

Страхование как инструмент управления киберрисками

Как оценить финансовый ущерб от кибератаки, распределить риск между бизнесом и страховщиком и обеспечить устойчивость компании после инцидента

Дмитрий Болтенков

руководитель направления страхования
информационных рисков

Ингосстрах



Четыре шага от риска к устойчивости бизнеса

- 01 Киберриск изменился
- 02 ИБ и страхование — не альтернативы
- 03 Что и как страхуется
- 04 Как это работает на практике

Атака — это не утечка данных. Это остановка бизнес-процесса и денежного потока.

Защита снижает вероятность инцидента.
Страхование управляет остаточным финансовым риском.

Собственные убытки и расходы, включая убытки от простоя (Business Interruption), ответственность за ущерб третьим лицам.

Андеррайтинг, определение лимита, первые 24 часа после инцидента и куда движется рынок.



Что произойдёт с бизнесом, если критическая
ИТ-система перестанет работать на 24+ часа?

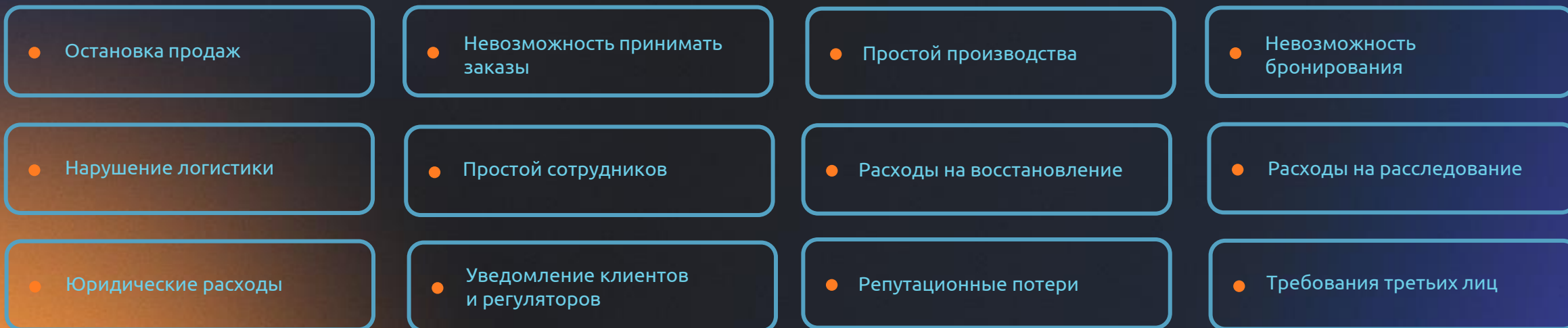
Не «что случится с сервером», а что случится с продажами, клиентами и деньгами компании



Кибератака — это остановка бизнеса, а не строчка в ИБ-отчёте



Реальные последствия инцидента шире, чем «утечка данных»:



