

Роман Краснов

Заместитель директора по разработке
средств защиты промышленных систем

Уязвимости и основные вектора атак на КИИ

INFOSECURITY 2017

Круглый стол: «О безопасности критической информационной инфраструктуры»

POSITIVE TECHNOLOGIES

ptsecurity.ru

Positive Technologies в цифрах

Крупнейший центр противодействия киберугрозам

Санкт-Петербург

Москва

Нижний Новгород

Самара

Томск

Новосибирск

ЛУЧШИЕ СПЕЦИАЛИСТЫ

750+ сотрудников

250+ экспертов по защите ERP, SCADA, банков и телекомов, веб- и мобильных приложений

 Check Point
SOFTWARE TECHNOLOGIES LTD.

SIEMENS


CISCO™

Google

 Microsoft

НАДЕЖНЫЕ ПАРТНЕРЫ

100+ ведущих интеграторов в сфере ИТ и ИБ

50+ крупнейших мировых производителей ПО и оборудования

Нам доверяют более 1000+ компаний в 30 странах



15

Многолетняя экспертиза в корпоративной, промышленной безопасности и разработке ПО



Десятки широкомасштабных исследований защищенности промышленных предприятий ежегодно



Нами обнаружены сотни уязвимостей в промышленных системах и оборудовании



Участник национального комитета СИГРЭ



phd7 THE STANDOFF ENEMY INSIDE 23-24 мая 2017

Positive Hack Days

Видео с PHDays

О форуме Программа The Standoff Принять участие Новости Контакты Выставка Архив

ОРГАНИЗАТОР

POSITIVE TECHNOLOGIES

НОВОСТИ

The Best of Positive Hack Days VII

18.07.2017
Конкурентная разведка на PHDays: шпионим через Инстаграм и Фейсбук

Онлайновый конкурс по конкурентной разведке проводится на конференции Positive Hack Days уже шестой год подряд - и наглядно показывает, как легко в современном мире получить различную ценную информацию о людях и компаниях.
[Подробнее](#)

05.07.2017
PHDays HackBattle: ломаем один на один

В мае на конференции по практической информационной безопасности

Positive Hack Days — международный форум по практической безопасности, который проходит в Москве ежегодно начиная с 2011 года. Организатор — компания Positive Technologies.

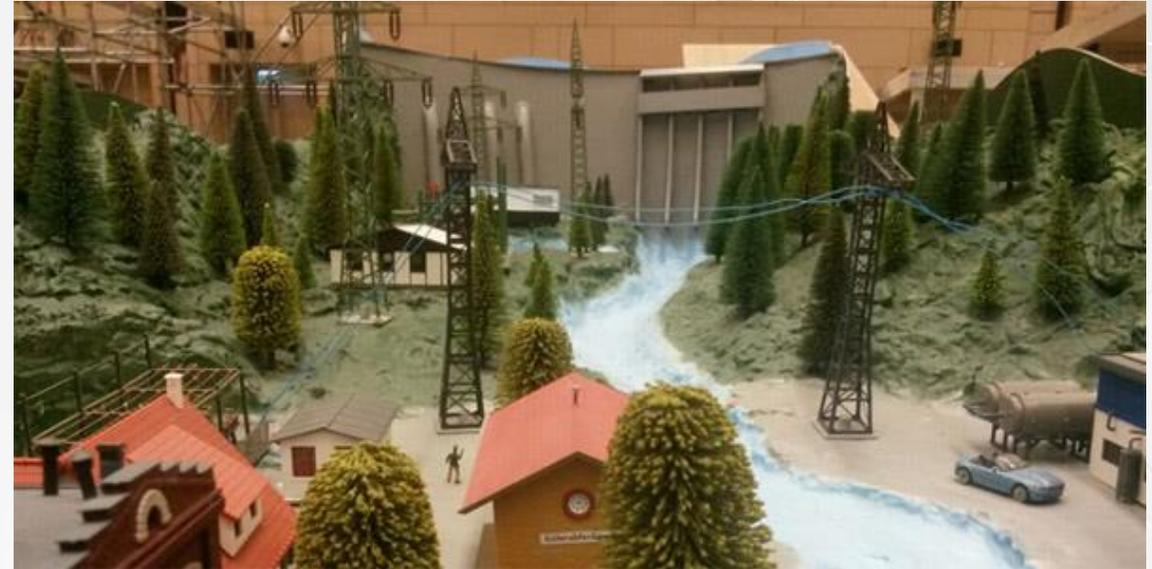
На два дня форум собирает вместе разработчиков, ИБ-экспертов и хакеров, представителей госструктур, крупных бизнесменов, представителей СМИ. Positive Hack Days — не просто площадка для обсуждения острых вопросов безопасности, а огромный исследовательский полигон для самых смелых экспериментов. Организаторы следуют неизменному правилу: минимум рекламы и максимум практики, интересных докладов и захватывающих конкурсов.

