Александр Рогозин
Консультант по результативной кибербезопасности Positive Technologies

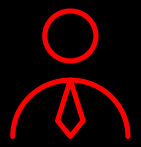
Подход РКБ

От формирования фокуса защиты до достижения киберустойчивости

Что такое результат

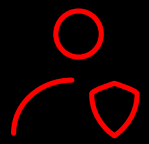
Какой результат должна показать ИБ?

Отсутствие критически опасных инцидентов или их наличие не является показателем эффективности ИБ для компании



Руководство

- Чего хотеть от ИБ?
- Как понять, что ИБ действительно эффективна?
- В чем измерять эффективность ИБ?



ИБ

- Как ИБ стать полноценной частью бизнес-процессов?
- Как доказать свою эффективность?
- Как сформировать и обосновать стратегию развития?

Общее

- Что про ИБ думают в ИТ?
- Чего действительно не должно произойти в организации?

Инструменты принятия решений

Менеджерское чутье
Принятие решений на основе менеджерской интуиции, прямых и косвенных аргументов

Управление рисками
Принятие решений на основе структурированного риск-менеджмента

Управление зрелостью
Принятие решений на основе соответствия лучшим практикам по ИБ

Соответствие требованиям
Принятие решение на основе требований законодательства

Результативная кибербезопасность
Принятие решений на основе определения недопустимых для организации событий и практическая проверка невозможности их наступления

Ключевые тезисы РКБ

1. **Определение фокусов защиты**

   Высшее руководство формирует запрос на защиту организации, тем самым определяя зоны ответственности ИБ

2. **Увеличение TTA, уменьшение TTR**

   ИТ и ИБ трансформируются, чтобы замедлить и усложнить продвижение злоумышленника по инфраструктуре и сократить время локализации атаки

3. **Практическое подтверждение киберустойчивости**

   Проверяется возможность реализации недопустимых событий с целью оценки эффективности ИБ и выполненных мерпо трансформации

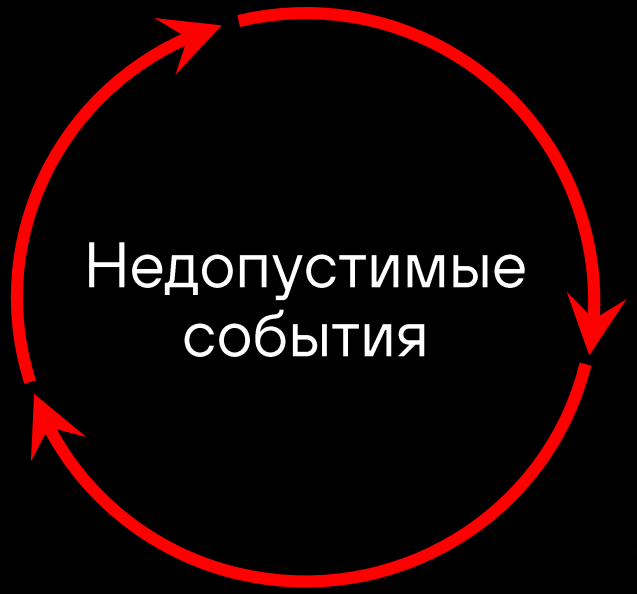
Недопустимое событие (НС) – событие, делающее невозможным достижение организацией операционных и стратегических целей или приводящее к длительному нарушению основной деятельности в результате кибератаки

