Роман Краснов

Заместитель директора по разработке
средств защиты промышленных систем

Уязвимости и основные вектора атак на КИИ

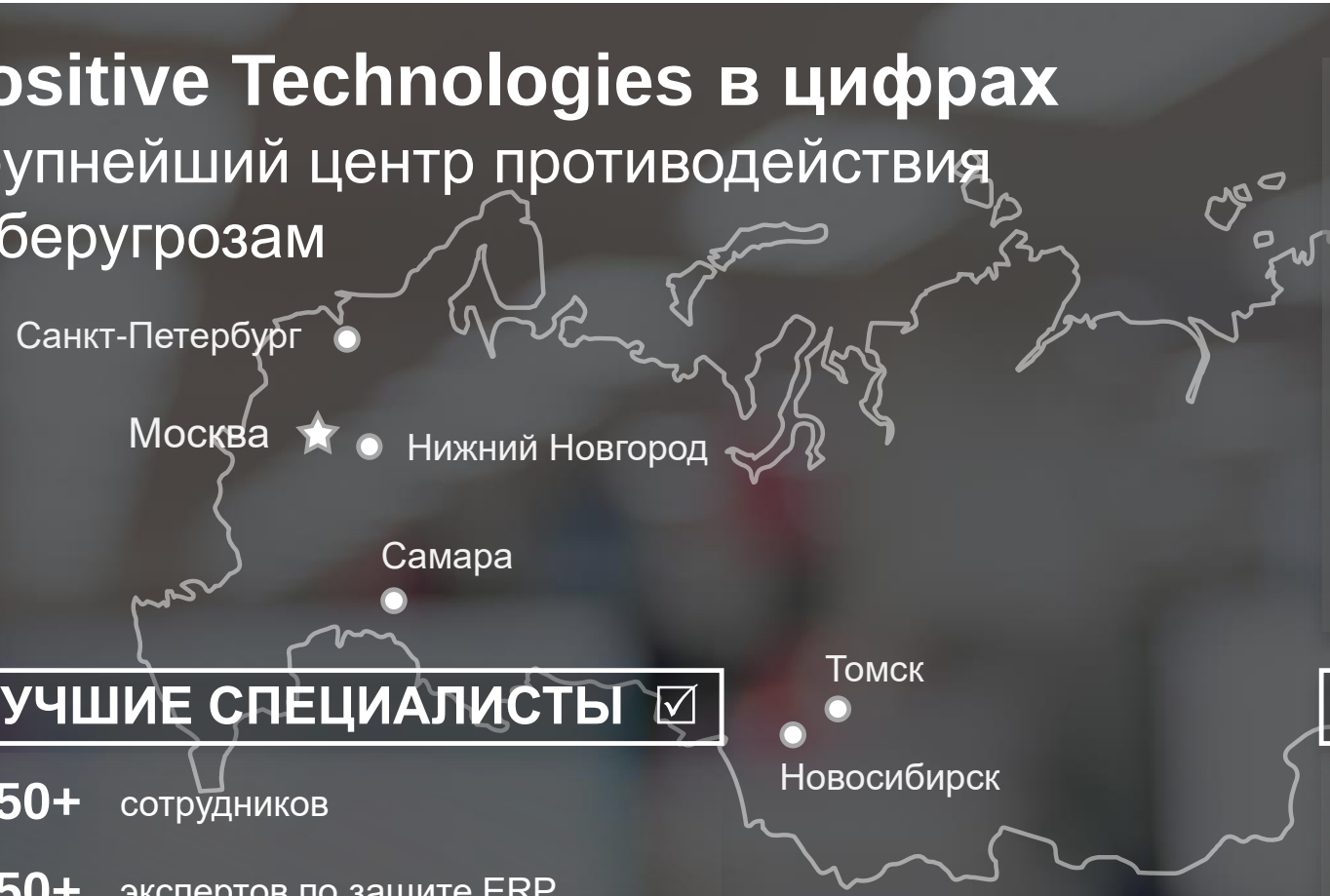
INFOSECURITY 2017
Круглый стол: «О безопасности критической информационной инфраструктуры»

