17 МАЯ,

Безопасность систем промышленной автоматизации

Лафицкий Алексей

Лаборатория Касперского

МАСШТАБ УГРОЗ

1994

1

новый вирус
каждый час

2006

1

новый вирус
каждую минуту

2011

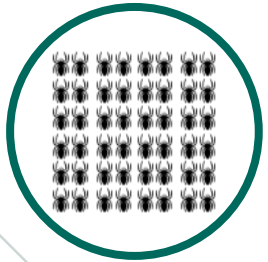
1

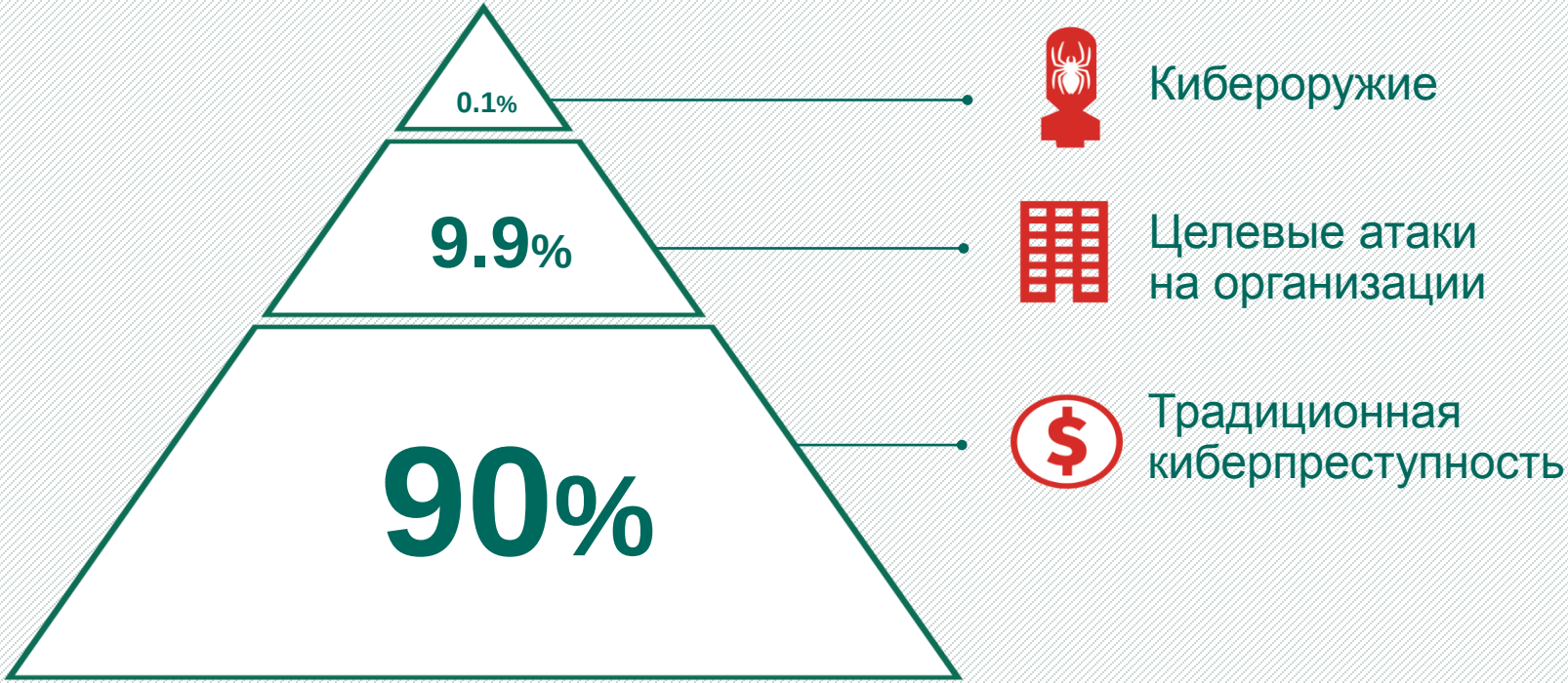
новый вирус
каждую секунду

2017

370 000

новых вредоносных
образцов в день

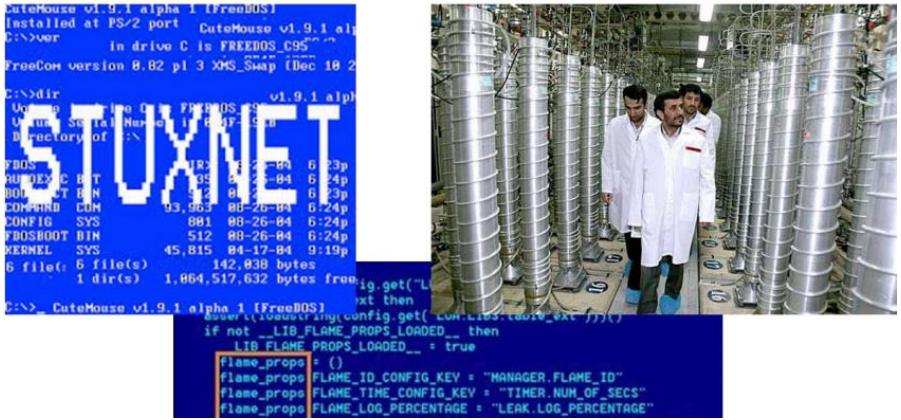



0.1%
9.9%
90%
Кибероружие
Целевые атаки
на организации
Традиционная
киберпреступность

