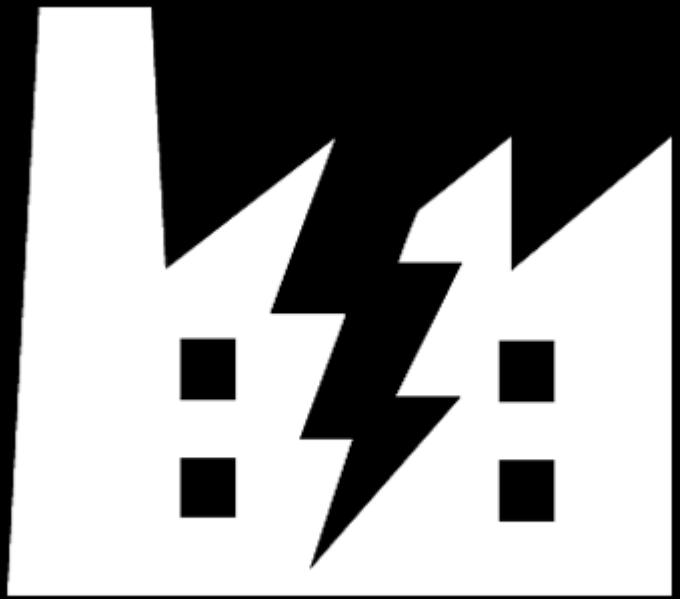




Кибербезопасность промышленных инфраструктур

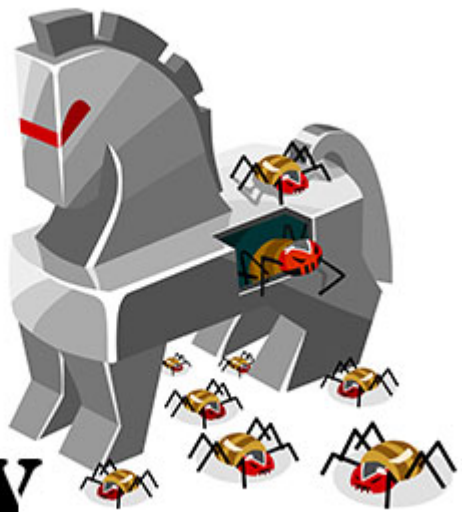


STUXnet



INDUSTROYER

**BLACK
ENERGY**



LOCKERGOGA

44 %

**USB-накопителей
содержат вредоносные файлы**

26%

**угроз могут вызвать
потерю контроля**

2% - Triton

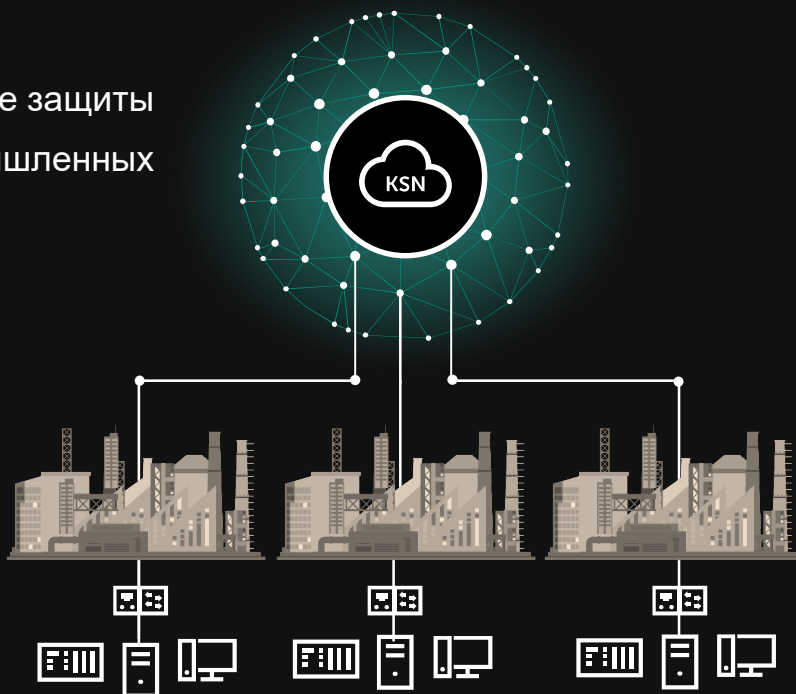
2% - Stuxnet

1% - WannaCry

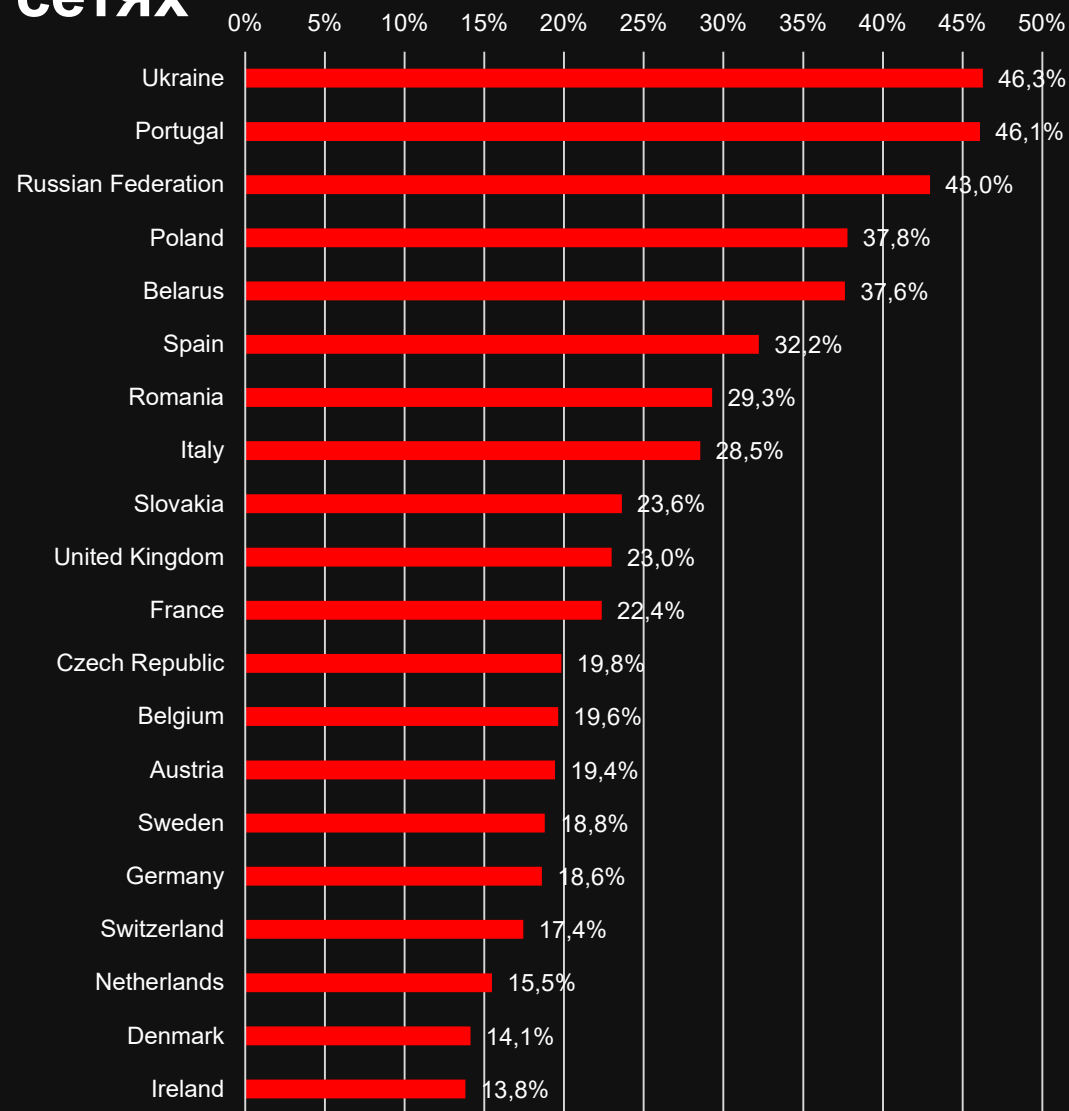
Данные ЛК об угрозах в промышленных сетях

KASPERSKY LAB
ICS CERT

Обозревает состояние защиты
более 100 000 промышленных
узлов по всему миру



В 2018 ГОДУ
БОЛЕЕ 40%
КОМПЬЮТЕРОВ В АСУ ТП В МИРЕ
ПОДВЕРГЛИСЬ АТАКЕ



Статистика Kaspersky Security Network

KASPERSKY

Ландшафт угроз



Проблематика



Непрозрачная инфраструктура

Индустриальные сети строятся и поддерживаются фрагментарно в разное время, нет единой точки мониторинга



Локальные практики базовой ИБ

На разных установках – разные средства и политики ИБ, нет централизации даже для самых простых мер (АВ, контроль устройств..)



Неосведомленность персонала

Нехватка специалистов в ИБ АСУ ТП.
Неосведомленность о рисках среди инженерного состава

К чему приводят?



- **Случайное заражение**
(Например шифровальщик WannaCRY)
- **Целевая атака на АСУТП**
(Например Stuxnet, BlackEnergy)



Риски для предприятия?



- **Простой**
- **Ущерб оборудованию**
- **Утечка данных**

Риски для государства?

- **Жертвы / Социальные последствия**
- **Нарушение жизнедеятельности**
- **Снижение обороноспособности**

Чем мы можем помочь?



Непрозрачная инфраструктура

Индустриальные сети строятся и поддерживаются фрагментарно в разное время, нет единой точки мониторинга



Локальные практики базовой ИБ

