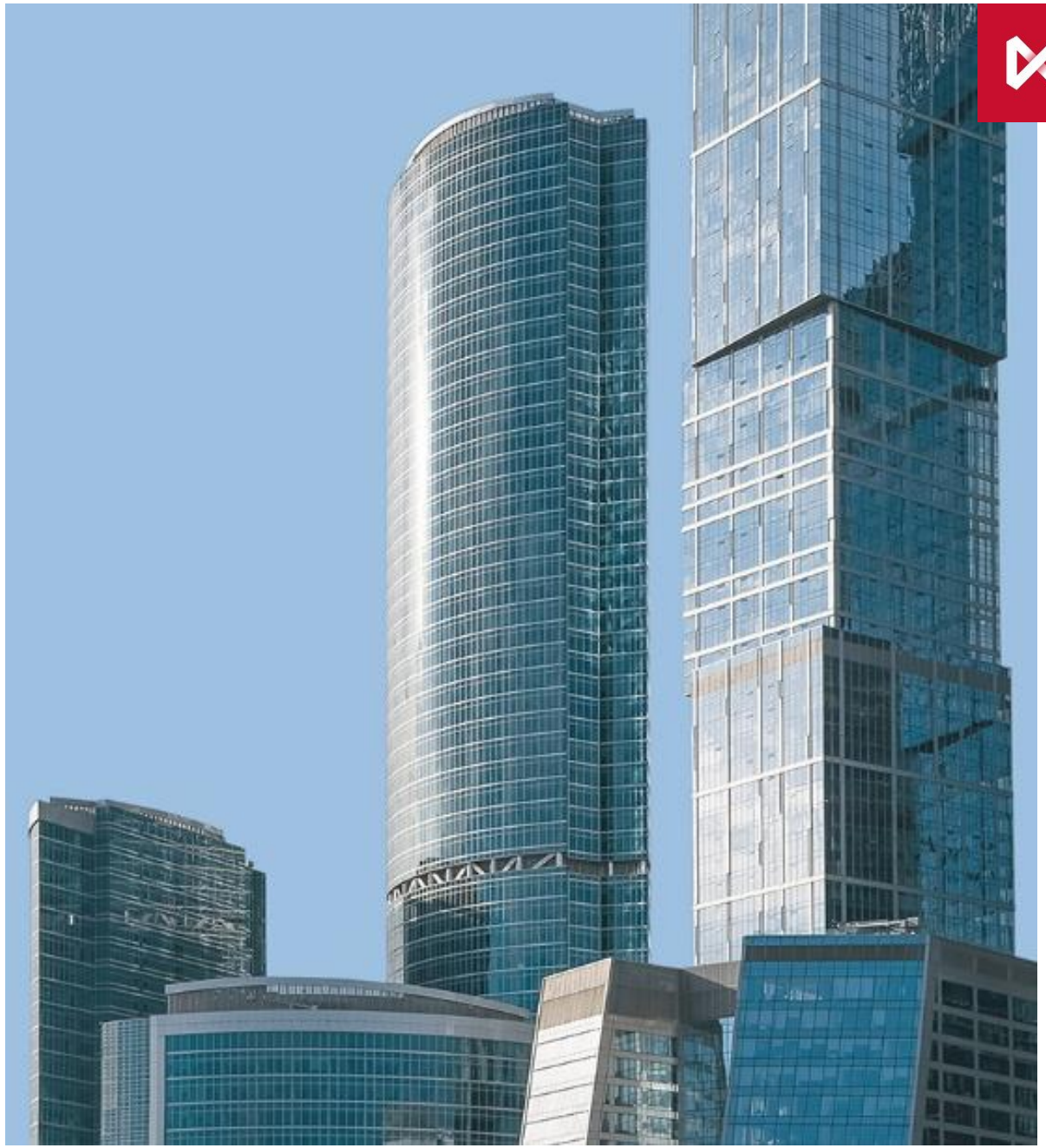


МОСКОВСКАЯ БИРЖА

Эдуард Сергиенко

Управление рисками информационной безопасности

СОДЕРЖАНИЕ

Зачем управлять рисками ИБ

Главная целью любой организации

выполнение своих показателей, характеризующих результат её деятельности

Риск ИБ

это то, что (может) мешает в достижении цели; входят в тройку наиболее вероятных рисков и в список из шести наиболее критичных рисков по возможному ущербу

