

Андрей Ужаков, руководитель обособленного подразделения Иннополис АО «Лаборатория Касперского»

11.10.2018, г. Тюмень



Практика работы с объектами и субъектами КИИ

Мы считаем, что каждый — от пользователя домашнего компьютера до крупной компании и правительства — должен иметь возможность защитить то, что дорого для него. Неважно, идет ли речь о частной жизни, семье, финансах, бизнесе или **критической инфраструктуре**, мы работаем над тем, чтобы обеспечить защиту всего.

200
терр
ми

270 тыс.
корпоративных
клиентов во
всем мире

и
в
стра

более
400 млн.
пользователей

4000
ников



Kaspersky®
Industrial
CyberSecurity

K A S P E R S K Y L A B
ICS CERT

Причины киберинцидентов

66%

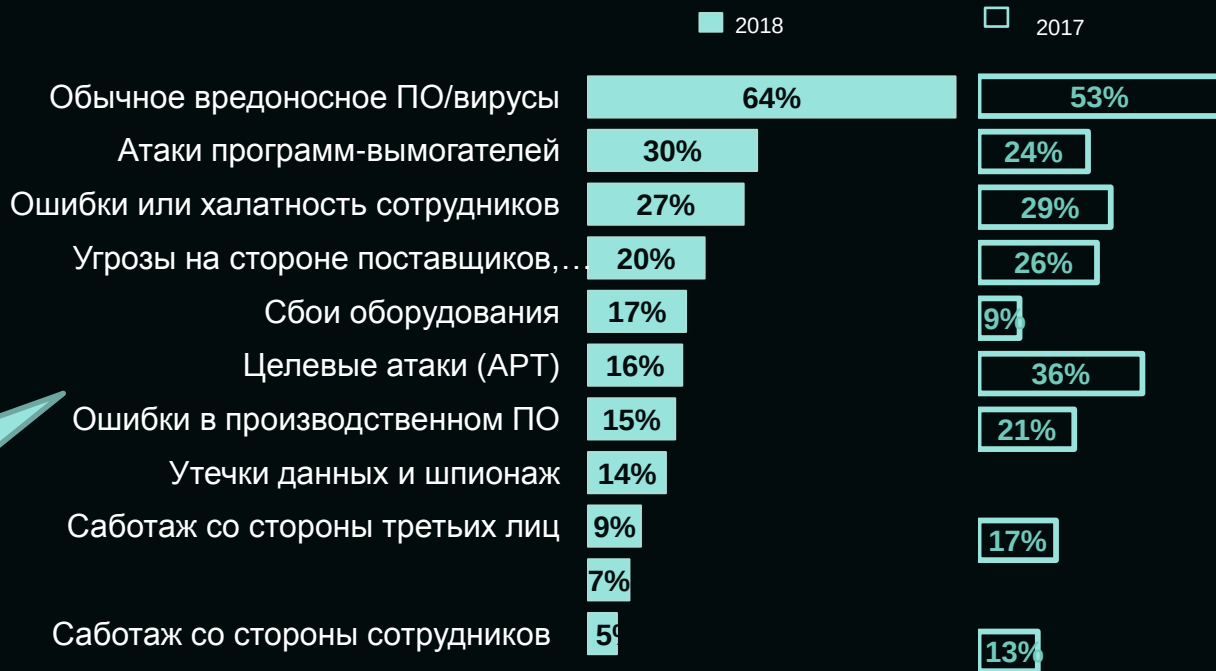
компаний считают
серьезной угрозой
целевые/APT атаки

НО

Для 64%

причиной инцидента
остается обычное
вредоносное ПО

Что стало причиной инцидентов, связанных с АСУ ТП, за последний год?



Что произошло за 20 лет?



В памяти многих останутся:

<https://thehackernews.com/>

What's Next?



WannaCry
Original Authors

WannaCry
(diff. Kill-Switch)
Original Authors

WannaCry 2
(NO Kill-Switch)
Copy Cat Hackers



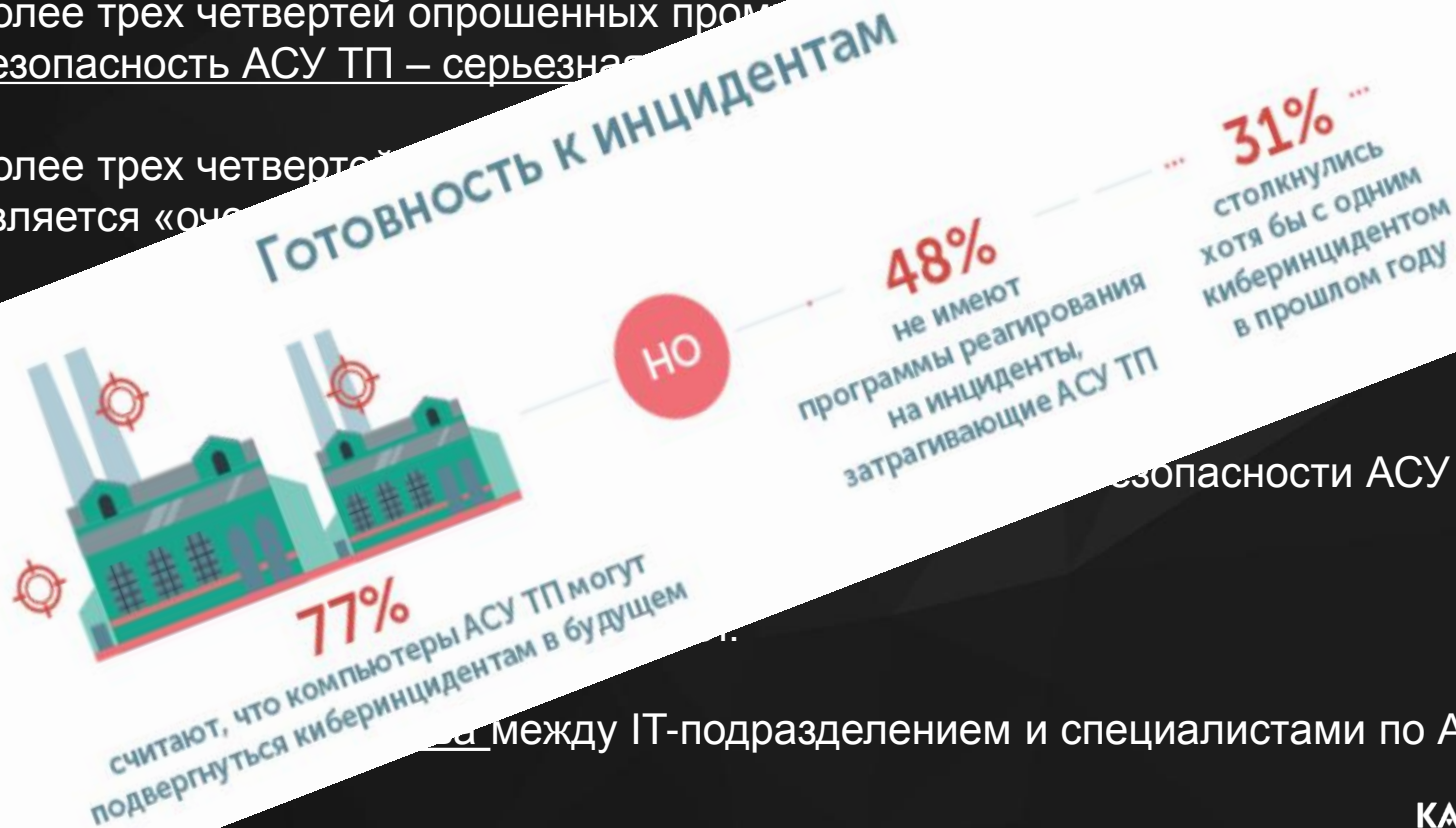
Из Анализа тенденций (июнь 2018 г.)

