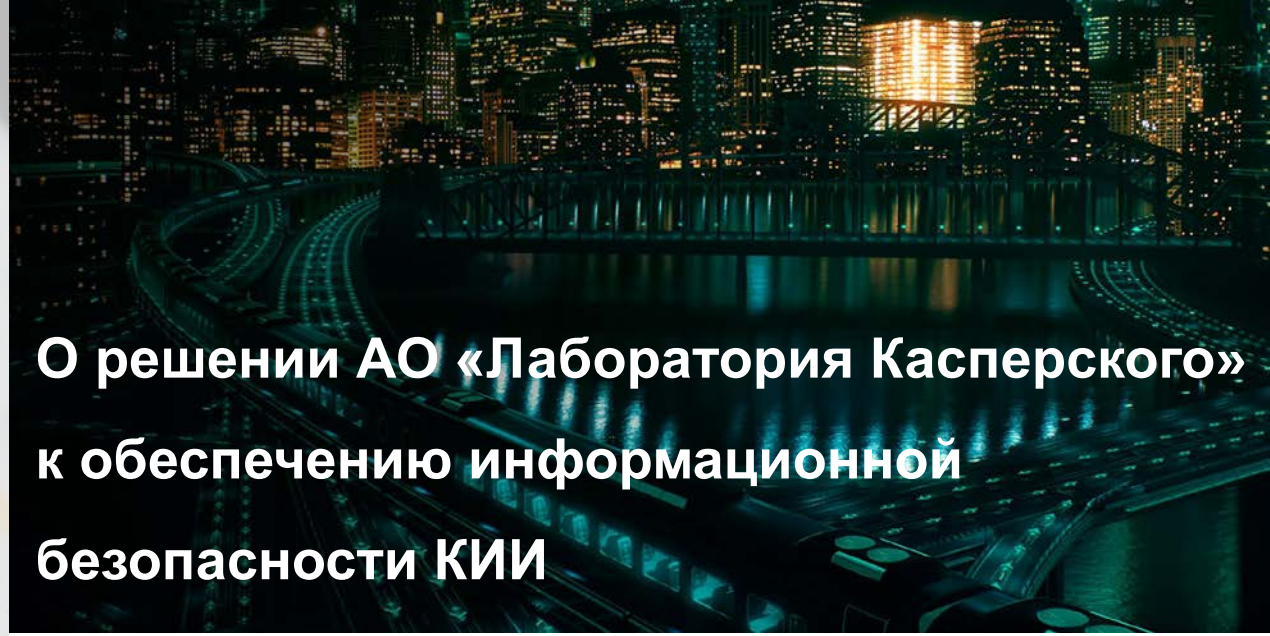
КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

08 ФЕВРАЛЯ 2018
УФА



О решении АО «Лаборатория Касперского» к обеспечению информационной безопасности КИИ