POSITIVE TECHNOLOGIES

ptsecurity.ru

Positive Technologies в цифрах

Крупнейший центр противодействия киберугрозам



ЛУЧШИЕ СПЕЦИАЛИСТЫ ☑

750+ сотрудников

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

НАДЕЖНЫЕ ПАРТНЕРЫ ☑

Check Point SOFTWARE TECHNOLOGIES LTD.
SIEMENS
CISCO
Google
Microsoft

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

cigré Russian National Committee

Организатор Positive Hack Days

POSITIVE TECHNOLOGIES

phd Positive Hack Days

Анализ защищенности АСУ ТП: Практический опыт

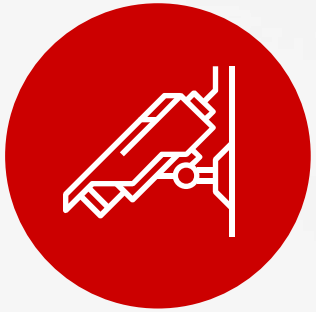
Анализ защищенности: 1. Проникновение извне

POSITIVE TECHNOLOGIES

Вектора проникновения

POSITIVE TECHNOLOGIES

Рабочие станции привилегированных пользователей

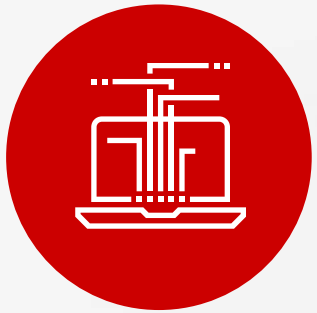


Подключение напрямую вне пределов контролируемой зоны

Уязвимые OPC-сервисы и серверы MES-инфраструктуры

Вектора проникновения

POSITIVE TECHNOLOGIES



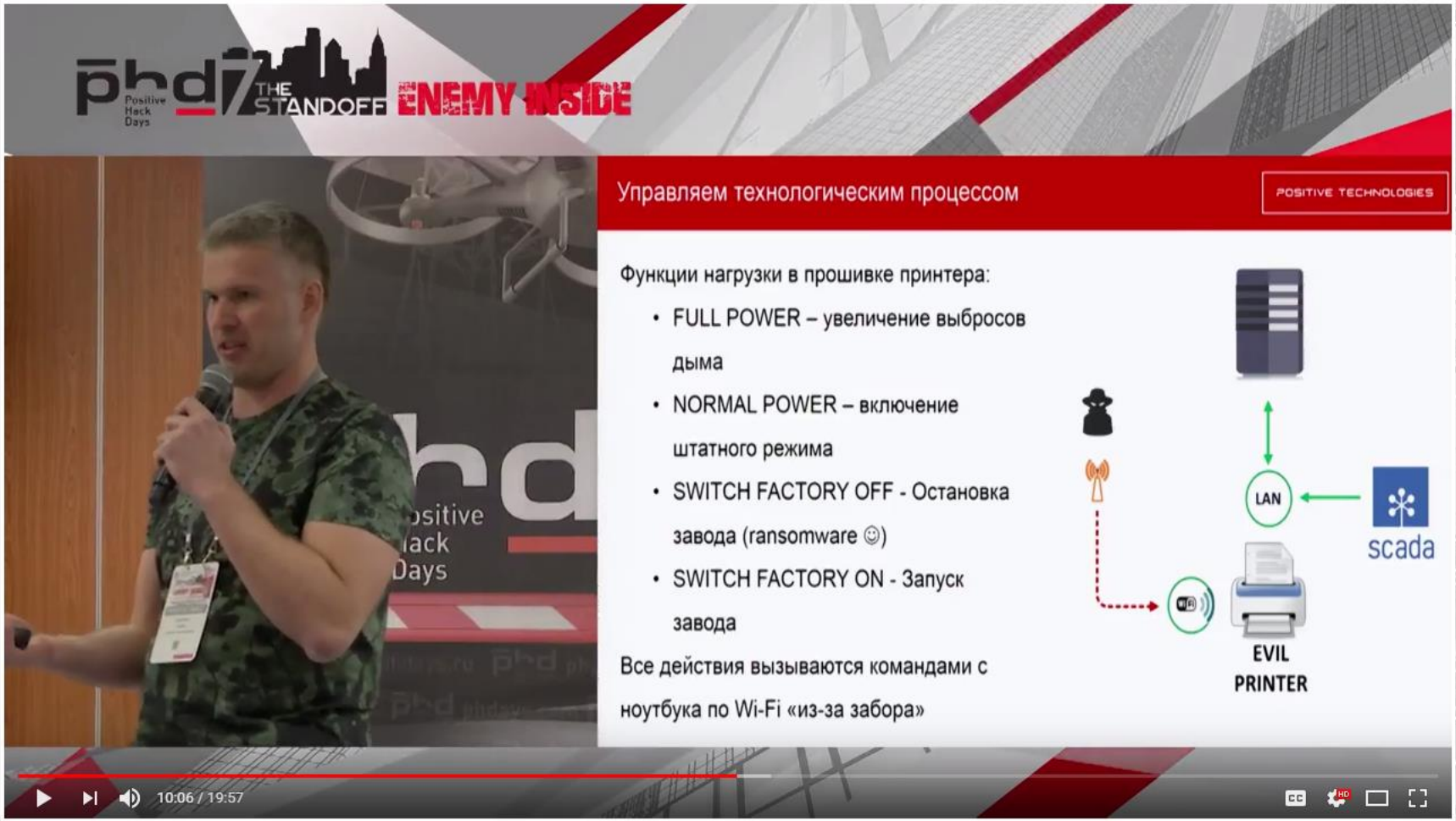
Гостевые беспроводные сети

Интернет

Ошибки конфигурирования межсетевых экранов и других устройств сетевой инфраструктуры

