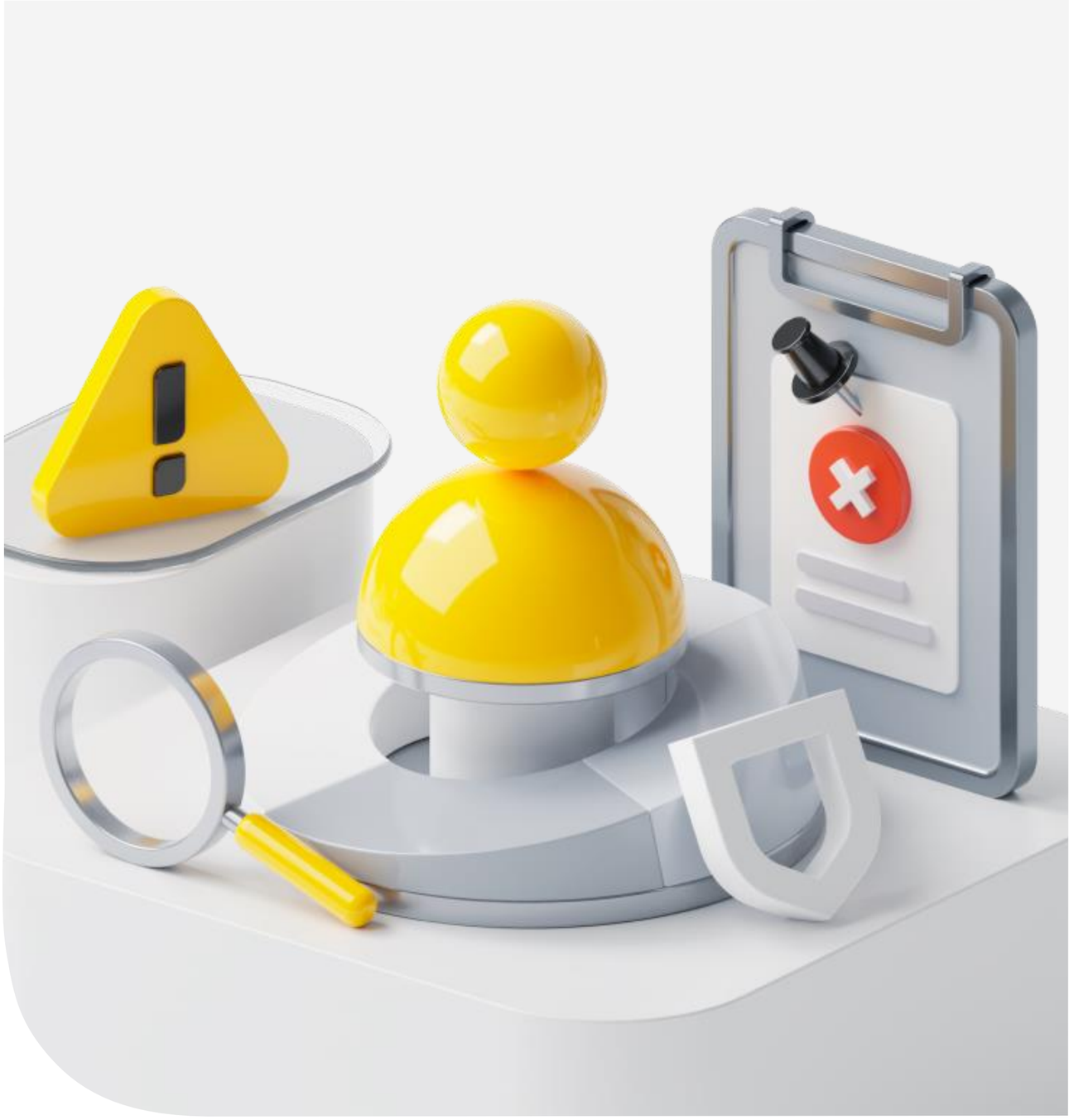
IT's TINKOFF

Анализ безопасности проектов



Кирилл Вотинцев

Security business partner Тинькофф

k.votintsev@tinkoff.ru

- Общий подход к анализу проектов
- Какие проблемы бывают на практике
- Как сделать хорошо

Что будет в презентации

Безопасность проектов и систем

Основной вопрос

Запускаем или нет?