«Кибербезопасность систем промышленной автоматизации»

✓ Более трех четвертей опрошенных промышленных предприятий считают кибербезопасность АСУ ТП – серьезной проблемой.

✓ Более трех четвертей опрошенных предприятий является «очень рискованной».

✓ Более

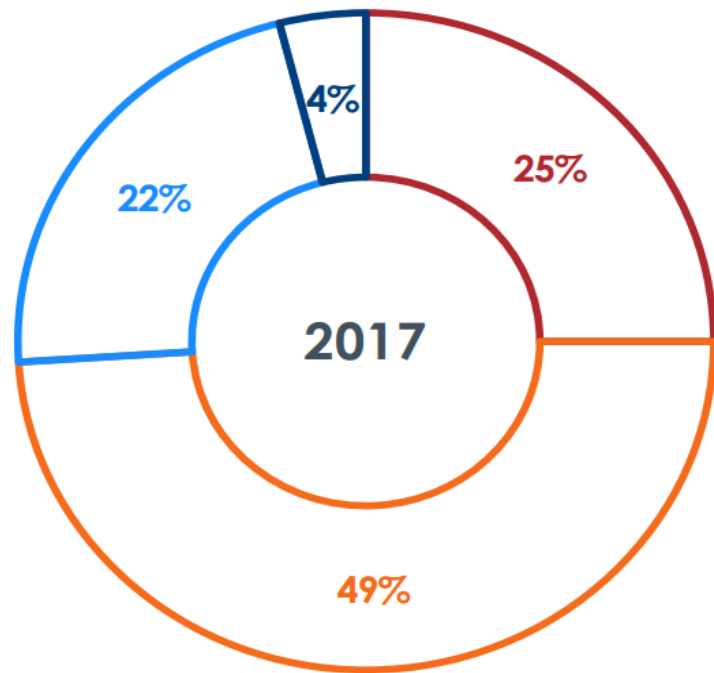


... между IT-подразделением и специалистами по АСУ ТП,

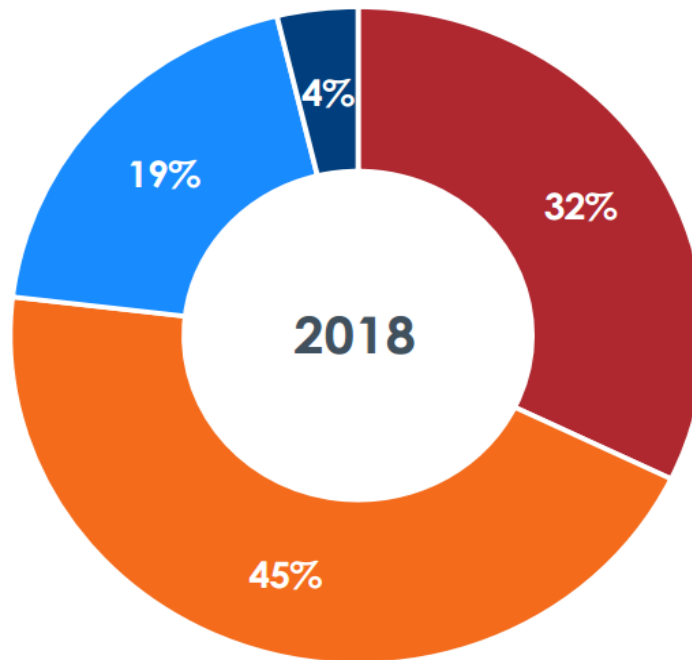
... между IT-подразделением и специалистами по АСУ ТП.

Из Анализа тенденций (июнь 2018 г.)

«Кибербезопасность систем промышленной автоматизации в 2018 г.»



■ Очень вероятно
■ Маловероятно



■ Достаточно вероятно
■ Очень маловероятно

Основные понятия Критической Информационной Инфраструктуры (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;

ФЗ от 26.07.2017 №187



Что делать Субъектам КИИ в рамках подготовки к реализации 187-ФЗ сегодня:

- ? Подготовлены **планы** по реализации мер по обеспечению информационной безопасности (имеющихся объектов КИИ)
 - > Запланированы **ресурсы** (Инсорсинг / Аутсорсинг)
 - > сформированы **бюджеты** (Средства защиты/ Услуги)
 - > **выбраны подходящие решения** (Средства защиты/ Услуги)
 - > проведен анализ рынка услуг и средств защиты и т.д.
- ? Разработаны организационные мероприятия в целях планирования обеспечения информационной безопасности новых (проектируемых) объектов КИИ
 - > Раздел проектной документации (том) **информационная безопасность**
- ? **запустить процесс** обеспечению информационной безопасности
 - > «PDCA»
 - > **регламентирующие документы** внутри организации
 - > **политика** информационной безопасности организации



решение KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)