Нескучный сетевой принтер

POSITIVE TECHNOLOGIES



Evil Printer: собираем нескучную прошивку

89 views

4 0 SHARE

PositiveTechnologies
Published on Jul 7, 2017

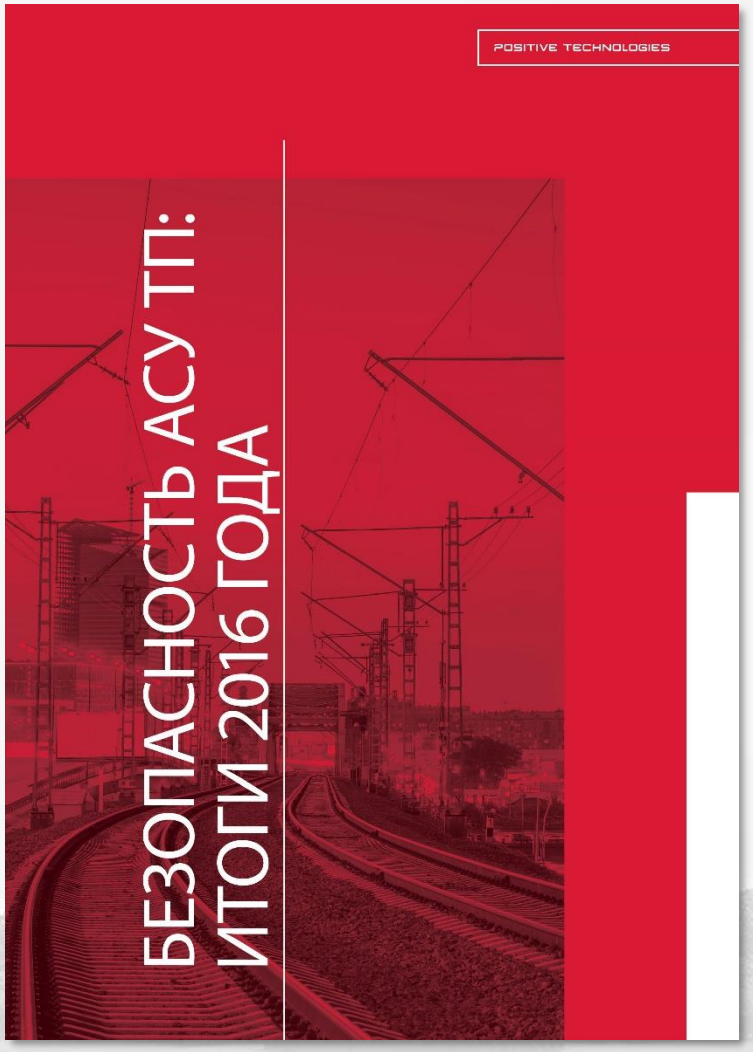
SUBSCRIBE 4.3K

Анализ защищенности: 2. Атака на АСУ ТП

POSITIVE TECHNOLOGIES

Positive Research 2017: Безопасность АСУ ТП