Андрей Ужаков
Руководитель офиса
АО «Лаборатория Касперского» в г.Иннополис

ТЕЛЕФОН: +7 (987) 297-39-63

EMAIL: Andrey.Uzhakov@kaspersky.com

KASPERSKY lab

#CODEIB

ГЛОБАЛЬНАЯ ОСВЕДОМЛЕННОСТЬ РАСТЕТ

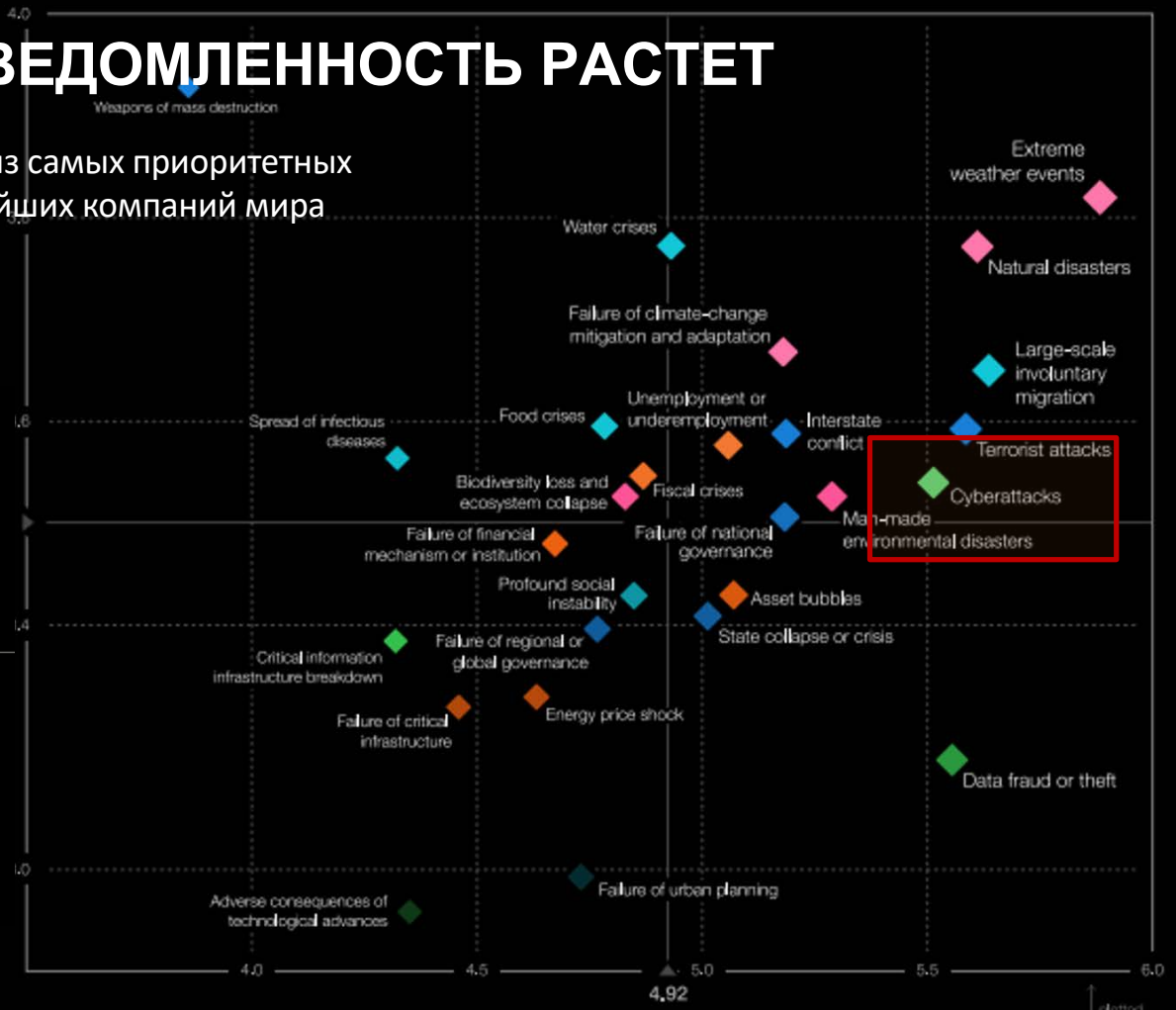
Киберугрозы признаются одними из самых приоритетных рисков топ-менеджментом крупнейших компаний мира

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2017
12th Edition



Основные понятия № 187-ФЗ от 26.07.2017 г: «О безопасности критической информационной инфраструктуры Российской Федерации»

КИИ – объекты КИИ (**ИС, ИТС, АСУ** субъектов КИИ), а также сети электросвязи, используемые для организации взаимодействия таких объектов;

субъекты КИИ – госорганы, госучреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТС, АСУ, функционирующие в **сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности**, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;

ФОИВ КИИ – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ (с задачей обеспечения информационной безопасности объектов КИИ, включая их категорирование) = **ФСТЭК**;