Почему фокус на НС

Топ-менеджмент

Выстраивание понятного диалога между бизнесом, ИБ и ИТ

Приоритеты, основанные на целях бизнеса



Понятные метрики оценки эффективности ИБ

Формирование точек приложения усилий

Информационная безопасность

Информационные технологии

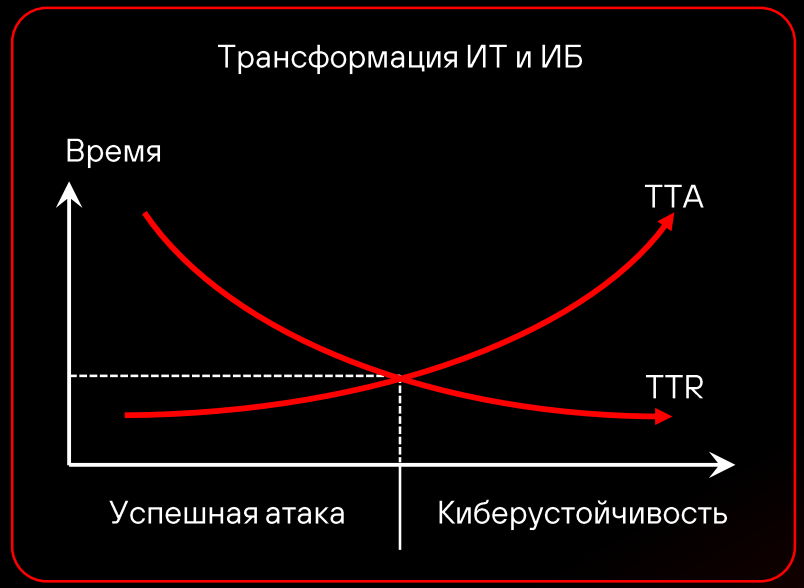
Определение кросс-KPI между ИБ и ИТ

Результативная кибербезопасность

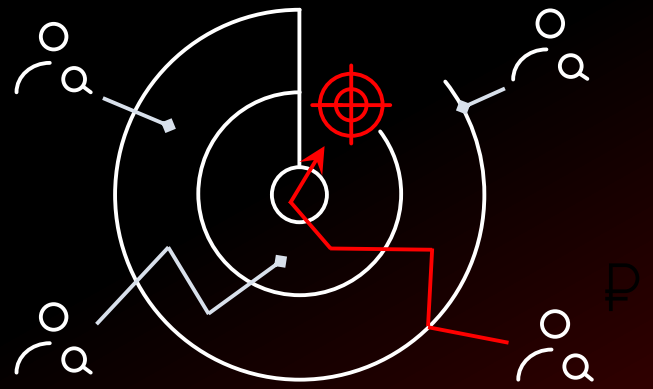
Целеполагание

- Недопустимые события
- Сценарии реализации
- Целевые и ключевые системы
- Формирование цели

Защита



Оценка



Целеполагание

Недопустимые события

Фиксация недопустимых событий и (или) других критически опасных инцидентов для бизнеса

Сценарии реализации

Уточнение критериев и бизнес-сценариев реализации НС

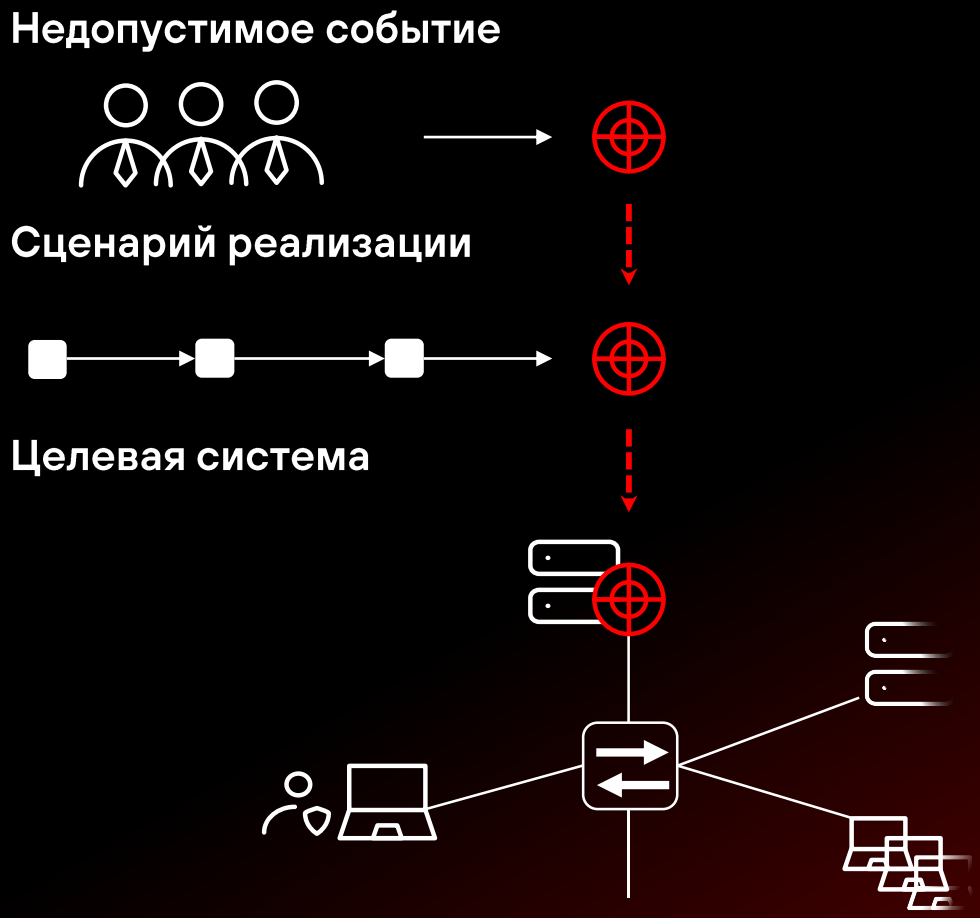
Целевые и ключевые системы

Определение целевых систем в сценариях реализации недопустимых событий и связанных с ними ключевых систем