На разных установках – разные средства и политики ИБ, нет централизации даже для самых простых мер (АВ, контроль устройств..)



Неосведомленность персонала

Нехватка специалистов в ИБ АСУ ТП.
Неосведомленность о рисках среди инженерного состава



Анализ
Защищенности

Оценка текущей защищенности и конкретные методы ее повышения



KICS
for Networks

Инвентаризация тех сети и выявление вторжений



KICS
for Nodes

Централизованные базовые средства защиты для всей инфраструктуры



Обучающие
программы

Тренинги
(Профессиональные и для широкого круга)

Чем мы можем помочь?

CERT

Advanced
Consultancy



Kaspersky®
ICS CERT

Данные об угрозах,
Специальные отчеты



Kaspersky®
Threat Intelligence

Тренинг по тесту на
проникновение



Kaspersky®
Security Awareness

Тренинг по поиску
уязвимостей



Kaspersky®
Security Awareness

SOC

Услуга по мониторингу и
реагированию



Kaspersky®
Managed Protection

Интеграция
с SIEM



Тренинг по
расследованиям



Kaspersky®
Security Awareness

Реагирование на
инциденты



Kaspersky®
Incident Response

Площадка/Предприятие

Тесты на
проникновение

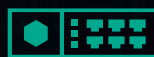


Kaspersky®
Security Assessment

Защита конечных узлов
Мониторинг сетей



KICS
for Nodes



KICS
for Networks

Повышение
осведомленности



Kaspersky®
Security Awareness

Реагирование на
инциденты



Kaspersky®
Incident Response

Выявление
аномалий



Machine Learning
for Anomaly
Detection

Комплексная безопасность промышленных объектов

МОДЕЛЬ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ (ISA-95)*

УРОВЕНЬ 4

Бизнес-планирование и логистика



Управление непрерывной цепочкой поставок. Формирование базового режима работы предприятия: производство, использование материалов, доставка.