Указ Президента РФ от **25.11.2017 N 569** «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю»

Что делать Субъектам КИИ в рамках реализации № 187-ФЗ в период 2017-2020:

1 **инвентаризировать объекты КИИ (ИС, ИТС, АСУ субъектов КИИ);**

1.1 установить рабочие контакты с ФОИВ;

2 **запланировать работы по категорированию и обеспечению информационной безопасности объектов КИИ;**

Проект приказа по категорированию: http://www.garant.ru/products/ipo/prime/doc/56628335/

Критерии:

- охват количества людей, которым возможно причинение ущерба;
- размер территории на которой нанесен ущерб;
- размер прямого или косвенного ущерба в денежном выражении;
- масштаб и категории нарушения деятельности Государственных органов;
- нарушение условий заключенного международного договора России;
- снижение показателей государственного оборонного заказа.

3 **запланировать мероприятия и бюджеты по защите объектов КИИ**

3.1 провести анализ рынка услуг и средств защиты и т.д. (в целях выбора подходящих решений).

Решение Kaspersky Industrial CyberSecurity

Как выглядит система безопасности на решениях АО «ЛК»

МОДЕЛЬ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ (ISA-95)*

УРОВЕНЬ 4

БИЗНЕС-ПЛАНИРОВАНИЕ И ЛОГИСТИКА

УРОВЕНЬ 3

УПРАВЛЕНИЕ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ

КСПД

ERP, MES, …

Kaspersky Security для бизнеса

УРОВЕНЬ 1 / УРОВЕНЬ 2

КОНТРОЛЬ ПАКЕТОВ / ПОСТОЯННОЕ РЕГУЛИРОВАНИЕ / АВТОНОМНОЕ УПРАВЛЕНИЕ

Технологическая сеть

SCADA, HMI, …

Kaspersky Industrial CyberSecurity (KICS)

УРОВЕНЬ 0

ФИЗИЧЕСКИЙ

= ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

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

В чем особенность ИНДУСТРИАЛЬНЫХ СИСТЕМ с точки зрения принципов ИБ?

> **КОРПОРАТИВНАЯ IT-БЕЗОПАСНОСТЬ – ЭТО ЗАЩИТА ДАННЫХ**

> **ИНДУСТРИАЛЬНАЯ БЕЗОПАСНОСТЬ – ЭТО ЗАЩИТА ПРОЦЕССА**

ПРОЦЕСС ДОЛЖЕН БЫТЬ В ПЕРВУЮ ОЧЕРЕДЬ НЕПРЕРЫВНЫМ, А УЖЕ ЗАТЕМ БЕЗОПАСНЫМ

КОРПОРАТИВНЫЕ СИСТЕМЫ	
1	КОНФИДЕНЦИАЛЬНОСТЬ
2	ЦЕЛОСТНОСТЬ
3	ДОСТУПНОСТЬ

ИНДУСТРИАЛЬНЫЕ СИСТЕМЫ	
1	ДОСТУПНОСТЬ
2	ЦЕЛОСТНОСТЬ
3	КОНФИДЕНЦИАЛЬНОСТЬ

В ЧЕМ ПРИЧИНА «БУМА» КИБЕРБЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ ТЕХОЛОГИЧЕСКИМИ ПРОЦЕССАМИ?

1. АСУТП интегрируются с корпоративными ИС;

2. Компоненты АСУТП уязвимы;

3. Последствия киберинцидентов уже не информационные, а физические.

4. Восстановление компонентов технологического процесса требует значительного времени

Как вредоносное ПО проникает в индустриальные сети?

- Передача данных из индустриальных сетей в систему управления и планирования производства;
- Маршрутизаторы и сетеобразующее оборудование распределенной сети передачи данных – общее как для корпоративных сервисов, так и для АСУ ТП;
- Неконтролируемое использование сменных носителей и ПО персоналом;
- Подключение 3-х лиц (подрядных организаций) к индустриальной сети.