ИСТОРИЯ ИНЦИДЕНТОВ– 2010, НАЧАЛО

КОГДА: 2010

ГДЕ: ИРАН (+15 СТРАН)



КИБЕР-УРОН: зараженные USB– MS OS уязвимости – обнаружение Win CC – конфигурация S7 PLC

ФИЗИЧЕСКИЙ УРОН: (DB890, FC1865,1874) – вредоносные измения в программу ПЛК, сокращен срок службы центрифуг

ФИНАНСОВЫЙ: 20% ЦЕНТРИФУГ ВЫВЕДЕНЫ ИЗ СТРОЯ РАНЕЕ ПОЛОЖЕННОГО СРОКА

KASPERSKY lab

ИСТОРИЯ ИНЦИДЕНТОВ – 2012, SHAMOON, SAUDI ARAMCO

КОГДА: 2012

ГДЕ: САУДОВСКАЯ АРАВИЯ

КИБЕР-УРОН: фишинговый имейл, 35 000 компьютеров выведены из строя (стерта память)

ФИЗИЧЕСКИЙ: остановлена местная отгрузка нефти

Saudi Aramco suffered the worst hack in world history in 2012.

ФИНАНСОВЫЙ: ПРОСТОЙ – 17 ДНЕЙ, НА 18ЫЙ КОМПАНИЯ НАЧАЛА ОТГРУЗКИ БЕСПЛАТНО

KASPERSKY lab

ИСТОРИЯ ИНЦИДЕНТОВ – **2017**, SHAMOON 2.0, STONEDRILL

КОГДА: 2016-2017

ГДЕ: САУДОВСКАЯ АРАВИЯ

КИБЕР-УРОН: 11 Жертв (Правительство, Телеком, Промышленность)

ОСОБЕННОСТИ:

-НЕТ СВЯЗИ С CNC (ВЫСОКАЯ СКРЫТНОСТЬ)

-ЗАЩИТА ОТ ПЕСОЧНИЦЫ

-РАСПОЛАГАЮТСЯ В ДРАЙВЕРАХ, ПАМЯТИ БРАУЗЕРОВ

-ДОБАВЛЕНЫ МОДУЛИ ШИФРОВАНИЯ

ДЕКАБРЬ 2015

КОГДА: ДЕКАБРЬ 2015

ГДЕ: УКРАИНА

КИБЕР-УРОН: Заражение **BlackEnergy2** посредством фишингового имейла, Прошивки RTU изменены, диспетчерские ПК атакованы и «затерты», DDoS атака на колл-центры.

ФИЗИЧЕСКИЙ УРОН:, удаленное уравление операторами выведено из строя, отключение напряжения на 7 110kV и 23 35 kV подстанциях

ФИНАНСОВЫЙ: ОТКЛЮЧЕНИЕ ЭКЛЕКТРОЭНЕРГИИ В 5 РЕГИОНАХ НА 6 HOURS

KASPERSKY lab

МАРТ 2016

КОГДА: МАРТ 2016

ГДЕ: Водоочистные системы «неназванной компрании»

КИБЕР-УРОН: Эксплуатация архитектурных уязвимостей сети, удаленный доступ к устаревшему серверу, управляющему тех процессом

ФИЗИЧЕСКИЙ УРОН:, Произвольное изменение уровня химикатов в цехе водоочистки

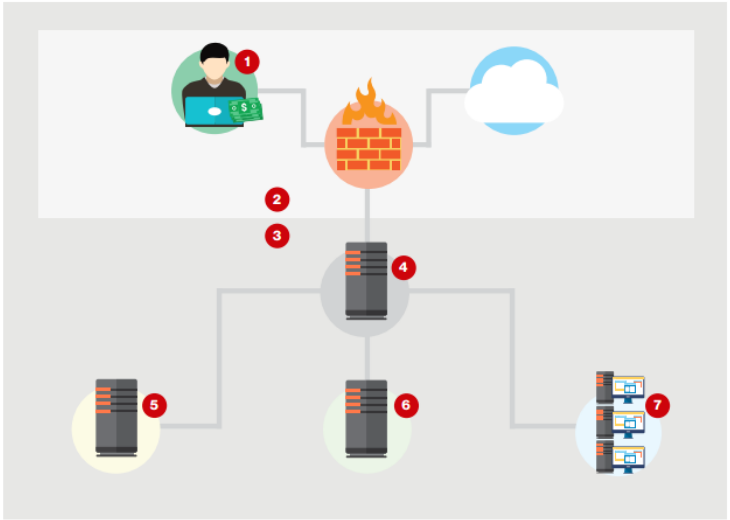


Figure 2

1. Customer access to payment system
2. External (Internet)
3. Internal (Corporate access)
4. AS400
5. PLC management
6. Finance access (PII access)
7. IT management

ТЕКУЩАЯ СИТУАЦИЯ В БЕЗОПАСНОСТИ АСУТП

Растущий тренд — количество инцидентов растет (ICS-CERT)

FY 2014

245

Инцидентов

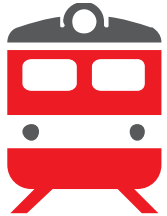
FY 2015

295

Инцидентов

59%

Нефтегаз, Генерация (Hydro, Nuclear), КВО



25%

Транспорт и коммуникации

ЦЕЛЬ — ПОЛУЧИТЬ ДОСТУП К SCADA СИСТЕМАМ, ПЛК И НАНЕСТИ ВРЕД ТЕХ ПРОЦЕССУ

KASPERSKY lab

ЧТОБЫ СТАТЬ ЖЕРТВОЙ – НЕ НУЖНО БЫТЬ ЦЕЛЬЮ

Отчет ЛК (2016) – «ICS AVAILABILITY»