ИБ ≠ управление финансовым последствием инцидента

ДАЖЕ ЕСЛИ У КОМПАНИИ ЕСТЬ

SOC

EDR

SIEM

MFA

Резервное
копирование

Сегментация
сети

Антивирус

Pentest

Обучение
сотрудников

риск не становится нулевым

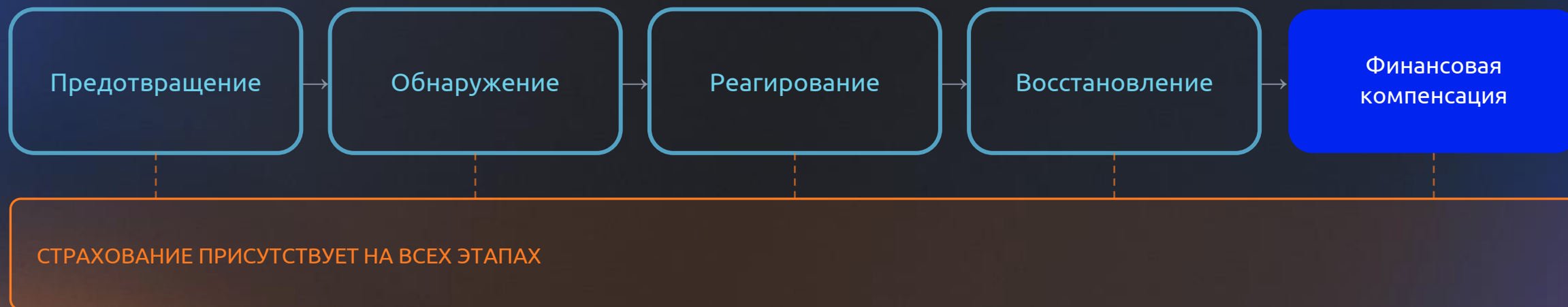
КЛЮЧЕВАЯ ИДЕЯ

**ИБ снижает вероятность
и масштаб инцидента**

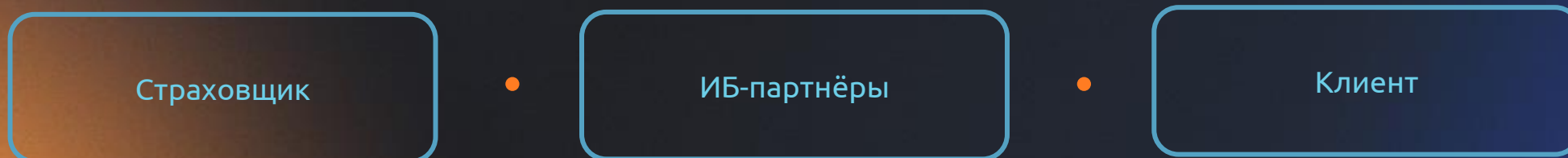
**Страхование управляет
остаточным финансовым риском**

*Это не противопоставление, а разделение труда внутри
одной системы управления риском*

Страхование — часть системы, а не действие «после атаки»



Современная модель управления киберриском — это не «страховщик приходит после атаки», а единая система:



Что реально страхуется

СОБСТВЕННЫЕ УБЫТКИ

- Простой и потеря прибыли / маржи
- Дополнительные расходы на ведение бизнеса
- Восстановление данных и систем
- Расходы на реагирование, минимизацию, локализацию
- Уведомление субъектов персональных данных
- PR- и кризисные коммуникации
- Юридические расходы
- Расходы при ransomware — в рамках применимого законодательства и условий полиса

ОТВЕТСТВЕННОСТЬ ПЕРЕД ТРЕТЬИМИ ЛИЦАМИ

- Требования клиентов
- Требования партнёров и контрагентов
- Требования субъектов персональных данных
- Требования регуляторов — в рамках применимого законодательства

Оговорка

Штрафы регуляторов не подлежат страхованию по российскому праву.

Для бизнеса самый большой ущерб чаще возникает не из-за стоимости восстановления техники, а из-за остановки бизнес-процесса

Кейс: атака на страховую компанию, ноябрь 2025

- **С ЯНВАРЯ 2025**
Группировка вела кампанию атак на российские организации; в СК проникла через скомпрометированного партнёра — аудиторскую компанию
- **11–12 НОЯБРЯ**
Массированная атака на ИТ-инфраструктуру: повреждена вся виртуальная инфраструктура, уничтожена часть резервных копий
- **НОЯБРЬ–ДЕКАБРЬ**
Простой сервисов почти 3 недели: недоступны ОСАГО, КАСКО, ДМС и почта; клиентов перевели на бумажный документооборот
- **РАСКРЫТО ПОЗЖЕ**
Совет директоров компании публично признал: бюджет на кибербезопасность был недостаточным для риска такого масштаба

Атаку пережил сам страховщик — напоминание, что дисциплину киберзащиты андеррайтинг требует не только от клиентов

ОФИЦИАЛЬНО РАСКРЫТЫЙ УЩЕРБ

900 млн ₽

данные раскрыты самой компанией — редкий случай точной цифры на российском рынке

~3 недели

на восстановление инфраструктуры и сервисов

Через подрядчика

точка входа — скомпрометированный партнёр-аудитор

Ещё четыре распространенных сценария

1 Ransomware

Шифрование серверов → остановлены ERP/CRM → остановлены продажи → простой → восстановление → доп. расходы