KASPERSKY INDUSTRIAL CYBERSECURITY

ТЕХНОЛОГИИ



KICS
FOR NODES



KICS
FOR NETWORKS



KASPERSKY
SECURITY CENTER

СЕРВИСЫ

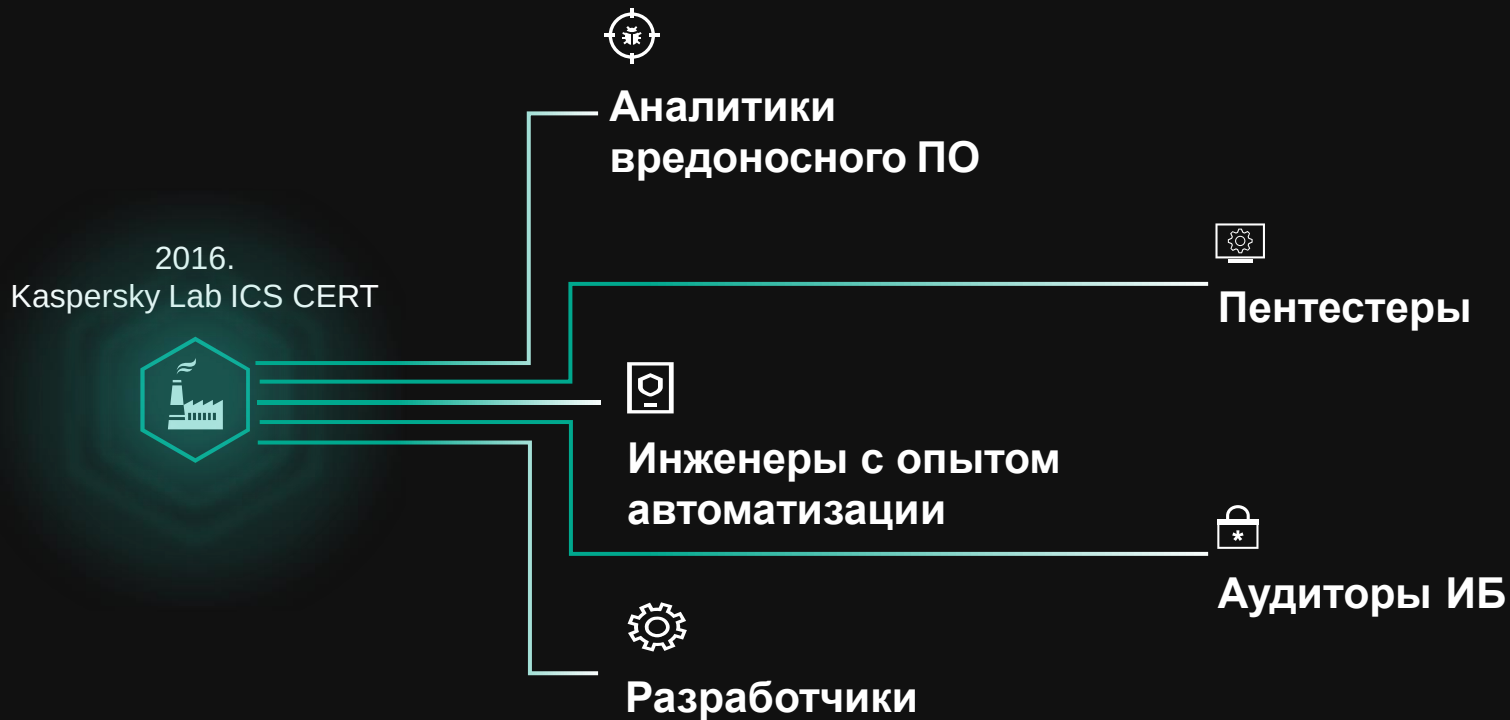


ОБУЧАЮЩИЕ
СЕРВИСЫ



ЭКСПЕРТНЫЕ
СЕРВИСЫ

ЭКСПЕРТНЫЕ СЕРВИСЫ



KASPERSKY LAB ICS CERT

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.



УСЛУГИ



ОПОВЕЩЕНИЯ



ОТЧЕТЫ



КОНТАКТЫ

ОПОВЕЩЕНИЯ

В популярной системе электронного документооборота обнаружены множественные уязвимости

12 февраля 2018

Еще несколько уязвимостей обнаружены и устранены в популярном менеджере лицензий

03 октября 2017

Использование зараженной версии CCleaner в промышленных системах

25 сентября 2017

В популярном менеджере лицензий

ОТЧЕТЫ

Больше, чем «умные» камеры. Под присмотром неуставленных лиц

12 марта 2018

Дорогой бензин? Сделаем его дешевым!

13 февраля 2018

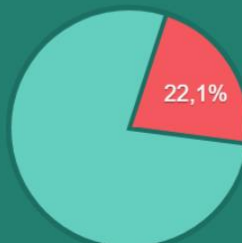
Закон о безопасности КИИ в вопросах и ответах

06 февраля 2018

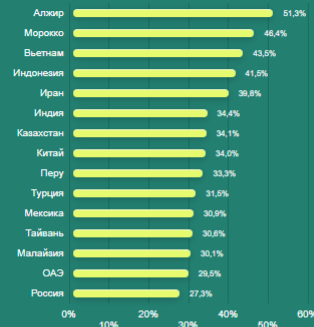
Серебряная пуля для атакующего. Исследование безопасности лицензионных токенов

INDUSTRIAL CYBERTHREATS REAL-TIME MAP

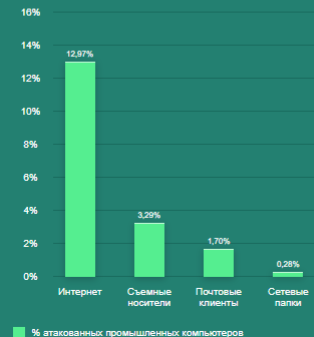
Процент атакованных промышленных компьютеров, Февраль 2018



