Ростелеком

Информационная безопасность в эпоху цифровизации

Игорь Ляпунов
Вице-президент ПАО «Ростелеком»
по информационной безопасности

СОВРЕМЕННЫЙ ЛАНДШАФТ КИБЕРУГРОЗ

47% НА СТОЛЬКО ВЫРОСЛО ЧИСЛО ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ЗА ГОД

49% ВРЕДОНОСНОГО ПО УСТАНАВЛИВАЕТСЯ ЧЕРЕЗ ЭЛЕКТРОННУЮ ПОЧТУ

54% ВСЕХ АТАК НА ОРГАНИЗАЦИИ БЫЛИ ЦЕЛЕВЫМИ

65% ВТОРЖЕНИЙ ПРИВОДЯТ К ПОЛНОМУ КОНТРОЛЮ ДАННЫХ

69% КРИТИЧНЫХ ИНЦИДЕНТОВ ПРОИСХОДЯТ НОЧЬЮ

74% УСПЕШНЫХ АТАК В ГОССТРУКТУРАХ НАЧИНАЛИСЬ С ФИШИНГА

83% ФИШИНГОВЫХ АТАК ПРОХОДЯТ БЕЗ ЖАЛОБ ПОЛЬЗОВАТЕЛЕЙ

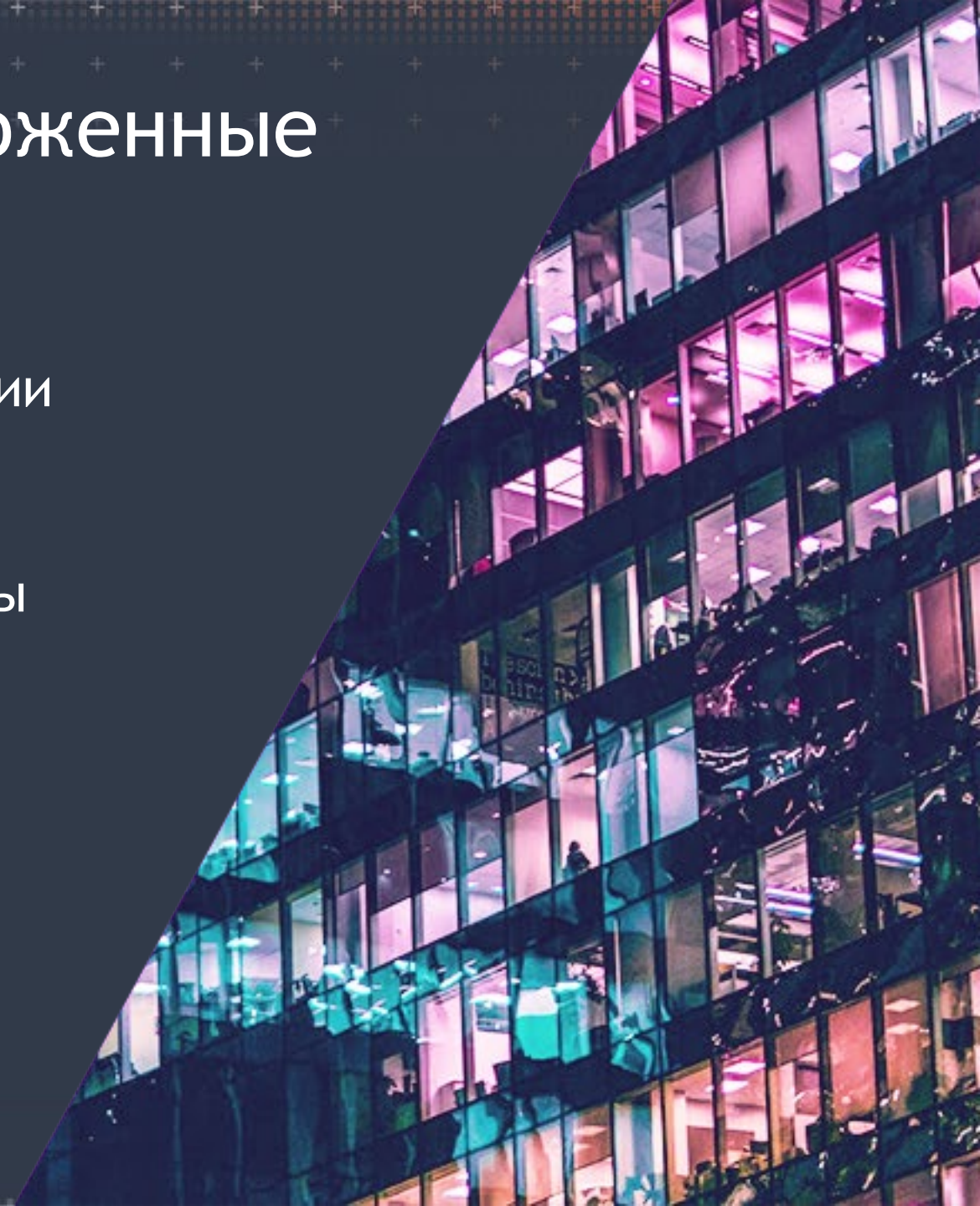
100% ВЕБ-ПРИЛОЖЕНИЙ СОДЕРЖАТ УЯЗВИМОСТИ

Ростелеком

ДАННЫЕ: SOLAR JSOC, POSITIVE TECHNOLOGIES И VERIZON, 2018

Компании наиболее подверженные кибератакам

- Кредитно-финансовые организации
- ТЭК и обладатели критической информационной инфраструктуры
- Системы государственного управления
- E-commerce и online-сервисы



ГЛОБАЛЬНЫЕ ТРЕНДЫ

Технологии определяют бизнес

Бизнесу нужен новый темп

Цифровизация бизнеса и производства

Бизнес осознает уязвимость ИТ

ВЫЗОВЫ ДЛЯ ИБ

- Динамика внешних угроз
- Скорость изменений в ИТ
- Сложные ИБ-технологии, которыми нужно управлять
- Дефицит кадров
- Необходимость защиты ядра бизнеса

Надежный подход к кибербезопасности

ЗАЩИТА

- ✓ СЕТИ
- ✓ ПРИЛОЖЕНИЙ
- ✓ ИНФОРМАЦИИ

УПРАВЛЕНИЕ

КОНТРОЛЬ

Безопасность периметра сети

Стоящие задачи:

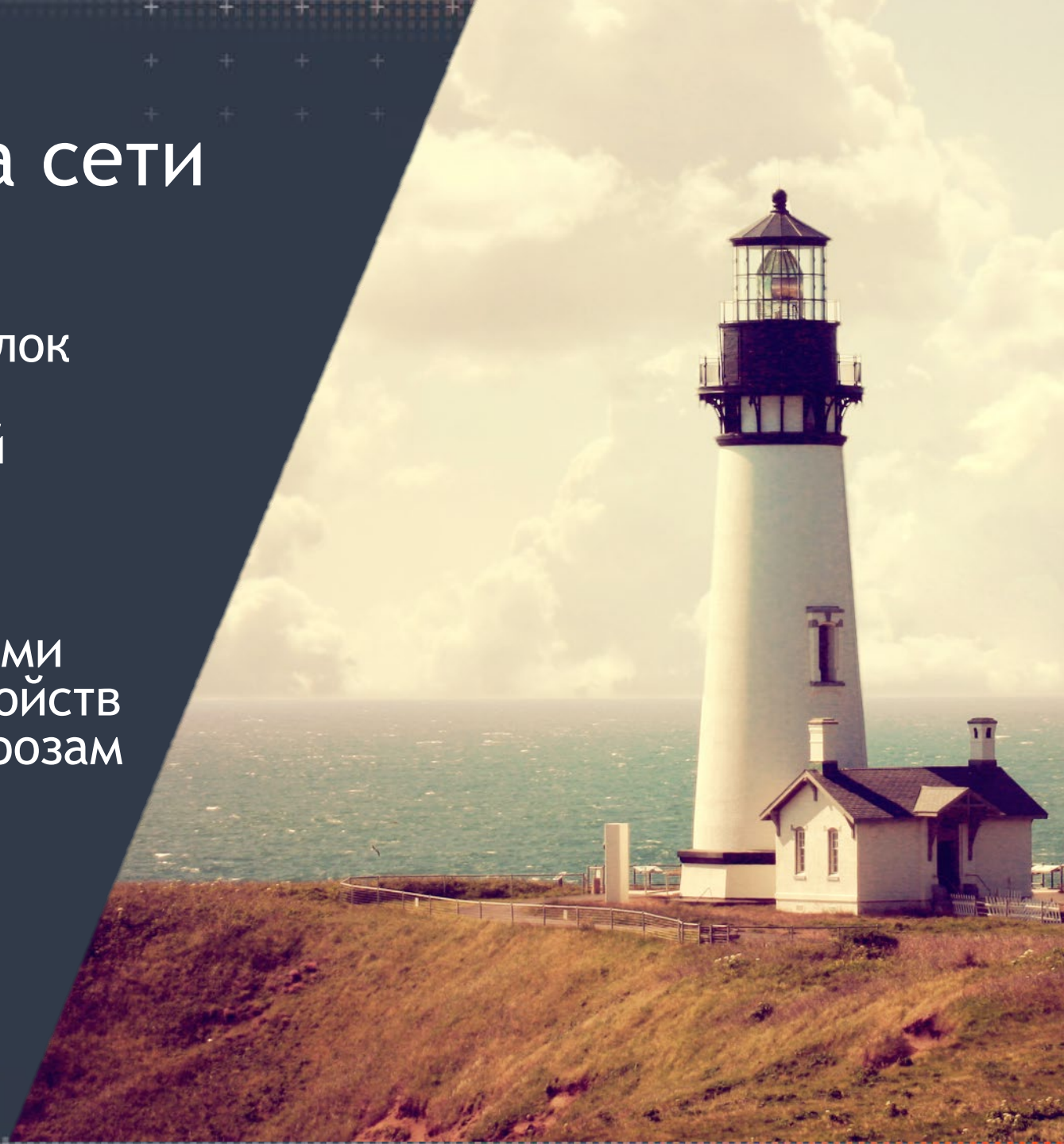
Защита от фишинговых рассылок
Защита от Интернет-угроз
Защита от массовых эпидемий

Решение:

Подключение вместе с каналами Ростелеком виртуальных устройств защиты и противодействия угрозам

Срок:

в течение 3-х дней



Защита приложений

Выявление уязвимостей и backdoor-ов

в мобильных приложениях
в e-commerce и бизнес-приложениях

Предоставление сервиса: от 30 минут

Защита онлайн-приложений

от массовых и DDoS-атак
от «происков» конкурентов
от целевых атак

Предоставление сервиса: до 3-х дней

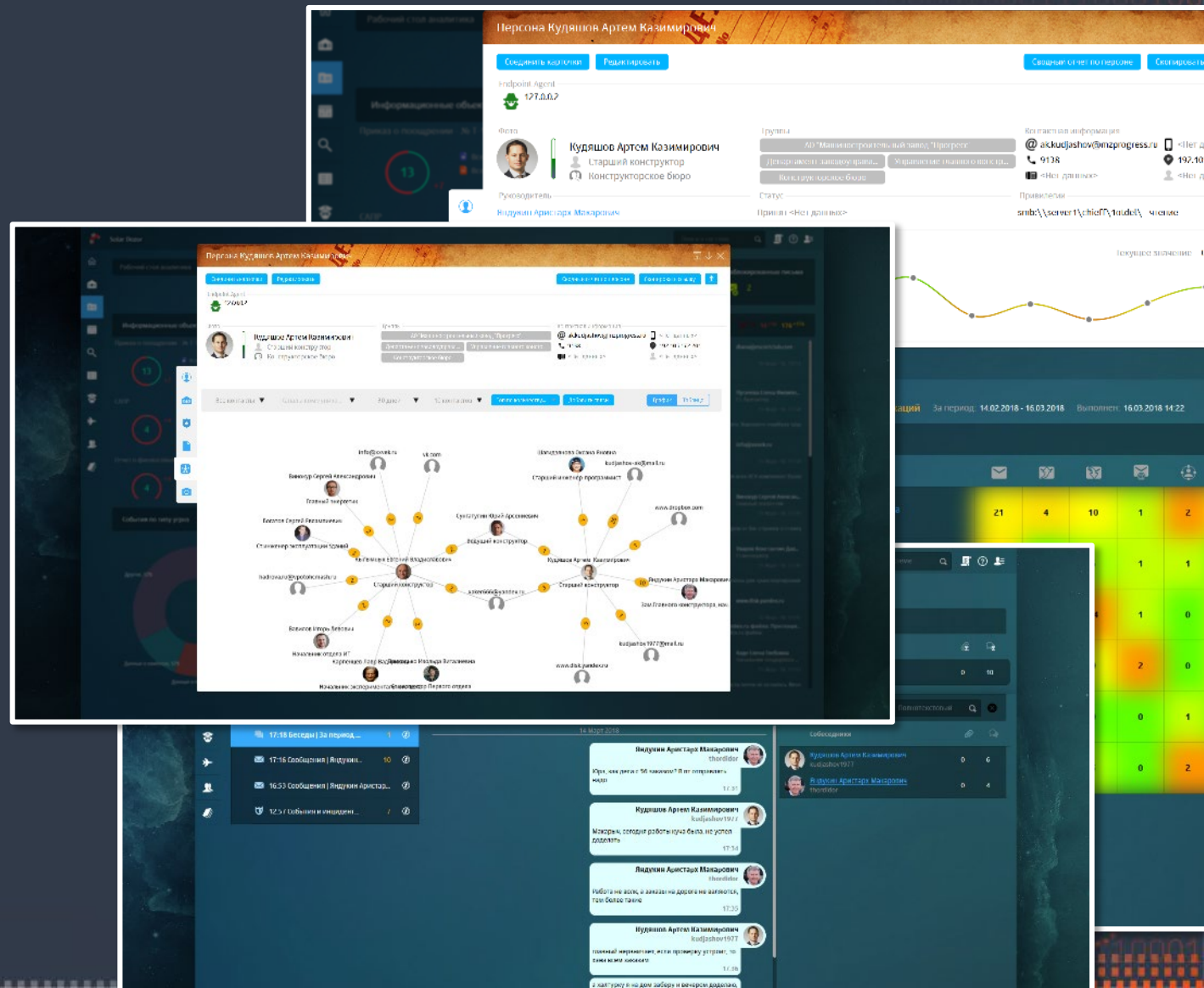
Защита конфиденциальной информации

Задачи:

1. Защита от утечек информации
2. Выявление конфликтов интересов и фрода

Инструменты:

1. Контроль коммуникаций
2. Контроль копирования на внешние носители
3. Контроль печати



