КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | Минск

10.11.2022

ТИНЬКОФФ

Управление Рисками в ИБ

Кирилл Вотинцев

Security business partner Тинькофф

Что такое риск?

Риск = **Вероятность** × **Ущерб**

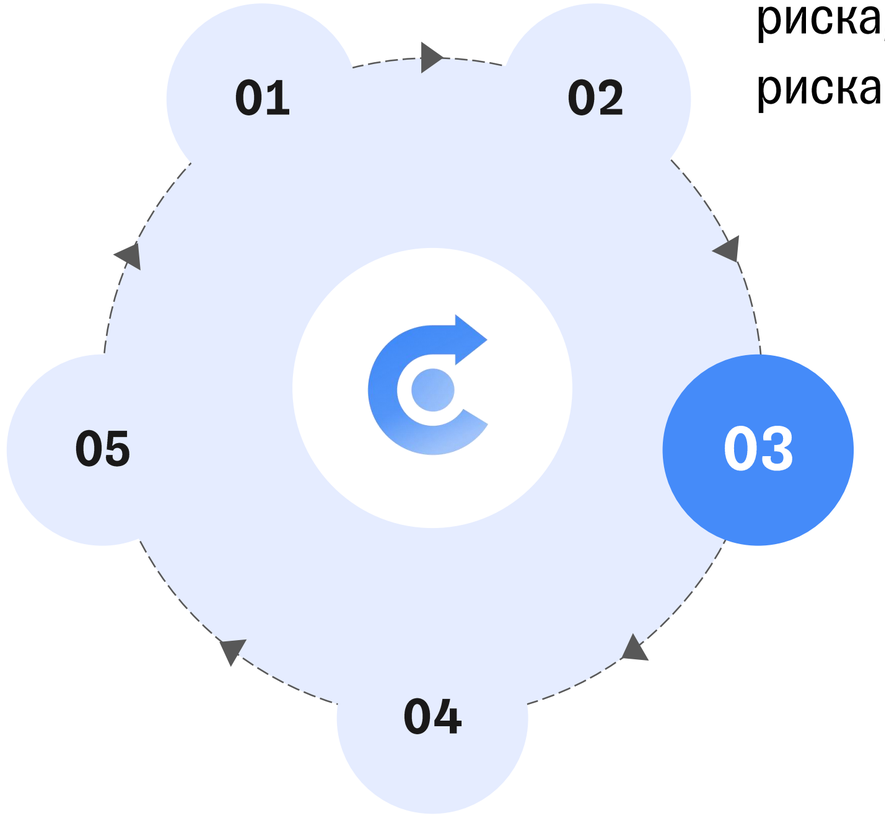
Что делать с рисками?