КАК ЗЛОУМЫШЛЕННИКИ ЭТИМ ПОЛЬЗУЮТСЯ?

Эксплуатация человеческого фактора (Соц инженерия)

CROUCHING YETI

Атака на КСПД, «угон» учетных данных администраторов тех. сети

BLACKENERGY 2

Атака на Подрядные организации или поставщиков

Заражение USB, распространение и перенос информации между компьютерами КСПД и тех. сети

STUXNET, FLAME, EQUATION, SAURON

КАКОВЫ ПОСЛЕДСТВИЯ КИБЕРАТАКИ
на АСУТП предприятия?

В РЕЗУЛЬТАТЕ АТАК НА ВЕРХНИЙ УРОВЕНЬ АСУТП:

- Потеря связи с удаленными объектами, отсутствие возможности мониторинга параметров технологического процесса (в частности, полностью автоматизированных).

В РЕЗУЛЬТАТЕ АТАК НА УРОВЕНЬ ПЛК:

- Перевод АСУ ТП, РСУ и управляемых объектов в аварийный режим с последующим остановом (срабатывание СПАЗ) – нарушение цепочки технологических процессов.

В РЕЗУЛЬТАТЕ АТАК НА ОБЪЕКТЫ ЭНЕРГЕТИКИ:

- Прекращение электроснабжения производственных мощностей

КАК СТРОЯТСЯ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ АСУТП?

-АНАЛИЗ ЗАЩИЩЕННОСТИ ПРОМЫШЛЕННЫХ СИСТЕМ,

АУДИТ И КЛАССИФИКАЦИЯ ПО ТРЕБОВАНИЯМ (ФСТЭК …)

- КАКОВ «ТИПОВОЙ» НАБОР СРЕДСТВ ЗАЩИТЫ?

- КТО С НИМИ РАБОТАЕТ?

КРИТИЧНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИБ АСУТП

ЗАЩИТА ОТ ТИПОВЫХ АТАК

- «Легкие» и надежные средства защиты узлов **- KICS**
- Сегментация сетей (Межсетевые экраны)
- Резервное копирование
- Управление доступом

ОБНАРУЖЕНИЕ ЦЕЛЕВЫХ АТАК

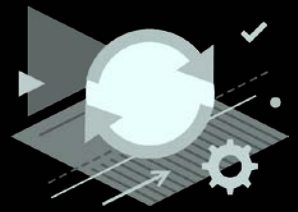
- Специализированные промышленне СОВ **- KICS**
- Персонал и центры реагирования **- KICS**

КРИТИЧНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИБ АСУТП

УПРАВЛЕНИЕ ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ

- Специализированные курсы для «не специалистов» **- KICS**
- Обучение и тестирование знаний автоматизированными средствами