Формирование цели защиты и кибериспытаний

Варианты недопустимых событий:

- нарушение работы и недоступность ключевого сервиса
- искажение данных и публикация недостоверной информации
- утечка или уничтожение операционных данных



Защита

Фокус защиты — предотвращение реализации недопустимых событий

Кибертрансформация ИТ

- Оценка уровня устойчивости инфраструктуры
- Управление активами
- Харденинг
- Сетевая сегментация
- Управление уязвимостями
- и прочее

Кибертрансформация ИБ

- Мониторинг и реагирование (продукты и процессы)
- NGFW, 2FA, AppSec
- Secure by Design для всех сервисов
- Выстраивание процессов, консалтинг
- MSS и MDR
- и прочее

Вариативность старта

> Целеполагание «от А до Я»

Целеполагание «от А до Я»

Топ-менеджмент (высшее руководство)

Декомпозиция недопустимых событий

Функциональные лидеры (линейные руководители)

Описание ландшафта ИТ и ИБ

ИТ и ИБ

Определение условий и ограничений

CISO

Требования к повышению киберустойчивости

> Целеполагание Fast start

Недопустимые события

CISO

Сценарии реализации

CISO

Целевые и ключевые системы

ИТ

Цель защиты и независимой оценки

Подтверждение результата и масштабирование подхода

Если начинать с семинара

Действия

- Запустить инициативу по целеполаганию.
- Поучаствовать в семинаре для определения недопустимых событий

Цель

Собрать гипотезы для формирования общего перечня недопустимых для организации событий

Аудитория

- Высшее руководство
- Ключевые эксперты функциональных направлений
- Профильные специалисты в области ИТ и ИБ

Программа семинара

1 Вводная часть

Ознакомление с принципами и ключевыми понятиями подхода РКБ

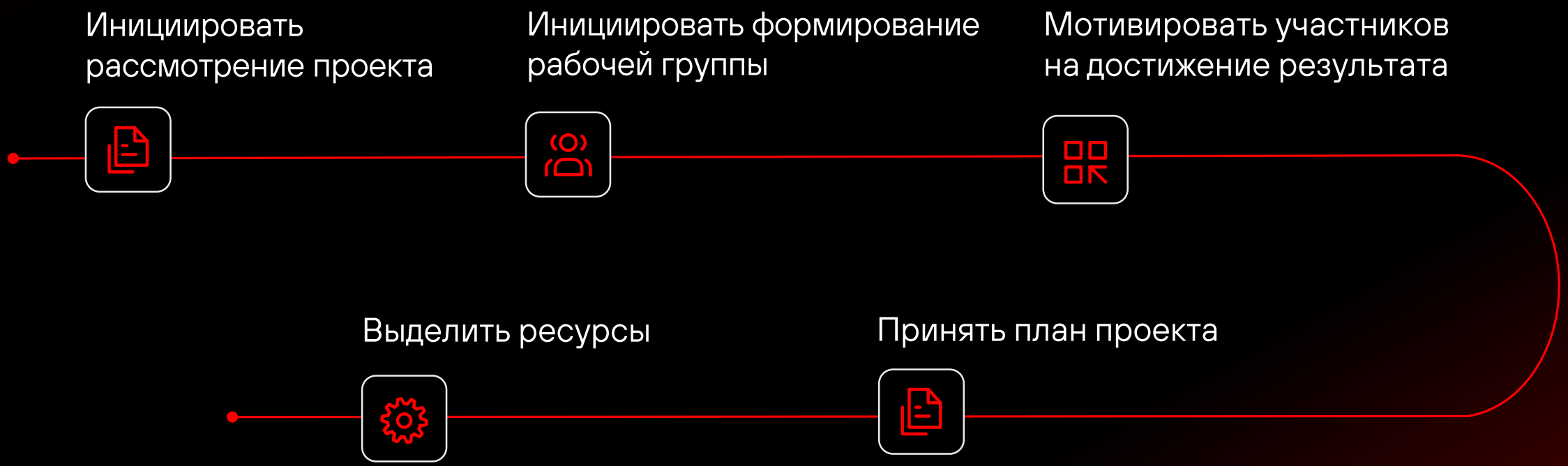
2 Основное обсуждение

Обсуждение вариантов недопустимых событий, возможным последствий и пороговых значений ущерба

Длительность семинара

≈1,5 часа

С чего уже можно начать



Спасибо!