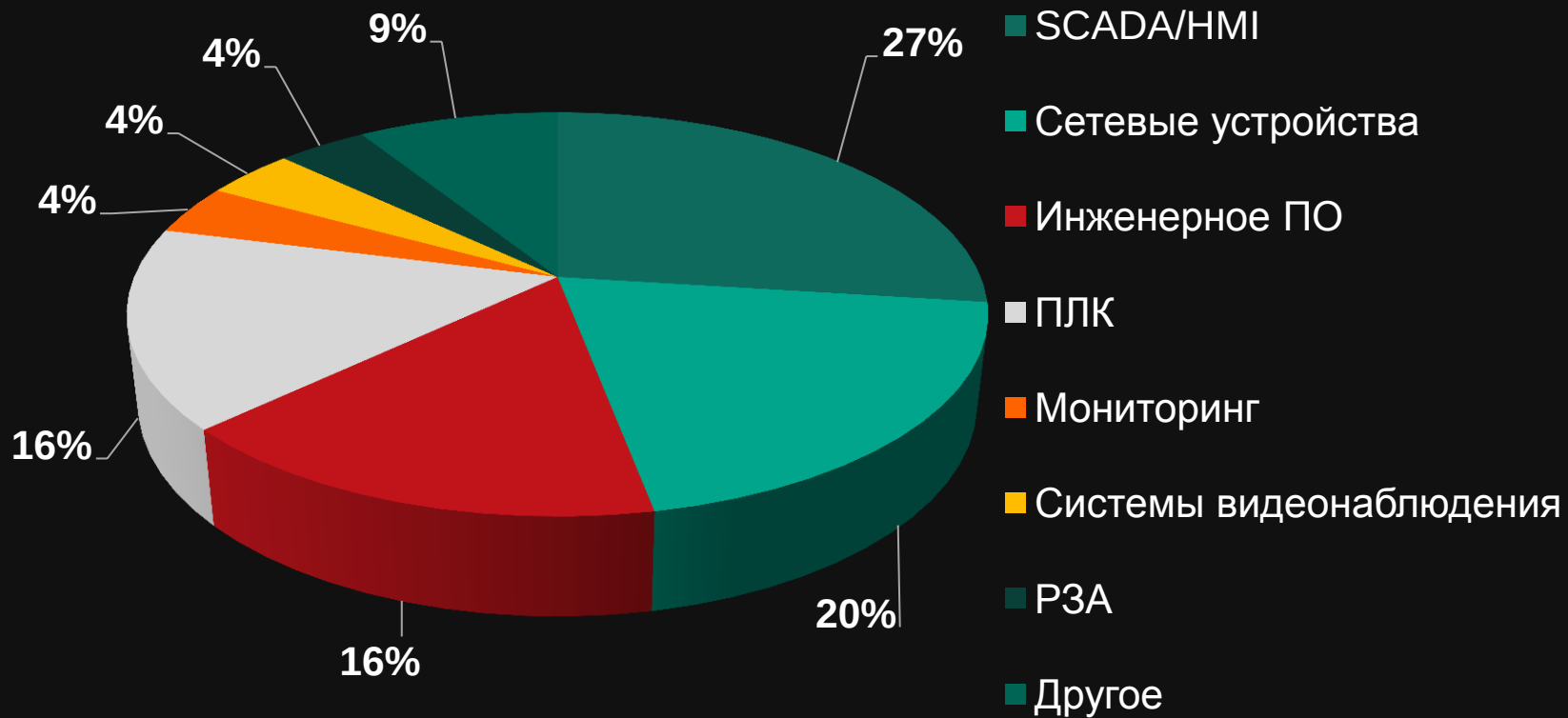
Топ стран по проценту атакованных промышленных компьютеров, Февраль 2018



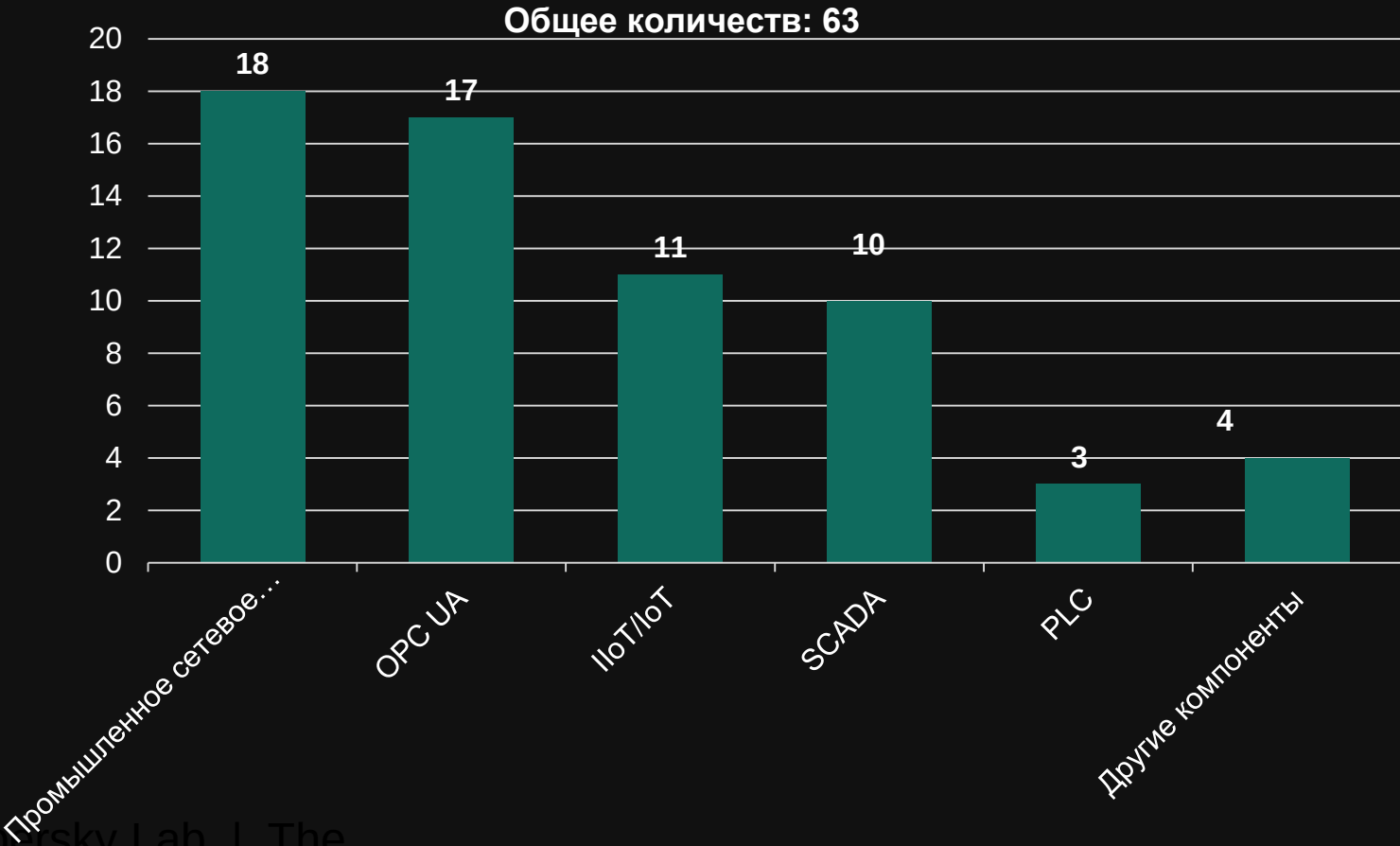
Источники угроз, Февраль 2018



Уязвимые компоненты



Уязвимости, обнаруженные Kaspersky Lab ICS CERT



ПРОБЛЕМЫ ЗАКРЫТИЯ УЯЗВИМОСТЕЙ В АСУТП

Приоритеты исправления выявленных уязвимостей в соответствии с их критичностью отсутствуют;

