Kaspersky
Industrial
CyberSecurity

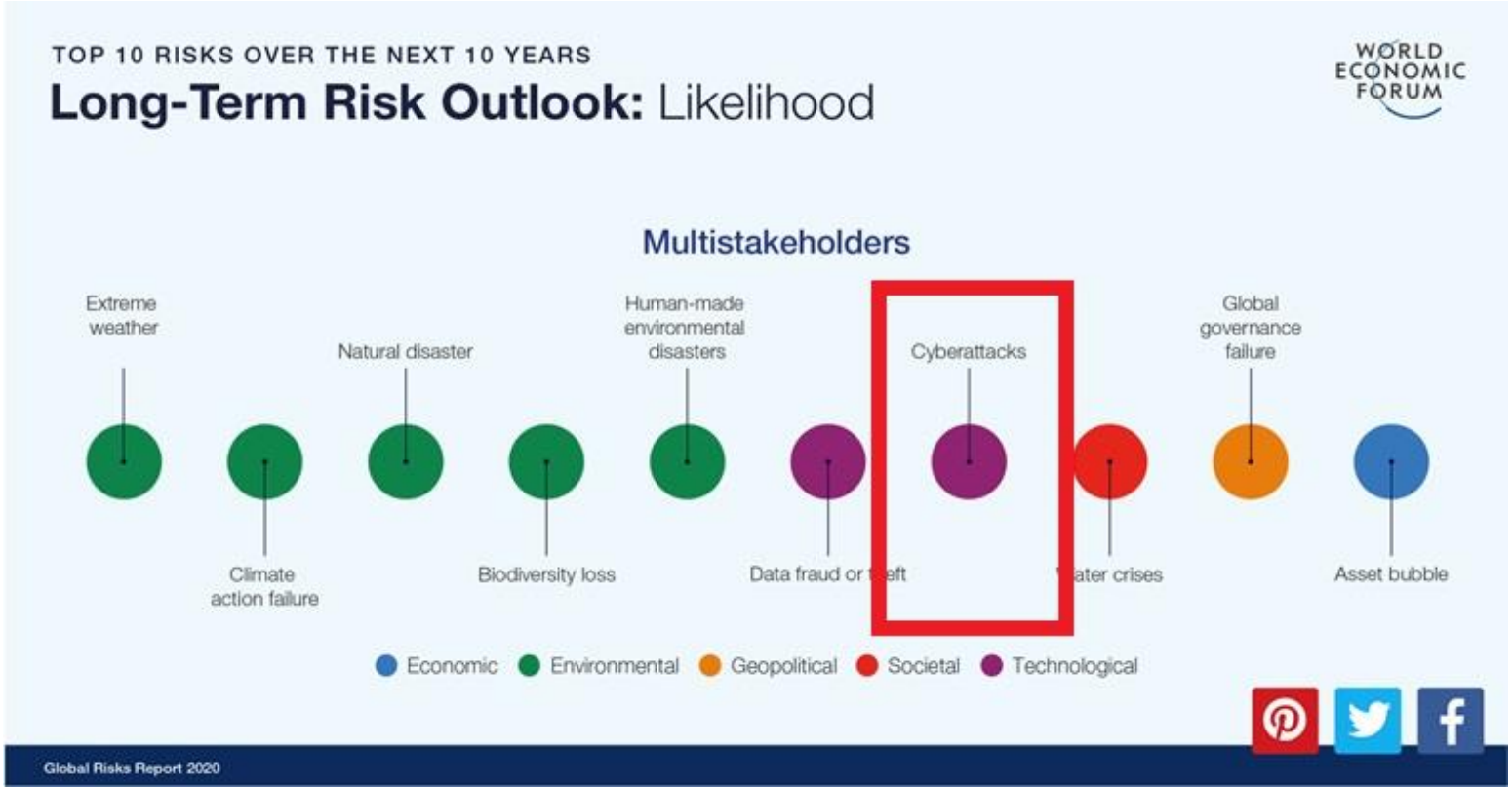
Kaspersky ICS CERT:
Ландшафт киберугроз в условиях пандемии

Решение по контролю удаленного доступа в АСУ ТП

Бондюгин Андрей
KICS Presales Manager

Содержание

Киберугрозы в ТОП-10 наиболее вероятных рисков для предприятий на ближайшее будущее



Kaspersky ICS CERT

Первый индустриальный CERT в коммерческой организации

Около 30 экспертов в области исследования угроз и уязвимостей, расследования инцидентов и анализа защищенности АСУ ТП

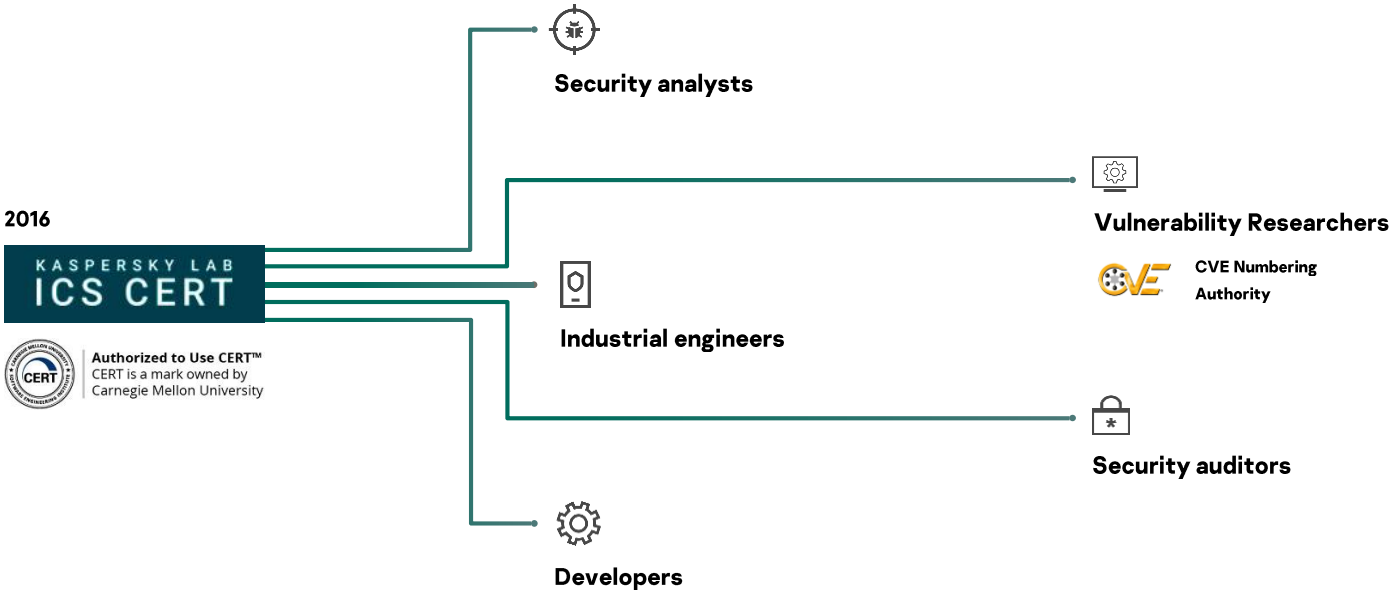
Статус CVE Numbering Authority (CNA)

Обнаружили несколько сотен уязвимостей «нулевого дня» в компонентах АСУ ТП и IIoT

Членство в международных организациях:

ITU ISO IEEE Advancing Technology for Humanity FIRST GlobalPlatform industrial internet CONSORTIUM

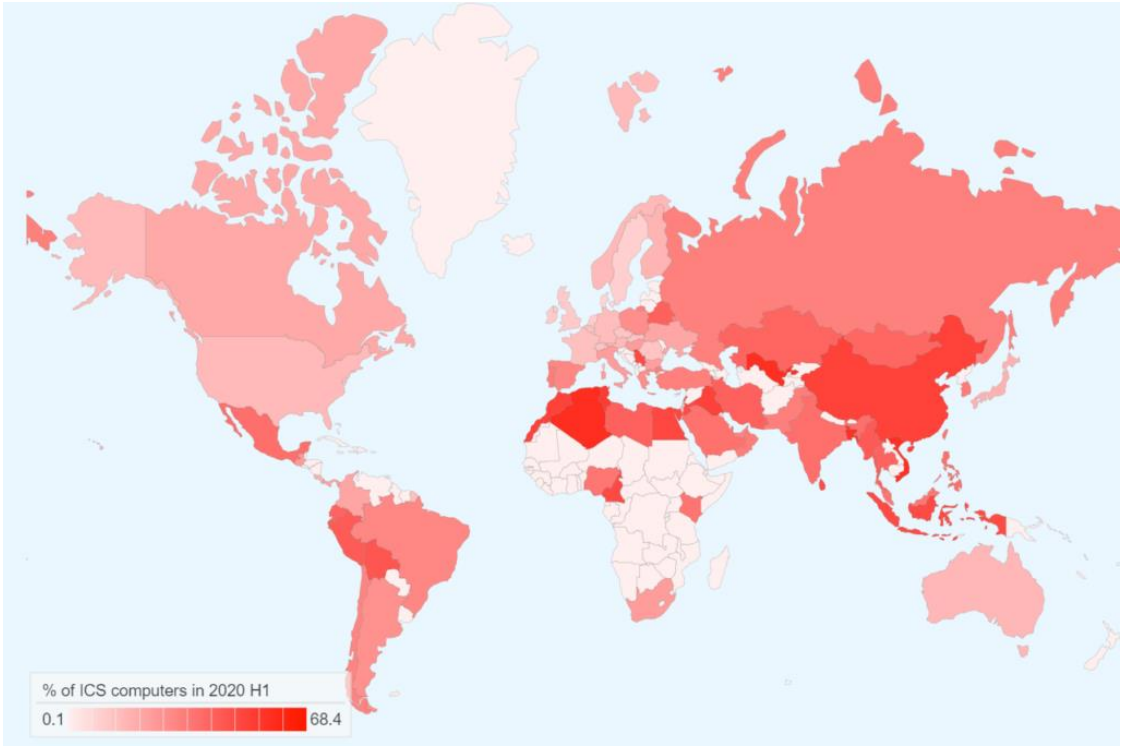
Kaspersky Lab ICS CERT



Источники данных

- Kaspersky Security Network (KSN) и открытые источники
- Kaspersky Industrial CyberSecurity сервисные проекты
- Глобальные опросы