POSITIVE TECHNOLOGIES

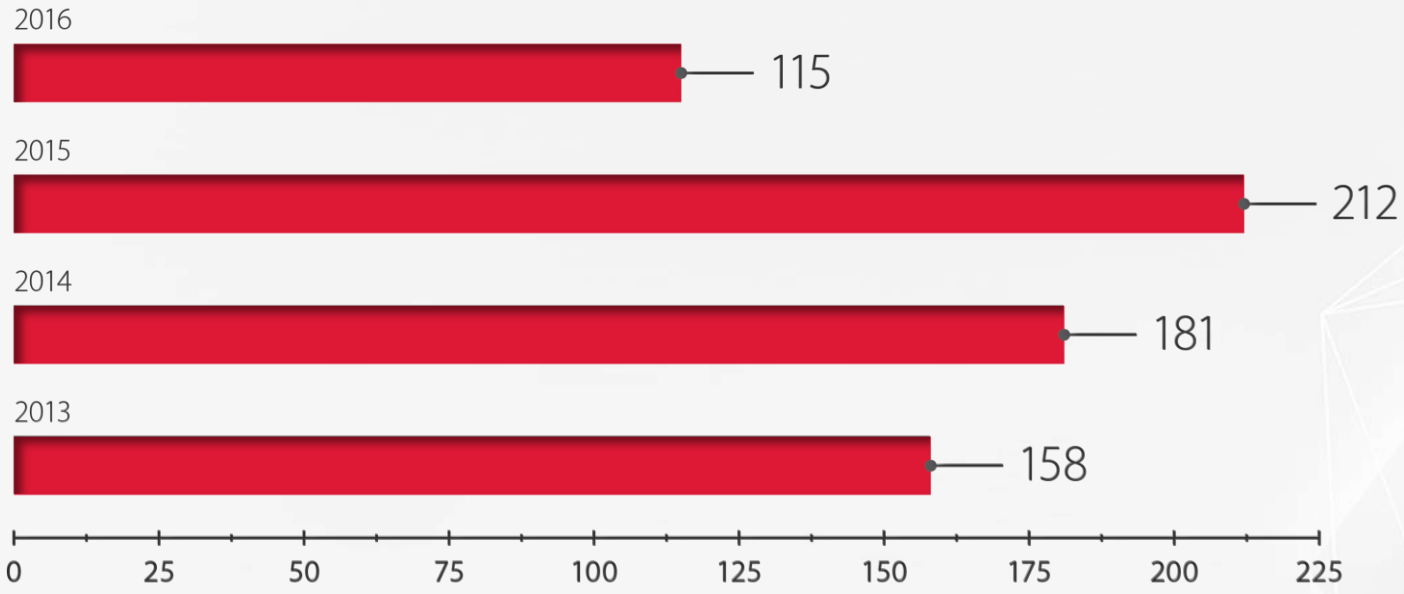


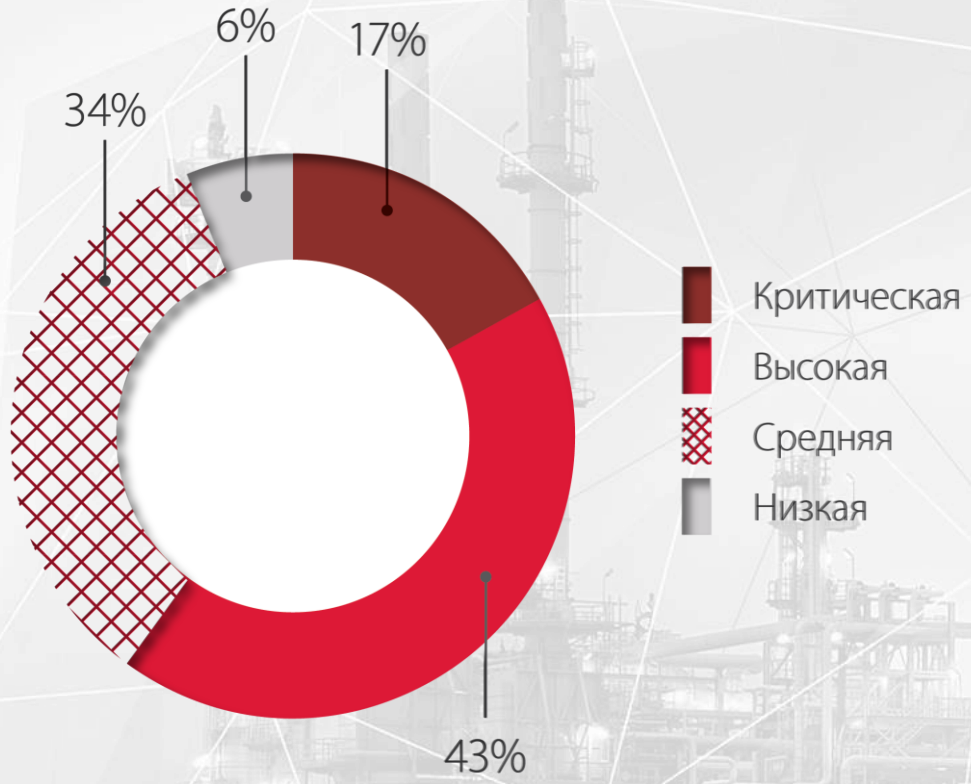
В качестве основы для исследования была использована информация из общедоступных источников

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

Positive Research 2017: Безопасность АСУ ТП

POSITIVE TECHNOLOGIES





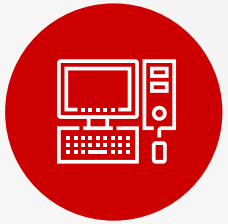
Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП

Распределение уязвимостей по степени риска

Positive Research 2017: Безопасность АСУ ТП

POSITIVE TECHNOLOGIES

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

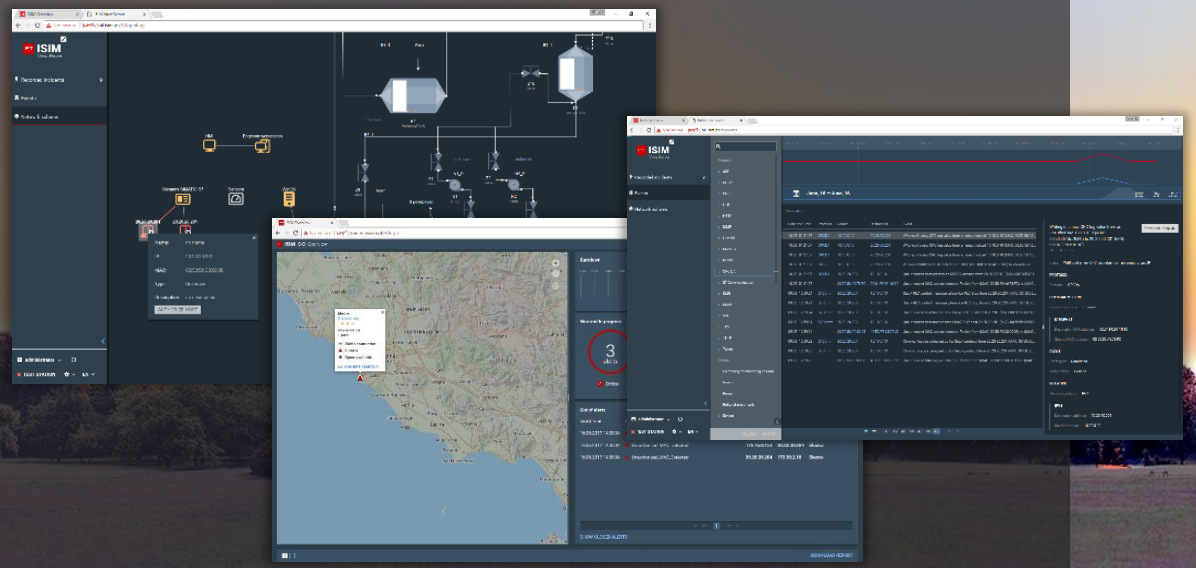
Комплексный подход к кибербезопасности промышленных систем