Обновления безопасности для уже используемого ПО не выпускаются, уязвимости закрываются в следующем релизе этого ПО;

Уведомления об уязвимостях не осуществляются

Вендор

Обновления на различные компоненты промышленных систем не устанавливаются годами

Эксплуатант

РЕЗУЛЬТАТ: Некоторые критичные уязвимости остаются незакрытыми более 1,5 лет

ЭКСПЕРТНЫЕ СЕРВИСЫ

- ❑ ОБЩАЯ ОЦЕНКА БЕЗОПАСНОСТИ
- ❑ ИНФОРМАЦИЯ ОБ УГРОЗАХ
- ❑ АНАЛИЗ НА СООТВЕТСТВИЕ
- ❑ ТЕСТ НА ПРОНИКНОВЕНИЕ
- ❑ КООРДИНАЦИЯ И УСТРАНЕНИЕ
- ❑

https://ics-cert.kaspersky.ru/contacts/

Региональный порт: PROMT Ариба HELP Ариба Партнеры ЛК Блог Л Блог ЛК Cyberthreat Новости ИБ Киберзащита KPI No Ransom

KASPERSKY LAB
ICS CERT

Услуги Оповещения Отчеты Контакты

Главная / Контакты

Контакты

Для получения дополнительной информации по условиям предоставления сервисов кратко опишите ваши вопросы и пожелания и отправьте их по электронной почте на адрес ics-cert@kaspersky.com.
Наши дежурные сотрудники свяжутся с вами в рабочее время с 9 до 18 часов по московскому времени.

ЦЕНТРАЛЬНЫЙ ОФИС «ЛАБОРАТОРИИ КАСПЕРСКОГО» ▾

 Россия, Москва, 125212
Ленинградское шоссе, д.39А,
стр.3
БЦ «Олимпия Парк»

 Электронная почта:
ics-cert@kaspersky.com

СООБЩИТЬ О ПРОИСШЕСТВИИ

KL ICS CERT стремится оперативно реагировать на заявки наших пользователей. Для точного определения причин и подготовки средств обнаружения / устранения, мы должны получить подробное описание возникшего инцидента. Пожалуйста, укажите в вашем сообщении как можно больше деталей о случившемся инциденте.

Описание:

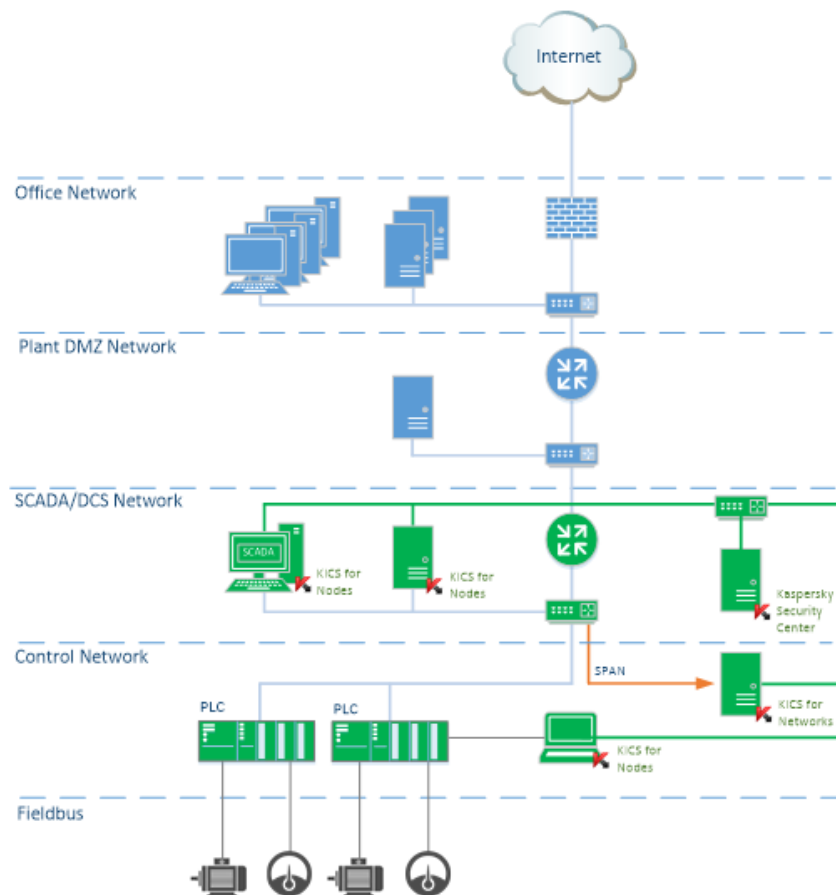
Контактные данные (email, телефон):

☐ Я даю компании АО «Лаборатория Касперского» прямое согласие на сбор и обработку моих данных согласно политике конфиденциальности «Лаборатории Касперского»

