# Управление Рисками в ИБ

**Вотинцев Кирилл**

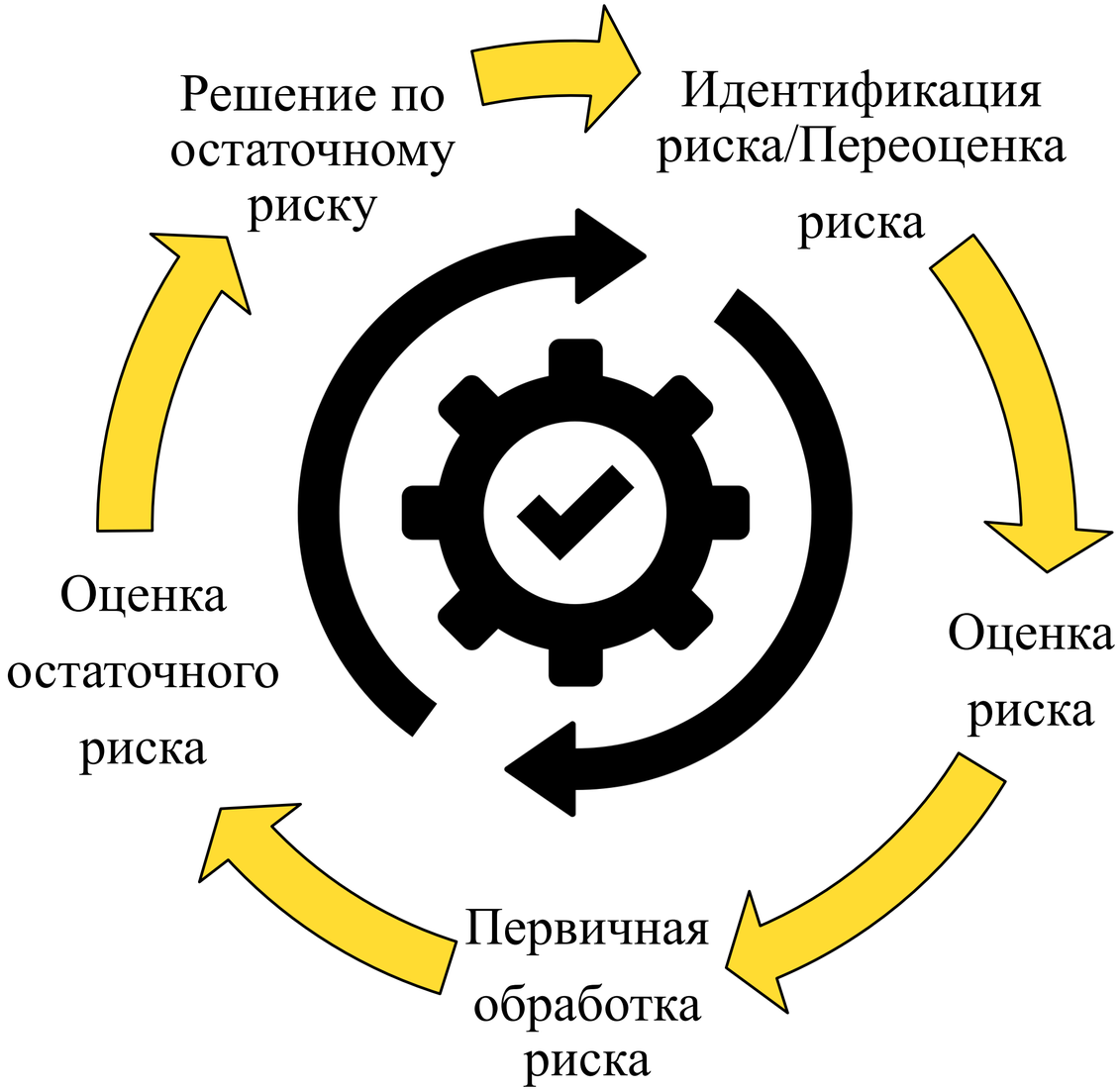
ТИНЬКОФФ

# Что такое риск?

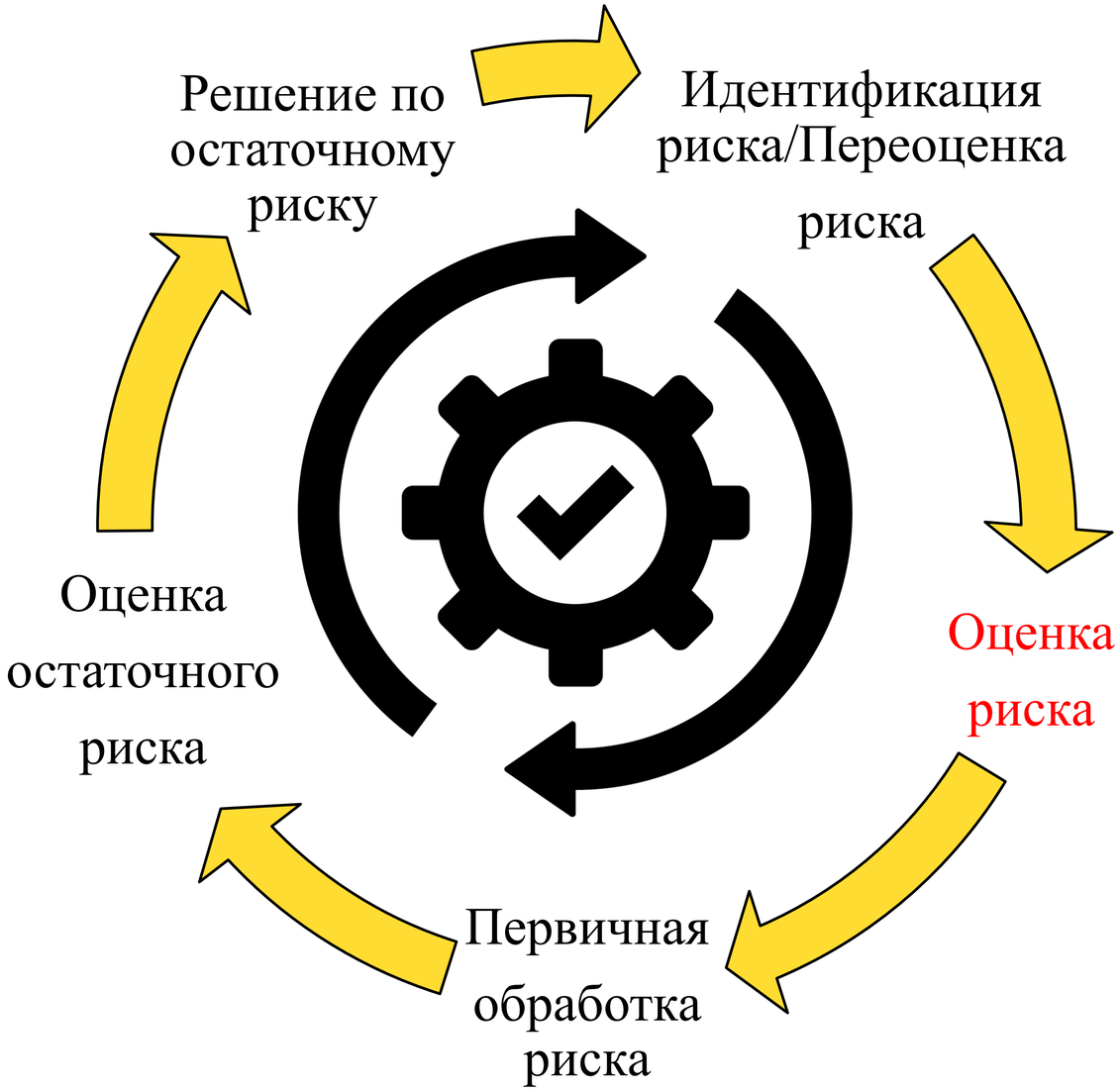
Риск = Вероятность × Ущерб

# Что делать с рисками?

# Цикл процесса управления рисками



# Цикл процесса управления рисками



# Что самое важное в оценке рисков?

# Понятность!

# Ошибки оценки рисков

Исходить  от последствий, забывать про вероятность

# Ошибки оценки рисков

Перестраховаться

На всякий случай,
а то вдруг что…

# Ошибки оценки рисков

При оценке вероятности не учитывать период времени

# Что нужно учесть в процессе оценки рисков

Вероятность:
мотивация злоумышленника

Основной вопрос:
Были попытки реализации сценария?