УРОВЕНЬ 3

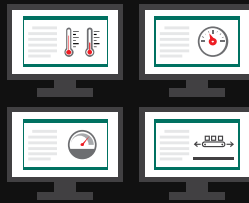
Управление производственными операциями



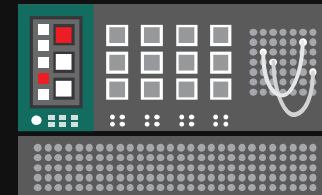
Контроль рабочего потока/параметров с целью произвести желаемый конечный продукт. Поддержка записей и оптимизация производственного процесса.

УРОВНИ 2, 1

Контроль производственных процессов



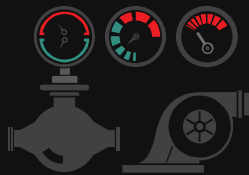
Мониторинг, управление в диспетчерском режиме и автоматизированное управление производственными процессами



Считывание производственного процесса, управление производственным процессом

УРОВЕНЬ 0

Физический



Физические устройства



Kaspersky®
Anti Targeted
Attack
platform



Kaspersky®
Endpoint
Detection and
Response



Kaspersky®
Industrial
CyberSecurity



Machine
Learning for
Anomaly
Detection

* ISA-95 – международный стандарт от Международного сообщества автоматизации, принятый для разработки автоматизированного интерфейса между предприятием и системами промышленного контроля

Комплексный Подход



Kaspersky®
Industrial
CyberSecurity

Сервисы

Продукты

Тренинги

Экспертные сервисы

Защита конечных
узлов

Мониторинг сетей
и обнаружение
вторжения

Централизованное
управление



Базовая
осведомленность
персонала

Профессио-
нальные
тренинги

Анализ
Защищенности

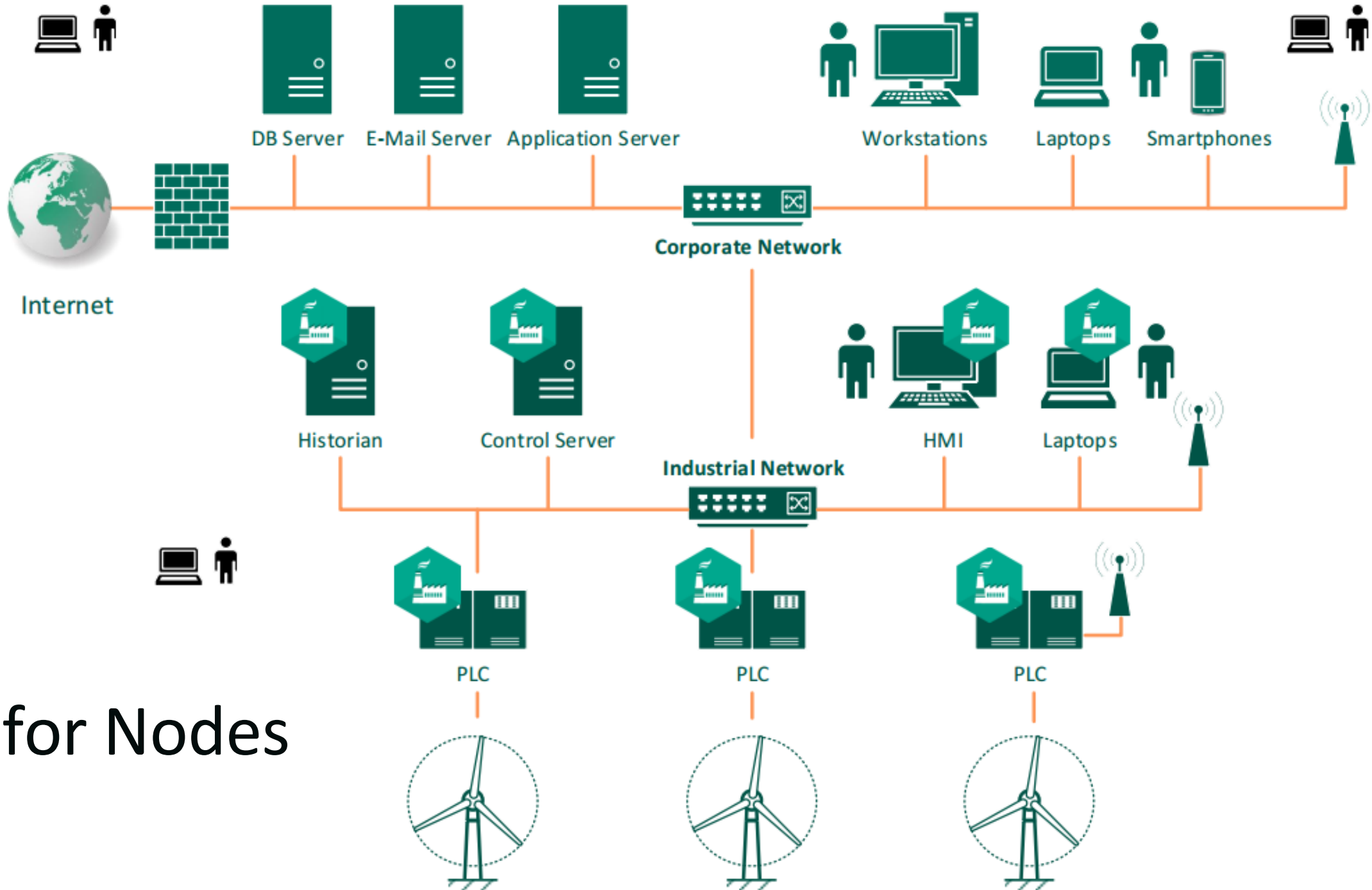
Реагирование
на
инциденты

Потоки
данных

KICS
for Nodes

KICS
for Networks

Kaspersky®
Security
Center



KICS for Nodes

Не применимость «Офисных» средств защиты в технологических сетях



ПРОБЛЕМЫ В ТЕХНОЛОГИЧЕСКОЙ СЕТИ:



Высокое потребление ресурсов защищаемой системы



Высокая вероятность ложного срабатывания

КЛАССИЧЕСКОЕ РЕШЕНИЕ:



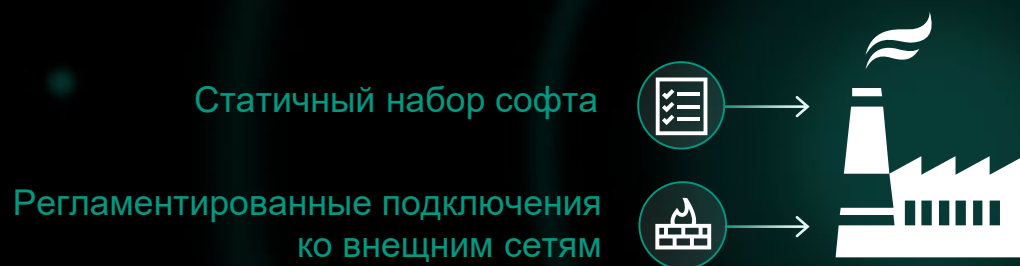
Тонкий «тюнинг» средств защиты:

- Исключение областей проверок
- Отключение защитных технологий
- Особые регламенты работы



СЛОЖНО И ДОРОГО

Промышленная кибербезопасность на примере Endpoint Protection



Промышленные средства защиты

- Ограничение программной среды
- Периодические проверки

ТРЕБОВАНИЯ К СПЕЦИАЛИЗИРОВАННОМУ ПРОДУКТУ ДЛЯ ЗАЩИТЫ КОМПОНЕНТ АСУ ТП:



Прогнозируемое потребление ресурсов защищаемой системы



Отсутствие ложных срабатываний

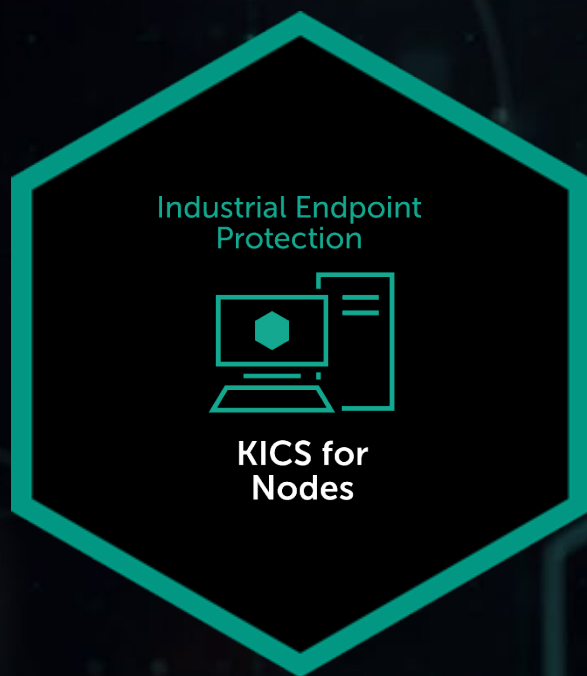


Легкая установка и настройка



Поддержка старых ОС

KICS FOR NODES – СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ



ПРЕДОТВРАТИТЬ ЗАПУСК НЕЖЕЛАТЕЛЬНОГО ПО APPLICATION STARTUP CONTROL

- Автоматическое создание белого списка ПО для каждого узла
- Запрет запуска неизвестного ПО по умолчанию
- Затрудняет целевые атаки
- Предотвращает случайные заражения и нежелательное поведение пользователей



ДЕТЕКТ ВРЕДНОСОВ БЕЗ ЗАМЕДЛЕНИЯ РАБОТЫ УЗЛОВ

- Мульти-процессная архитектура интеллектуально распределяет и ограничивает потребление ресурсов
- Анти-Криптор
- Анализ логов