☐ I'm not a robot 

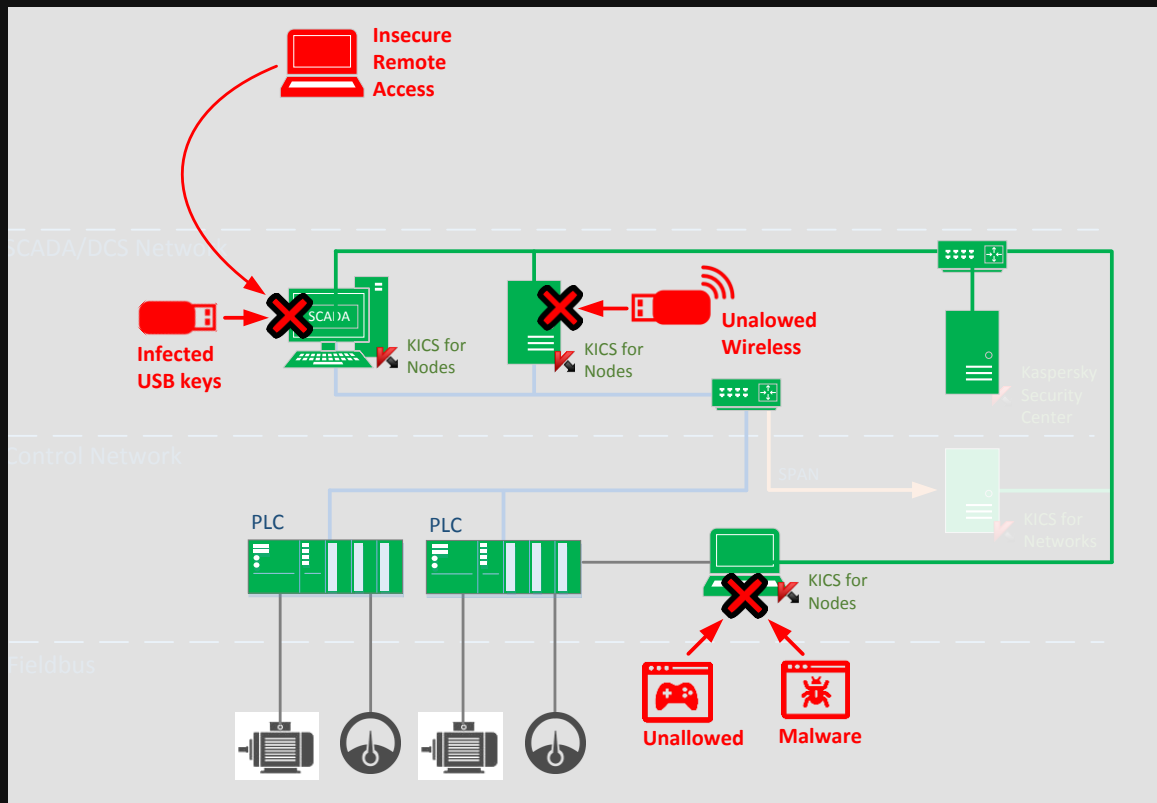
reCAPTCHA
Privacy • Terms

▶ СОЗДАТЬ ОТЧЕТ О ПРОИСШЕСТВИИ



KICS for Nodes: Функционал

- Контроль запуска приложений
- Контроль устройств
- Антивирус
- Пассивный анализ логов ОС
- Защита от шифровальщиков
- Контроль целостности PLC
- Контроль целостности файлов
- Firewall Менеджмент
- +
- Сертификация с вендорами АСУТП
- Сертификация ФОИВ



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

Сертификация с вендорами ПТК АСУТП

SIEMENS



valmet automotive



Honeywell

THE POWER OF CONNECTED

Schneider
Electric



ABB

Rockwell
Automation



...



(<https://ics.kaspersky.ru/cooperation/>)

Локальная Задача: Обеспечить совместимость с применяемыми ПТК АСУТП

https://ics.kaspersky.ru/cooperation/

Региональный порт PROMT Ариба HELP Ариба Партнеры ЛК Блог Л

Решение Сотрудничество Конференция KLICS CERT

инструменты, которые помогают построить защищенную и гибкую промышленную среду. Наша экспертиза позволяет производителям встраивать передовое защитное решение, полностью сочетающееся с требованиями и рекомендациями регуляторов. Результат этого — интегрированное решение, которое件 полезно не только для защиты конечных пользователей, но и для каждого участника цепи поставок.

- [Сертификат совместимости от GE Digital](#)
- [Сертификат совместимости от FTM professional control GmbH](#)
- [Сертификат совместимости от Iconics](#)
- [Сертификат совместимости от Schneider Electric](#)
- [Сертификат совместимости от ARC Informatique](#)
- [Сертификат совместимости от ЗАО «Монитор Электрик»](#)
- [Сертификат совместимости от ООО НПФ «Круг»](#)
- [Сертификат совместимости от ООО «НТК Интерфейс»](#)
- [Сертификат совместимости от ООО «Прософт-Системы»](#)
- [Сертификат совместимости от ООО «Эмерсон»](#)
- [Сертификат совместимости от ООО «ЭнергопромАвтоматизация»](#)

АКТ ПРОВЕРКИ СОВМЕСТИМОСТИ

Между программными продуктами
Kaspersky Industrial Cyber Security
продукция компании

АО «Лаборатория Касперского»
Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2
Здесь и далее именуемый как «KICS» и «Лаборатория Касперского»,
соответственно

и

Программный комплекс СК-11 (версия 11.5.2)
продукция компании

ЗАО «Монитор Электрик»
Россия, 357506, Ставропольский край, г. Пятигорск, ул. Подстанционная, 28
Здесь и далее именуемые как «СК-11» и «Монитор Электрик» соответственно

АКТ ПРОВЕРКИ СОВМЕСТИМОСТИ

Между программными продуктами
Kaspersky Industrial Cyber Security
продукция компании

АО «Лаборатория Касперского»
Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2
Здесь и далее именуемый как «KICS» и «Лаборатория Касперского»,
соответственно

и

Программный комплекс ARIS SCADA
продукция компании

ООО «Прософт-Системы»
Россия, 620102 г. Екатеринбург, ул. Волгоградская, 194а
Здесь и далее именуемые как «ARIS SCADA» и «Прософт-Системы»,

АКТ ПРОВЕРКИ СОВМЕСТИМОСТИ

Между программными продуктами
Kaspersky Industrial Cyber Security
продукция компании

АО «Лаборатория Касперского»
Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2
Здесь и далее именуемый как «KICS» и «Лаборатория Касперского»,
соответственно

и

SCADA NPT Expert
продукция компании

ООО «ЭнергопромАвтоматизация»
196273, г. Санкт-Петербург, Пискаревский пр., д. 63, лит. Б
Здесь и далее именуемые как «SCADA NPT Expert» и
«ЭнергопромАвтоматизация», соответственно

АКТ ПРОВЕРКИ СОВМЕСТИМОСТИ

Между программными продуктами
Kaspersky Industrial Cyber Security
продукция компании

АО «Лаборатория Касперского»
Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2
Здесь и далее именуемый как «KICS» и «Лаборатория Касперского»,
соответственно

