разумеется все не заканчивается, а только начинается. Данный момент это базис – корреляция целей бизнеса с целями безопасности, на котором можно построить систему позволяющую оценивать ее эффективность, делать экономическую оценку, закрепить ключевые показатели, построить систему мотивации, участвовать в инвестиционных программах на паритетных началах и многое другое

Спасибо за внимание!

Готов ответить на вопросы!

dmitriy.manannikov