Цикл процесса управления рисками

Цикл процесса управления рисками

Решение по остаточному у риску

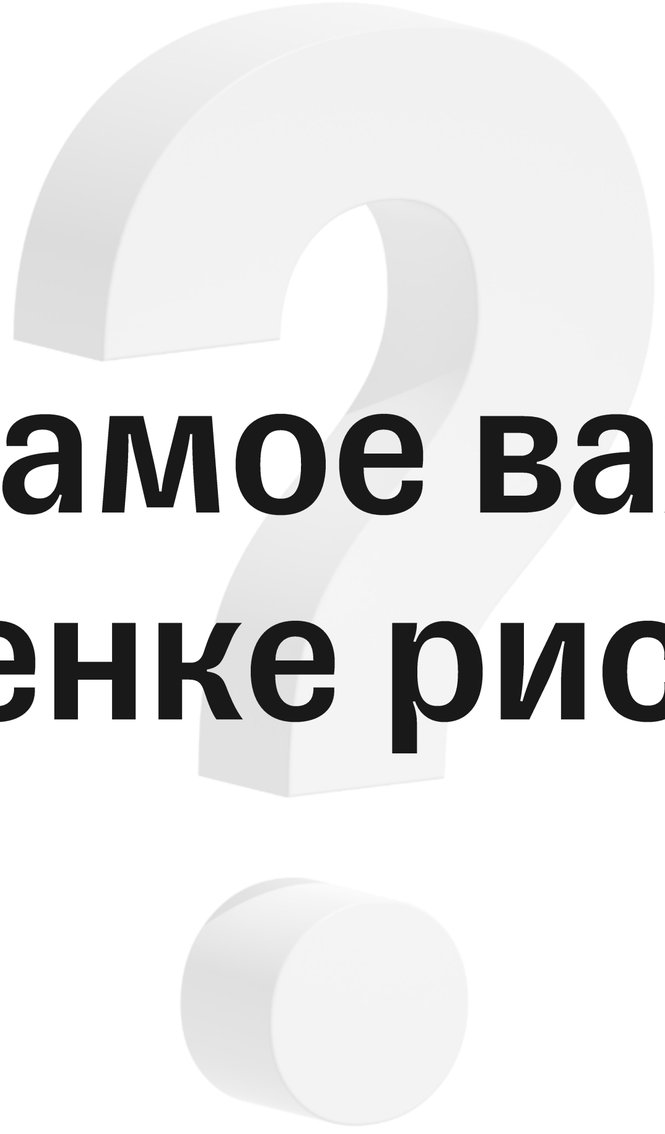
Идентификация риска/ Переоценка риска



Оценка риска

Оценка остаточного риска

Первичная обработка риска



Что самое важное в оценке рисков?

Понятность!

Ошибки оценки рисков

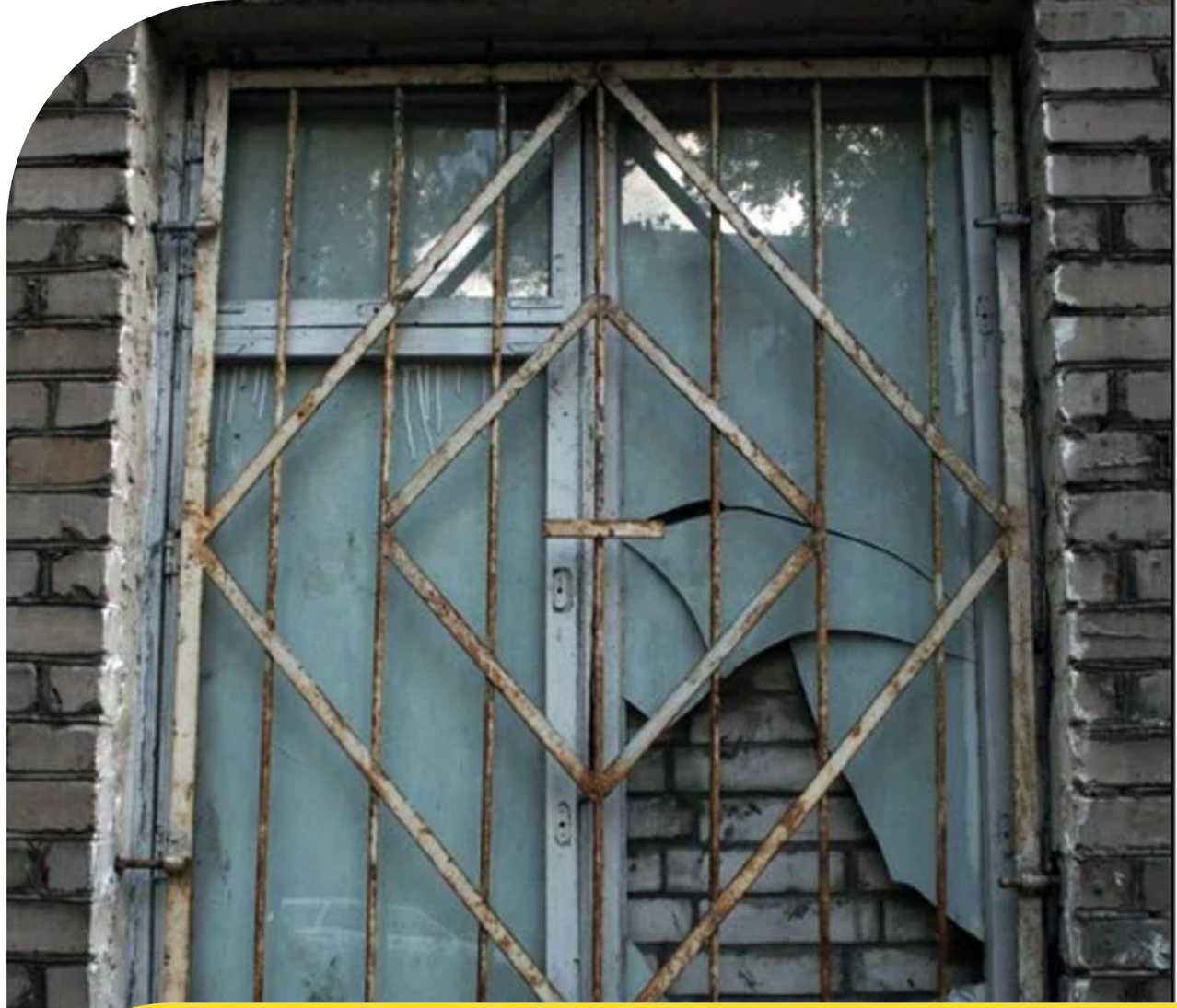
- Исходить от последствий, забывать про вероятность