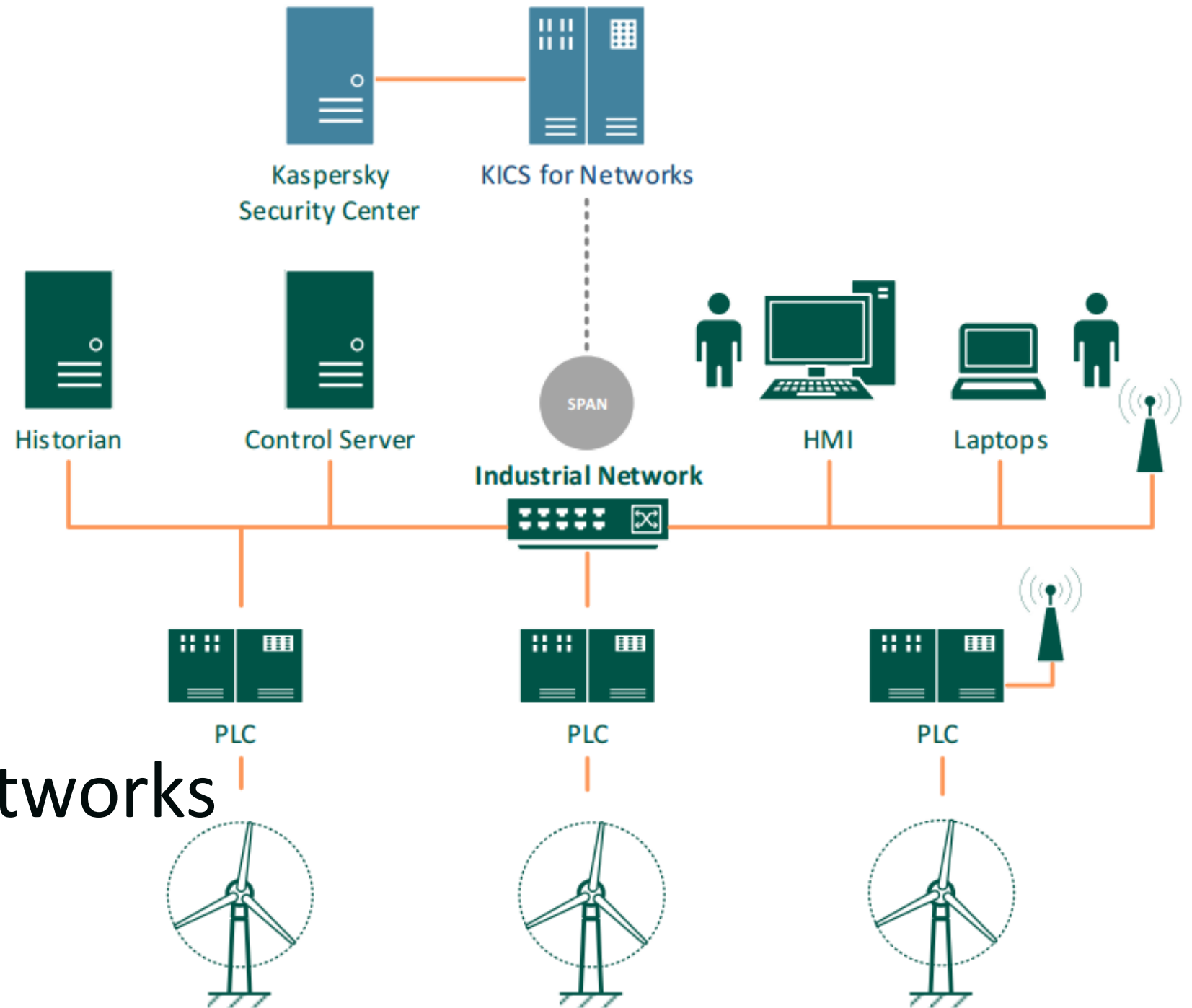
КОНТРОЛЬ ПРОГРАММНО-АППАРТНОГО ОКРУЖЕНИЯ

- Контроль устройств
- Контроль подключения к WiFi
- Контроль целостности файлов

Сертификаты совместимости

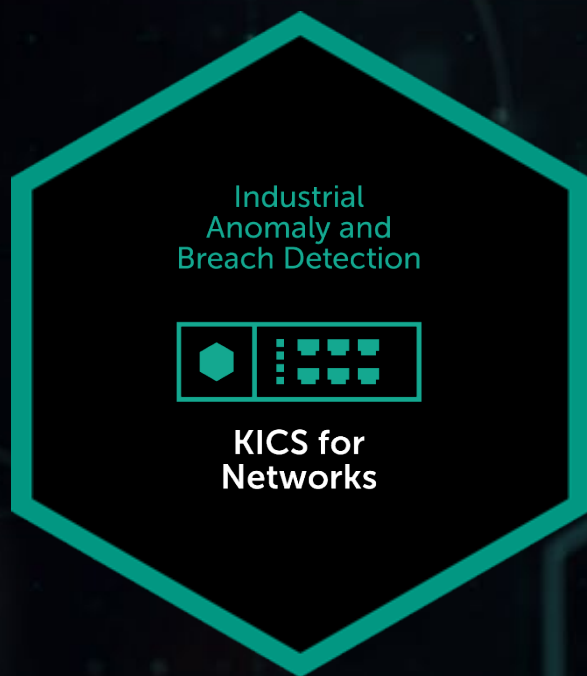
-  [Statement of compatibility with GE Cimplicity 8.2/9.0/9.5, GE Historian 5.5/7.0, GE Machine Edition 9.0 from GE Digital](#)
-  [Statement of compatibility with products from Iconics, Inc.](#)
-  [Statement of compatibility with WinCC Open Architecture 3.14 from ETM professional control GmbH](#)
-  [Акт проверки совместимости с АГАТ-2000 от ОАО «АГАТ-системы управления»](#)
-  [Акт проверки совместимости с «Вибробит Web.Net.Monitoring» от ООО НПП «Вибробит»](#)
-  [Акт проверки совместимости с ДельтаВ 13.3.1 \(русская версия\) от ООО «Эмерсон»](#)
-  [Акт проверки совместимости с программным комплексом ARIS SCADA от ООО «Прософт-Системы»](#)
-  [Акт проверки совместимости с программным комплексом СК-11 от ЗАО «Монитор Электрик»](#)
-  [Акт проверки совместимости с ПТК КРУГ-2000 версии не ниже 4.2 от ООО НПФ «КРУГ»](#)
-  [Акт проверки совместимости с «ОИК-Диспетчер НТ» от ООО «НТК Интерфейс»](#)
-  [Акт проверки совместимости со SCADA NPT Expert от ООО «ЭнергопромАвтоматизация»](#)
-  [Заключение о совместимости с EKRASCADA от ООО НПП «ЭКРА»](#)
-  [Заклучение о совместимости с EKRASMS от ООО НПП «ЭКРА»](#)
-  [Заклучение о совместимости с EKRASMS-SP от ООО НПП «ЭКРА»](#)
-  [Заявление о совместимости с EcoStruxure Foxboro DCS \(Foxboro Evo\) от Schneider Electric](#)
-  [Заявление о совместимости с HOLLiAS MACS от Hangzhou HollySys Automation Co., Ltd.](#)
-  [Заявление о совместимости с PCS 7 V8.2 SP1 от ООО «Сименс»](#)
-  [Заявление о совместимости с PcVue от ARC Informatique](#)
-  [Заявление о совместимости с Wonderware System Platform от Aveva](#)
-  [Заявление о совместимости с продуктами Schneider Electric](#)