РАБОТА С УЯЗВИМОСТЯМИ

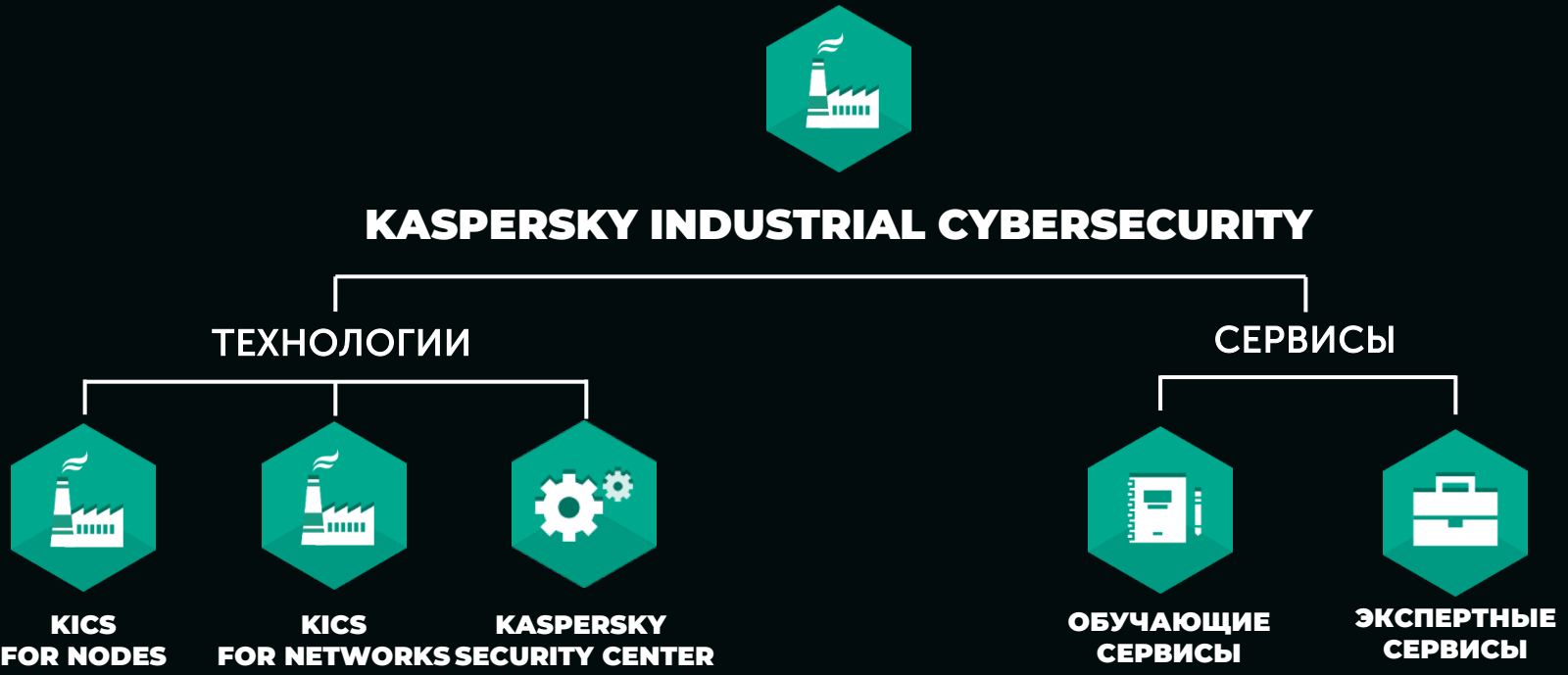


- Политика установки обновлений в индустриальной сети
- Выбор поставщика ПТК по критерию кибер-безопасности
- Сегментация внутри технологической сети
- Средства мониторинга уязвимостей и патч-менеджмента **- KICS**

KASPERSKY INDUSTRIAL CYBERSECURITY

Описание программной составляющей

Структура решения
KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)



Kaspersky Industrial Cybersecurity (KICS) программные решения

Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes)

Защита рабочих станций, серверов и PLC в промышленной сети от угроз

Kaspersky Industrial CyberSecurity for Networks (KICS for Networks)

Пассивный мониторинг сетевого трафика промышленной сети и обнаружение угроз

Kaspersky Security Center (KSC)

Централизованный мониторинг и управление компонентами KICS, интеграция с SIEM/MES/SCADA/… , возможность выстраивания иерархично подчиненных KSC

17

KICS for Nods: Поддерживаемые ОС

Настольные:

- Windows XP Pro с пакетами обновлений SP2 / SP3;
- Windows 7 Pro / Enterprise;
- Windows 8 Pro / Enterprise;
- Windows 8.1 Pro / Enterprise
- Windows 10 Pro / Enterprise;
- Windows 10 IoT Enterprise.

Встраиваемые:

- Windows XP Embedded x86;
- Windows Embedded Standard 7 x86 / x64;
- Windows Embedded 8.1 Industry Pro x86 / x64;
- Windows Embedded 8.0 Standard x86 / x64.