Основной вопрос

- Какие критерии решения?
- Как ответить за приемлемое время?
- Какие требования предъявить?

Лайфхак!

Декомпозируйте процесс: разбивайте сложный анализ на простые составляющие

Алгоритм анализа

Тут все просто

Идентифицируем риски

Находим решение по рискам

PROFIT!

Какими бывают риски?

Финансовые

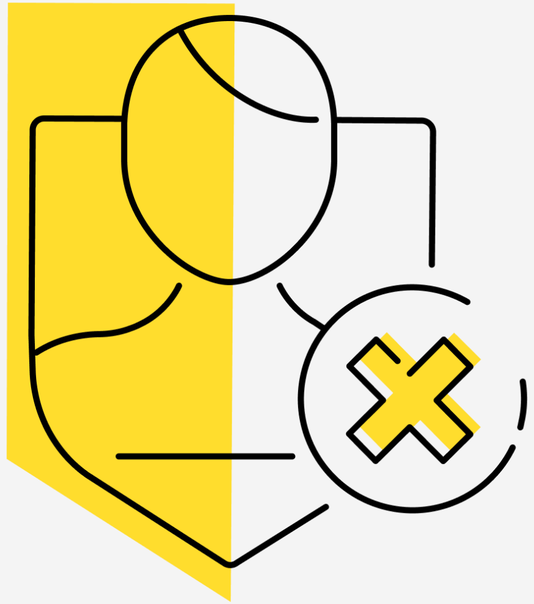
Репутационные

финансовый риск

Учесть

- Неполученную выгоду
- Потери компании (в т.ч. штрафы)
- Потери партнеров
- Потери клиентов

Репутационный риск



Учесть

- Ущерб в глазах акционеров
- Ущерб в глазах регулятора
- Ущерб в глазах клиентов

Как найти риски?

Пройти по основным доменам безопасности:

01

Infrastructure

02

SOC (Log&Response)

03

Antifraud

04

Application Security

05

Compliance

06

Business logic

Лайфхак!

Сделайте чек-лист по каждому домену,
учитывающий особенности вашей организации

01

Риски инфраструктуры

Основные:

Уязвимости используемых технологий (OS, протоколов)

Лишние сетевые доступы

Неверная сегментация

Недостаточная отказоустойчивость

02

Риски SOC

Основные:

Не ведется учет
и передача событий

Не настроен процесс
реагирования на события

03

Риски Антифрода

Основные:

Процессы позволят получить избыточную информацию сотрудникам

Бизнес-сценарии содержат ошибки, приводящие к возможности совершить мошенничество

04

Риски приложений

Основные:

- Кривая архитектура приложений
- Ошибки в логике взаимодействия компонентов
- Уязвимости в коде
- Токсичные зависимости

05

Риски комплаенса

Основные:

Несоответствие требованиям регуляторов

Нет NDA, учитывающего риски третьей стороны

06

Риски бизнес-логики

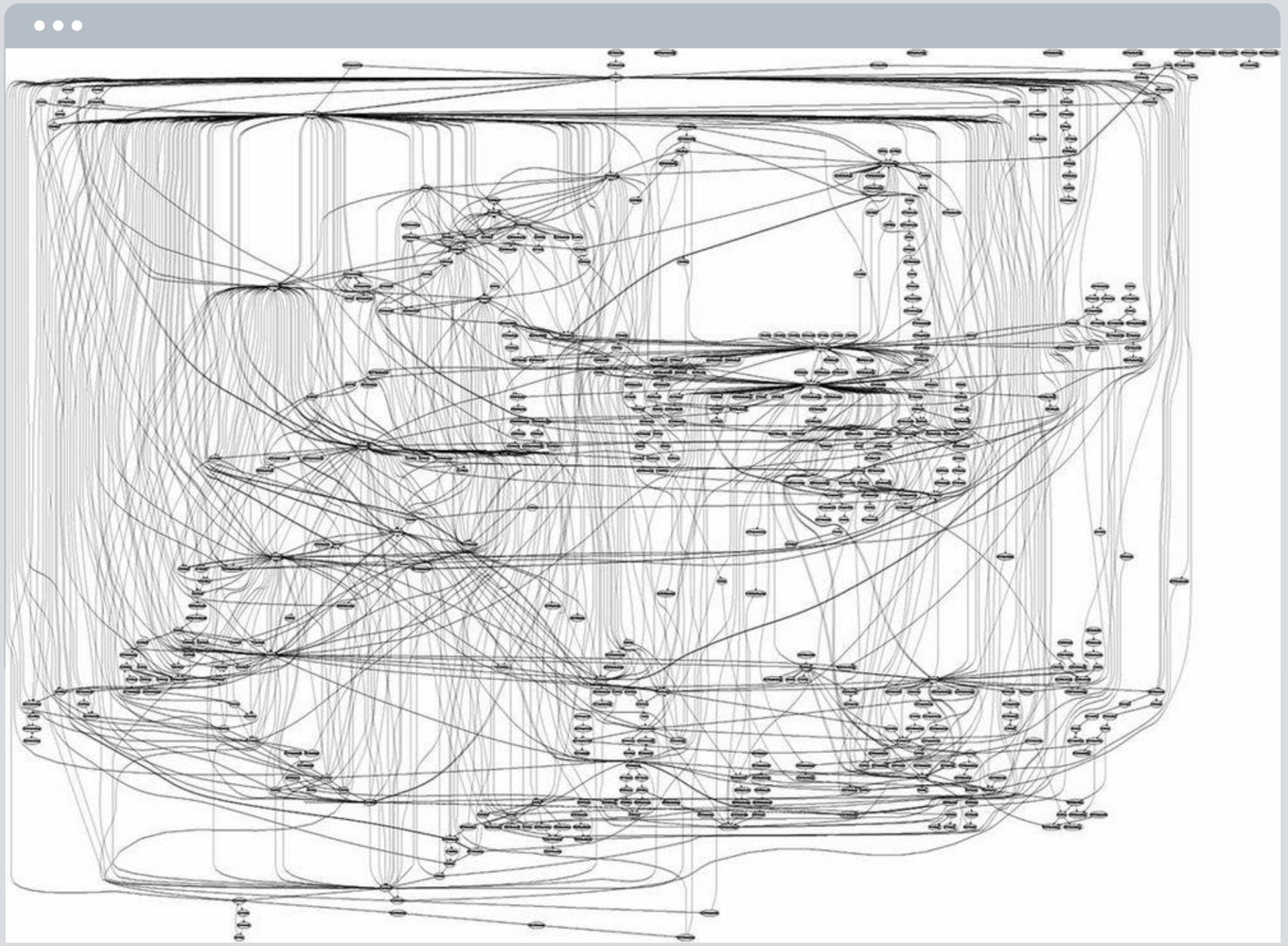
Основные:

Небезопасные бизнес-сценарии

Не учтены связанные риски

Все так просто

Дружище,
пожалуйста,
посмотри схему.
Завтра релиз!