Количество элементов АСУ ТП, доступных из Internet.
220,558

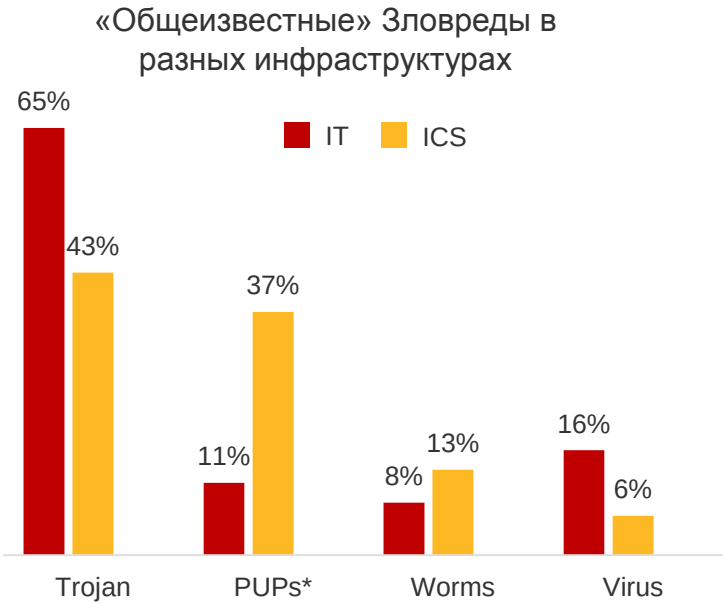
Известные уязвимости, доступные из Internet.
13,033 на 11,882 узлах

Множество крупных промышленных компаний .
1,433

https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Availability_Statistics.pdf

KASPERSKY lab

ЧТОБЫ СТАТЬ ЖЕРТВОЙ – НЕ НУЖНО БЫТЬ ЦЕЛЬЮ



Стандартное вредоносное ПО

- Citadel, Kido, Shamoon, итд.

Таргетированные Атаки (APTs)

- Duqu, Flame, Gauss, Crouching Yeti (Energetic Bear), Epic Turla, Equation

Кибероружие

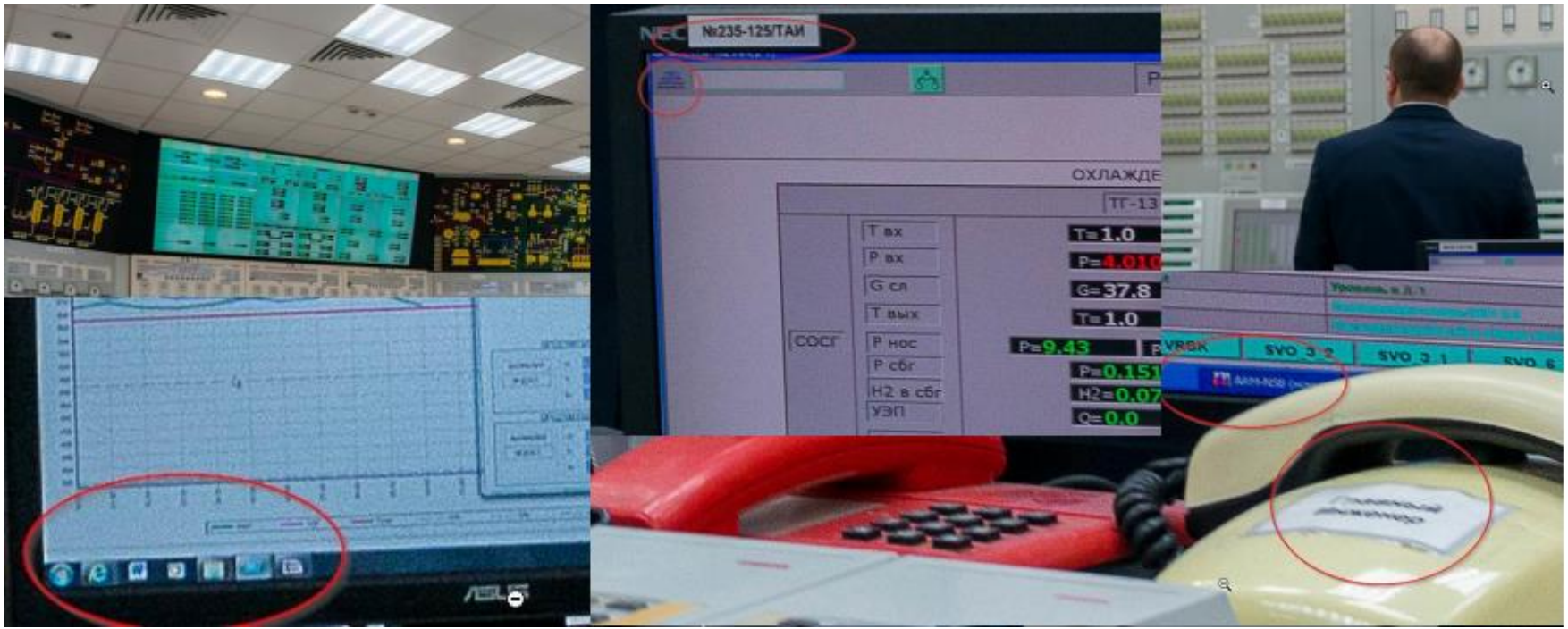
- Stuxnet

** **PUPs** — Potentially unwanted programs*
*** Source: Kaspersky Security Network*

KASPERSKY lab

УЯЗВИМОСТИ: ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Социальная инженерия