В 2011 году форум посетило 500 человек. Сейчас количество участников PHDays достигает 6000 человек из разных стран мира: Америки, Израиля, Кореи, Италии, Франции, Германии, Казахстана, Белоруссии, Индии, Польши.

Владимир Воронцов
ONsec

Алексей Красов
Газинформсервис

Владимир Стиран
БМС Консалтинг



Анализ защищенности АСУ ТП: Практический опыт





В нашу технологическую сеть не пробраться злоумышленнику!!!11111



Рабочие станции привилегированных пользователей



Подключение напрямую вне пределов контролируемой зоны



Уязвимые OPC-сервисы и серверы MES-инфраструктуры



Гостевые беспроводные сети



Интернет



Ошибки конфигурирования межсетевых экранов и других устройств сетевой инфраструктуры

phd7 Positive Hack Days **THE STANDOFF ENEMY INSIDE**

Управляем технологическим процессом

POSITIVE TECHNOLOGIES

Функции нагрузки в прошивке принтера:

- FULL POWER – увеличение выбросов дыма
- NORMAL POWER – включение штатного режима
- SWITCH FACTORY OFF - Остановка завода (ransomware ☺)
- SWITCH FACTORY ON - Запуск завода

Все действия вызываются командами с ноутбука по Wi-Fi «из-за забора»

```
graph TD; Laptop[Laptop] <--> LAN((LAN)); SCADA[SCADA] <--> LAN; LAN <--> Printer[EVIL PRINTER]; Laptop -.->|Wi-Fi| Printer;
```

Evil Printer: собираем нескучную прошивку

89 views



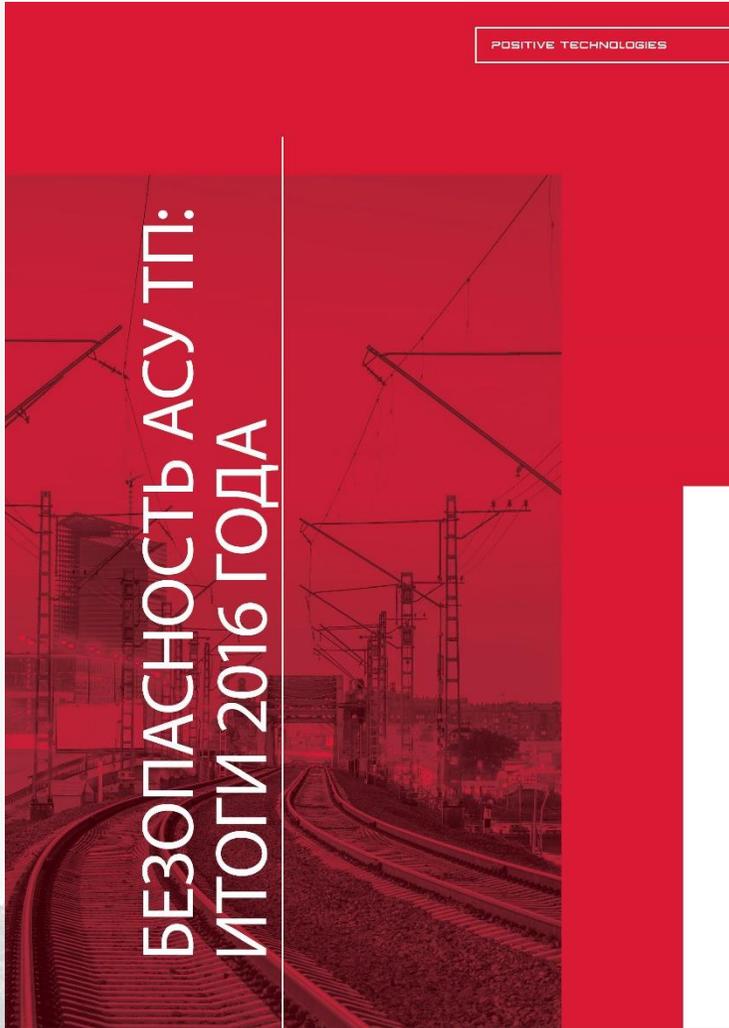
PositiveTechnologies
Published on Jul 7, 2017

