



# Информационная безопасность в эпоху цифровизации

**Игорь Ляпунов**

Вице-президент ПАО «Ростелеком»  
по информационной безопасности



# Развитие экспертизы ИБ

## 2018 год

ПАО «Ростелеком» приобрело компанию Solar Security и выделило информационную безопасность в ключевое направление развития бизнеса

## 2019 год

В штате компании уже более 450 специалистов по предоставлению клиентских сервисов информационной безопасности





Ростелеком

Киберугроза:  
миф или реальность?



# СОВРЕМЕННЫЙ ЛАНДШАФТ КИБЕРУГРОЗ

**47%** НА СТОЛЬКО ВЫРОСЛО  
ЧИСЛО ИНЦИДЕНТОВ  
БЕЗОПАСНОСТИ ЗА ГОД

**69%** КРИТИЧНЫХ  
ИНЦИДЕНТОВ  
ПРОИСХОДЯТ НОЧЬЮ

**49%** ВРЕДНОСНОГО ПО  
УСТАНОВЛИВАЕТСЯ ЧЕРЕЗ  
ЭЛЕКТРОННУЮ ПОЧТУ

**74%** УСПЕШНЫХ АТАК В  
ГОССТРУКТУРАХ  
НАЧИНАЛИСЬ С ФИШИНГА

**54%** ВСЕХ АТАК  
НА ОРГАНИЗАЦИИ  
БЫЛИ ЦЕЛЕВЫМИ

**83%** ФИШИНГОВЫХ АТАК  
ПРОХОДЯТ БЕЗ ЖАЛОБ  
ПОЛЬЗОВАТЕЛЕЙ

**65%** ВТОРЖЕНИЙ ПРИВОДЯТ  
К ПОЛНОМУ КОНТРОЛЮ  
ДАННЫХ

**100%** ВЕБ-ПРИЛОЖЕНИЙ  
СОДЕРЖАТ  
УЯЗВИМОСТИ

**Ростелеком**

ДАННЫЕ: SOLAR JSOC, POSITIVE TECHNOLOGIES И VERIZON, 2018



# Компании наиболее подверженные кибератакам



Кредитно-финансовые организации



Обладатели критической  
информационной инфраструктуры



Системы государственного  
управления



E-commerce и online-сервисы

# Защита от внешних угроз

**UTM**

УНИВЕРСАЛЬНАЯ ЗАЩИТА  
ОТ ИНТЕРНЕТ-УГРОЗ

**WAF**

ЗАЩИТА WEB-СЕРВИСОВ  
И ИНТЕРНЕТ-ПЛОЩАДОК

**SEG**

ЗАЩИТА КОРПОРАТИВНОЙ  
ПОЧТЫ

**Ростелеком**



# ЕДИНАЯ ПЛАТФОРМА СЕРВИСОВ КИБЕРБЕЗОПАСНОСТИ



Ростелеком

# Защита от внутренних угроз

## DLP (Data Leak Prevention)

1. Контроль коммуникаций сотрудников
2. Контроль копирования на внешние носители
3. Контроль печати конфиденциальных документов





# Управление информационной безопасностью

Вроде бы все сделано...