Цель управления рисками ИБ

снижение риска ИБ до приемлемого уровня

Основа

анализ угроз ИБ и уязвимостей информационных ресурсов

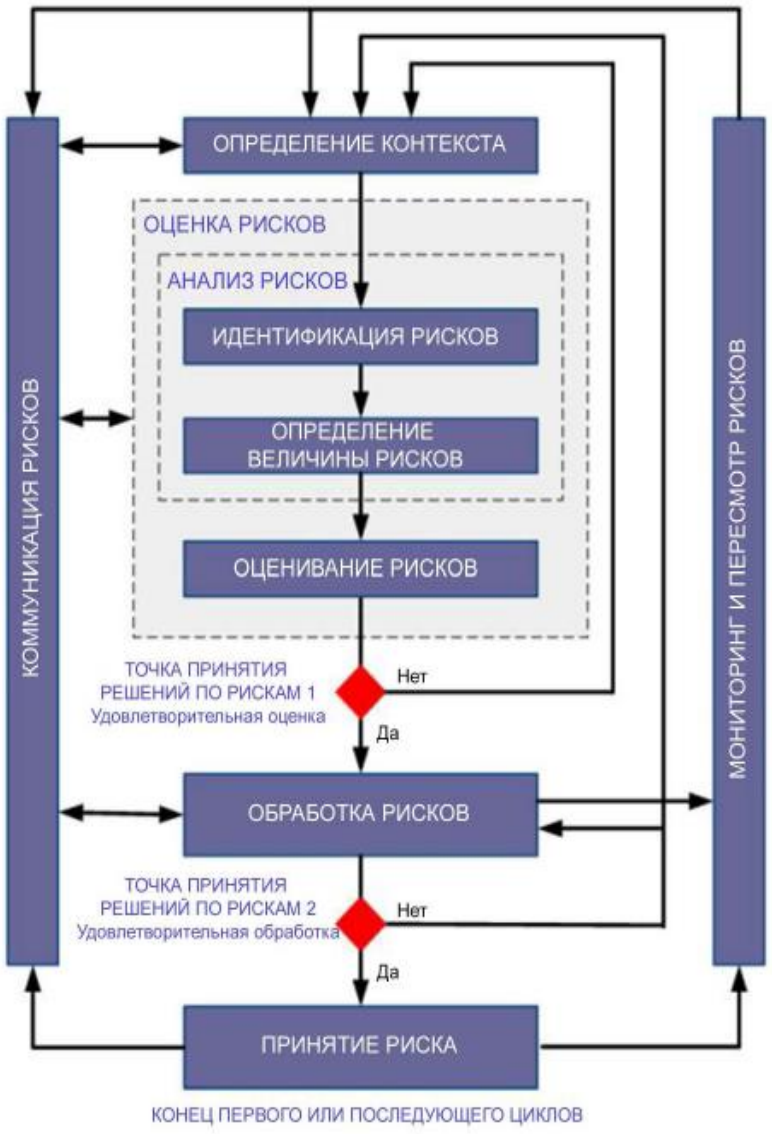
Как устроен процесс управления рисками ИБ

Главные характеристики

- Управление рисками ИБ - непрерывный и цикличный процесс.
- Потенциальный ущерб и вероятность реализации – то, что характеризирует все риски (не только ИБ).

В целом состоит из следующих этапов

- Определение контекста
- Оценка рисков
  - Идентификация, анализ и оценка рисков
  - Ранжирование и оценка рисков
    - ущерб от реализации рисков,
    - вероятность реализации,
    - ИТ-активы и бизнес-процессы, затрагиваемые риском,
    - общественный резонанс и репутационный ущерб от реализации риска и иные.
- Обработка рисков
  - Оценка эффективности реализованных мер
- Принятие рисков



МОСКОВСКАЯ БИРЖА

Биржа: ключевые особенности управления рисками ИБ

Управление рисками ИБ встроено в Единая систему управления финансовыми и нефинансовыми рисками

Операционные риски являются частью операционных рисков и управляются в рамках единой стратегии управления нефинансовыми рисками Биржи

Отсутствуют случаи реализации рисков информационной безопасности

В Группе не было ни одной атаки, по результатам которых реализовывался которое привело к каким бы то ни было значимым убыткам.

Атака на торговые системы может привести к существенным последствиям, поскольку оборот торгов может достигать 4 трлн. руб. в день.