Серверные:

- Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP1 и выше
- Windows Server 2003 R2
- Windows Server 2008 Standard / Enterprise / Datacenter x86 / x64
- Windows Server 2008 Standard / Enterprise / Datacenter x86 / x64
- Windows Server 2008 R2 Standard / Enterprise / Datacenter x64
- Windows Server 2008 R2 Standard / Enterprise / Datacenter x64
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter x64
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter x64
- Windows Server 2016

18

ПО «KASPERSKY INDUSTRIAL CYBERSECURITY»

Необходимый функционал

Сертификация ФСТЭК, ФСБ

Сертификация с Индустриальными вендорами

Разработан с учетом индустриальной специфики

KASPERSKY INDUSTRIAL CYBERSECURITY

Обучающие сервисы

Подход, который формирует правильное поведение

- Полезные привычки вместо заучивания

Игровые тренинги, обучение на практике, имитация атак и другие методы формируют у участников правильные модели поведения

- **Разные навыки для разных ролей**

Отдельные тренинги для высшего руководства, линейных менеджеров и рядовых сотрудников.

- **Простое управление и оценка результатов**

Компьютерные тесты легко администрируются отделом ИБ или кадровым отделом.

- **Всегда актуальные знания**

Курсы разработаны ведущими экспертами с учетом современных угроз.

Интенсив-практикум «Кибербезопасность современных промышленных систем»

Самара
05-06 марта

Educational Partner

ics.abiroy.com

Интенсив-практикум «Кибербезопасность современных промышленных систем»

ЦЕЛИ ПРОГРАММЫ:

- Повысить осведомленность персонала об инцидентах ИБ в АСУТП
- Предоставить основу для улучшения организационных и технических мер защиты АСУТП
- Дать специальные рекомендации по внедрению лучших практик и средств ИБ
- Предоставить актуальную информацию о методах, используемых злоумышленниками

Интенсив-практикум «Кибербезопасность современных промышленных систем»

РЕЗУЛЬТАТ:

- Сравнение существующей системы ИБ АСУТП с лучшими мировыми практиками
- Составление предварительного чек-листа на соответствие ИБ АСУТП современным требованиям защиты от кибератак
- Уменьшение вероятности сбоев в работе производства вследствие кибератак