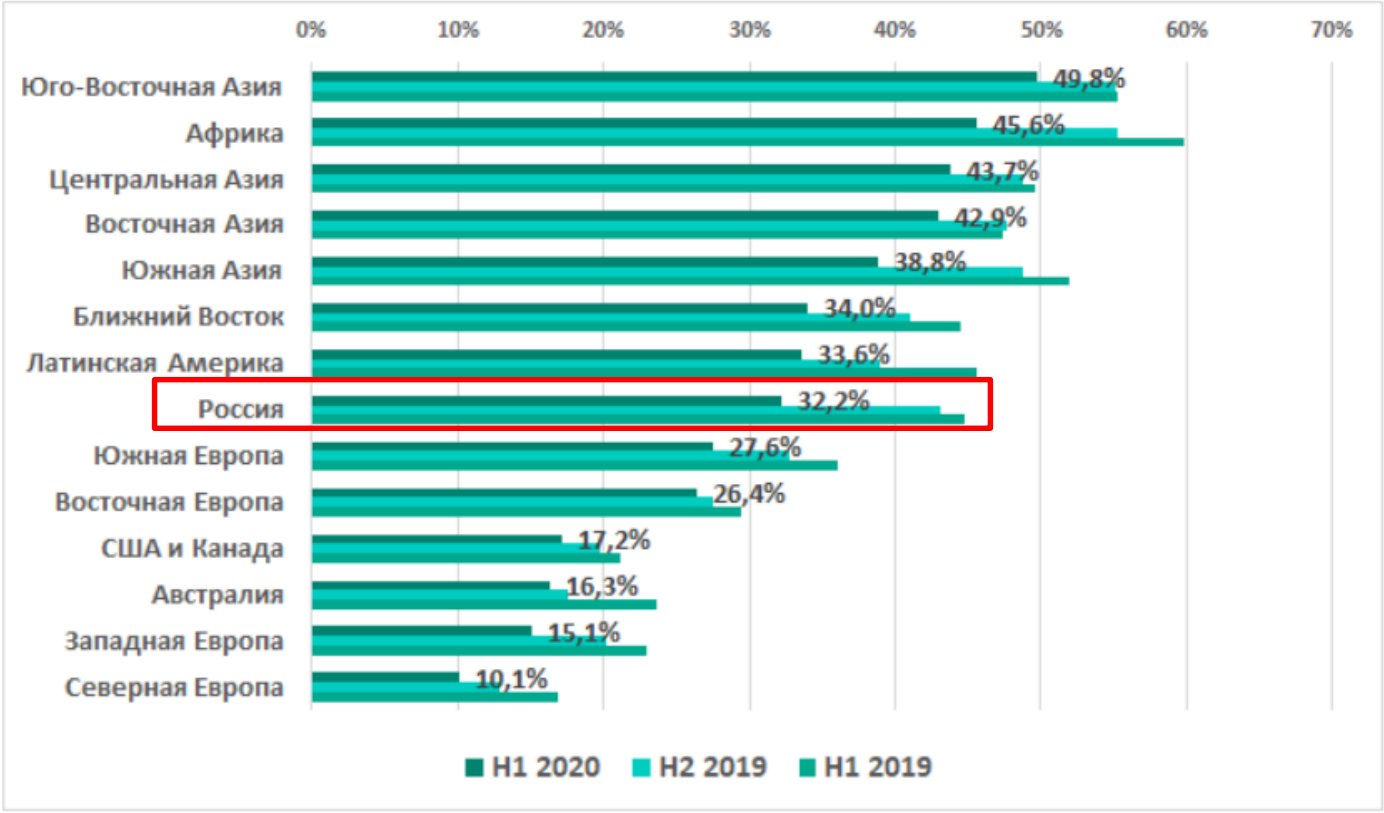
География атак* на системы промышленной автоматизации, 2020



*процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

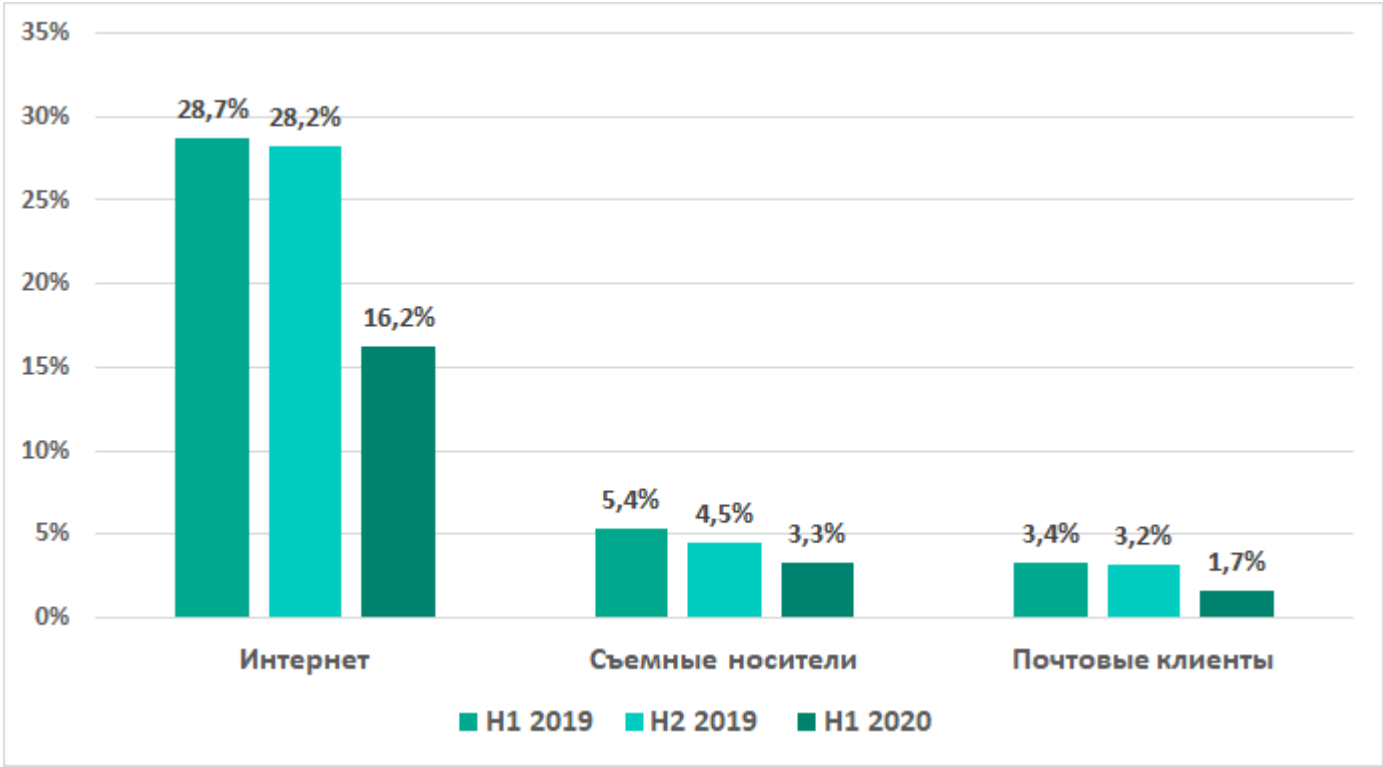
https://ics-cert.kaspersky.ru/media/KASPERSKY_H1_2020_ICS_REPORT_RUS.pdf

Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты



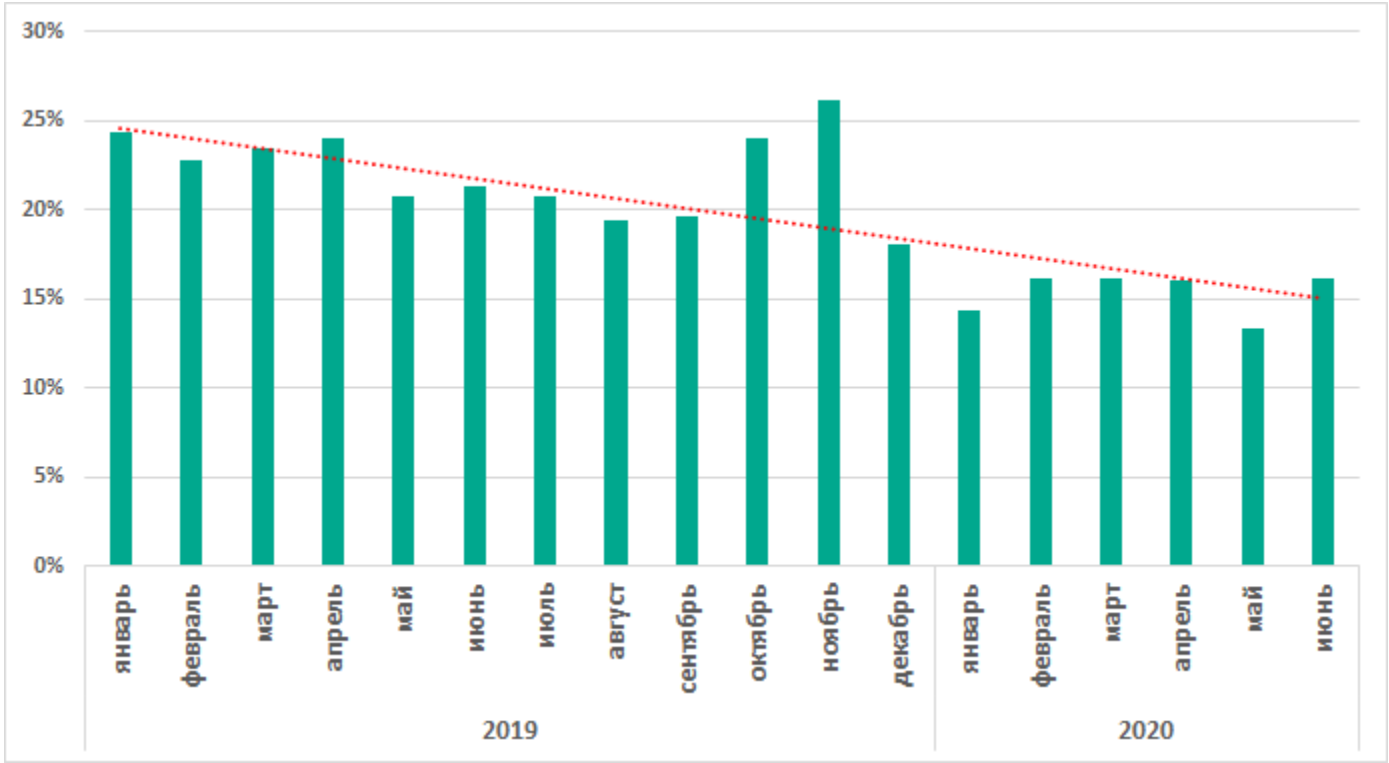
https://ics-cert.kaspersky.ru/media/KASPERSKY_H1_2020_ICS_REPORT_RUS.pdf