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

Веротяность

Мотивация злоумышленника

Основной вопрос

Были попытки реализации сценария?

Что нужно учесть в процессе оценки рисков

Веротяность

- Как трудно реализовать сценарий в условиях вашей системы?
- Что даст реализация злоумышленнику?

Основной вопрос

Оценка систем защиты

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

Как начать?

Вход в процесс

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

Договориться

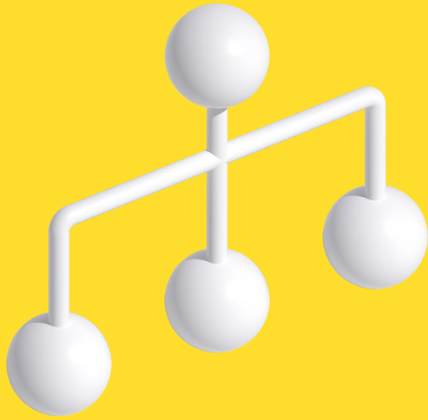
Что учесть?

01.

Стек технологий

02.

Требования Бизнеса



03.

Процессы

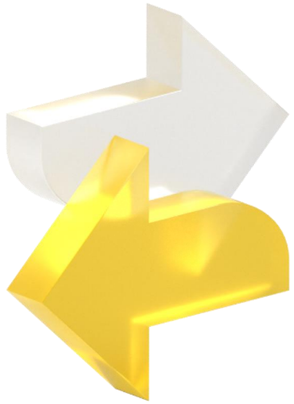
04.

Люди

Инструменты?

01.

Диалог



02.

Гибкость

03.

Требования

04.

Обратная связь

Кто к вам пришел?

- Каковы его полномочия?
- Какие у него задачи?
- Вам нужен стейкхолдер!

Залог успеха

- Думать как Бизнес
- Глубоко понимать как функционирует Бизнес
- Добиться слияния Бизнеса и безопасности

Залог успеха

- Думать как Бизнес
- Глубоко понимать как функционирует Бизнес
- Добиться слияния Бизнеса и безопасности

- Говорить на языке собеседника
- Давать обратную связь и мониторить ее эффективность
- Запрашивать и работать с обратной связью
- Быть исчерпывающим и лаконичным одновременно

Залог успеха

- Думать как Бизнес
- Глубоко понимать как функционирует Бизнес
- Добиться слияния Бизнеса и безопасности

- Говорить на языке собеседника
- Давать обратную связь и мониторить ее эффективность
- Запрашивать и работать с обратной связью
- Быть исчерпывающим и лаконичным одновременно

- Никогда не говорить «нельзя», не предложив альтернатив
- Быть проактивным
- Четко определить баланс между риск-аппетитами и допустимой границе рисков, постоянно выдерживать его
- Быть поставщиком решений

Залог провала

- Думать как технический специалист
- Разделять Бизнес и Безопасность
- Вникать только в те аспекты Бизнеса, с которыми приходится работать

Залог провала

- Думать как технический специалист
- Разделять Бизнес и Безопасность
- Вникать только в те аспекты Бизнеса, с которыми приходится работать
- Говорить на своем языке всегда и со всеми
- Не запрашивать или игнорировать обратную связь
- Не давать обратной связи коллегам
- Быть многословным и непонятным