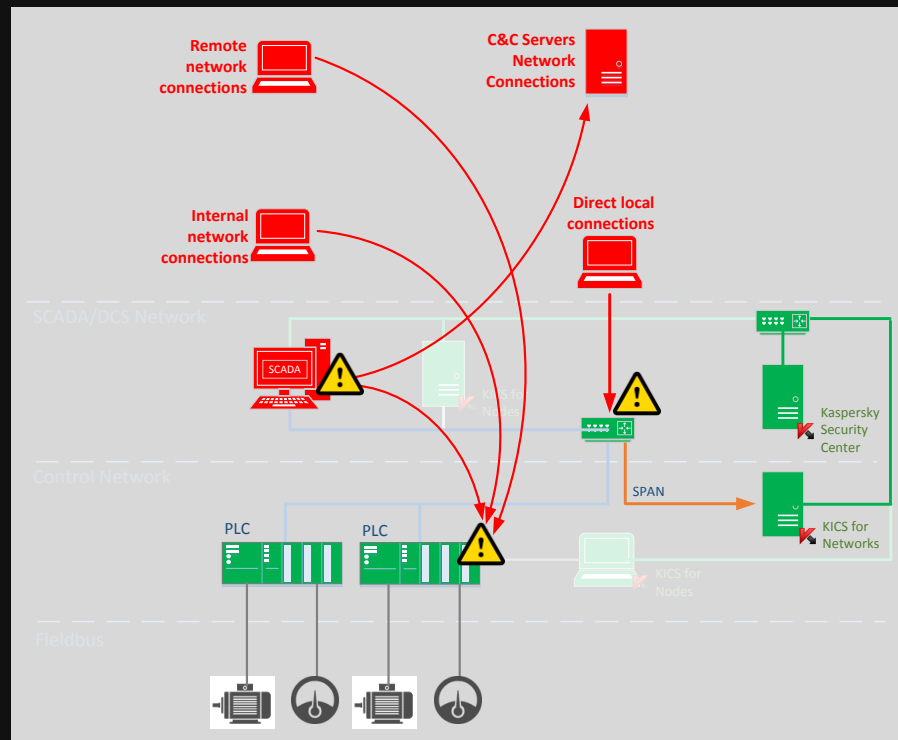
и

ОИК-ДИСПЕТЧЕР НТ
продукция компании

ООО «НТК ИНТЕРФЕЙС»
Россия, 620043 г. Екатеринбург, ул. Заводская 77
Здесь и далее именуемые как «ОИК-ДИСПЕТЧЕР НТ» и «НТК ИНТЕРФЕЙС»,

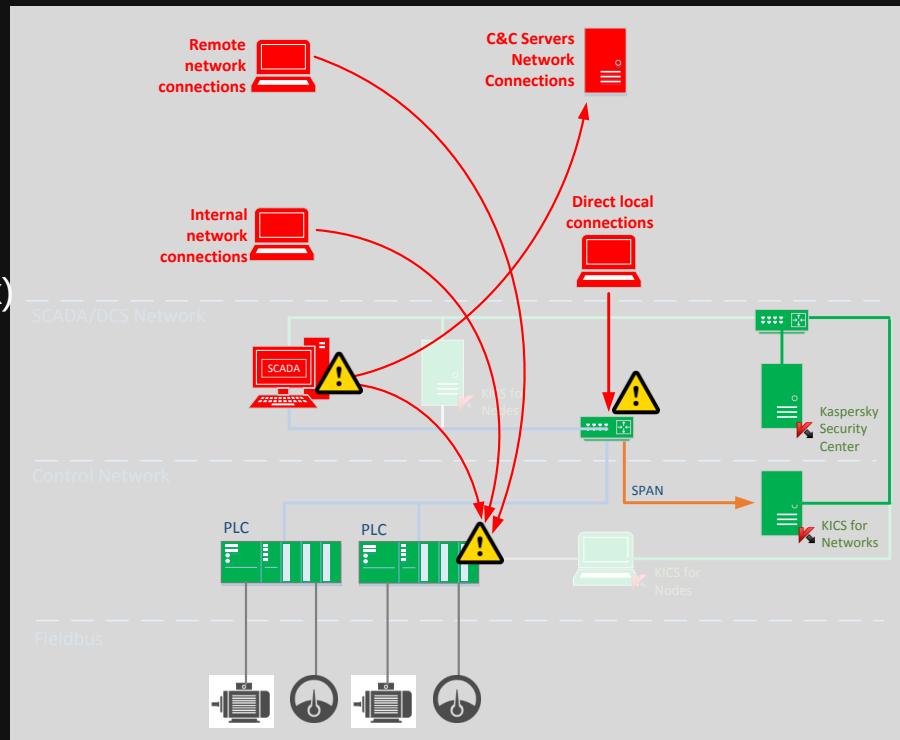
KICS for Networks: Сценарии использования

1. Инвентаризация
 1. Устройства в промышленной сети (PCs, Servers, laptops, PLCs, routers)
 2. Действительные коммуникации
2. Обнаружение нелегитимных связей и коммуникаций
 1. Новые хосты в сети
 2. Удаленный доступ
 3. Сканирование сети
 4. Соединения с бот нетами
 5. Распространение вредоносного ПО
 6. Эксплуатация уязвимостей
 7. Брутфорс атаки



KICS for Networks: Сценарии использования

3. Обнаружение критических команд к ПЛК (DPI)
 1. Чтение/запись программы/проекта ПЛК
 2. Попытки аутентификации
 3. Start/stop команды
 4. Чтение/запись конфигураций и прочее...
4. Контроль параметров технологического процесса
 1. Границы конкретных параметров ($\text{Min} < X < \text{Max}$)
 2. Связи между параметрами и значениями (if..and/or..if..then)
 3. Попытки фрода
 4. Ошибки конфигурации
5. Сбор и хранение информации для расследования инцидентов
 1. Security logs
 2. Technological events
 3. Raw network dump