Основные источники угроз

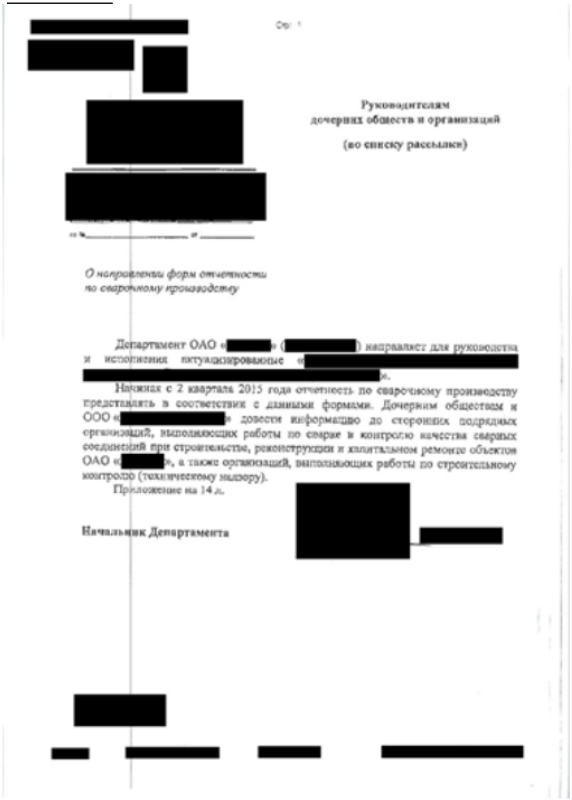


https://ics-cert.kaspersky.ru/media/KASPERSKY_H1_2020_ICS_REPORT_RUS.pdf

Процент компьютеров АСУ в России, на которых были заблокированы вредоносные объекты



https://ics-cert.kaspersky.ru/media/Kaspersky-Attacks-on-industrial-enterprises-using-RMS-and-TeamViewer-RUS.pdf



Руководителям
дочерних обществ и организаций

(по списку рассылки)

О направлении форм отчетности по сварочному производству

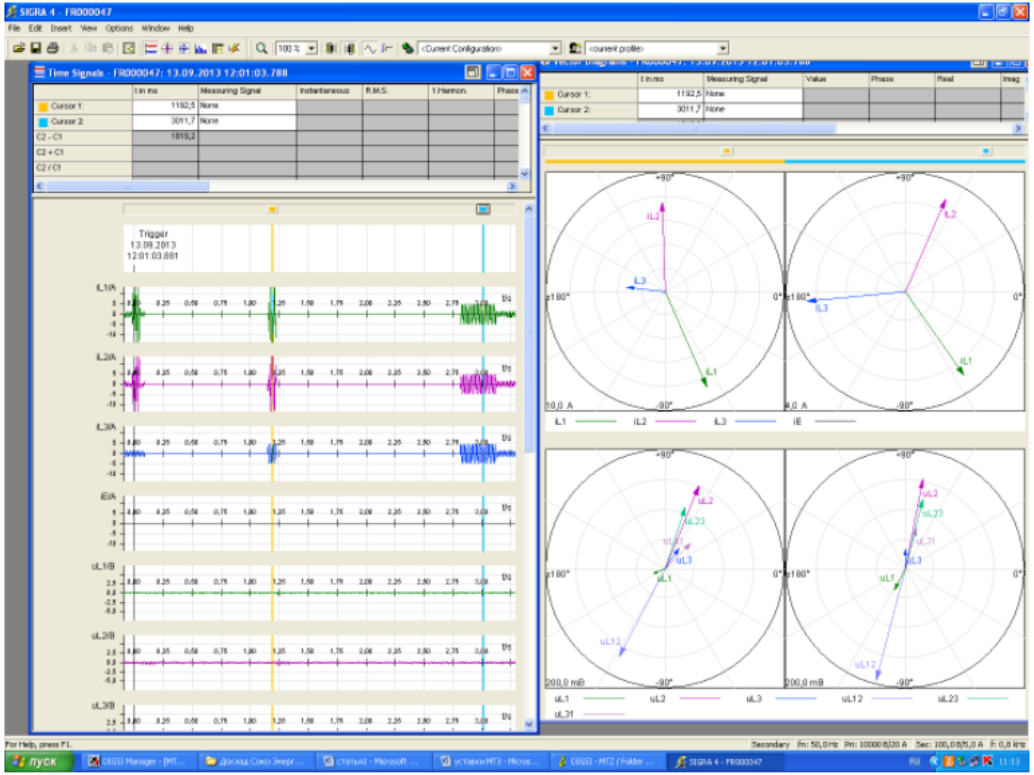
Департамент ОАО «[redacted]» ([redacted]) направляет для руководства и исполнения актуализированные [redacted].

Начиная с 2 квартала 2015 года отчетность по сварочному производству представлять в соответствии с данными формами. Дочерним обществам и ООО «[redacted]» довести информацию до сторонних подрядных организаций, выполняющих работы по сварке и контролю качества сварных соединений при строительстве, реконструкции и капитальном ремонте объектов ОАО «[redacted]», а также организаций, выполняющих работы по строительному контролю (техническому надзору).

Приложение на 14 л.

Начальник Департамента [redacted]

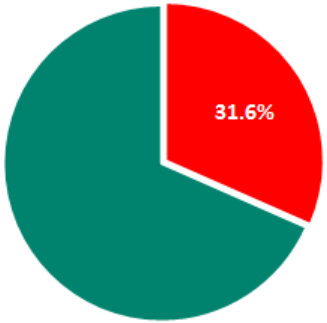
Пример PDF документа с распоряжением для дочерних предприятий, который использовали злоумышленники



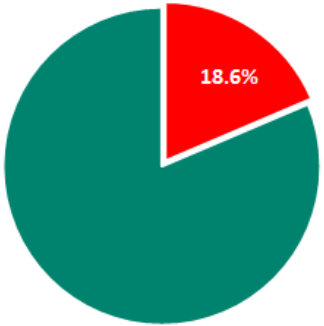
Скриншот векторных диаграмм с осциллограммами

https://ics-cert.kaspersky.ru/media/Kaspersky-Attacks-on-industrial-enterprises-using-RMS-and-TeamViewer-RUS.pdf