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

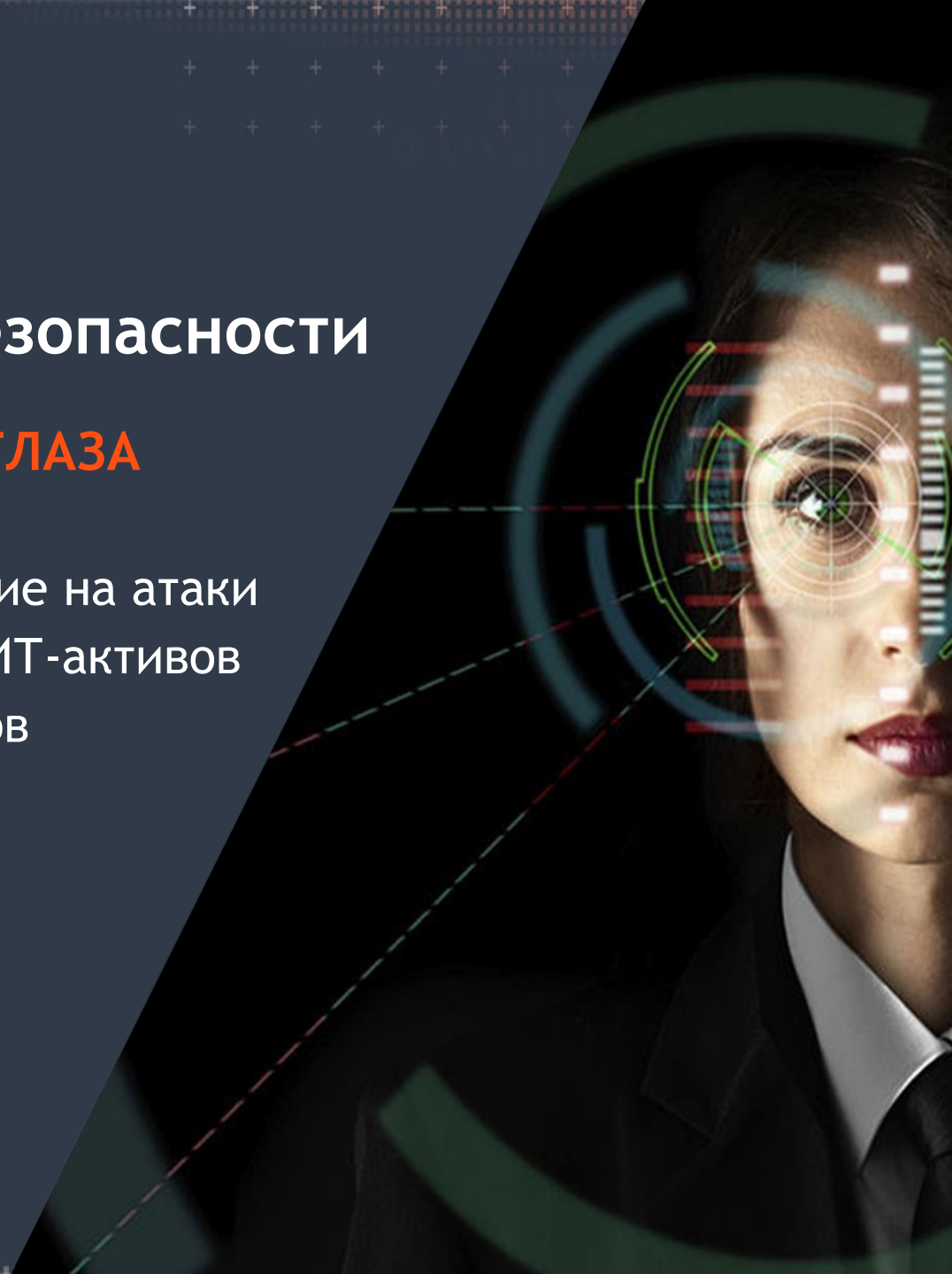
**НО! 100% ТЕСТОВ  
НА ПРОНИКНОВЕНИЕ  
УСПЕШНЫ**