# Что нужно учесть в процессе оценки рисков

Вероятность:
Оценка систем защиты

Основные вопросы:
Как трудно реализовать сценарий в условиях вашей системы?
Что даст реализация злоумышленнику?

# Что нужно учесть в процессе оценки рисков

Ущерб:
Репутационный ущерб

Учесть:
Ущерб в глазах акционеров
Ущерб в глазах регулятора
Ущерб в глазах клиентов

# Что нужно учесть в процессе оценки рисков

Ущерб:

Финансовый ущерб

Учесть:

Неполученную выгоду

Потери компании

Потери партнеров

Потери клиентов

# Что нужно учесть в процессе оценки рисков

Сформировать модель оценки риска, в которой правильно расставить приоритеты при оценке вероятности и ущерба

Учесть:
Не забыть об ошибках при оценки рисков ☺
Особенности вашей компании: риск-аппетит

Забыть:
Субъективную эмоциональность, влияющую на результат процесса оценки

# Как управлять рисками?

# Риск-ориентированное Бизнес-Партнерство

Процесс, выстроенный совместно Бизнесом и Безопасностью, целью которого является управление рисками ИБ, присущими Бизнесу

# Риск-ориентированное Бизнес-Партнерство: как начать?

## Вход в процесс

- [x] Утвердить формат рисков
- [x] Определить зоны ответственности
- [x] Оценить риск-аппетит
- [x] Понять и разделять философию Бизнеса

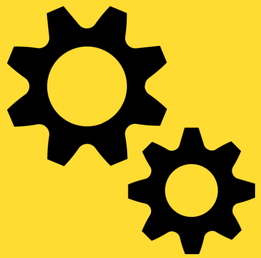
## Договориться

# Риск-ориентированное Бизнес-Партнерство: что учесть?

Стек технологий

Требования Бизнеса

Процессы



Люди

# Риск-ориентированное Бизнес-Партнерство: инструменты

01 ДИАЛОГ

02 ГИБКОСТЬ

03 ТРЕБОВАНИЯ

04 ОБРАТНАЯ СВЯЗЬ

# Риск-ориентированное Бизнес-Партнерство: залог успеха

- ✓ Говорить на языке собеседника
- ✓ Думать как Бизнес
- ✓ Добиться слияния Бизнеса и безопасности
- ✓ Запрашивать и работать с обратной связью
- ✓ Давать обратную связь и мониторить ее эффективность
- ✓ Глубоко понимать как функционирует Бизнес
- ✓ Никогда не говорить «нельзя», не предложив альтернатив
- ✓ Четко определить баланс между риск-аппетитами и допустимой границе рисков, постоянно выдерживать его
- ✓ Быть исчерпывающим и лаконичным одновременно
- ✓ Быть проактивным
- ✓ Быть поставщиком решений

# Риск-ориентированное Бизнес-Партнерство: залог провала

- Говорить на своем языке всегда и со всеми
- Думать как технический специалист
- Разделять Бизнес и Безопасность
- Не запрашивать или игнорировать обратную связь
- Не давать обратной связи коллегам
- Вникать только в те аспекты Бизнеса, с которыми приходится работать
- Давать отказы, не предлагая разумных альтернатив
- Не учитывать риск-аппетиты Бизнеса или недооценивать риски
- Быть многословным и непонятным
- Работать от задаче к задаче
- Быть поставщиком проблем и задач

# Риск-ориентированное Бизнес-Партнерство: требования

- Персональная ответственность
- Эффективный менеджмент
- Продвинутые коммуникации
- Проактивность

# Риск-ориентированное Бизнес-Партнерство: требования

Стоимость решения по риску не должна быть выше стоимости потерь от реализации риска!