Использование инструментов RAT в АСУ ТП по данным KSN

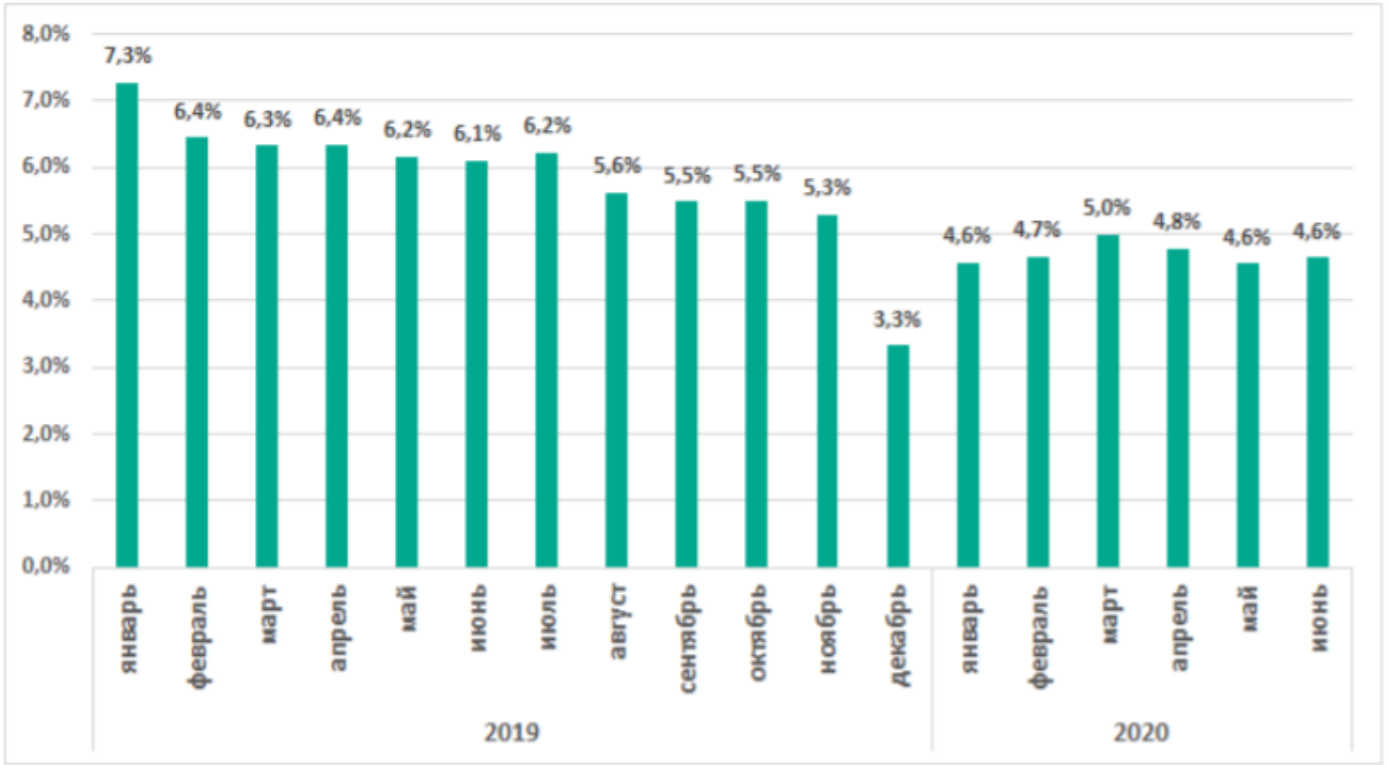


Процент компьютеров АСУ, на которых легитимно установлены RAT



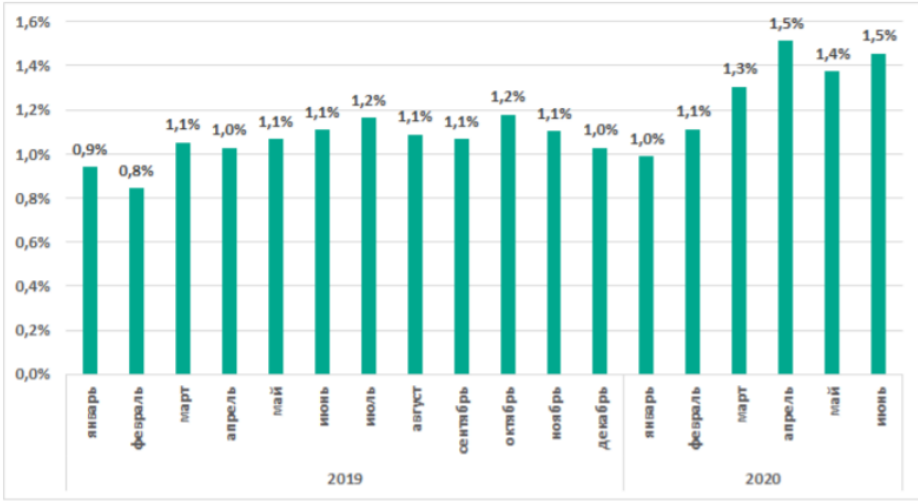
Процент RAT, установленных вместе с продуктами АСУ, среди всех обнаруженных RAT на компьютерах АСУ

Процент компьютеров АСУ, на которых использовался RAT

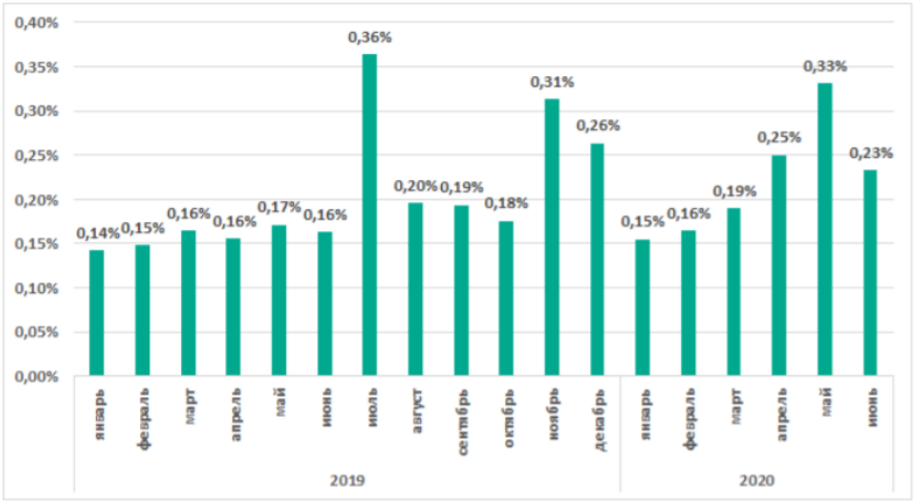


https://ics-cert.kaspersky.ru/media/KASPERSKY_H1_2020_ICS_REPORT_RUS.pdf

Ландшафт киберугроз для систем промышленной автоматизации 2020



Процент компьютеров АСУ, доступных по RDP



Процент компьютеров АСУ, на которых фиксировались попытки подбора паролей к RDP

https://ics-cert.kaspersky.ru/media/KASPERSKY_H1_2020_ICS_REPORT_RUS.pdf

1. **Целевая кампания WildPressure**
   APT-кампания по распространению троянца Milum

2. **Кампании против правительственных и промышленных объектов Азербайджана**
   Использование ранее неизвестного троянца удаленного доступа (RAT), который получил название PoetRAT, особенный интерес к SCADA-системам

3. **Атака на водоочистные сооружения Израиля**
   Атака на SCADA, попытка изменить параметры очистки воды/оставить производственный процесс

Обзор рекомендаций по безопасной удаленной работе для предприятий критической инфраструктуры и не только

1. **ФСТЭК России** – Рекомендации по обеспечению безопасности объектов КИИ при удаленной работе в связи с COVID-19.
2. **Национальный координационный центр по компьютерным инцидентам** – уведомление об угрозах безопасности информации, связанных с пандемией коронавируса.
3. **Институт SANS** – «Security Awareness Deployment Guide – Securely Working at Home»: список материалов для проведение обучения сотрудников по безопасной работе из дома.
4. **Национальный институт стандартов и технологий США (NIST)** – бюллетень с рекомендациями по безопасному удаленному доступу и удаленной работе.
5. **Американское агентство кибербезопасности и безопасности инфраструктуры (CISA)** – вопросы обеспечения кибербезопасности организаций в рамках глобального процесса управления рисками, связанными с COVID-19.
6. **Агентство Европейского союза по кибербезопасности (ENISA)** – советы по кибербезопасности при удаленной работе.

https://ics-cert.kaspersky.ru/reports/2020/04/30/secure-remote-work-for-critical-infrastructure/

Последствия COVID-19

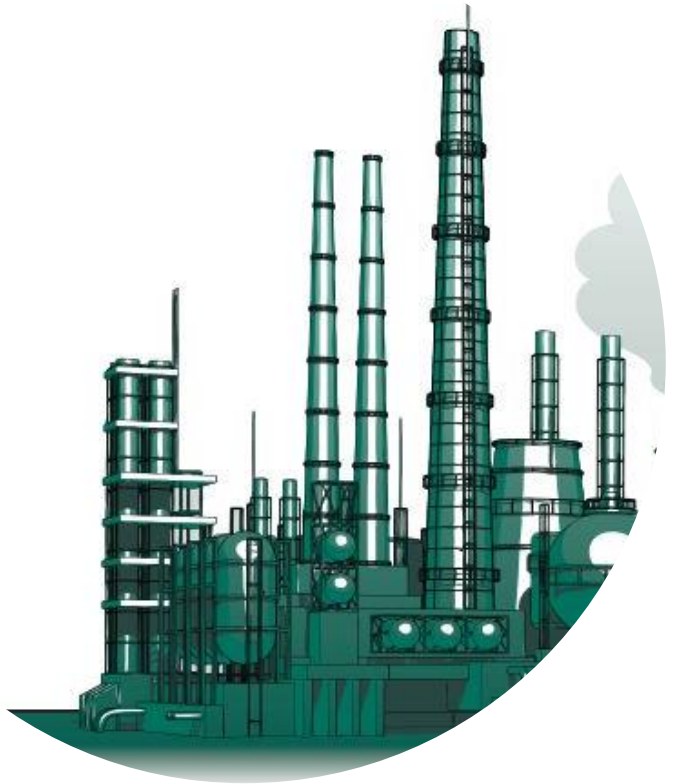
1. «Заморозка» усиления защиты периметра, установки и настройки нового оборудования
2. Необходимость организации удаленного доступа
3. Сокращение количества оперативного персонала на местах
4. Ухудшение экономической обстановки
5. Цифровизация сервисов

1. Число серьёзных инцидентов уменьшаться не будет.
2. Увеличение срока реакции на инцидент.
3. Увеличение масштаба распространения вредоносного ПО и усугубление последствий киберинцидентов.
4. Пополнение рядов хакеров, подкуп работников предприятий.
5. Новые кросс-платформенные атаки:

МФЦ и Госуслуги – МВД – системы видеонаблюдения – управление транспортом – СКУД

Прогноз. Случайные заражения и вымогательское ВПО

1. Заражения будут становиться **менее случайными** или иметь неслучайные продолжения.
2. Доступ к компьютерам будут **перепродавать продвинутым группировкам**.
3. Появление **новых** интересных **сценариев** атак на АСУ ТП и полевые устройства, а также неожиданных **схем монетизации**.
4. Снятие с поддержки **Windows 7** и **Server 2008** и утечка исходных кодов **Windows XP** приведет к **повторению** сценария наподобие WannaCry.
5. Промышленные предприятия будут в числе **наиболее** пострадавших.



https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-Threat-Predictions-2021-RU.pdf

Прогноз. APT и кибершпионаж

1. Активность группировок будет **коррелировать с локальными конфликтами**: кибератаки будут использоваться как инструмент военных действий наряду с беспилотниками и информационными атаками через СМИ.
2. Более **активные действия**, вероятность **продолжения серии** Stuxnet — Black Energy — Industroyer — Triton.
3. Проблемы с разграничением доступа в OT-сетях могут сделать их привлекательной **точкой входа** в корпоративную сеть или в инфраструктуру других организаций.
4. Санкционная политика и стремление к технологической независимости приведут к тому, что среди **мишеней атаки** будут **тактические и стратегические партнеры** — никому нельзя будет доверять.

https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-Threat-Predictions-2021-RU.pdf