Фб: свыше 450 атак на компании РФ в 2025 г., выкупы 4–40 млн Р. Кейс «Винлаб»: простой сети магазинов, прямые убытки около 1,5 млрд Р

2 Утечка данных

Компрометация базы → расследование → уведомления субъектов → требования третьих лиц → репутационные потери

Роскомнадзор: в 2024 г. — 135 утечек / 710+ млн записей; с 30.05.2025 действуют оборотные штрафы за повторные нарушения

3 DDoS

Сайт или приложение недоступны → невозможно совершать операции → прямая потеря продаж

RED Security: число DDoS-атак на бизнес в РФ в 2025 г. выросло в 2,7 раза, до 186 тыс. инцидентов

4 Компрометация подрядчика

Атакован IT-поставщик → недоступна критическая система компании → бизнес останавливается

Атаки на цепочки поставок — одна из наиболее распространённых угроз для бизнеса РФ в 2025 г. (BI.ZONE)

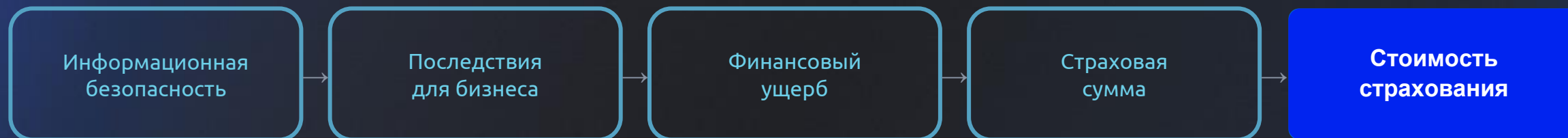
Киберстрахование начинается не с полиса

- 1 Что критично для бизнеса?
- 2 Что произойдёт при остановке этого критичного?
- 3 Сколько стоит час простоя?
- 4 Какие сценарии наиболее вероятны?
- 5 Что компания может предотвратить сама?
- 6 Какой остаточный риск можно передать страховщику?
- 7 **Какая страховая сумма действительно нужна?**

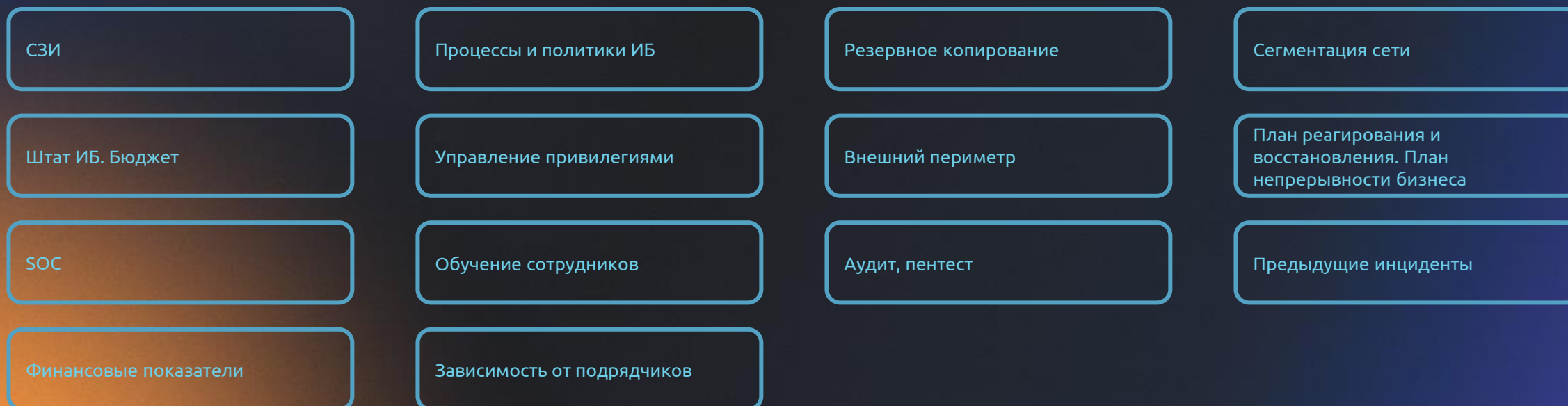
ЭТО НЕ ПОКУПКА ПОЛИСА

Это методика управления риском, результат которой — обоснованная страховая сумма и осознанное решение, что компания оставляет на себе, а что передаёт страховщику.