4 0 SHARE

SUBSCRIBE 4.3K

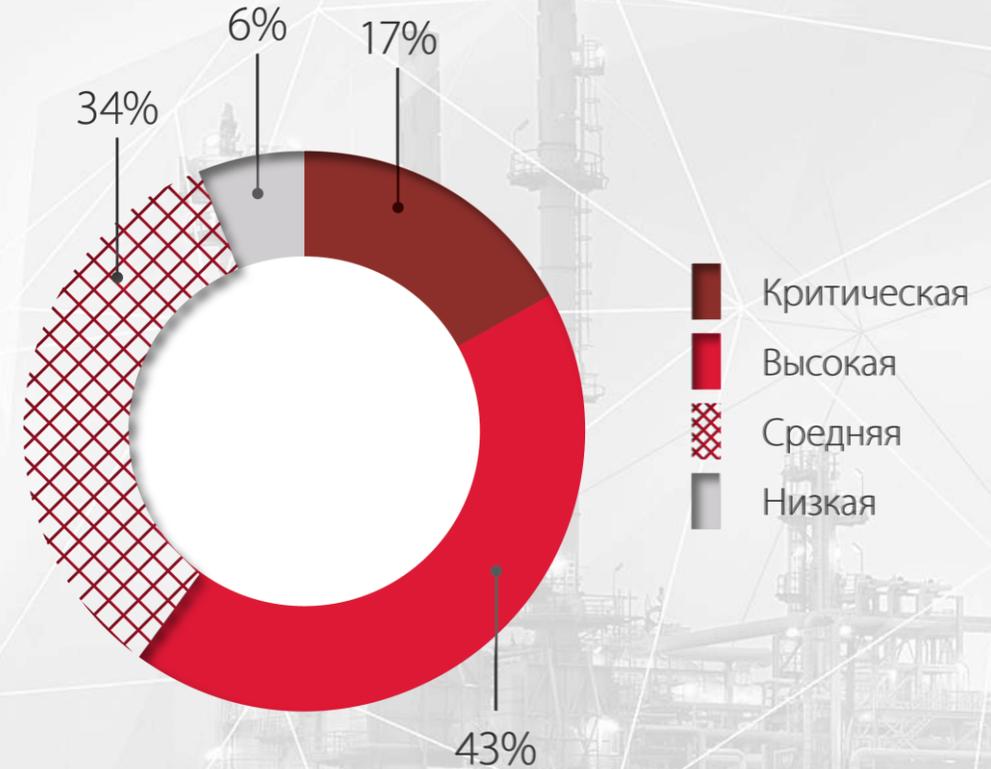
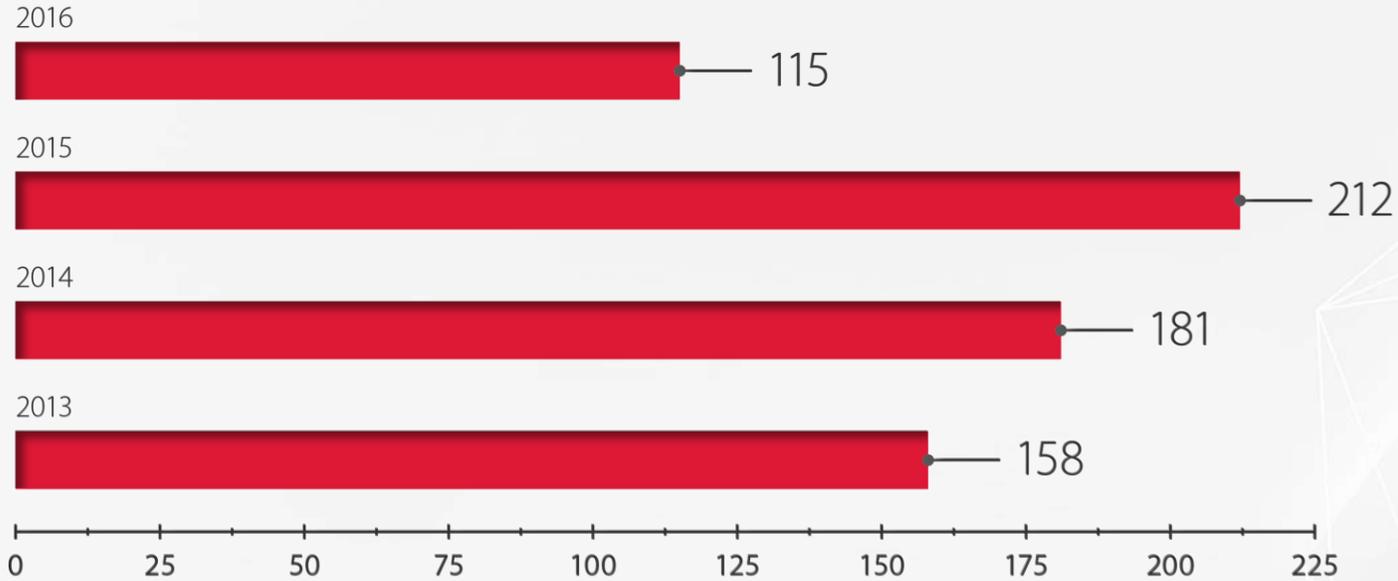