Kaspersky Industrial Cybersecurity (KICS). Описание решения

Kaspersky Industrial CyberSecurity

СЕРВИСЫ

Обучение и программы повышения осведомленности

- Kaspersky® Security Awareness
- Kaspersky® Security Trainings

Экспертные сервисы и данные об угрозах

- Kaspersky® Security Assessment
- Kaspersky® Incident Response
- Kaspersky® Threat Intelligence

ТЕХНОЛОГИИ

Защита промышленных компьютеров

- KICS for Nodes

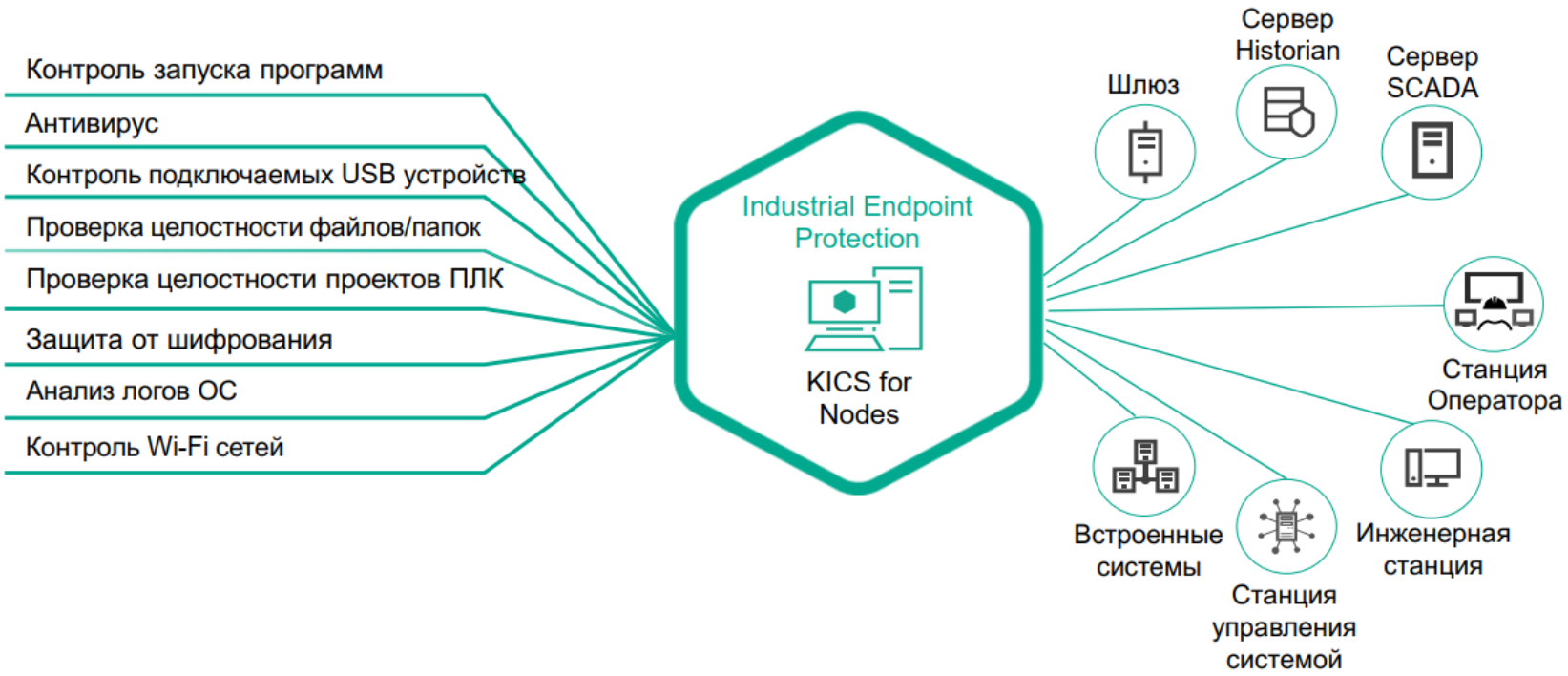
Обнаружение аномалий и угроз в промышленной сети

- KICS for Networks

Централизованное управление безопасностью

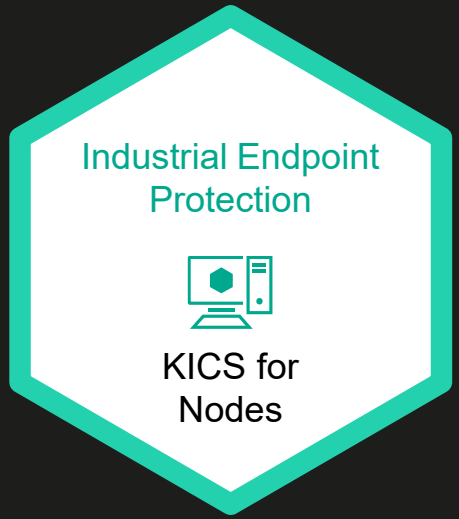
- Kaspersky Security Center

KICS for Nodes



KICS for Nodes: промышленная специфика

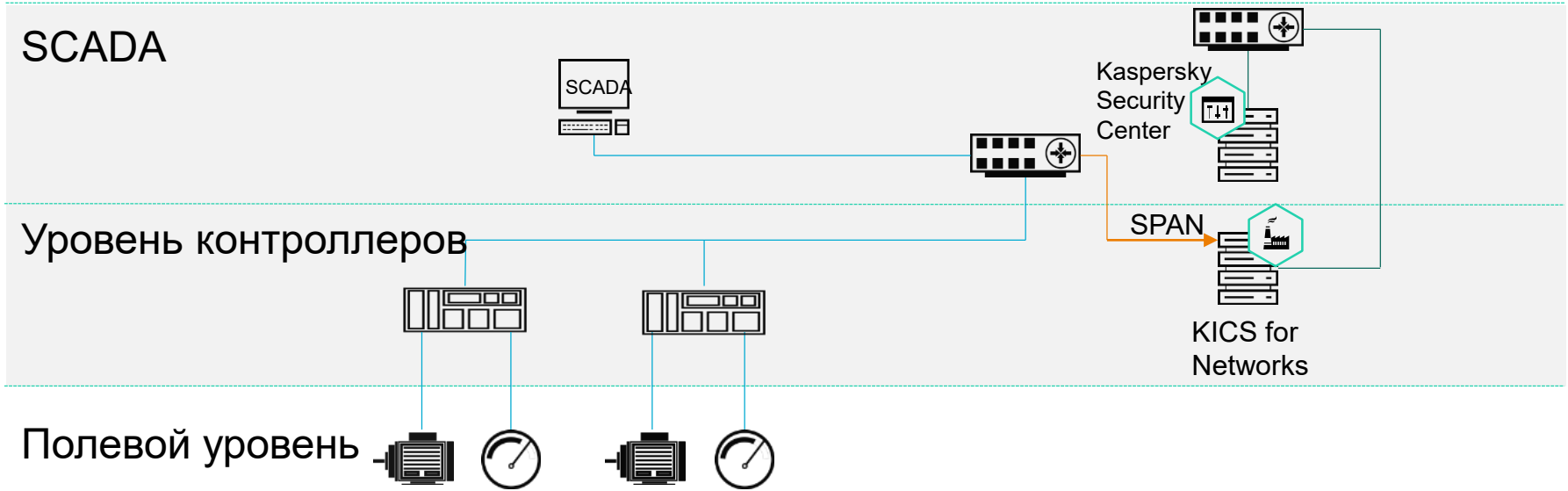
Почему нужно использовать KICS вместо корпоративного антивируса для защиты АСУ ТП?



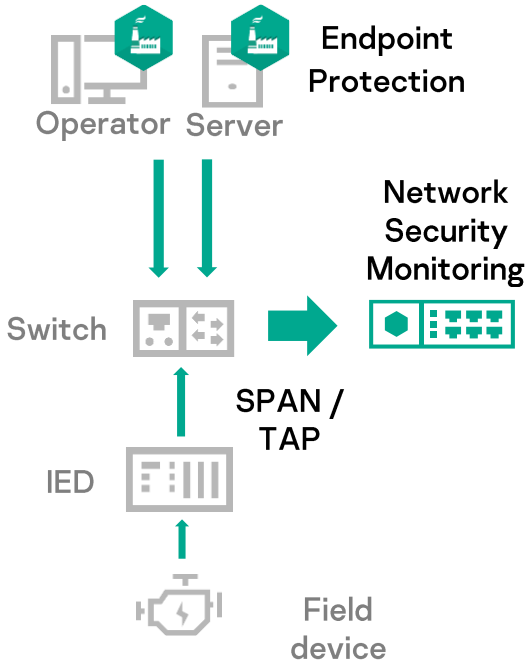
- Уменьшено потребление ресурсов
  - 512 MB Оперативной памяти для Windows XP SP2 / XP Embedded
- Установка / Обновление / Удаление без перезагрузки
- Возможность работы в полностью неблокирующем режиме
- Возможность обнаружения угроз нулевого дня (в том числе в неблокирующем режиме)
  - Контроль запуска приложений
  - Анализ логов
  - Мониторинг файловых операций

KICS for Networks

- Пассивный мониторинг сети в режиме реального времени
- Анализ зеркалированной копии трафика (SPAN)



KICS for Networks



DPI	Deep Packet Inspection – контроль параметров тех. процесса в реальном времени
NIC	Network Integrity Control – контроль целостности сети
IDS	Intrusion Detection System – система обнаружения компьютерных атак
CC	Command Control – инспекция команд, передаваемых по промышленным протоколам
EXT	External Systems – внешние источники + результаты корреляции

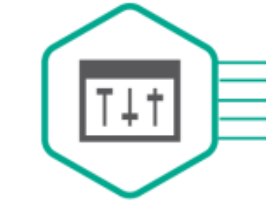
+

Управление инцидентами

+

Интеграция с third-party системами (CEF, Syslog, API)

Kaspersky Security Center



Kaspersky Security Center

УПРАВЛЕНИЕ СИСТЕМОЙ

- Централизованная система сбора данных
- Централизованное развертывание ПО
- Обнаружение уязвимостей и управление обновлениями
- Расширенные возможности управления клиентами