KICS for Networks

KICS FOR NETWORKS – Сценарии использования



Инвентаризация и контроль целостности сети

- Пассивное определение устройств и их сетевых взаимодействий
- Визуализация карты сети
- «Белые списки» коммуникаций



Обработка инцидентов

- Немедленное уведомление о важных событиях
- Корреляция событий в инциденты
- Хранение и менеджмент истории



Интеграция корпоративной и пром ИБ

- Kaspersky Security Center
- Syslog Server
- SIEM



Мониторинг Технологического процесса

- Анализ параметров тех процесса
- Выявление воздействий на тех процесс

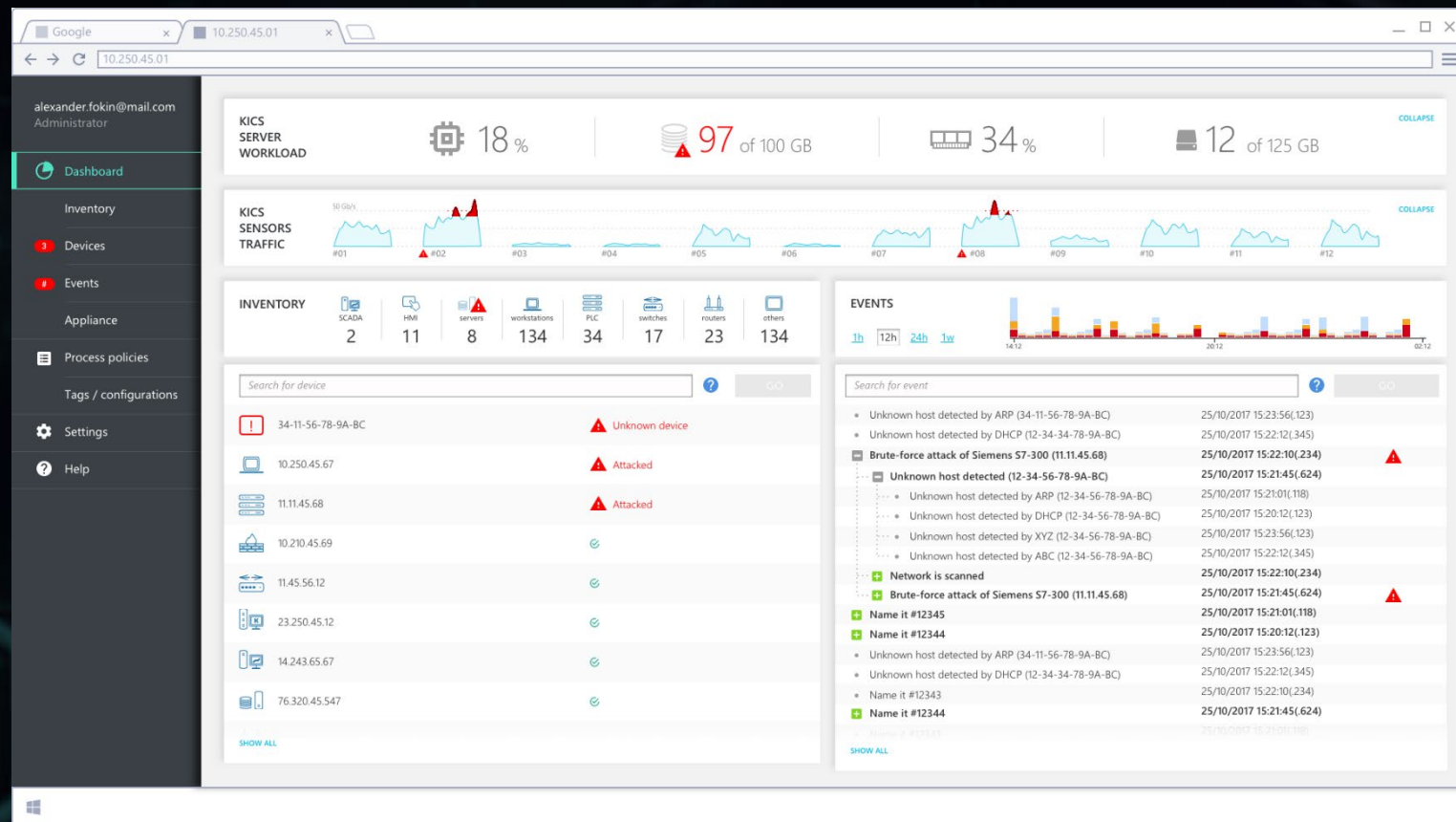


Мониторинг команд к промышленному оборудованию (ПЛК)

- Конфигурируемые правила на различные команды к ПЛК
- Выявление подключений, авторизации, чтения/записи памяти ПЛК, сервисных команд

KICS FOR NETWORKS USE CASES

1. Автоматическая инвентаризация Обнаружить устройства (PCs, Servers, laptops, PLCs, routers)



KICS FOR NETWORKS USE CASES

1. Автоматическая инвентаризация Обнаружить устройства (PCs, Servers, laptops, PLCs, routers)

The screenshot displays the KICS web interface. On the left is a navigation sidebar with options: Admin Administrator, Dashboard, Inventory, Devices (selected), Events, Appliance, Process policies, Tags / configurations, Settings, and Help. The main content area is titled 'Devices' and features a table with columns for Device, Security status, Transactions, and Commands. The first row, 'Device_0178', is highlighted in green. Below the table, a detailed view for 'DEVICE_0178' is shown, including sections for 'IN COMMUNICATIONS WITH...' (listing PLC_0002, Device_0957178, PLC_ABR6, Ethernet, and S7Comm) and '[Commands]' (listing Start PLC, Stop PLC, and Upload User Program). A warning message at the bottom states: 'Поиск остановлен. Добавить выбранные устройства, транзакции, команды в белый список?'.