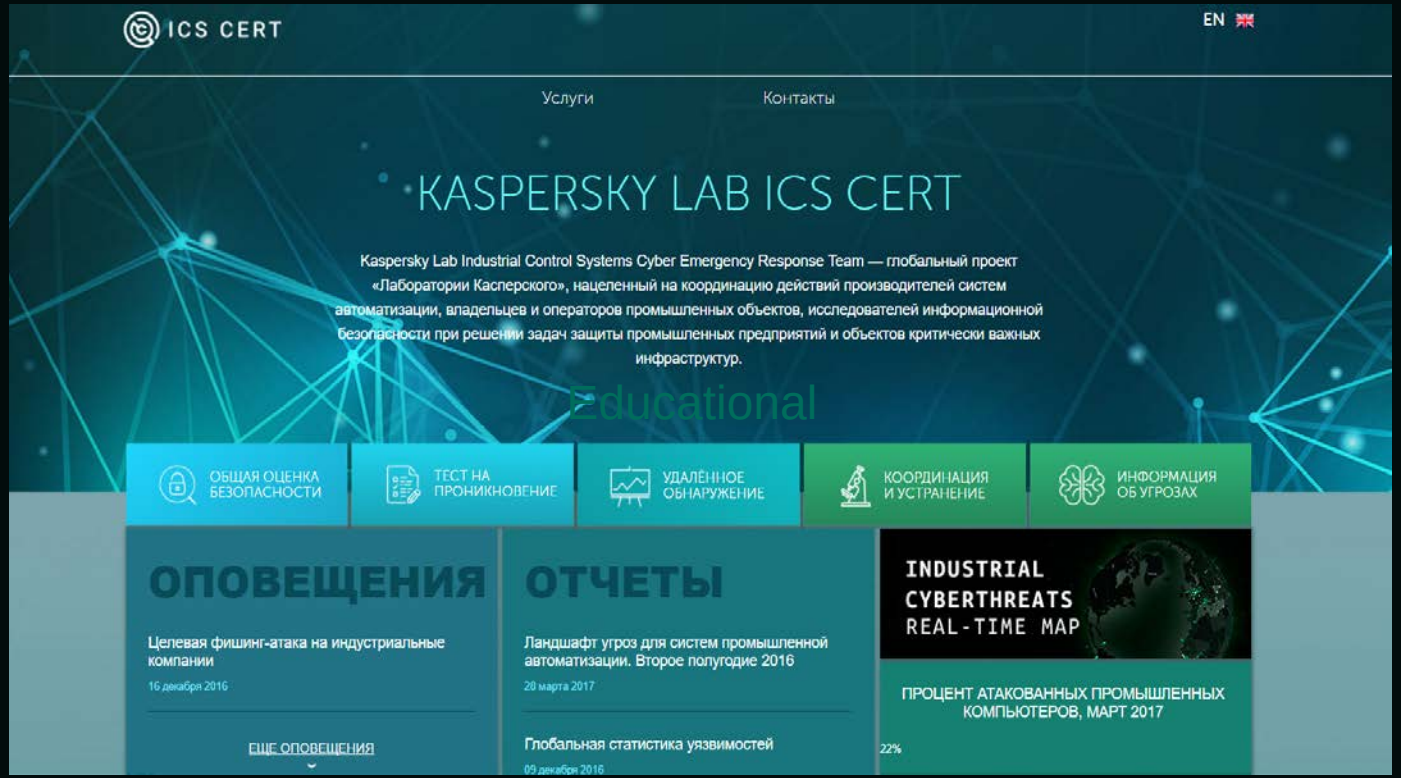
ПРИОБРЕТАЕМЫЕ НАВЫКИ:

- Осознанное следование политикам информационной безопасности
- Противодействие методам социальной инженерии
- Определение возможного вектора кибератаки и составление плана противодействия киберугрозам
- Идентификация киберугроз
- Реагирование на киберинциденты

KASPERSKY INDUSTRIAL CYBERSECURITY

Экспертные сервисы

KASPERSKY ICS CERT



https://ics.kaspersky.ru

KASPERSKY

Сервиса «Анализа защищенности…»

Цели:

• Независимая оценка устойчивости систем и приложений к наиболее распространенным видам внешних атак («пентест»).

• Независимая оценка соответствия АСУ ТП требованиям нормативных документов.