ИНТЕГРАЦИЯ С SIEM

- ArcSight, Splunk, QRadar
- Syslog сервер

УПРАВЛЕНИЕ ПОЛИТИКАМИ

- Централизованное управление политикой безопасности
- Удаленное планирование и выполнение задач

ИНТЕГРАЦИЯ С HMI

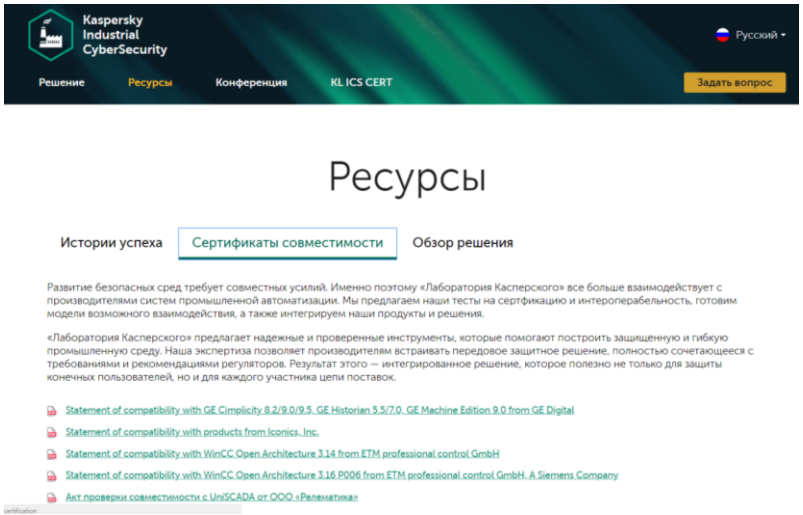
ИНТЕГРАЦИЯ ПАНЕЛИ MES

- Состояние безопасности доставляется на совместимый с IEC 104 / OPC 2.0 хост

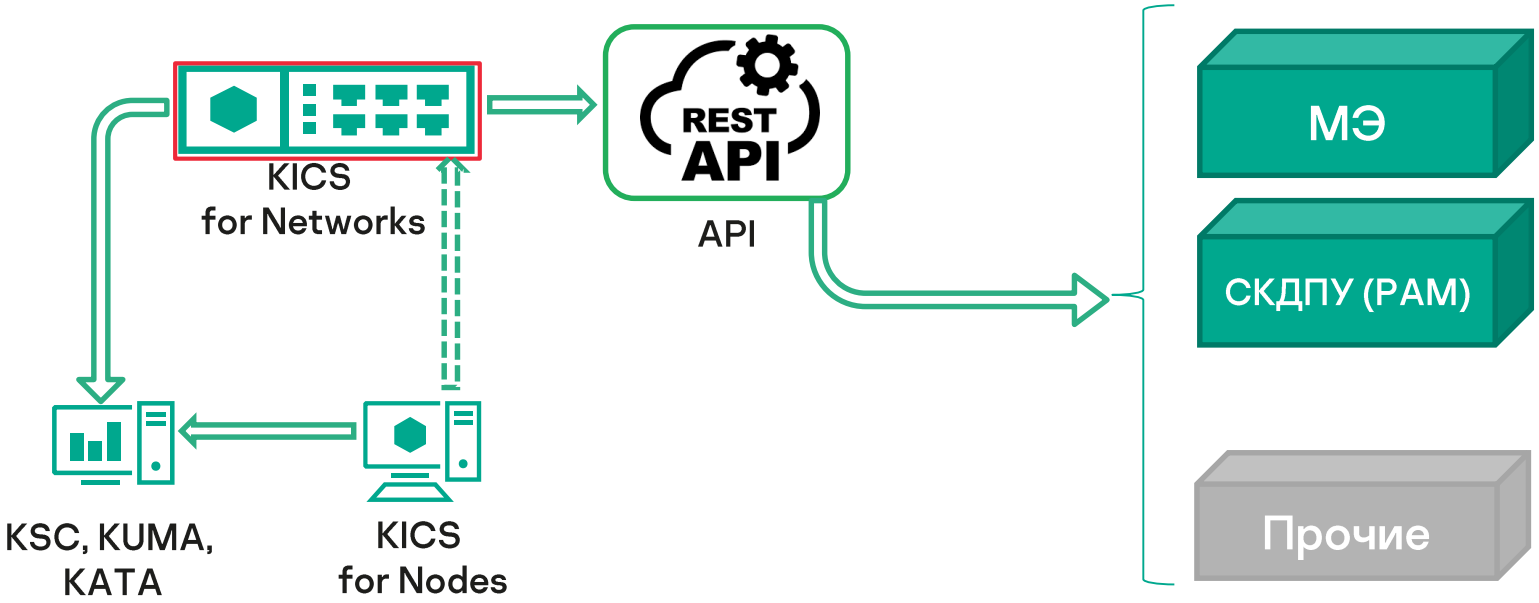
ОТЧЕТНОСТЬ И УВЕДОМЛЕНИЯ

- Регистрация событий
- Отчетность
- Уведомления по SMS/Email

Сертификация с поставщиками АСУ ТП



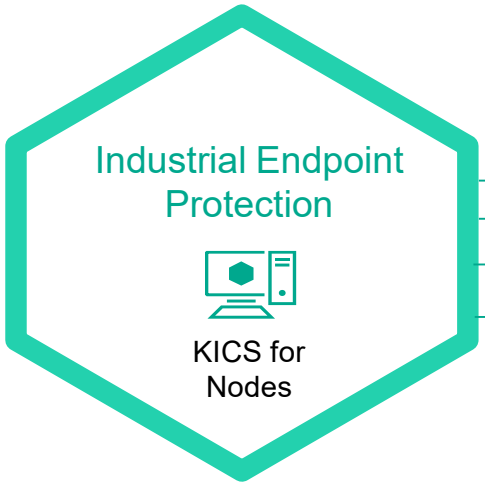
Как с помощью KICS контролировать удаленный доступ?



KICS позволяет создавать интегрированную экосистему средств защиты информации АСУ ТП

Сценарии защиты удаленного доступа

Сценарии защиты удаленного доступа. Активная защита (на конечных узлах)



ПРЕДОТВРАЩЕНИЕ ЗАПУСКА НЕЖЕЛАТЕЛЬНОГО ПО

- Контроль за тем, какое приложение может быть запущено на каждом конкретном узле
- Работа от «белого списка».
  Возможность протестировать «белый список» перед применением