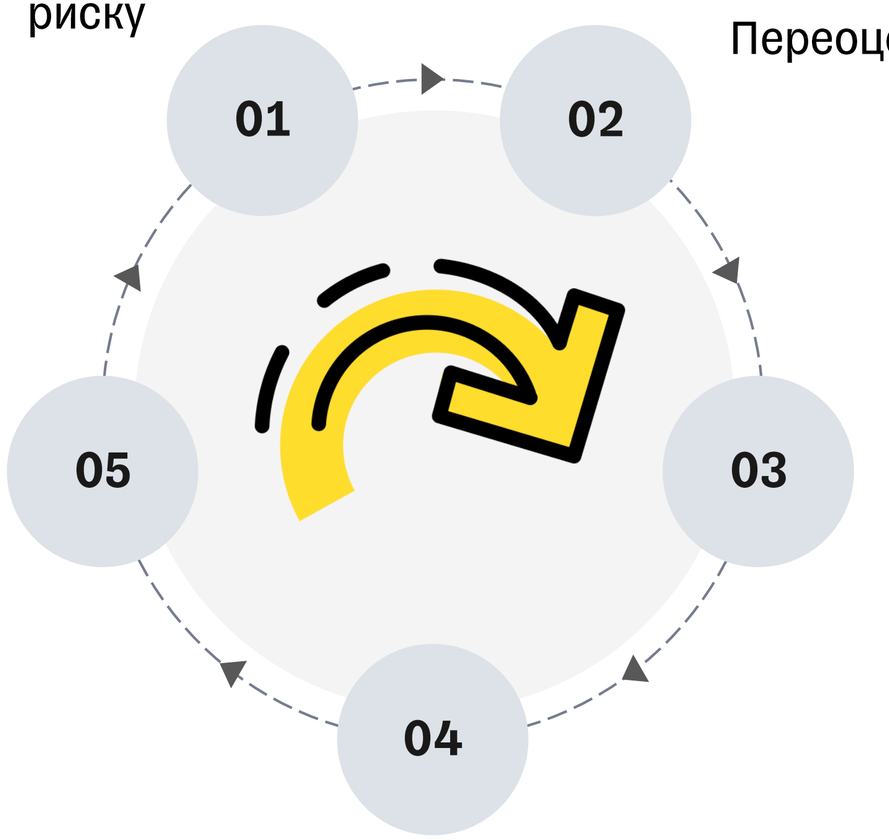


А что самое критичное?

Наиболее критичные риски

- Аутентификация/авторизация
- Управление доступами
- Внутренние и (особенно!) внешние интеграции
- Проведение операций с финансами
- Публикация в интернет
- Работа с критичными данными
- Большое число пользователей

Цикл управления рисками



Решение по остаточному риску

Идентификация риска/ Переоценка риска

Оценка остаточного риска

Оценка риска

Первичная обработка риска

Варианты

Избегание риска

Снижение риска

Передача риска

Принятие риска

Варианты

Избегание риска

Снижение риска

Передача риска

Принятие риска

Лайфхак!

У вас уже должен быть отработанный алгоритм действий для известных или похожих рисков

Как снизить риски?

01 Сокращение поверхности атаки

02 Следовать принципу минимизации доступов

03 Использование 3х-уровневой сетевой архитектуры

04 Использовать безопасные технологии

05 Использовать лучшие практики и подходы

А что делать с новыми рисками

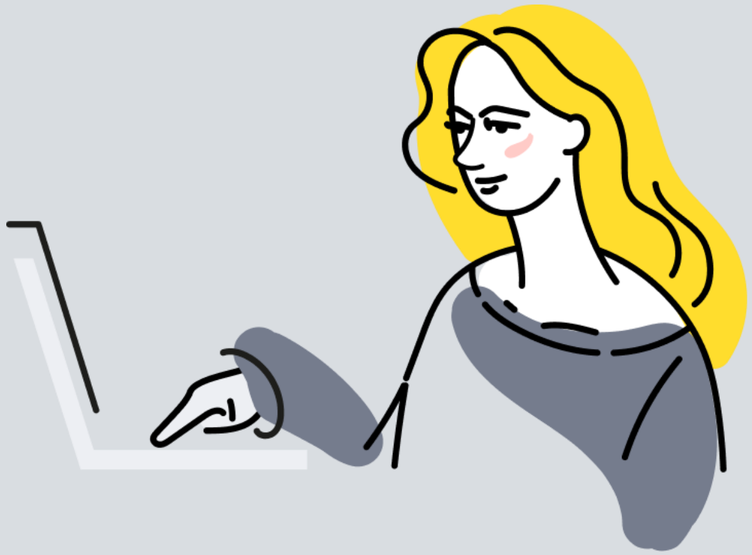
Договориться

Остаточные риски на старте

- Обсудите со стейкхолдером величину рисков и готовность принять их
- Назначьте ответственного за исправление и определите срок
- Контролируйте договоренности

Этого достаточно

Проблемы



Проектов больше,
чем ресурсов на
полноценный анализ

Высокие требования
к time2market

Сроки запуска
«вчера»

Сложность
и комплексность
проектов

А самая большая проблема?

Про безопасность забыли
и вообще не пришли!

Есть ли решение?

Security by design!

Профиты

Security by design

- Команды сами делают безопасно, но в случае чего позовут на помощь безопасность
- Ничего важного не пропустите
- К вам скорее всего придут раньше, чем за день до релиза – заранее спланируете время

Что включает Security by design?

- Все нужные процессы безопасности
- Заранее описанные и доведенные до команд требования по критичным рискам
- Прозрачное взаимодействие
- Обучение всех причастных

Что запомнить?

01 Декомпозировать задачу

02 Сделать чеклист по каждому домену

03 Иметь алгоритм действий по известным рискам

04 Принять решение по рискам с ответственным

05 Следовать к концепции Security by design

IT's TINKOFF

Ваши вопросы?

Вотинцев Кирилл

k.votintsev@Tinkoff.ru

@Votintsev_Kirill


IT's
TINKOFF