У нас тут тоже всё надежно и защищено! ... Но это не точно



В качестве основы для исследования была использована информация из общедоступных источников

- **Positive Research Center**
- **ICS-CERT**
- **NVD/NIST, CVE/MITRE**
- **Siemens Product CERT**
- **Schneider Cybersecurity Portal**



Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП

Распределение уязвимостей по степени риска



Количество уязвимостей обнаруживаемых в АСУ ТП остается стабильно высоким с каждым годом



Большая часть уязвимостей, найденных в 2016 году, приходится на устройства, выполняющие функции диспетчеризации и мониторинга (HMI/SCADA)

60%

Большинство выявленных уязвимостей систем АСУ ТП имеют высокую и критическую степень риска



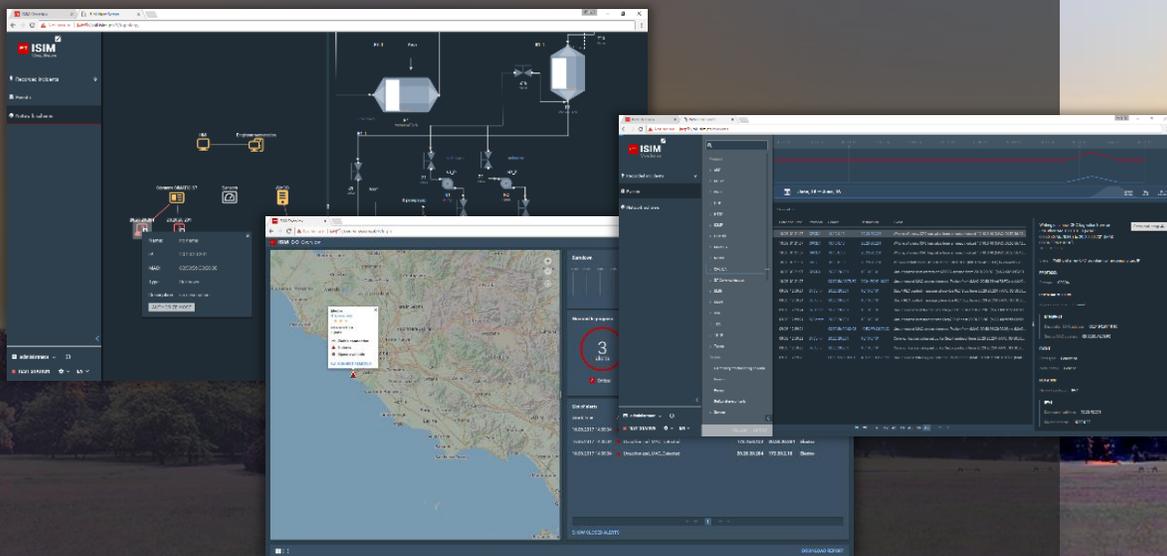
Устранение проблем производителем всё еще затруднительный и непрозрачный процесс

Комплексный подход к кибербезопасности промышленных систем

POSITIVE TECHNOLOGIES

PT ISIM

- Непрерывный мониторинг защищенности
- Поддержка основных платформ АСУ ТП
- Нулевое влияние на технологическую сеть
- Эффективное управление инцидентами ИБ
- Оперативный анализ бизнес-рисков
- Распределенная архитектура (SOC)