| Device | Security status | Transactions | Commands |
|-------------------|-----------------|---------------|----------|
| Device_0178 | NEW | PLC_011 (+12) | StartVol |
| Device_095638 | NEW | PLC_012 (+11) | — |
| Device_0956267178 | NEW | PLC_013 (+11) | DeleteSW |
| Device_0534526178 | NEW | PLC_011 (+12) | StartVol |
| Device_095634528 | NEW | PLC_012 (+11) | — |
| Device_095678 | NEW | PLC_013 (+11) | DeleteSW |
| Device_095267178 | NEW | PLC_011 (+12) | StartVol |
| Device_0963426778 | NEW | PLC_012 (+11) | — |
| Device_0963526178 | NEW | PLC_013 (+11) | DeleteSW |

KICS FOR NETWORKS USE CASES

1. Автоматическая инвентаризация

Обнаружить устройства (PCs, Servers, laptops, PLCs, routers)

2. Карта сети

Визуализировать потоки данных между активами в тех сети

Конфигурация правил в интуитивном интерфейсе

Функция «Машины времени» для отслеживания развития нежелательных коммуникаций

The screenshot displays the KICS web interface for network management. The browser address bar shows the URL 10.250.45.01. The interface includes a sidebar with navigation options: Dashboard, Inventory, Devices (highlighted), Events, Appliance, Process policies, Tags / configurations, Settings, and Help. The main content area is titled 'All devices' and features a search bar and filter options for Status, Type, and Connection. Below these are tabs for 'List', 'Physical map', 'Communication map' (selected), and 'White-list rules'. The 'Communication map' shows a network diagram with various devices and their connections. A timeline at the bottom indicates communication activity from 14:32 to 15:00 on 20 Nov.

KICS FOR NETWORKS USE CASES

1. Автоматическая инвентаризация

Обнаружить устройства (PCs, Servers, laptops, PLCs, routers)

2. Карта сети

Визуализировать потоки данных между активами в тех сети

Конфигурация правил в интуитивном интерфейсе

Функция «Машины времени» для отслеживания развития нежелательных коммуникаций

3. Корреляция событий

-Корреляция связанных событий в единые инциденты

-Предсказать развитие инцидента для упреждающей реакции

The screenshot displays the Kaspersky Security Center (KSC) interface. On the left is a navigation sidebar with options like Dashboard, Inventory, Devices, Events, Appliance, Process policies, Tags / configurations, Settings, and Help. The main area shows 'All events' with a search bar and filters for severity and technology. A table lists events, with one event highlighted: 'Brute-force attack of Siemens S7-300 (11.11.45.12)'. To the right, a detailed view of this event is shown, including a 'Critical' severity indicator, a list of 'PROЙДЕННЫЕ ШАГИ' (Completed Steps), and 'ВАРИАНТЫ РАЗВИТИЯ СОБЫТИЙ (430)' (Event Development Variants). The first variant is circled in red and numbered '1', indicating a rule for 'Управление РЗА с неавторизованного хоста' (Control of RZS from unauthorized host).

| S... | Event | When |
|------|---|---------------------|
| | Unknown host detected by ARP (34-11-56-78-9A-12) | 25/10/2017 15:23:56 |
| | Unknown host detected by DHCP (12-34-34-78-9A-BC) | 25/10/2017 15:22:12 |
| | Brute-force attack of Siemens S7-300 (11.11.45.12) | 25/10/2017 15:21:01 |
| | Unknown host detected (12-34-56-78-9A-BC) | 25/10/2017 15:21:01 |
| | Unknown host detected by ARP (12-34-56-78-9A-BC) | - |
| | Unknown host detected by DHCP (12-34-56-78-9A-BC) | - |
| | 9 287 events hidden | SHOW ALL |
| | Unknown host detected by ABC (12-34-56-78-9A-BC) | - 1к 6д 12ч 23м 5 |
| | Network is scanned | 25/10/2017 15:22:10 |
| | Brute-force attack of Siemens S7-300 (11.11.45.68) | 25/10/2017 15:21:45 |
| | Name it #12345 | 25/10/2017 15:21:01 |
| | Name it #12344 | 25/10/2017 15:20:12 |
| | Unknown host detected by ARP (34-12-56-78-9A-BC) | 25/10/2017 15:23:56 |
| | Unknown host detected by DHCP (12-34-34-78-9A-BC) | 25/10/2017 15:22:12 |
| | Name it #12343 | 25/10/2017 15:22:10 |
| | Name it #12344 | 25/10/2017 15:21:45 |
| | Name it #12341 | 25/10/2017 15:21:01 |
| | Name it #12340 | 25/10/2017 15:20:12 |
| | Name it #12339 | 25/10/2017 15:23:56 |
| | Unknown host detected by DHCP (12-34-34-78-9A-BC) | 25/10/2017 15:23:56 |
| | Атака | 25/10/2017 15:22:12 |
| | Name it #12344 | 25/10/2017 15:21:45 |
| | Name it #12341 | 25/10/2017 15:21:01 |
| | Нелегитимное взаимодействие | 25/10/2017 15:20:12 |
| | Name it #12339 | 25/10/2017 15:23:56 |
| | Name it #12344 | 25/10/2017 15:23:56 |
| | Name it #12341 | 25/10/2017 15:22:12 |

ЭКСПЕРТНЫЕ СЕРВИСЫ



Kaspersky®
Security
Assessment

- Тест на проникновение – обнаружение актуальных способов проникнуть в пром сеть
- Набор приоритезированных рекомендаций по устранению проблем и целевая архитектура сети
- Опытная в АСУТП команда



Kaspersky®
Incident
Response

- Команда экстренного реагирования для локализации инцидента и выяснения его причин
- Доступна по запросу или по подписке