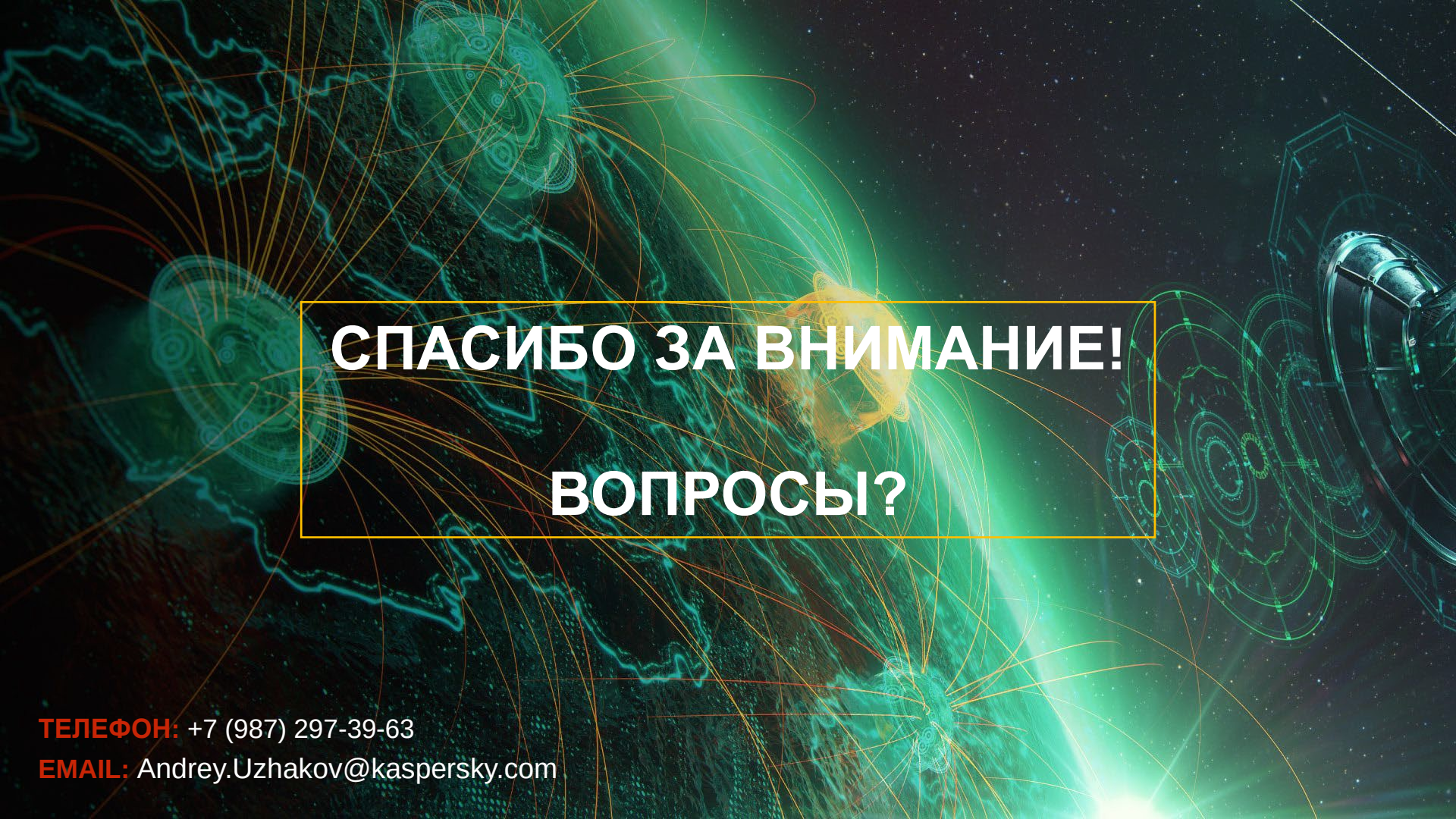
• Развитие системы управления информационной безопасностью и подготовка рекомендаций по реализации комплекса мер, направленных на повышение уровня защищенности АСУ ТП.

Заключение:

KASPERSKY INDUSTRIAL CYBERSECURITY это комплексное решение каждая из составляющих которого (анализ защищенности, повышение осведомленности, программное решение) направлена на повышение уровня защищенности технологического процесса от Кибератак (как от внутренних, так и от внешних источников).

Применение составляющих по отдельности непременно эффективно, а вместе дает синергетический эффект.

Давайте не ждать, а действовать проактивно.



ТЕЛЕФОН: +7 (987) 297-39-63
EMAIL: Andrey.Uzhakov@kaspersky.com

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

08 ФЕВРАЛЯ 2018
УФА

#CODEIB

Андрей Ужаков,
Руководитель офиса
АО «Лаборатория Касперского» в г.Иннополис

ТЕЛЕФОН: +7 (987) 297-39-63

EMAIL: Andrey.Uzhakov@kaspersky.com