KASPERSKY lab

УЯЗВИМОСТИ: ПО И ПТК АСУТП

Уязвимости ПТК

Alert (ICS-ALERT-15-225-02A)

Rockwell Automation 1766-L32 Series Vulnerability (Update A)

Original release date: August 13, 2015 | Last revised: August 20, 2015

Alert (ICS-ALERT-15-225-01A) More Alerts

Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A)

Original release date: August 13, 2015 | Last revised: August 20, 2015

Alert (ICS-ALERT-15-225-01A) More Alerts

Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A)

Original release date: August 13, 2015 | Last revised: August 20, 2015

Source: US ICS-CERT

Удаленный злоумышленник может получить доступ к ПЛК

KASPERSKY lab

УЯЗВИМОСТИ: УДАЛЕННЫЙ ДОСТУП

Коммунальная компания скомпрометирована – Слабый пароль

В 2014, неназванная публичная производственная компания подверглась удаленной кибератаке в результате которой был получен доступ к технологической инфраструктуре

ПО, используемое организацией для организации удаленного обслуживания было доступно через интернет.

Эти системы включали remote access ПО со слабыми паролями.

Системы были подтвержены множественным векторам атак. Предыдущие вторжения также были обнаружены.

Производители АСУ настаивают на настройке уданенного доступа/управления к их оборудованию

KASPERSKY lab

УЯЗВИМОСТИ: АРЕНДОВАННЫЕ КАНАЛЫ

Региональная электросетевая компания

Многие критические объекты – распределенные инфраструктуры / (Иногда принадлежат разным компаниям)

ПРОБЛЕМА: не возможно или экономически нецелесообразно строить собственные каналы связи

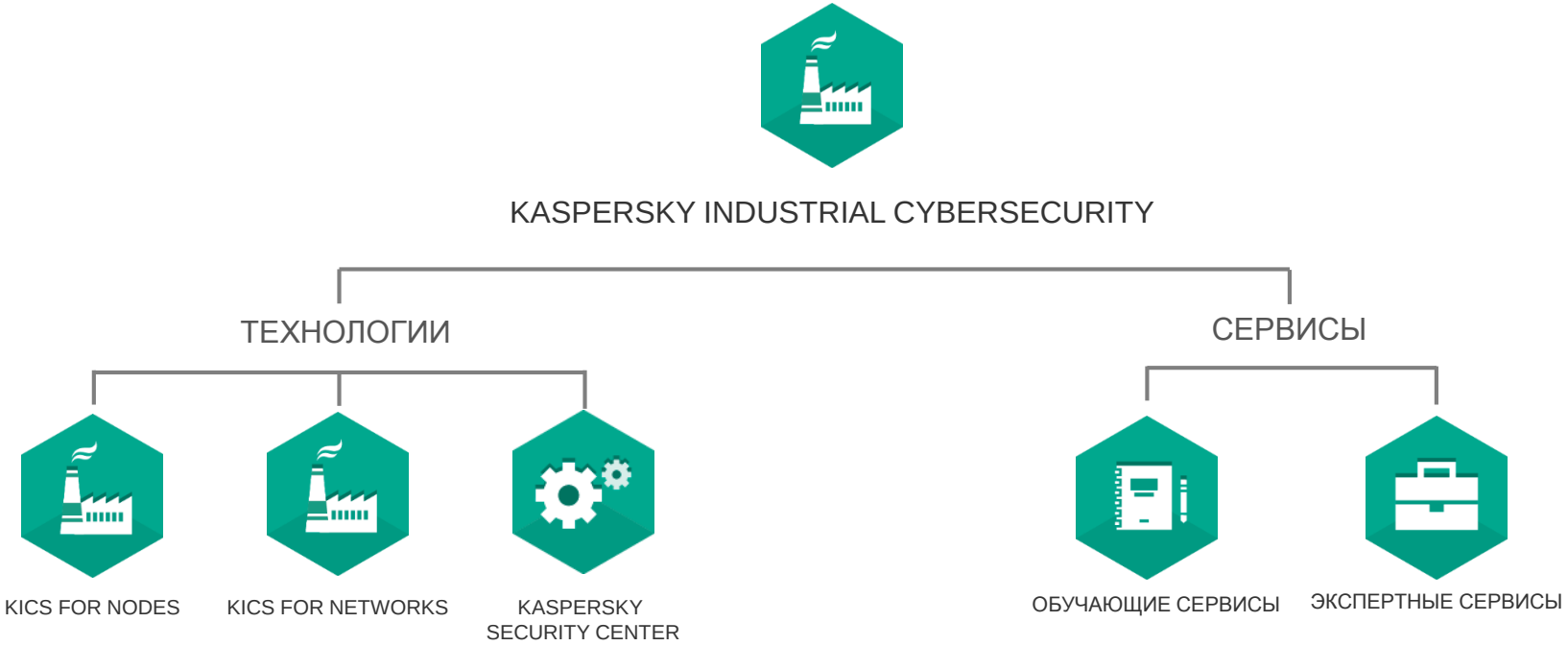
РЕШЕНИЕ: Используются каналы от провайдеров

ИНЦИДЕНТ:

- Потеряна связь между двумя подстанциями
- Расследование показало, что один из маршрутизаторов был размещен в жилом здании
- **Роутер был использован обычными жильцами, в том числе и нелигитимно**

KASPERSKY lab

KASPERSKY INDUSTRIAL CYBERSECURITY: СТРУКТУРА РЕШЕНИЯ



KASPERSKY INDUSTRIAL CYBERSECURITY

LEVEL 4

Business planning and logistics

Managing end-to-end supply chain.
Establishing the basic plant schedule – production, material use, delivery, and shipping.