Андеррайтинг — это не просто анкета



Факторы, которые оценивает страховщик:



У двух компаний одинаковая ИБ — но разный страховой риск

Компания А

ИНТЕРНЕТ-МАГАЗИН

~20 млн ₽

продаж в день

Простой сайта = прямая потеря продаж

Компания Б

ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ

ERP

система управления производством

Простой ERP = остановка производственной линии

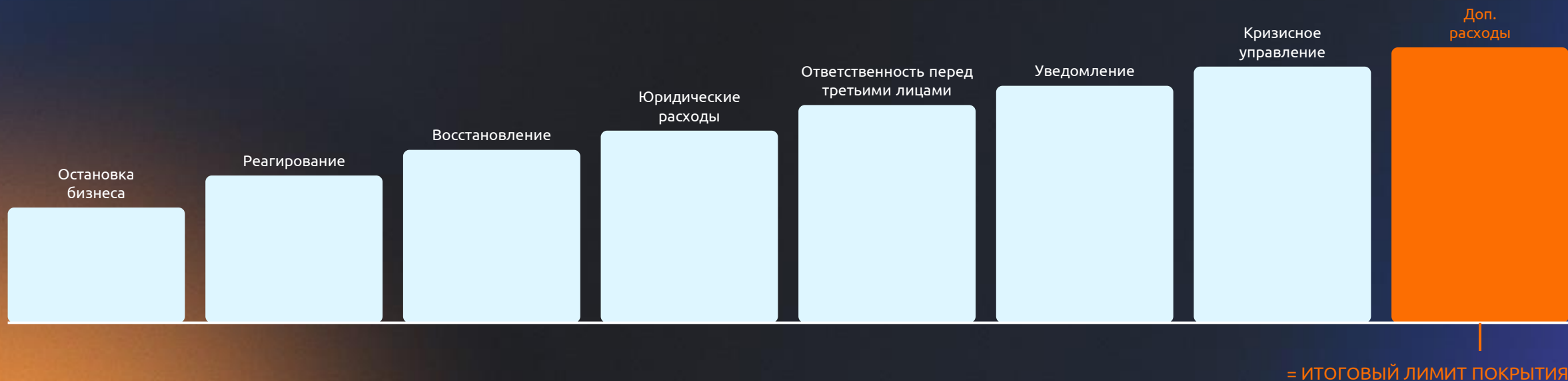
Одинаковый уровень ИБ ≠ одинаковый страховой риск.

Главный фактор — что происходит с бизнесом, когда ИТ перестаёт работать.

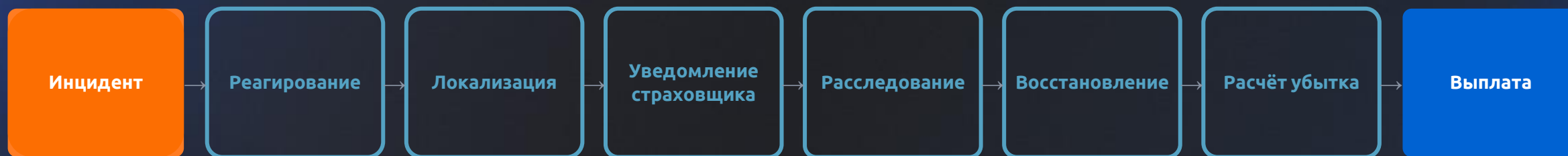
Как определить лимит: не «оборот × процент», а PML

✗ «У нас оборот 10 млрд ₽, значит лимит — 500 млн ₽» — так страховая сумма не определяется

Правильная модель Максимальный возможный ущерб / Вероятный максимальный ущерб / Воздействие на бизнес.
Страховая сумма складывается из компонентов.