Залог провала

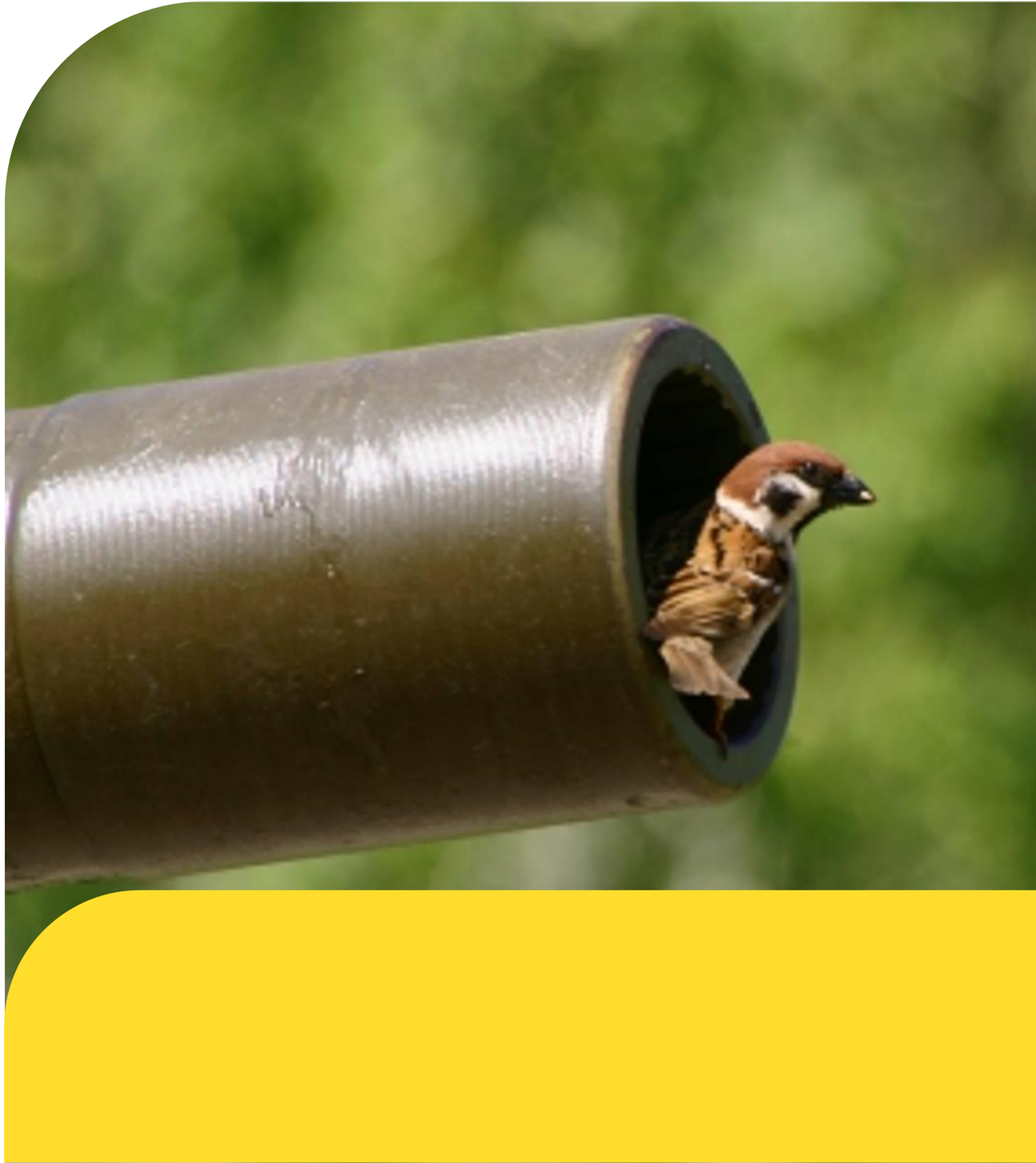
- Думать как технический специалист
- Разделять Бизнес и Безопасность
- Вникать только в те аспекты Бизнеса, с которыми приходится работать
- Говорить на своем языке всегда и со всеми
- Не запрашивать или игнорировать обратную связь
- Не давать обратной связи коллегам
- Быть многословным и непонятным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

Требования

- Персональная ответственность
- Эффективный менеджмент
- Продвинутые коммуникации
- Проактивность

Требования

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



Плюсы и минусы

- Гибкость
- Масштабируемость
- Результативность
- Экономическая эффективность

- Требования к менеджменту
- Требования к персоналу
- Ограничение применения

Спасибо
за внимание!

Вопросы?

Вотинцев Кирилл
Security Partner
k.votintsev@tinkoff.ru