POSITIVE TECHNOLOGIES

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)



Пример реализации комплексного подхода к ИБ АСУ ТП

POSITIVE TECHNOLOGIES

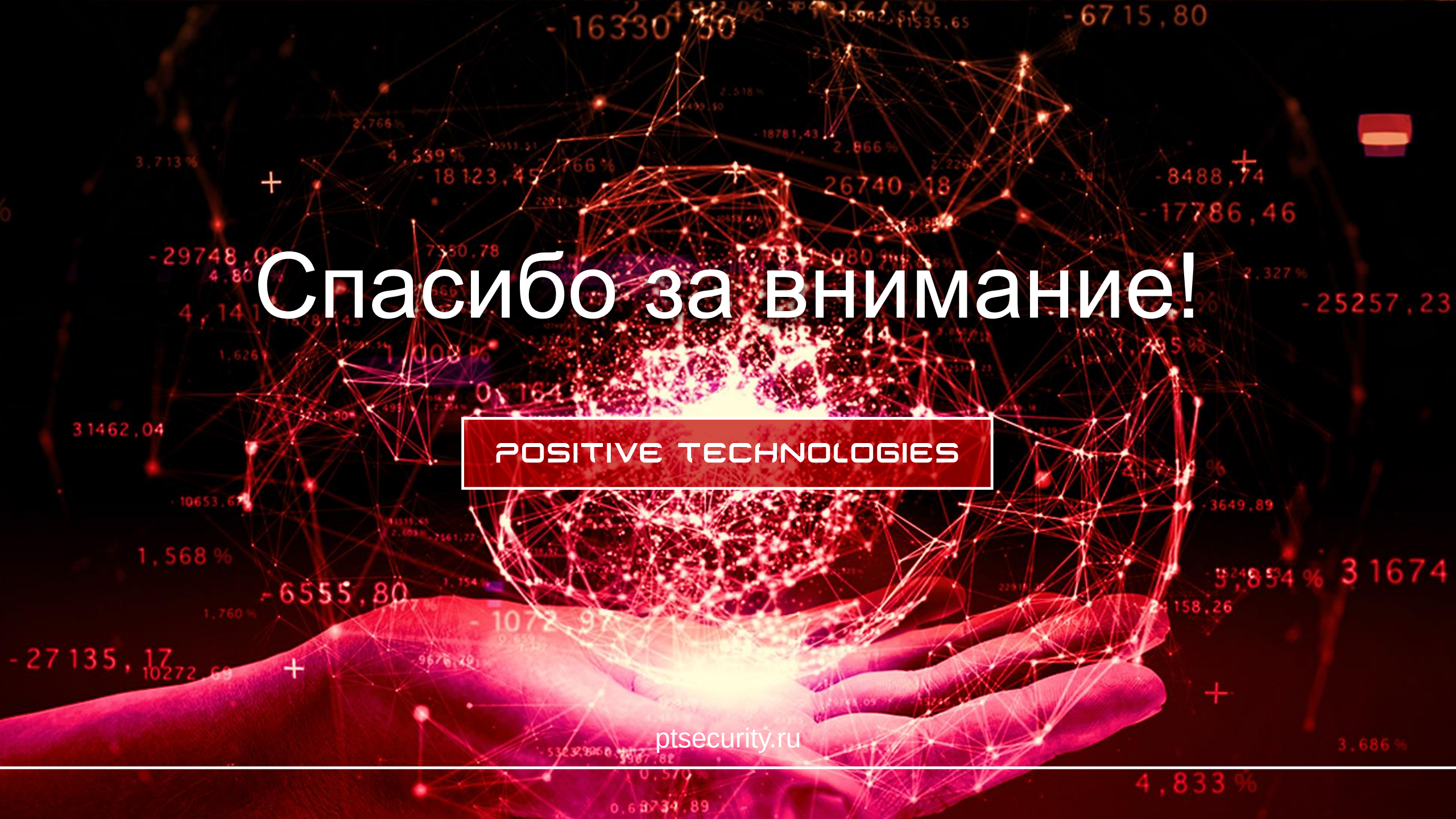
Заказчик: ОАО «РЖД»,
ООО «Бомбардье Транспортейшн (Сигнал)»

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