# Риск-ориентированное Бизнес-Партнерство: плюсы/минусы

## Плюсы

- ⊕ Гибкость
- ⊕ Масштабируемость
- ⊕ Результативность
- ⊕ Экономическая эффективность

## Минусы

- ⊖ Требования к менеджменту
- ⊖ Требования к персоналу
- ⊖ Ограничение применения

# СПАСИБО ЗА ВНИМАНИЕ!

**Вотинцев Кирилл**
**Security Partner**
**k.votintsev@tinkoff.ru**

# Мастер класс по управлению рисками в ИБ

## Простые правила

- ☑ 3 команды
- ☑ 3 недетерминированных кейса
- ☑ Максимум коммуникаций: общаемся, спрашиваем, уточняем
- ☑ Нет правильных ответов и найти их не сама цель ☺

# Мастер класс по управлению рисками в ИБ

## Команда №1: ИТ-стартап

Ваш бизнес – это облачный b2b сервис, приложение по доставке продуктов/еды для клиентов-физлиц. Суть приложения: под брендом заказчика вы делаете удобный интерфейс заказа/оплаты/отслеживания. Приложение скачивается из store/market. Общение с заказчиком по API. Бизнес работает 8 месяцев, есть два достаточно крупных заказчика, несколько поменьше и еще с рядом компаний ведутся переговоры. Заказчики регулярно приносят требования и задача стартапа постараться сделать как можно больше унифицированных решений, чтобы избежать высоких издержек на кастомизацию.

1. Co-founders: CEO, CTO
2. Штат из 10-12 разработчиков/тестировщиков, с планами набора до 50% за год (зависит от переговоров)
3. Еще человек 8-10 околоИТ: администраторы, аналитики, UX, продуктовики, с планами набора до 30% за год
4. Бухгалтерия/кадры/HR/юристы и т.д. на аутсорс
5. Продакшн инфраструктура в облаке, разработка в своей сети, сотрудники работают удаленно
6. Единственный безопасник в компании это вы ☺. В стартапе вы появились после того как один из клиентов упомянул что-то о безопасности в переговорах. Ваша задача определена как сделать приложение безопасным.

# Мастер класс по управлению рисками в ИБ

## Команда №2: финтех

Ваш бизнес – это банк, переходящий на этап финтеха. Есть отделения в крупных городах, банкоматная сеть, два ЦОД, свой процессинг и бэкофис. Также есть мобильное приложение, которое ранее писала аутсорс-команда, но Правлением было принято решение делать inhouse решение силами своей ИТ команды разработки. В связи со сменой команды разработки есть проблемы с доступностью приложения и/или его отдельных функций. Основной проект на текущий момент – смена формата, отказ от части офисов и максимальный переход в онлайн. Нагрузка на ИТ банка очень высока: приоритеты только на бизнесовые задачи,  ресурсов не хватает даже на них, большая очередь из регулярных задач. Много социальной инженерии из-за особенностей UX приложения.

1. В банке есть команда ИБ. Структура ИБ подчинена зампреду правления по ИТ и ИБ
2. Команда ИБ состоит из администраторов средств ИБ (DLP, FW, Antifraud), есть один методист для управления документацией (политики, регламенты и т.д.), два аудитора ИБ, несколько аналитиков. SOC – на аутсорс
3. Исторически в банке сложные отношения ИТ и ИБ
4. Вы – новый руководитель ИБ. Задачи, которые необходимо выполнить в ближайшие полгода: подготовиться к проверке ЦБ по ГОСТ (ранее этой задачей толком не занимались и по оценкам сделано не более 20-30% задачи), обеспечить безопасность нового приложения, снизить фрод по социальной инженерии

# Мастер класс по управлению рисками в ИБ

## Команда №3: аэропорт

Ваш бизнес – это аэропорт. Компания осуществляет управление авиагаванью в крупном городе. Инфраструктура аэропорта обеспечивает работу диспетчеров, обеспечивающих управление воздушным движением. Организована интеграция с авиакомпаниями, работающими в аэропорту, и службами, осуществляющими предусмотренные процедуры авиабезопасности. Большинство вопросов между сотрудниками авиакомпаний и аэропорта решаются по электронной почте. Инфраструктура исторически разделена «защищенную», где организовано взаимодействие с диспетчерами и ведомствами и «незащищенную», где работают сотрудники, развернут сайт с онлайн-табло, получающем информацию из инфраструктуры диспетчеров. Команда ИТ общая для всех систем аэропорта.