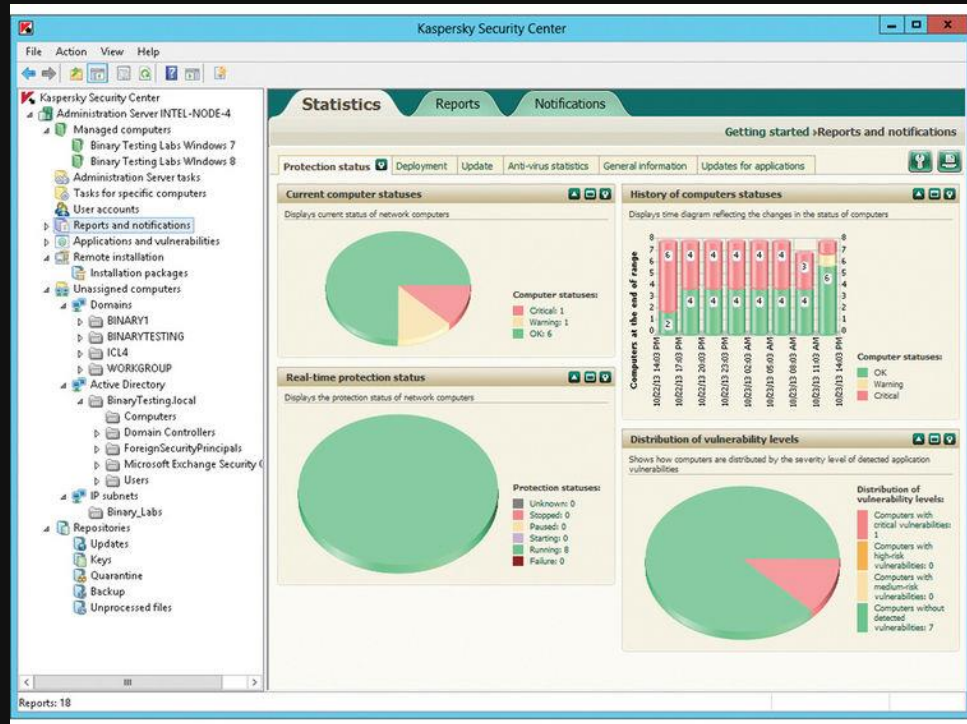
KICS for Networks: Поддерживаемое оборудование и протоколы

- Ethernet IEEE 802.3 link protocol
- IPv4 network layer protocol
- Industrial communication protocols in such programmable controllers as:
 - Siemens Simatic S7-300
 - Siemens Simatic S7-400
 - Siemens SIPROTEC 4 Series
 - Schneider Electric Modicom Momentum
 - Schneider Electric Modicom M340
 - Allen-Bradley/Rockwell Automation ControlLogix 5571
 - ABB Relion 670
 - Mitsubishi MELSEC-Q
 - Any vendors with IEC 61850 support
 - Any vendors with IEC 60870-5-104 support
 - *
 - ...

*Новое оборудование добавляется по плану, а так же по запросу

Kaspersky Security Center (KSC): Функционал

- Централизованное управление и мониторинг, на уровне устройств и групп;
- Централизованное обновление сигнатурных баз;
- Централизованное установка агентов;
- Ролевое управление
- Интеграция SIEM, HMI, ERP, BI;
- Интеграция со SCADA (**Kaspersky Security Gateway** поддерживает два протокола обмена данными со SCADA:
 - IEC 60870-5-104;
 - OPC 2.0 DA).



Сертификация ФОИВ: ФСТЭК, ФСБ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3907

Выдан 3 апреля 2018 г.
Действителен до 3 апреля 2021 г.

Настоящий сертификат удостоверяет, что средство защиты информации «Kaspersky Industrial CyberSecurity for Nodes», разработанное и производимое АО «Лаборатория Касперского» в соответствии с техническими условиями ТУ 643.46856491.00093-01, является средством антивирусной защиты, соответствует требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В третьего класса защиты. ИТ.САВЗ.ВЗ.ПЗ» (ФСТЭК России, 2012) и заданию по безопасности 643.46856491.00093-01 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00093-01 30 01.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «СИНКЛИТ» (аттестат аккредитации от 11.12.2017 № СИЗ RU.0001.01БИ00.5025) - техническое заключение от 25.12.2017, экспертного заключения от 06.03.2018 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СИЗ RU.0001.01БИ00.А002).

Заявитель: АО «Лаборатория Касперского» (ИНН 7713140469)
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов и заданию по безопасности, указанных в настоящем сертификате, осуществляется испытательной лабораторией ОАО «СИНКЛИТ».



ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/119-3407

от "15" июня 2018 г.

Действителен до "30" апреля 2021 г.

Выдан Акционерному обществу «Лаборатория Касперского».

Настоящий сертификат удостоверяет, что программное изделие «Kaspersky Industrial CyberSecurity for Networks» версии 2.6 в комплектации согласно формуляру 643.46856491.00094-02 30 01

соответствует требованиям ФСБ России к средствам обнаружения компьютерных атак класса Г и может использоваться в автоматизированных информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «Центр сертификационных исследований»

сертификационных испытаний образца продукции — дистрибутивов программного обеспечения (контрольные суммы: e7495360b5ea4915cebac59f553efccad7e923db1bedadbb0a7321c3a22b3ee, 026e98011f55a09ef34bb17b97100c167edad0c167c3e1985cb3af928744490b).

Безопасность информации обеспечивается при установке и использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру 643.46856491.00094-02 30 01.

Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России



А.М. Ивашко

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России

А.В. Парфенов

ПО «KASPERSKY INDUSTRIAL CYBERSECURITY»

Необходимый
функционал

Сертификация ФСТЭК,
ФСБ

Сертификация с
Индустриальными
вендорами

Разработан с учетом индустриальной специфики

ОБУЧАЮЩИЕ СЕРВИСЫ



КАК ВРЕДОНОСНОЕ ПО ПРОНИКАЕТ В ИНДУСТРИАЛЬНЫЕ СЕТИ?

- стыки ИНДУСТРИАЛЬНЫХ СЕТЕЙ И ЛВС предприятия:
 - Передача данных 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 ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ персоналом;
- подключение 3 ЛИЦ (подрядных организаций) К ИНДУСТРИАЛЬНОЙ СЕТИ.

ИТАК, В ЧЕМ ПРИЧИНА «АКТУАЛЬНОСТИ» КИБЕРБЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ?

1. АСУТП интегрируются с корпоративными ИС;
2. Компоненты АСУТП уязвимы;
3. Последствия киберинцидентов уже не информационные, а физические.

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 промышленные СОВ - **KICS**
- Персонал и центры реагирования - **KICS**



КРИТИЧНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИБ АСУТП

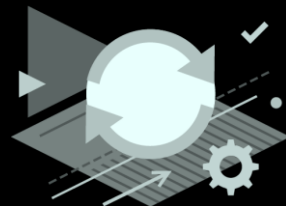
✓ УПРАВЛЕНИЕ ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ

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



✓ РАБОТА С УЯЗВИМОСТЯМИ

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



Заключение:

KASPERSKY INDUSTRIAL CYBERSECURITY это комплексное решение каждая из составляющих которого (сервисы, повышение осведомленности, программные решения) 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.



Спасибо за внимание.
...вопросы...

Андрей Ужаков, Andrey.Uzhakov@kaspersky.com

Алексей Петухов, Alexey.Petukhov@kaspersky.com