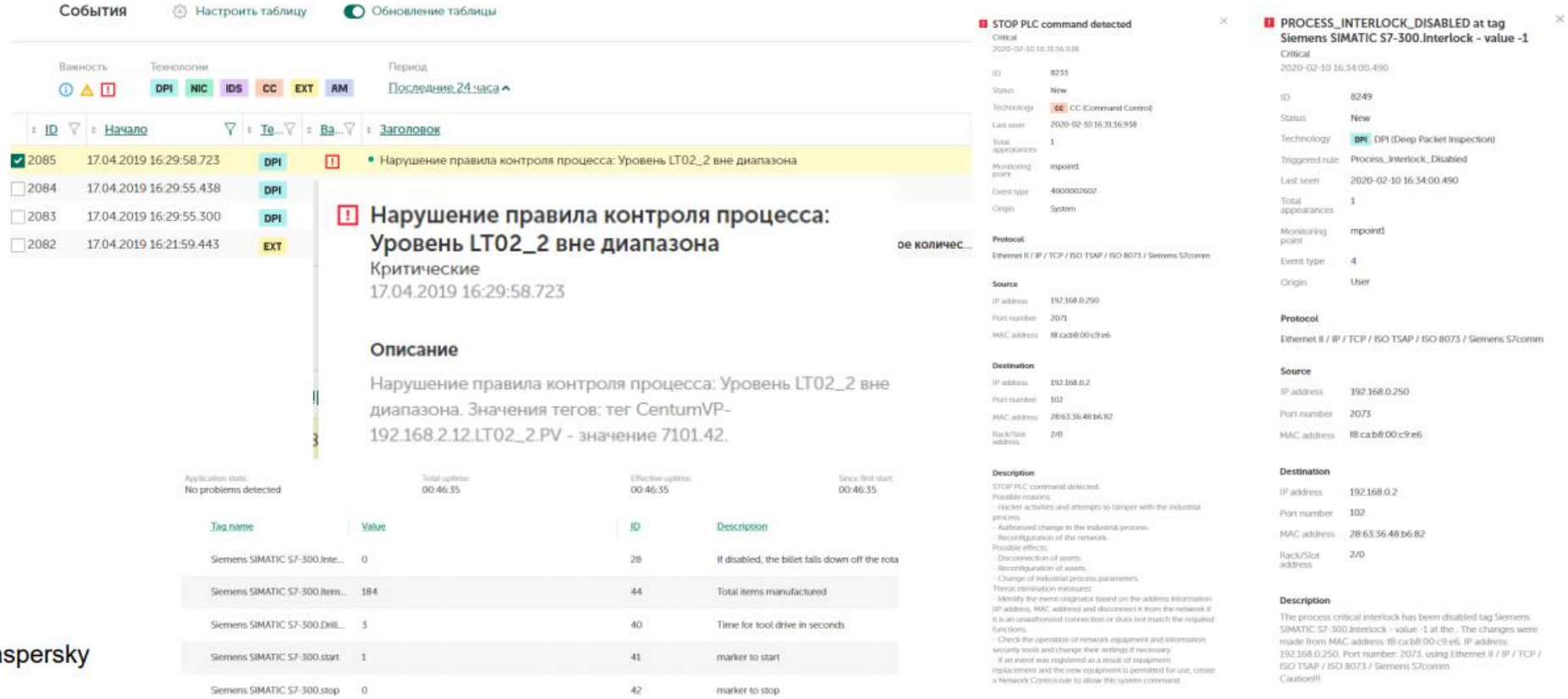
ЗАЩИТА ОТ ШИФРОВАЛЬЩИКОВ

МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В КОНТРОЛИРУЕМЫХ ОБЛАСТЯХ

КОНТРОЛЬ ИНФОРМАЦИОННОГО ОКРУЖЕНИЯ

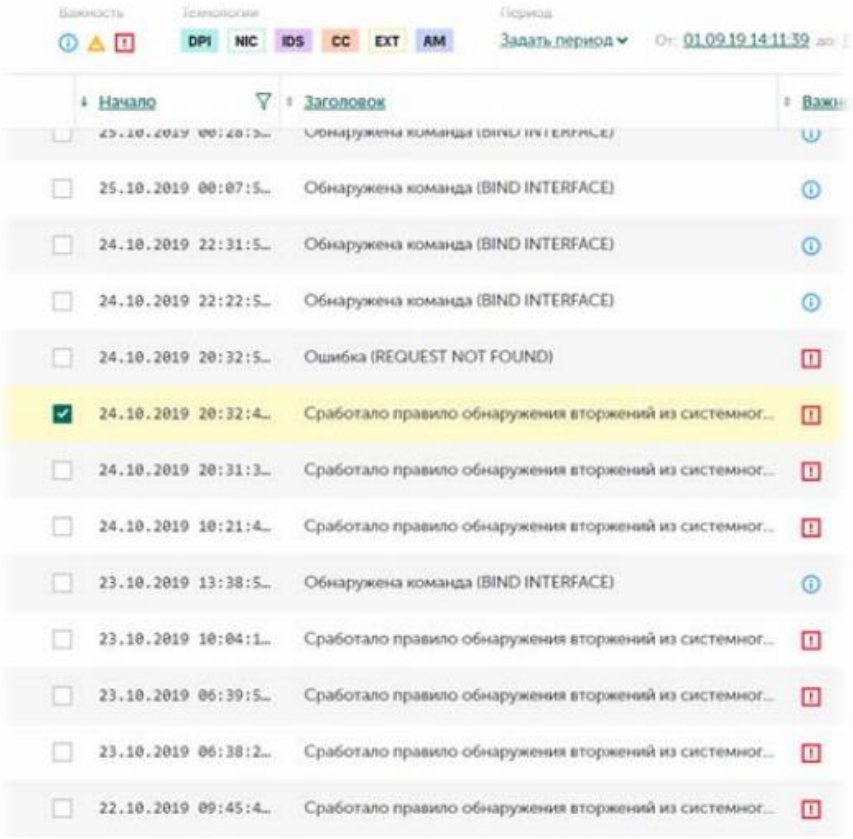
- Контроль подключаемых устройств
- Контроль подключения к Wi-Fi сетям

Сценарии защиты удаленного доступа. Контроль сетевой активности (в части использования промышленных протоколов и конфигурирования параметров тех. процесса)



Kaspersky

Сценарии защиты удаленного доступа. Контроль сетевой активности (в части обнаружения вторжений внутри периметра АСУ ТП)



Сработало правило обнаружения вторжений из системного набора правил: awp

Критические

24.10.2019 20:32:49.591 – 24.10.2019 20:32:49.591

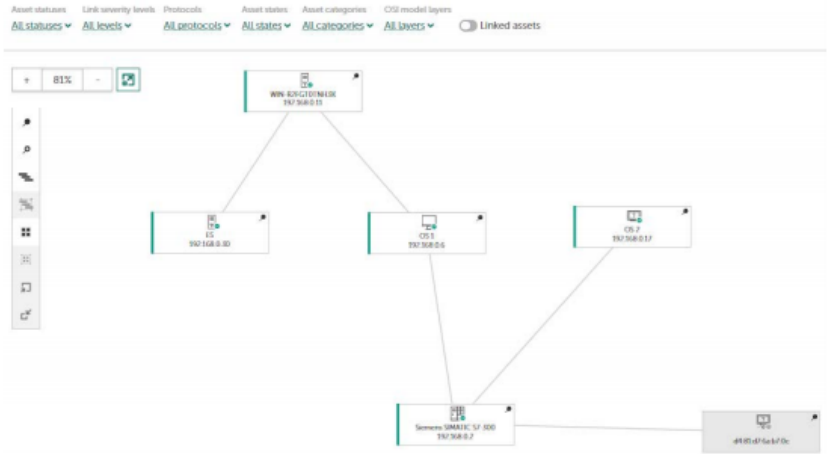
Описание

Сработало правило обнаружения вторжений из системного набора правил.
Класс: Signs of Trojan Activity.
Правило: Exploit.CVE-2010-0022.TCP.C&C.
Приоритет правила: 1.
Набор правил: awp.

ID	19111
Статус	Новое
Технология	IDS – Обнаружение вторжений

Сценарии защиты удаленного доступа. Контроль сетевой активности (в части выявления несанкционированных подключений)