Тут и помогает сценарный анализ

У нас нет «одиночного фрода», характерного для розничных банков

Например, риск доступа к счетам клиентов-физиков нам не присущ

Мы начинаем работать с физлицами

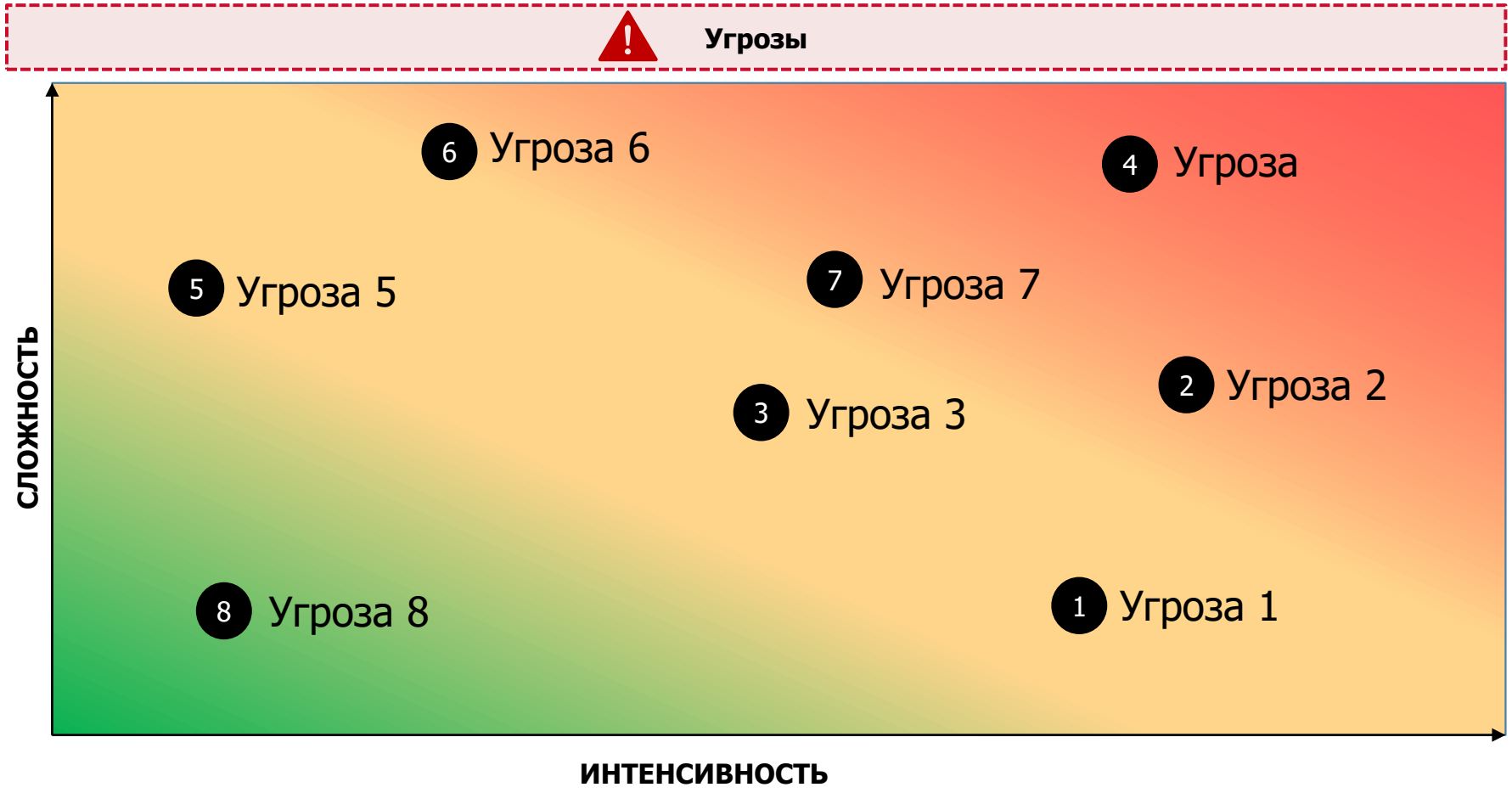
Но минимизируем большую часть рисков, так как только me2me переводы

Биржа: что делает для управления рисками ИБ

Цикл управления рисками вписан в Методику определения контрольных показателей риск-аппетита ПАО Московская Биржа, при этом:

- Стратегия ИБ Биржи
  - опирается на результаты оценки рисков,
  - синхронизирована с ИТ-стратегией,
  - охватывает всю Группу компаний.
- Установлен нулевой риск-аппетит к утечкам данных клиентов
- Оцениваем влияния на репутацию и применяем сценарный анализ с прогнозом негативных исходов
- Machine learning: прогнозирование потенциальных исходов
- Рисуем тепловую карт угроз
- Используем различные методы управления рисками ИБ

Биржа: тепловая карта угроз



МОСКОВСКАЯ БИРЖА

Биржа: как это работает

Анализ

Подразделение операционных рисков

определение Бизнес-владельца и Владельца риска

Бизнес-владелец риска

оценка степени влияния риска

Владелец риска

оценка области влияния и возможности реализации риска

Выявление

Проактивно:

- Самооценка
- Добровольные сообщения
- Ключевые индикаторы риска
- Диагностика процессов
- Стресс-тесты
- Внешние аудиты

Реактивно: Инциденты

Планирование

Бизнес-владелец риска

принимает решение о реагировании на риск

(принять, избегать, перевести, снизить)

Владелец риска

разрабатывает плана по снижению риска

Контроль

Подразделение операционных рисков

контроль исполнения плана по снижению риска

Биржа: страхование рисков

Кто - две Российские страховые компании

Объем покрытия

прямые финансовые потери от действий хакеров при попытках получения или получении доступа в электронные системы и хищения денежных средств с использованием любого компьютера или системы коммуникации, которые используются Застрахованными в своей деятельности.

Покрываемые риски:

- любого компьютера или системы коммуникации, которые используются Застрахованными в своей деятельности.
- Недобросовестность сотрудника
- Несанкционированный доступ
- Защита от социальной инженерии
- Поддельные электронные инструкции
- Профессиональная ответственность.

Инструменты

- ECC (Electronic and computer crime)
- PI (Professional Indemnity)