Ценность страховщика проверяется не при покупке полиса



ХОРОШИЙ ДОГОВОР СТРАХОВАНИЯ — ЭТО НЕ ТОЛЬКО НИЗКИЙ ТАРИФ

Страховая сумма + Скорость + Экспертиза + Партнеры = Качественное урегулирование

Качество страховой услуги проверяется не в момент подписания договора, а в первые часы после инцидента

Куда движется киберстрахование

- От страхования последствий к предотвращению

- Интеграция страховщика и ИБ-провайдеров

- Более точный расчёт ущерба

- Мониторинг внешнего периметра

- AI в андеррайтинге и урегулировании

- Динамическое ценообразование

- Сервисные подписки вместо разового полиса

- Страхование облачных рисков

- Страхование зависимости от подрядчиков

Полис будущего — это не документ, который лежит в сейфе. Это сервис, который сопровождает компанию до, во время и после киберинцидента.

Кибербезопасность снижает вероятность инцидента

Киберстрахование снижает его финансовые последствия

Управление киберриском — это работа с обеими составляющими

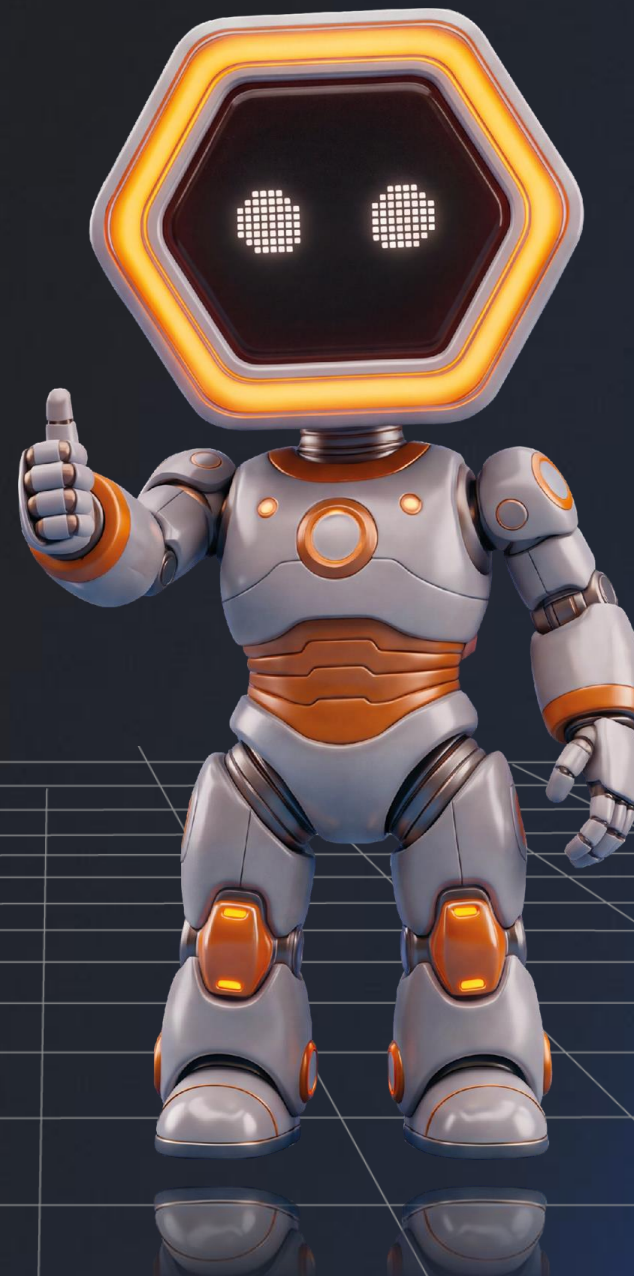
СТРАХОВАНИЕ КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ КИБЕРРИСКАМИ

Благодарю за внимание!

Дмитрий Болтенков

руководитель направления страхования
информационных рисков

Ингосстрах



Ampire 360°