LEVEL 3

Manufacturing Operations management

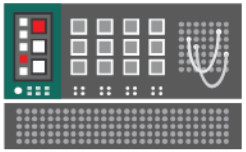
Work flow/recipe control to produce the desired end products.
Maintaining records and optimizing the production process.

Kaspersky Security for Business + Professional Services

LEVEL 2, 1

Batch Control.
Continuous Control.
Discrete Control.

Monitoring, supervisory control and automated control of the production process



Sensing the production process, manipulating the production process

Kaspersky Industrial CyberSecurity

LEVEL 0

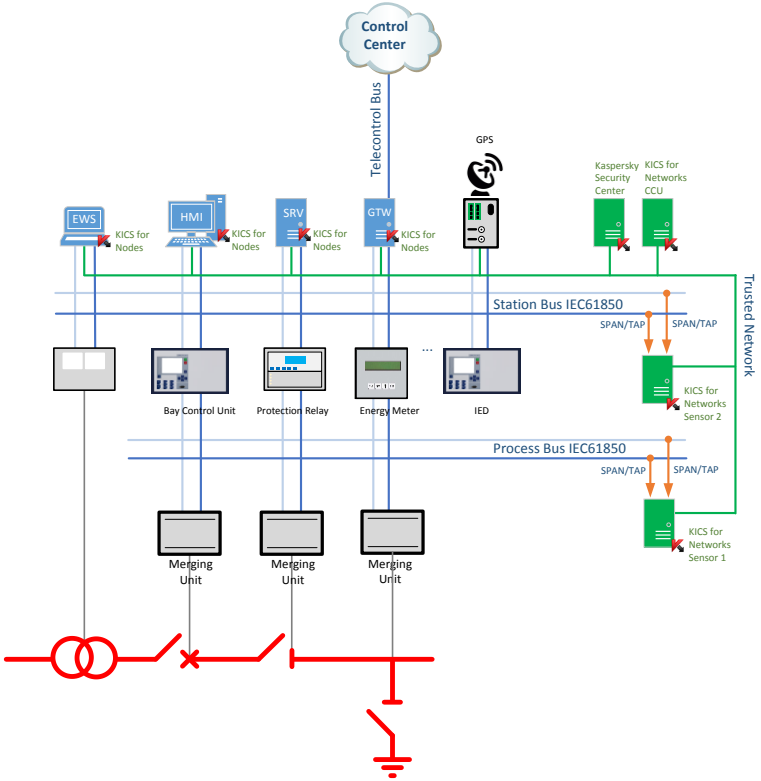
Physical

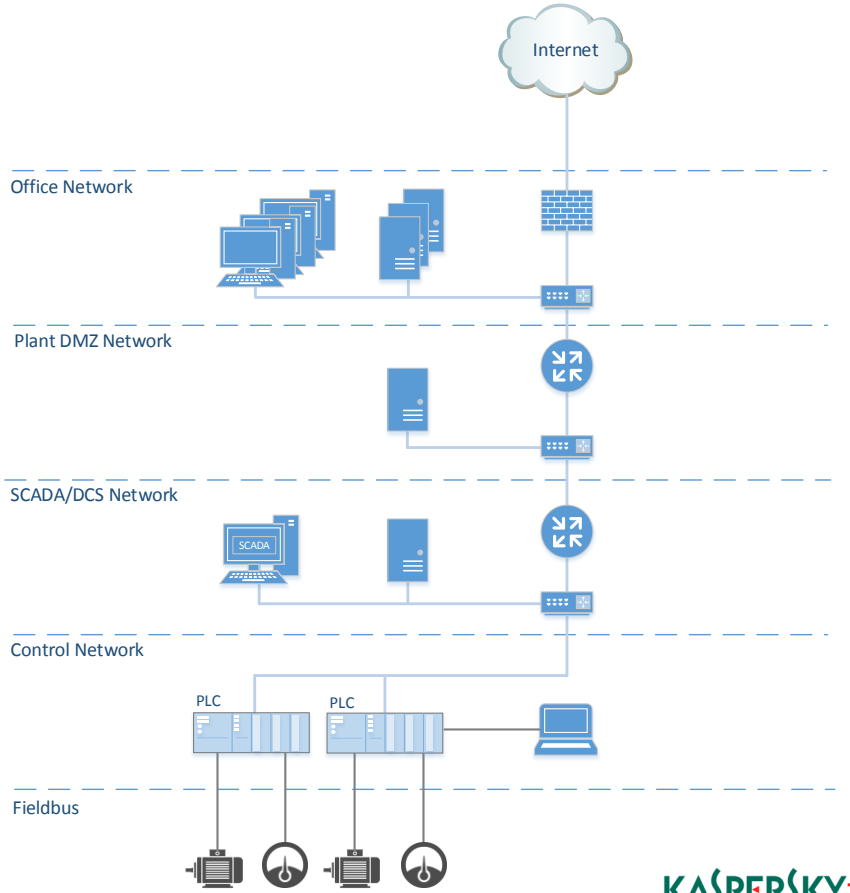
Physical devices

Physical security

KASPERSKY lab

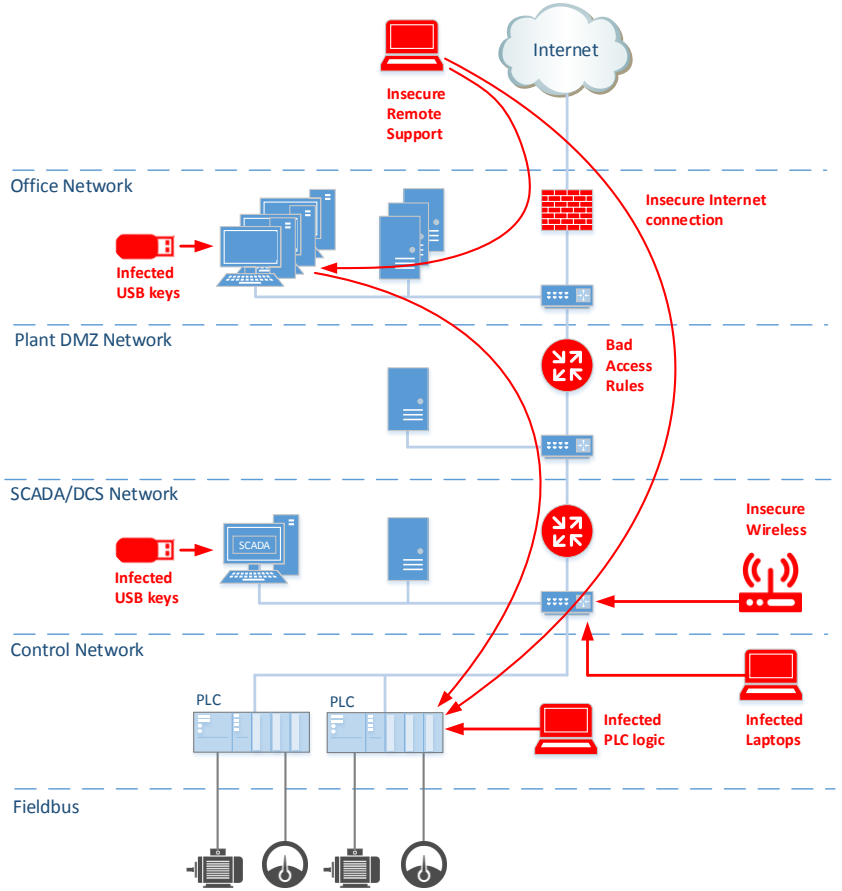
АРХИТЕКТУРА СЕТЕЙ ПРОМЫШЛЕННОГО ОБЪЕКТА





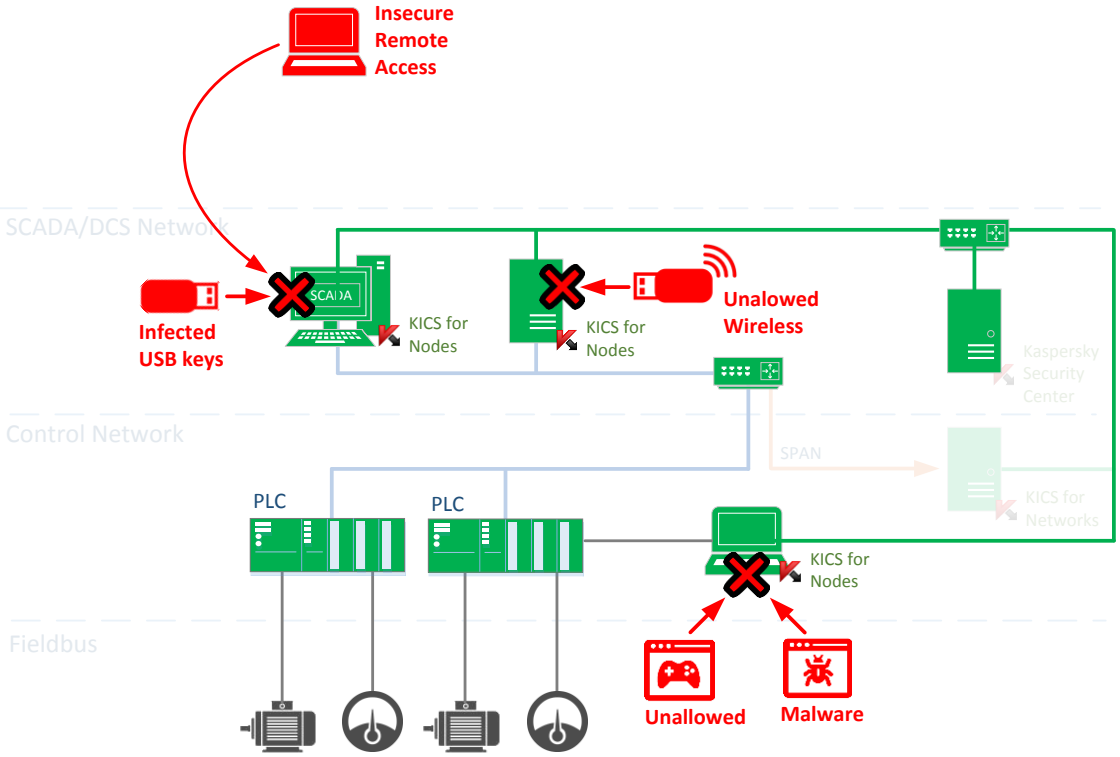
KASPERSKY lab

ВЕКТОРЫ КИБЕРАТАК



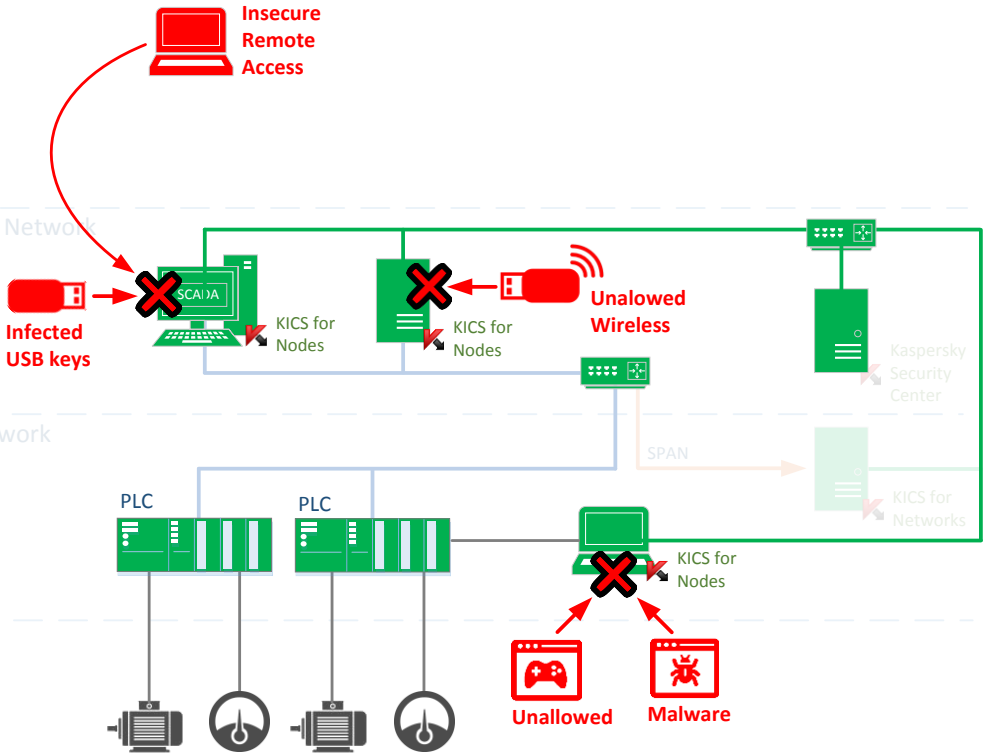
KICS FOR NODES: ФУНКЦИОНАЛ

- Контроль запуска приложений
- Контроль устройств
- Антивирус
- Защита от шифровальщиков