Заказчик: ОАО «РЖД»,
ООО «Бомбардье Транспортейшн (Сигнал)»



Отрасль: транспорт, производство
железнодорожной техники



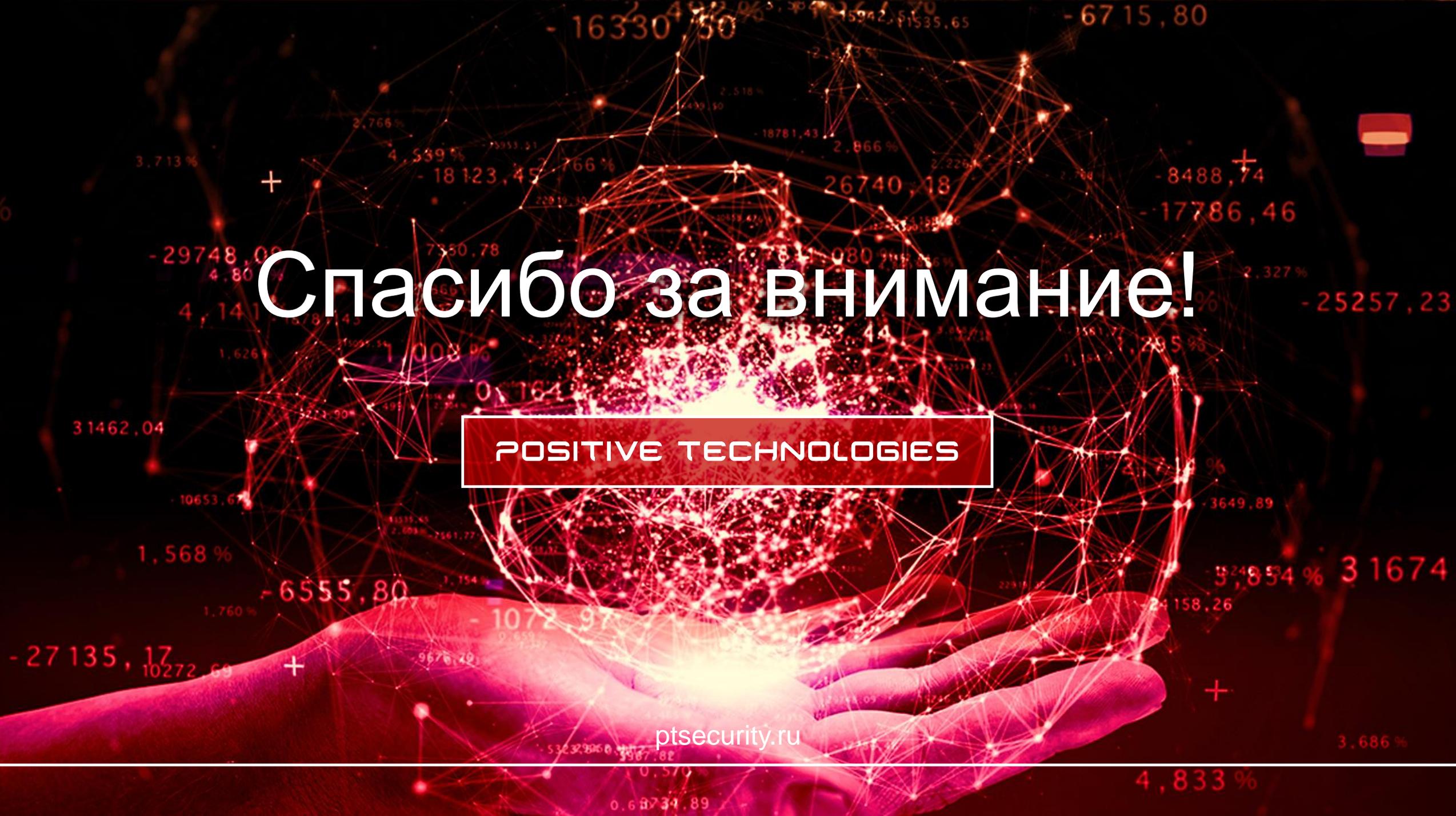
Задача: выявить новые киберугрозы для системы
микропроцессорной централизации EBILock 950,
повысить ее защищенность



Решение: Система управления инцидентами
кибербезопасности PT ISIM (Industrial Security Incident Manager)



**Лучшее отраслевое
решение, Global CIO 2016**



Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.ru