Управление информационной безопасностью

Вроде бы все сделано…

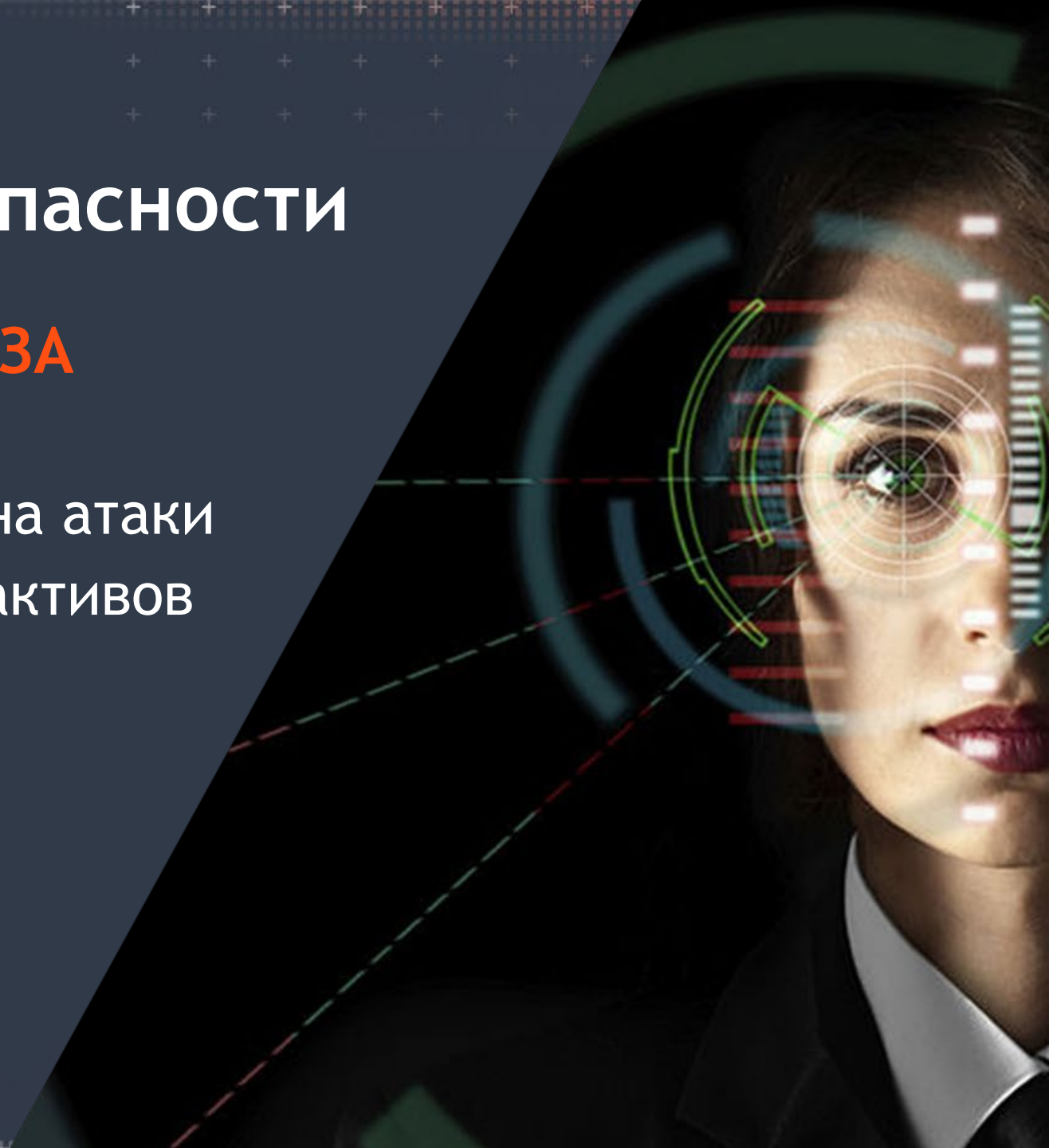
- Средства защиты установлены
- Акты подписаны, деньги инвестированы
- Внутренние документы созданы
- Системы защиты аттестованы

НО! 100% ТЕСТОВ НА ПРОНИКНОВЕНИЕ УСПЕШНЫ

Контроль информационной безопасности

БЕЗОПАСНОСТИ НУЖНЫ ГЛАЗА

1. Мониторинг и реагирование на атаки
2. Контроль защищенности ИТ-активов
3. Расследование инцидентов



Центр мониторинга и реагирования на киберугрозы

РОСТЕЛЕКОМ-SOLAR

#1
SOC в России

450+
экспертов по ИБ

28 млрд.
событий в сутки

10мин
детектирование атаки

30мин
реагирование и защита

90+
крупных клиентов

СЕРВИСЫ ИБ УЖЕ ИСПОЛЬЗУЮТ

Почта Банк · Ростех · Калашников Концерн · Тинькофф · Иркут · Банк России · FIFA World Cup Russia 2018 · Росфинмониторинг · e.on · СТС · ФСК · МТС Банк · MIR · Северсталь · Банк Санкт-Петербург · Leroy Merlin

Ситуационный центр ИБ
Security Operations Center (SOC)

Будьте под защитой Ростелеком