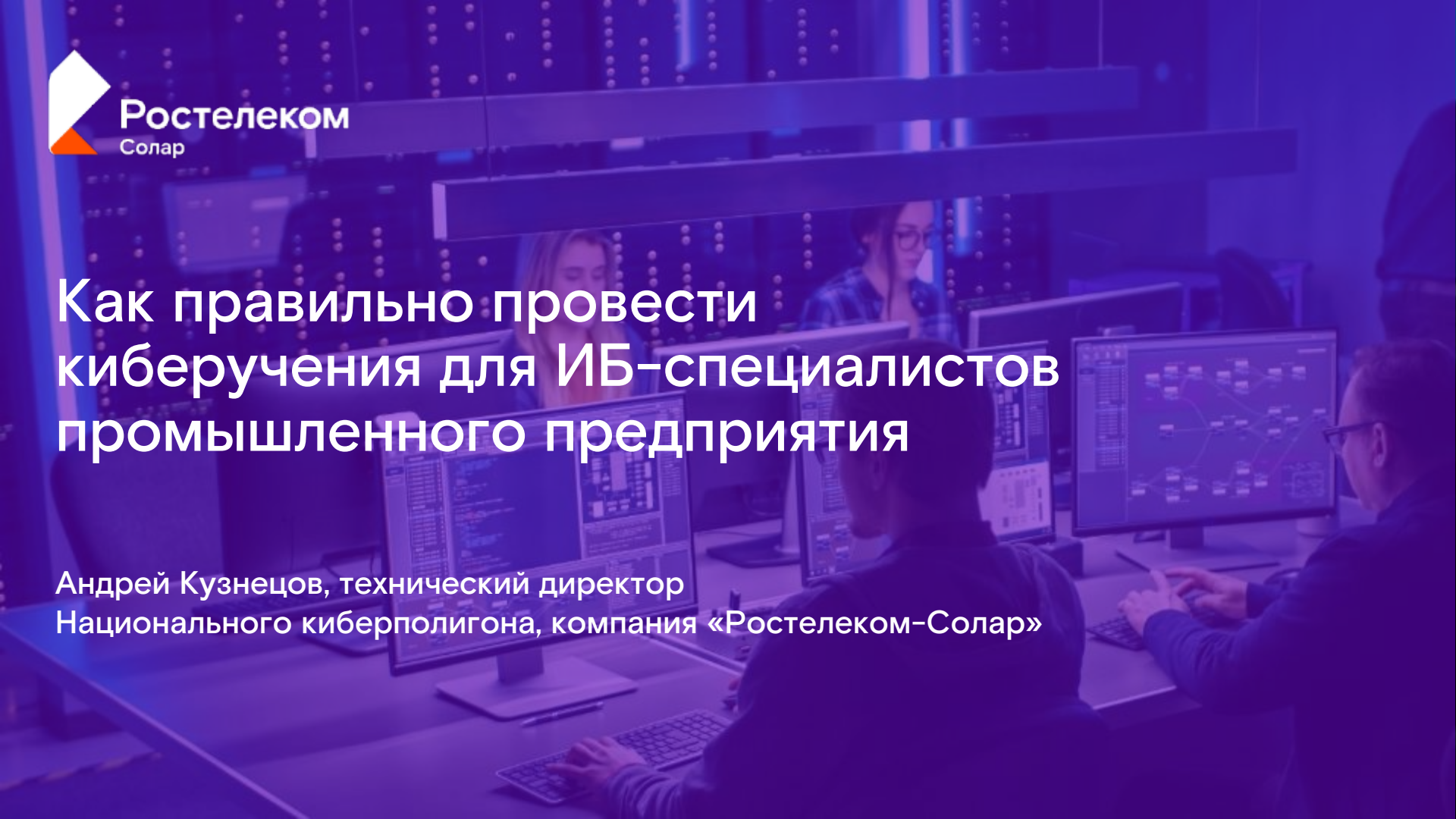



# Как правильно провести киберучения для ИБ-специалистов промышленного предприятия

Андрей Кузнецов, технический директор
Национального киберполигона, компания «Ростелеком-Солар»

# Сложности, с которыми мы сталкиваемся

1. Неукомплектованность штата ИБ-отделов компаний и общий кадровый голод на рынке
2. Недостаточный уровень квалификации специалистов по информационной безопасности
3. Отсутствие практических навыков реагирования на инциденты и слаженности команд
4. Появление новых угроз и необходимость отработки знаний для своевременного отражения кибератак
5. Сложности с настройкой инфраструктуры и закупкой нового оборудования
6. Появление новых продуктов на рынке, которые необходимо тестировать для внедрения в инфраструктуру компании



Ростелеком Солар

# Статистика Solar JSOC

+49% YtoY

**Подозрения на инцидент**:
Q1 2022: 180 144
Q2 2022: 235 917
Q3 2022: 214 302
Q4 2022: 281 214

+18% YtoY

**Подтвержденные инциденты**:
Q1 2022: 5 937
Q2 2022: 5 901
Q3 2022: 11 205
Q4 2022: 9 306

+10% YtoY

**Среднее значение подозрений на инциденты в компании**:
Q1 2022: 767
Q2 2022: 925
Q3 2022: 809
Q4 2022: 1004

Без изменений

**Среднее значение инцидентов в компании**:
Q1 2022: 25
Q2 2022: 23
Q3 2022: 42
Q4 2022: 33

**Топ-3 основных типов инцидентов:**

- заражение ВПО
- компрометация УЗ
- эксплуатация уязвимостей



Ростелеком Солар

# Архитектура киберполигона

Киберполигон от «Ростелеком-Солар»