- Early Boot Control
- Контроль целостности PLC
- Firewall



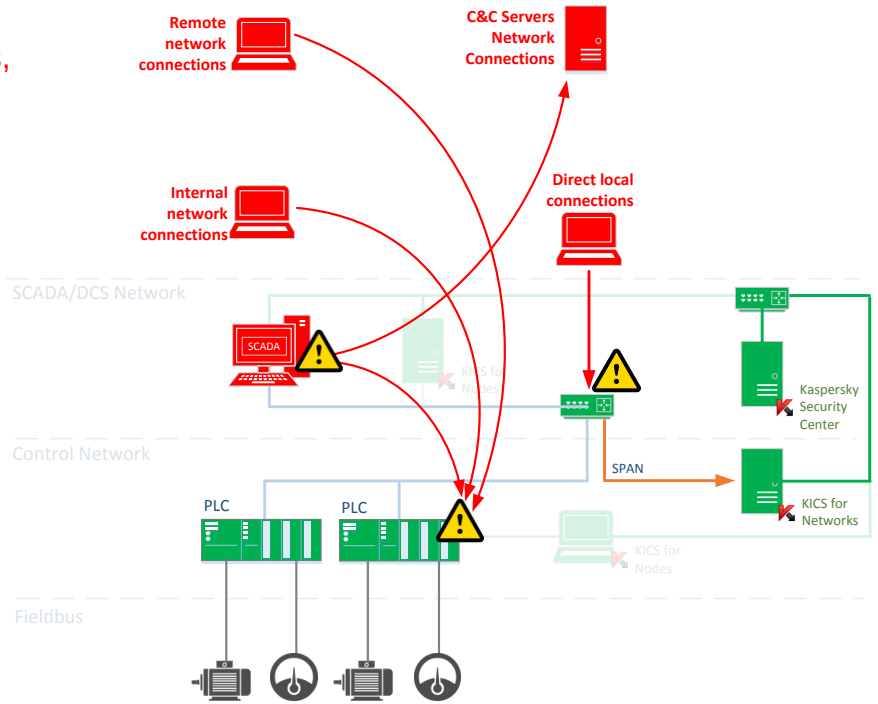
KICS FOR NODES: ИНДУСТРИАЛЬНАЯ СПЕЦИФИКА

- Оптимизированный набор компонентов
- Самостоятельная реализация Контроль запуска программ
- Добавлена Проверка целостности проектов PLC
- Самоограничение потребления ресурсов
- Возможность обновления с внешнего носителя
- Отключение монитора antimalware / только плановые проверки
- Сертификация с разработчиками компонент АСУ ТП