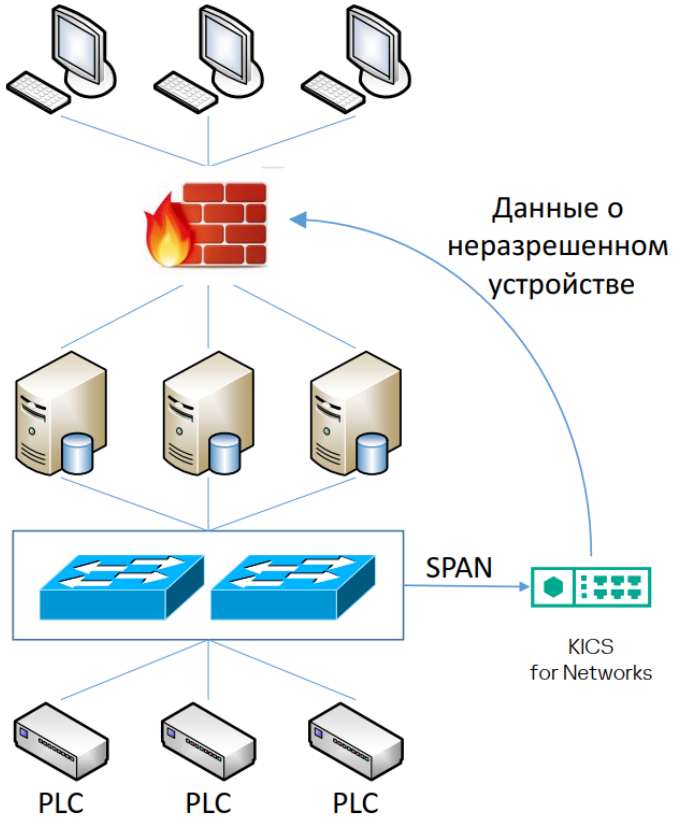
Ожидания



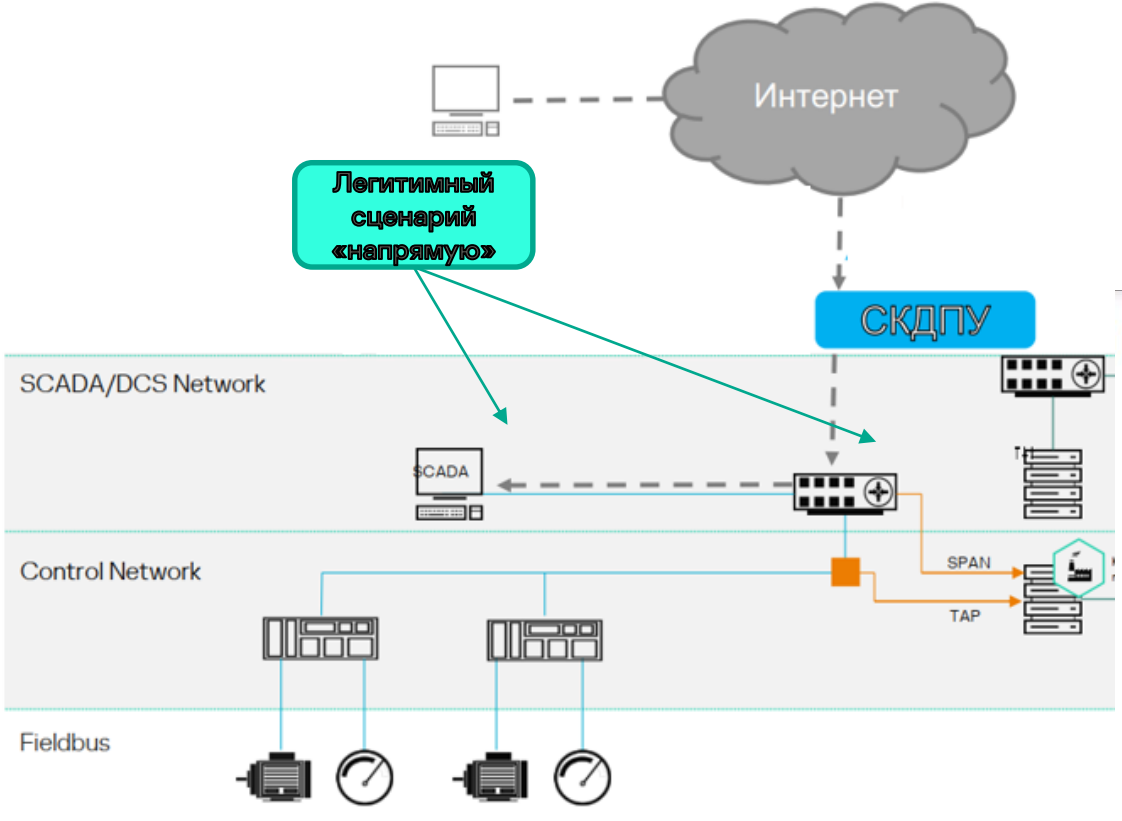
Реальность

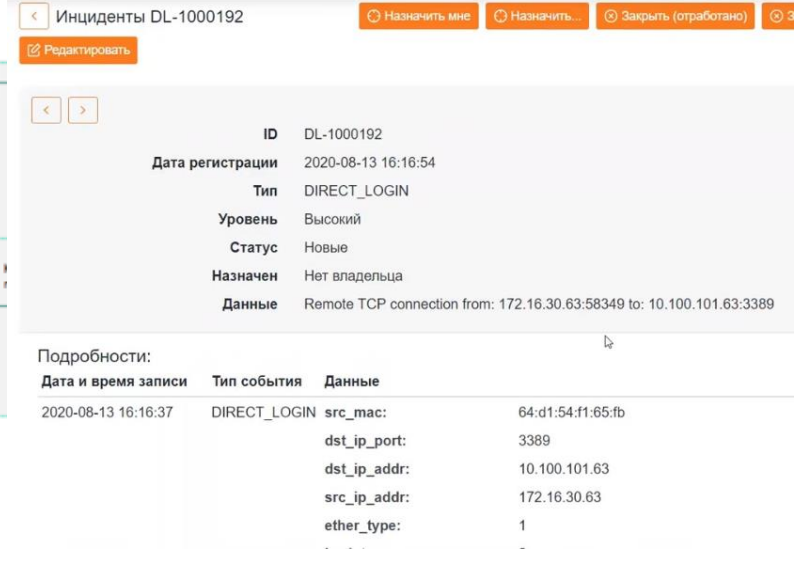
Name	Status	Address information	Category
ES	Authorized	00:0c:29:27:0d:1f; 192.168.0.30	Server
NB3	Authorized	f8:ca:b8:00:c9:e6; 192.168.0.250	Server
OS 1	Authorized	00:0c:29:4a:1d:2c; 192.168.0.6	Server
OS 2	Authorized	192.168.0.17	Other
OS 3	Authorized	00:0c:29:6c:0b:ba; 192.168.0.21	Other
Siemens SIMATIC S7-300	Authorized	28:63:36:48:b6:82; 192.168.0.2	PLC
WIN-JKA9BK70UV3	Unauthorized	48:61:a3:ca:17:b0; 192.168.0.230	Server
WIN-R2FGT0TNH3K	Authorized	00:0c:29:9a:85:52; 192.168.0.11	Server

Сценарии защиты удаленного доступа. Блокирование несанкционированных подключений. Интеграция с межсетевыми экранами

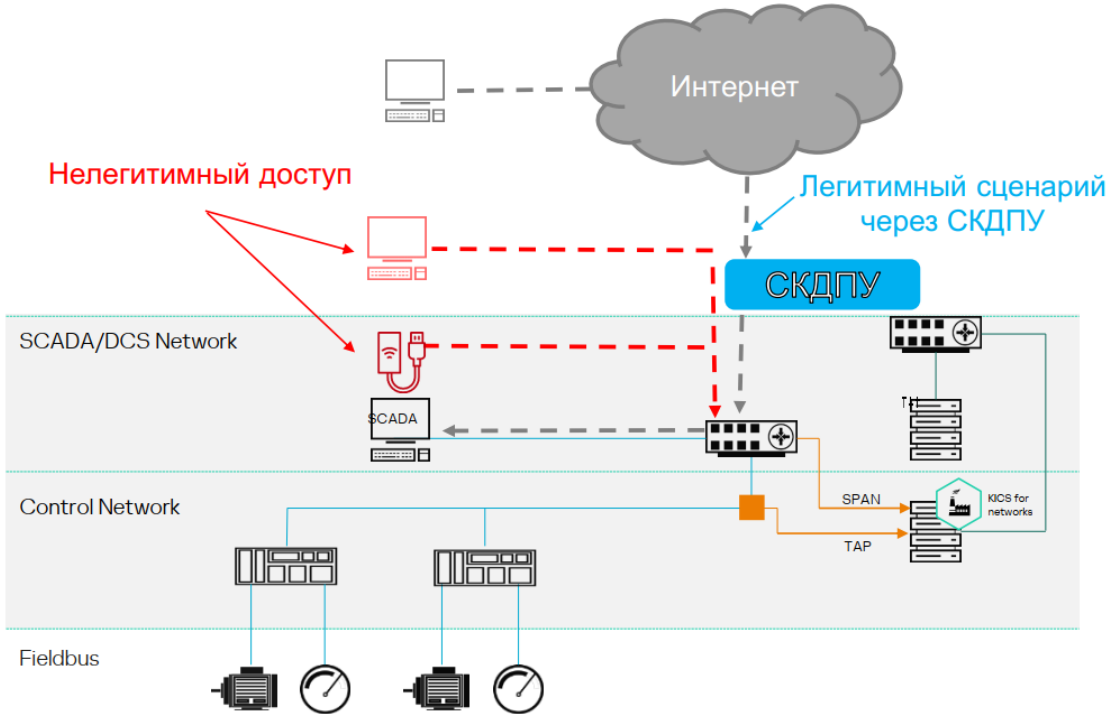


Сценарии защиты удаленного доступа. Контроль пользовательских сессий. Интеграция с СКДПУ. Локальное подключение

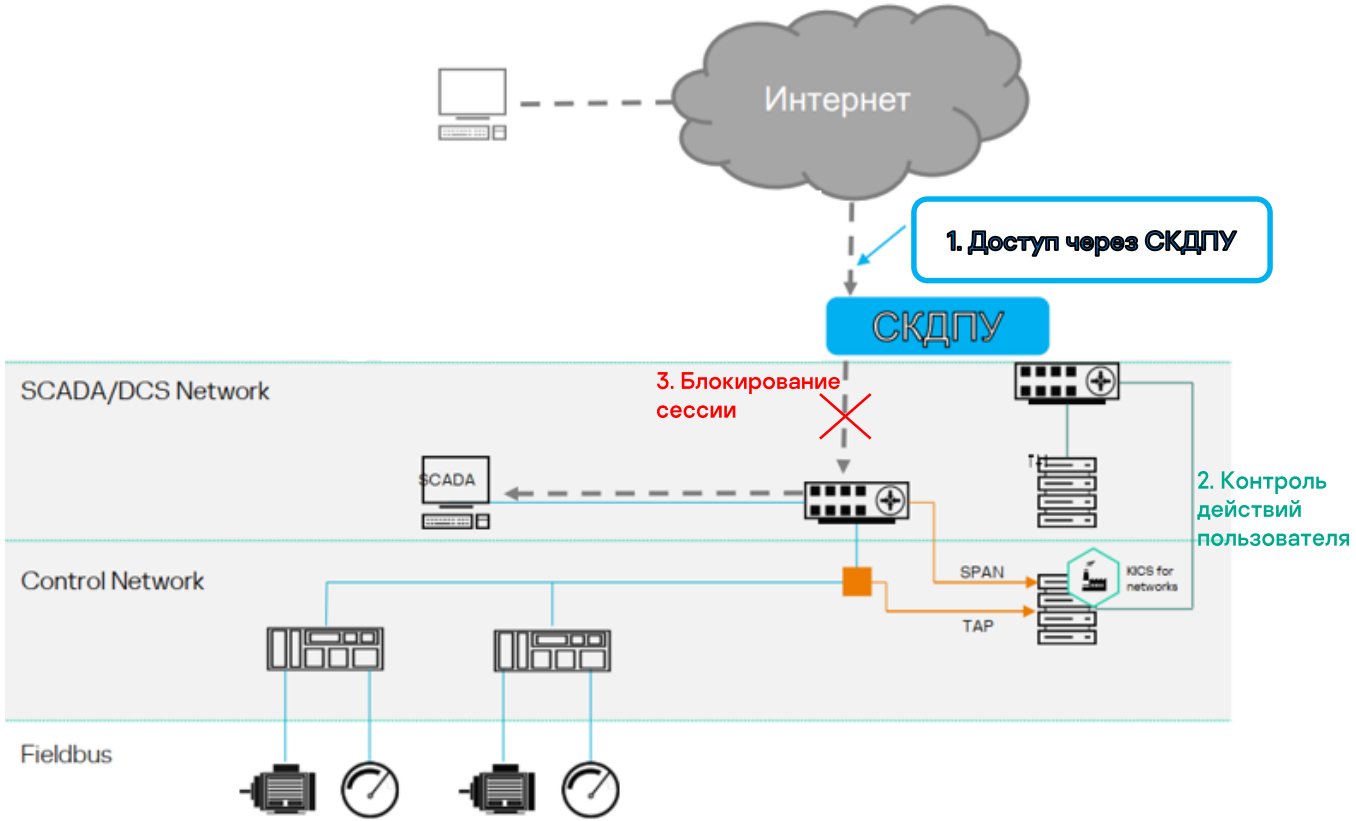




Сценарии защиты удаленного доступа. Контроль пользовательских сессий. Интеграция с СКДПУ. Удаленное подключение



Сценарии защиты удаленного доступа. Контроль пользовательских сессий. Интеграция с СКДПУ. Контроль удаленного подключения и разрыв сессии



Kaspersky ICS CERT – чем мы можем помочь?

Threat intelligence

Отчеты об угрозах и потоки данных

- Подписка на TI-отчеты об угрозах и уязвимостях
- Кастомизированные отчеты об угрозах и уязвимостях
- Поток данных (data feed) об угрозах в АСУ ТП
- Поток данных (data feed) об уязвимостях в АСУ ТП

Программы обучения

Повышение осведомленности и профессиональные тренинги

- Курсы по повышению осведомленности в области промышленной кибербезопасности
- Расследование инцидентов и цифровая криминалистика в АСУ ТП
- Тренинги по поиску уязвимостей в IoT-устройствах и фаззингу

Реагирование на инциденты

Реагирование и расследование инцидентов ИБ

- Реагирование на инциденты в АСУ ТП и цифровая криминалистика
- Разработка индивидуального руководства по реагированию на инциденты

Анализ защищенности

Анализ уязвимостей и пентест

- Аудит информационной безопасности АСУ ТП, включая тестирование на проникновение и моделирование угроз
- Поиск уязвимостей в отдельных IoT/IIoT устройствах

Product security

Анализ безопасности продуктов и сертификация

- Сертификация в соответствии с моделью зрелости безопасности
- Поиск уязвимостей в пред-релизных версиях продуктов
- Анализ безопасности продуктов на начальных этапах разработки

kaspersky

Kaspersky Industrial CyberSecurity

Активируем будущее вместе!

Андрей Бондюгин
Kaspersky Industrial CyberSecurity
Andrey.Bondyugin@Kaspersky.com
+7 966 168 97 63

ics.kaspersky.com