Kaspersky®
Threat
Intelligence

- Потоки данных об индустриальных угрозах
- Отчеты об угрозах в специфичных отраслях/странах

ОБУЧАЮЩИЕ СЕРВИСЫ



Kaspersky®
Security
Awareness

*Большинство инцидентов связаны с человеческим фактором
(Фишинг, нарушение регламентов)*

РЕШЕНИЕ:

- **Industrial CyberSecurity in Practice awareness training**

1 или 2 ДНЯ, 10-20 участников

ОЧЕВИДНОЕ отсутствие достаточного количества кадров на рынке

РЕШЕНИЕ:

- **ICS Penetration Testing for Professionals**

5 дней, до 10 участников

- **ICS Digital Forensics for Professionals**

4 дней, до 10 участников

- **ICS Vulnerability Research for Professionals**

8 дней, до 10 участников



Kaspersky®
Security
Trainings

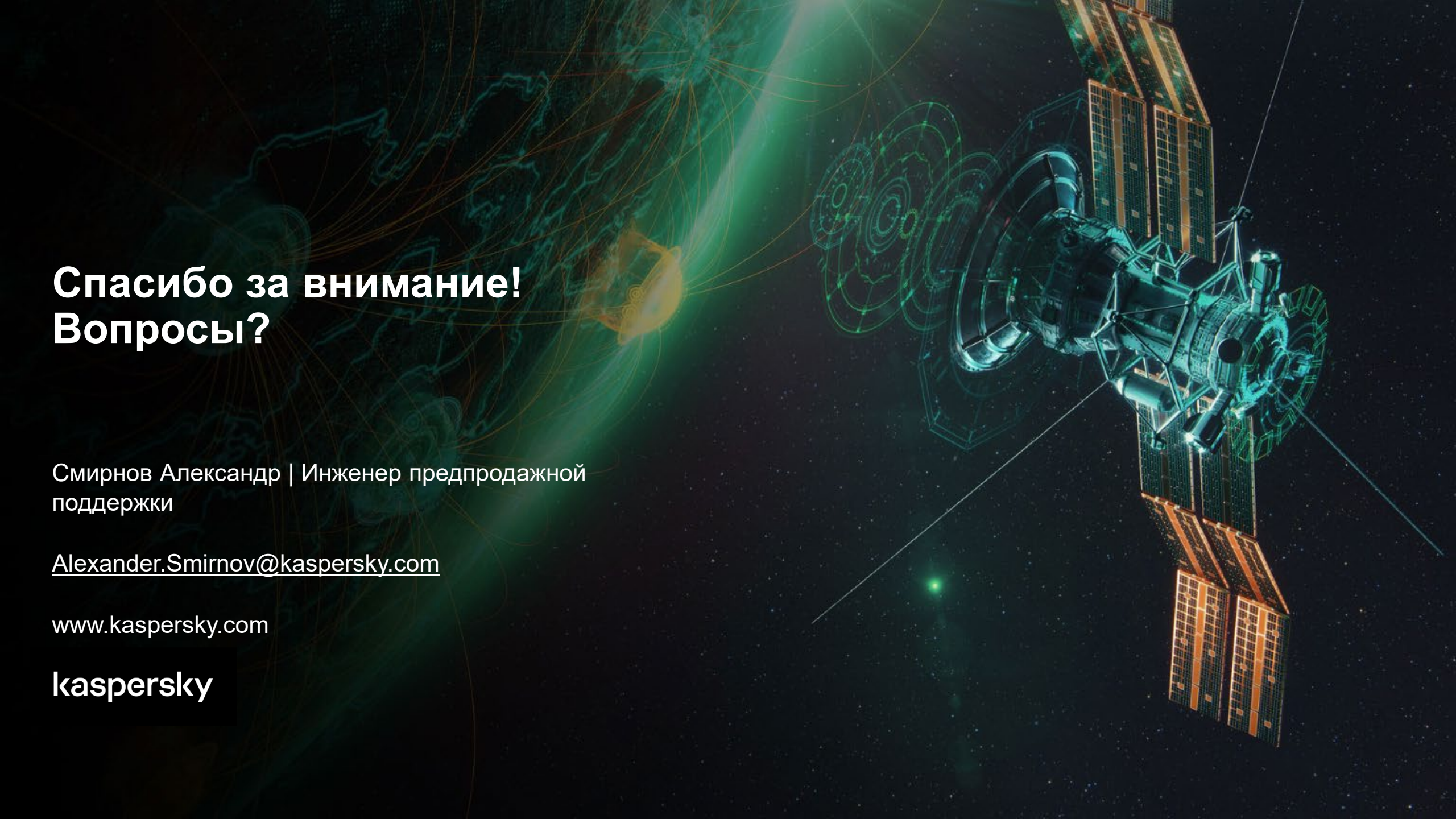
Опыт ЛК

Завершенные проекты по всему миру:

| Энергетика | Нефтегаз | Металлургия | Химия | Пищевая промышленность | Производство | Бумага | Коммунальное хоз-во | Иные | Всего |
|------------|----------|-------------|-------|------------------------|--------------|--------|---------------------|------|-------|
| 22 | 11 | 16 | 3 | 8 | 10 | 4 | 3 | 4 | 81 |

В таких регионах как:

Западная Европа, Россия, Ближний восток, Азия, Африка, Латинская Америка

A satellite is shown in space, illuminated by a bright green light source. The satellite has large solar panels and various instruments. A complex network of glowing green and orange lines and patterns is overlaid on the scene, suggesting a digital or data network. The background is a dark space with a few stars.

**Спасибо за внимание!
Вопросы?**

Смирнов Александр | Инженер предпродажной
поддержки

Alexander.Smirnov@kaspersky.com

www.kaspersky.com

kaspersky