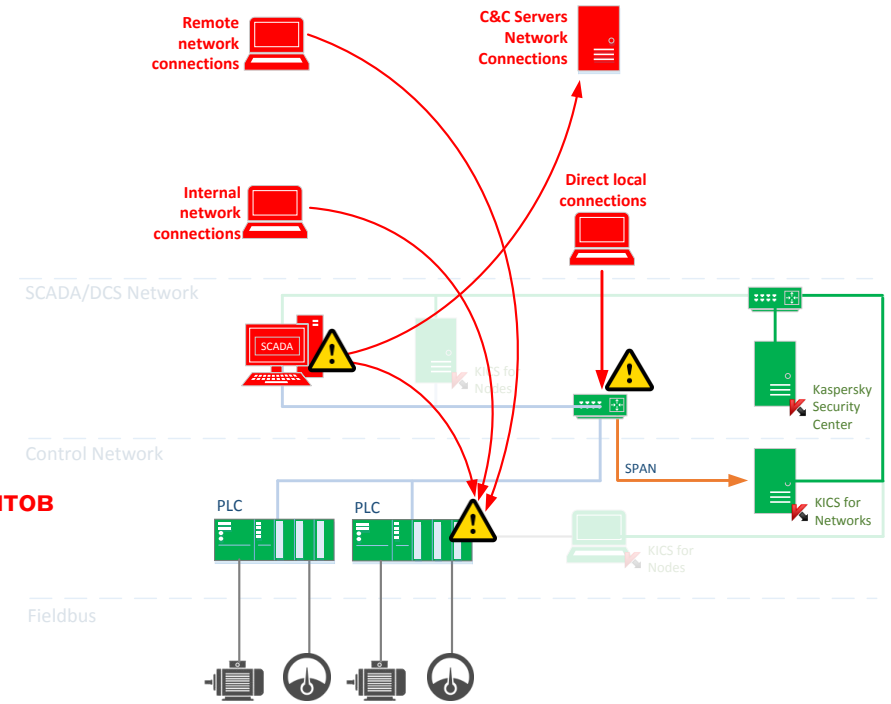
KICS FOR NETWORKS – СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

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
   5. И прочее…
4. **Контроль параметров технологического процесса**
   1. Границы конкретных параметров (Min < X < 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



KASPERSKY INDUSTRIAL CYBERSECURITY

LEVEL 4

Business planning and logistics

Managing end-to-end supply chain.
Establishing the basic plant schedule – production, material use, delivery, and shipping.

LEVEL 3

Manufacturing Operations management

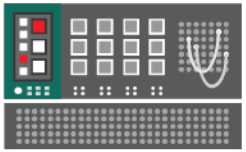
Work flow/recipe control to produce the desired end products.
Maintaining records and optimizing the production process.

Kaspersky Security for Business + Professional Services

LEVEL 2, 1

Batch Control.
Continuous Control.
Discrete Control.

Monitoring, supervisory control and automated control of the production process



Sensing the production process, manipulating the production process

Kaspersky Industrial CyberSecurity

LEVEL 0

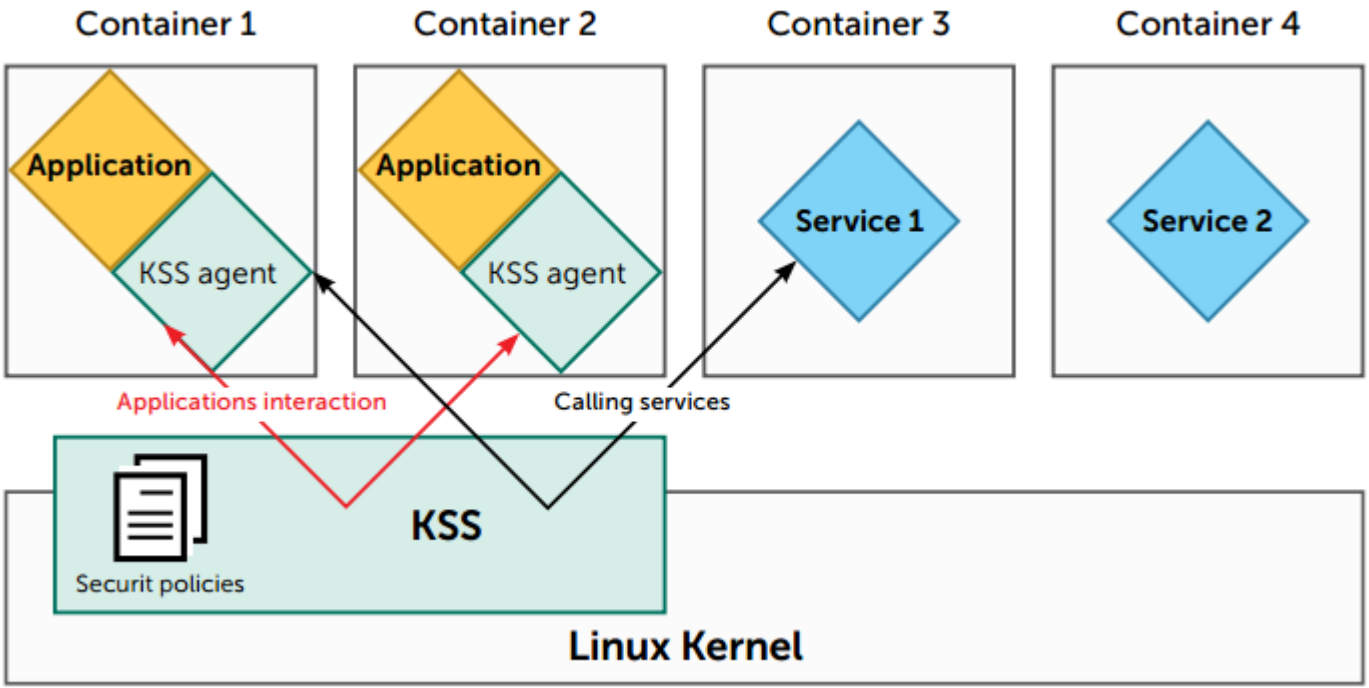
Physical

Physical devices

Physical security

KASPERSKY lab

KASPERSKY SECURITY SYSTEM FOR LINUX



ВОПРОСЫ?

KASPERSKY lab