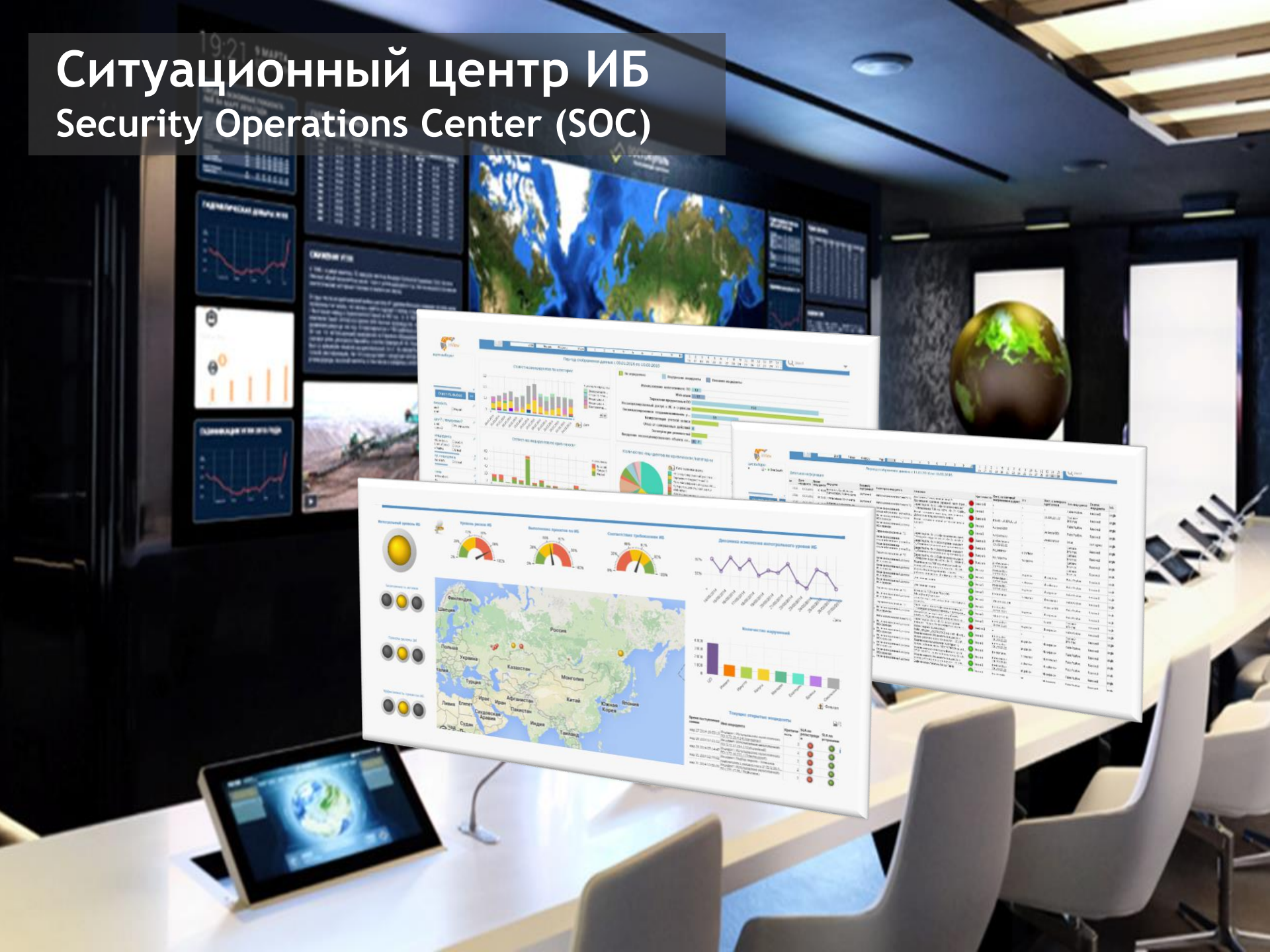
# Контроль информационной безопасности

## БЕЗОПАСНОСТИ НУЖНЫ ГЛАЗА

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



# Ситуационный центр ИБ Security Operations Center (SOC)



1921 2017

Административный отчет ИБ

Сводный ИБ

Циклы жизни инцидентов



Идентификатор	Дата	Время	Событие	Состояние	Приоритет	Имя оператора	Статус
INC-2018-001	2018-01-01	10:00	Фишинг	Закрыто	Низкий	Иванов	Завершено
INC-2018-002	2018-01-02	15:30	Малварь	Открыто	Средний	Петров	В процессе
INC-2018-003	2018-01-03	08:45	DDoS	Закрыто	Высокий	Сидоров	Завершено
INC-2018-004	2018-01-04	12:15	Спам	Закрыто	Низкий	Иванов	Завершено
INC-2018-005	2018-01-05	18:00	Иные	Открыто	Средний	Петров	В процессе

# Ситуационный центр ИБ РОСТЕЛЕКОМ-SOLAR

**#1**

СОС в России

**86%**

доля рынка сервисов СОС

**28+ млрд**

событий в сутки

**10мин**

детектирование атаки

**30мин**

реагирование и защита

**50+**

крупных клиентов

## СЕРВИСЫ ИБ УЖЕ ИСПОЛЬЗУЮТ





**Будьте под защитой  
Ростелеком**