1. ИТ-инфраструктура обновляется в соответствии с Бизнес-планом раз в 7 лет, обновлялась 4 года назад
2. В целом основным направлением деятельности Генеральный директор аэропорта считает хозяйственную, обеспечивающую основную деятельность: вылет-посадку самолетов, заправку судов, погрузку/разгрузку и т.д. Вопросы ИТ его волнуют только в части обеспечения основной деятельности.
3. Предыдущий ИБ специалист появился в компании согласно требованию Бизнес-плана собственника, занимался подготовкой документации по ИБ, в чем преуспел – в аэропорту полный набор нужных документов. Другими вопросами почти не занимался.
4. Вы не работали в авиаотрасли, но вам поставлена задача повысить безопасность «незащищенной» части сети

# Мастер класс по управлению рисками в ИБ

## Кейс №1: первая встреча с вашим руководителем

Руководитель попросил вас сформулировать основные 3 направления деятельности, которые вы можете предложить после экспресс-знакомства с ситуацией в вашей компании. На основе имеющейся информации проведите идентификацию рисков, оцените их и назовите 3 наиболее критичных.

# Мастер класс по управлению рисками в ИБ

## Кейс №2: публикация информации об уязвимости в оборудовании

В публичном доступе появилась информация о найденной уязвимости в сетевом оборудовании, используемом вашей компанией. Известно, что эксплуатация уязвимости позволяет получить копию трафика, проходящего через устройство, но не позволяет получить управление к нему. Устранение уязвимости вендором займет один год. Быстрое решение – переход на новую версию прошивки, которая будет стоить 150000 рублей на одно устройство. Для сравнения само устройство стоит 1 млн рублей. В парке организации №1 – 5 устройств, в парке организации №2 – 87 устройств, в парке организации №3 – 31 устройство. Что вы предпримете в такой ситуации?

# Мастер класс по управлению рисками в ИБ

## Кейс №3: индивидуальный случай в каждой компании

Для компании №1: Топовый заказчик просит убрать вход по логину и паролю в приложение, обосновывая это тем, что так лучше для пользователей. Ваше руководство в целом не против сделать доработку, т.к. заказчик важный. Сложность в том, что другие заказчики не хотели такой доработки, но если предложить, то может быть согласятся и мы получим унифицированное решение. Как лучше воздействовать на ситуацию с позиции рисков ИБ?

Для компании №2: ИТ-Директор сообщил, что задачу по установке антивирусов на Unix сервера он не сможет сделать до проверки ЦБ из-за высокой загрузки задачами от Бизнеса. Также ваш методист сказал, что не может подготовиться к проверке ЦБ без помощи аналитиков, которые занимаются проблемами антифрода. Что можно предложить сделать?

Для компании №3: Вы точно знаете, что сотрудники компании получали фишинговые рассылки, открывали письма и проходили по ссылкам. Никаких серьезных последствий это не имело, но есть тенденция на учащение рассылок. Решить задачу можно инфраструктурно – выделить критичные объекты в автономную сеть, купив оборудование, развернув его силами ИТ в течение 6-9 месяцев. Можно купить новый антивирус, который лучше предыдущего, но гарантий перехвата постоянно обновляющихся вирусов нет, развернуть можно в течение 2-3 месяцев. Также можно запустить программу обучения сотрудников и обучить всех сотрудников за 2-4 недели. Стоимость решений: 10 млн. рублей за оборудование, 5 млн. рублей за антивирус, 0,5 млн. рублей за обучение. Что вы предложите?