**Программная платформа «Солар Кибермир»**

Набор сценариев учебных атак

Отраслевые учебные инфраструктуры, эмулирующие работу компаний

Отказоустойчивая ИТ-инфраструктура на базе отечественных продуктов

**Отраслевые сегменты:**

- Корпоративный
- Банки
- Энергетика
- Нефтегаз
- Телеком

Инфраструктура сегментов максимально приближена к реальной. Киберучения проходят на платформе «Солар Кибермир» через веб-портал



Ростелеком Солар

# Аппаратная или программная реализация?

**Киберполигоны позволяют тренироваться с использованием реальных, физических и виртуальных сервисов и сетей**

**IT-службы:**
- Виртуальные машины
- Серверы Microsoft
- Серверные приложения Microsoft
- Серверы Linux и UNIX
- Приложения баз данных
- Услуги аутентификации

**IP-сети:**
- Маршрутизаторы и коммутаторы
- Устройства безопасности (межсетевой экран, IDS, IPS)
- Оптимизация приложений (SLB, прокси и т. д.)

**Критические инфраструктуры:**
- Моделирование реальных электростанций, систем водоснабжения, железнодорожной сети, аэропорта и т. д.
- SCADA
- MES

И многое другое!



Ростелеком Солар

# Требуется ли моделирование?

**Симулятор:**

Модель технологического процесса, элементы которой контролируются **реальными или программными компонентами АСУ ТП**

**Компоненты АСУ ТП:**

Терминалы РЗА, контроллеры, датчики, сенсоры и т. д. получают сигнал от контролируемого элемента **в модели** и по цифровым протоколам передают его в управляющие **диспетчерские системы**

**SCADA-системы:**

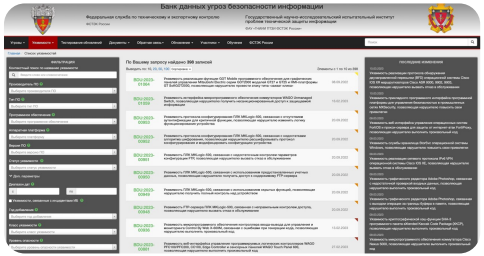
Получают сигнал по цифровым протоколам передачи данных от **компонентов АСУ ТП**. Оператор производит управляющее воздействие, которое через **контроллеры** передается на конечное оборудование в **симулятор АСУ ТП**



Ростелеком Солар

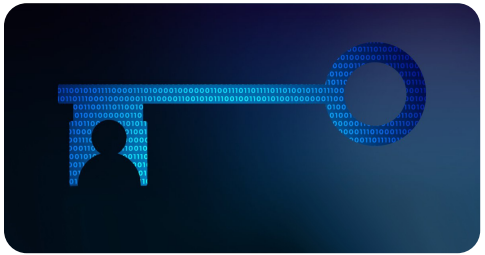
# Как мы собираем данные для написания сценариев?

## Открытые источники и TI-сервисы




## Мониторинг и реагирование SOC промышленных предприятий

## Результаты проведения тестирований на проникновение



## Результаты внутренних исследований ПО и аппаратных компонентов АСУ ТП



Ростелеком Солар

# Что делать до, во время и после киберучений?

1. Определить цель
2. Определить состав участников
3. Выбрать тип киберучений
4. Разработать механику киберучений
5. Подготовить инфраструктуру для проведения киберучений
6. Продумать скоринг
7. Подготовить справочную документацию
8. Обеспечить маркетинговую и PR-поддержку (для публичных киберучений)
9. Провести тестирование киберучений
10. Прописать риски
11. Контролировать ход мероприятия
12. Помогать участникам
13. Быть готовым к неожиданностям
14. Поработать с обратной связью
15. Провести ретроспективу мероприятия



Ростелеком Солар

# Чек-лист по проведению киберучений

**Скачайте чек-лист по проведению киберучений, чтобы ничего не забыть**



Ростелеком Солар

# Проведение практических киберучений

**«Трубная металлургическая компания»**

Практические киберучения для улучшения навыков защиты от киберугроз для технических специалистов

**Что было сделано:**

- Проведение киберучений в течение 3 дней в офлайн-формате
- Застройка площадки для проведения киберучений
- Создание кастомизированной для заказчика инфраструктуры
- Разработка отраслевых сценариев проведения киберучений
- Оценка работы и действий ИТ- и ИБ-подразделений в ходе киберучений
- Совместная отработка умений обнаружения и реагирования на атаки
- Составление индивидуальных рекомендаций для повышения навыков сотрудников

**Результат киберучений:**

- Обучены специалисты ИБ и ИТ
- Отработаны практические навыки обнаружения, реагирования и восстановления после атак
- Составлен план развития каждого сотрудника

**Подробнее:** https://rt-solar.ru/events/news/2385/



Ростелеком Солар

# Проведение полномасштабных киберучений

**Министерство энергетики**

Проведение командно-штабных тренировок
и практических киберучений

**Что было сделано:**

- Отработка модели управления и координации работ по противодействию кибератакам
- Отработка действий по ликвидации последствий кибератак и восстановлению штатного режима функционирования объектов нефтегазовой отрасли
- Оценка существующих планов реагирования на скоординированные кибератаки

**60** обученных специалистов

**Результат киберучений:**

- Выработка необходимых мер защиты и противодействия кибератакам
- Обмен лучшими практиками обеспечения безопасности индустриального интернета вещей на цифровых подстанциях

**Подробнее:** https://rt-solar.ru/events/news/1758/



Ростелеком Солар

# Текущий уровень информационной безопасности АСУ ТП и ЗОКИИ

**Примите участие в исследовании «Текущее состояние уровня информационной безопасности АСУ ТП и ЗОКИИ»**



Ростелеком Солар

Ростелеком
Солар

Центральный офис

## 125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

cybermir@rt-solar.ru