



Kaspersky
Industrial
CyberSecurity

Kaspersky ICS CERT:

Ландшафт киберугроз в условиях пандемии

Решение по контролю удаленного доступа в АСУ ТП

Бондюгин Андрей
KICS Presales Manager



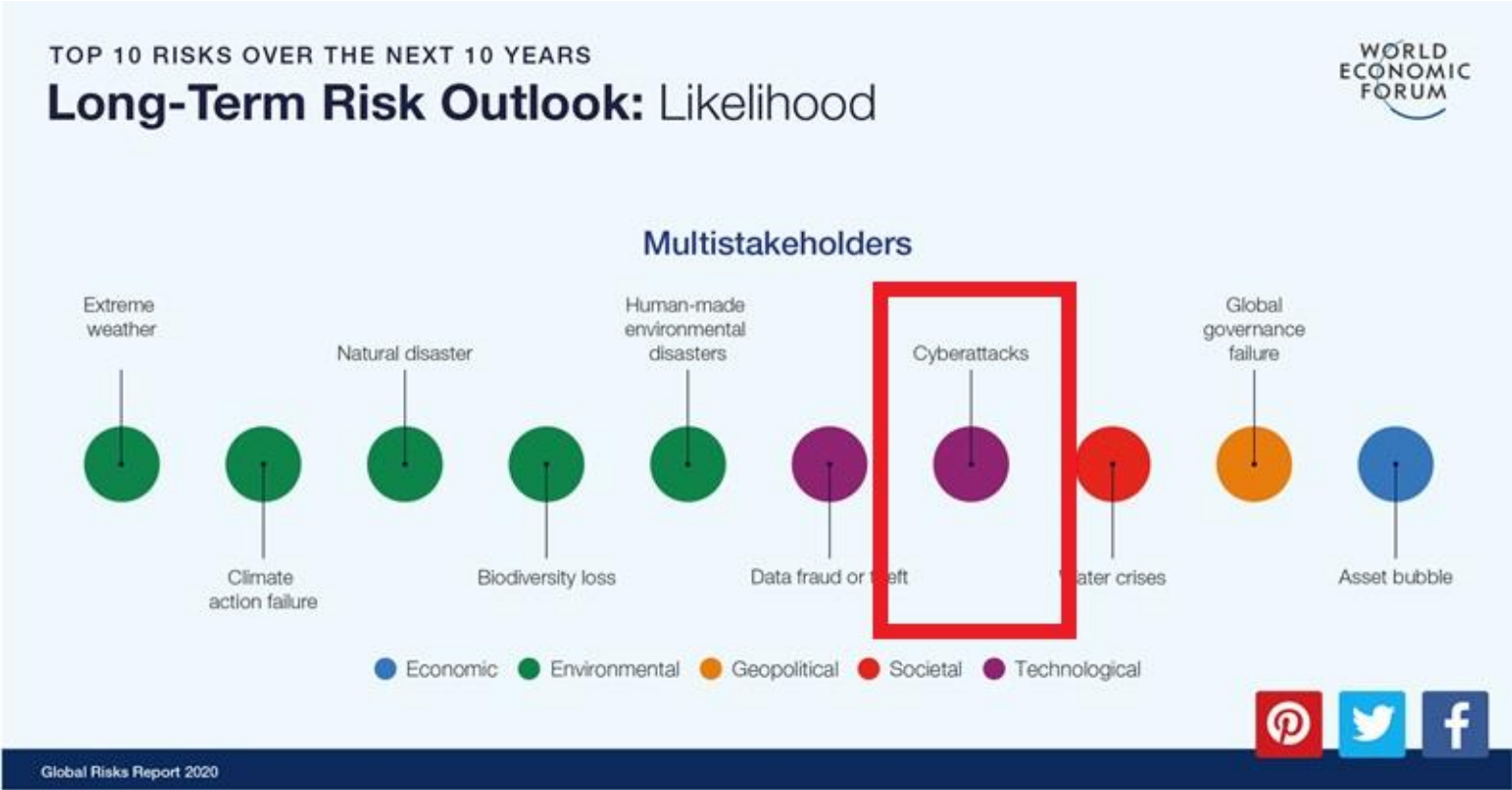
Содержание

Ландшафт угроз 2020

Прогнозы на 2021

Что такое KICS и как с его помощью можно контролировать удаленный доступ?

Kaspersky ICS CERT - чем мы можем помочь?



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)

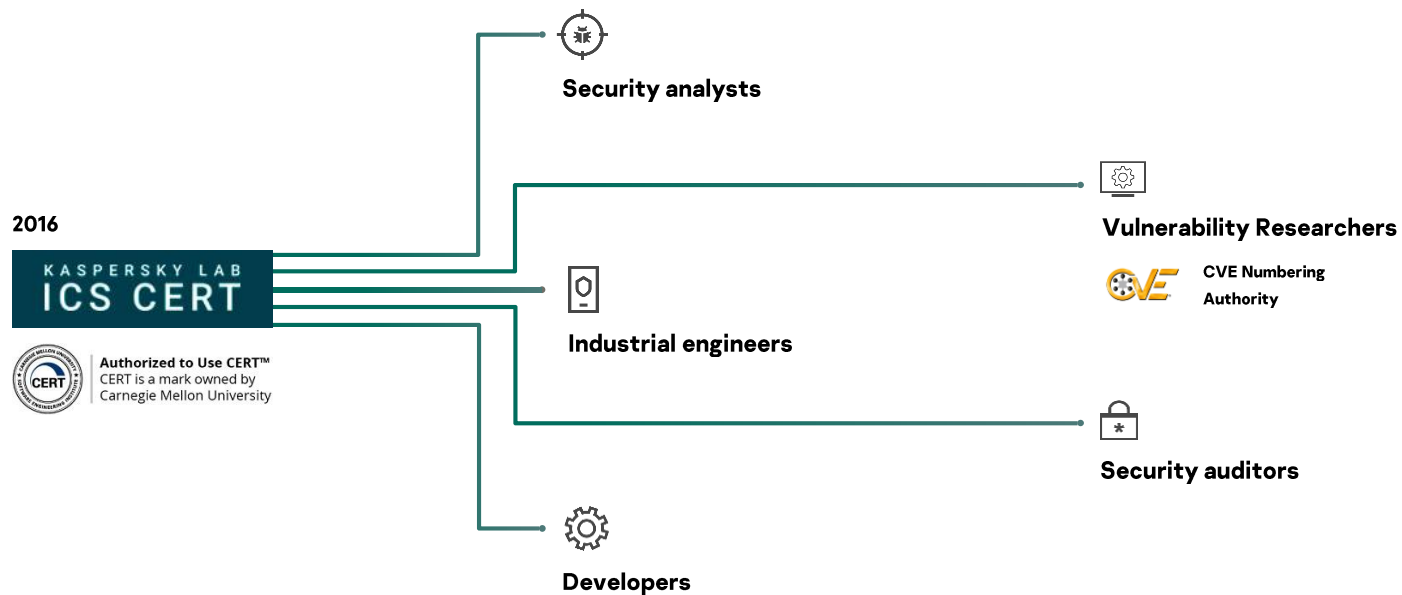
Обнаружили несколько сотен уязвимостей
«нулевого дня» в компонентах АСУ ТП и IIoT

Членство в международных организациях:



GLOBALPLATFORM[®]



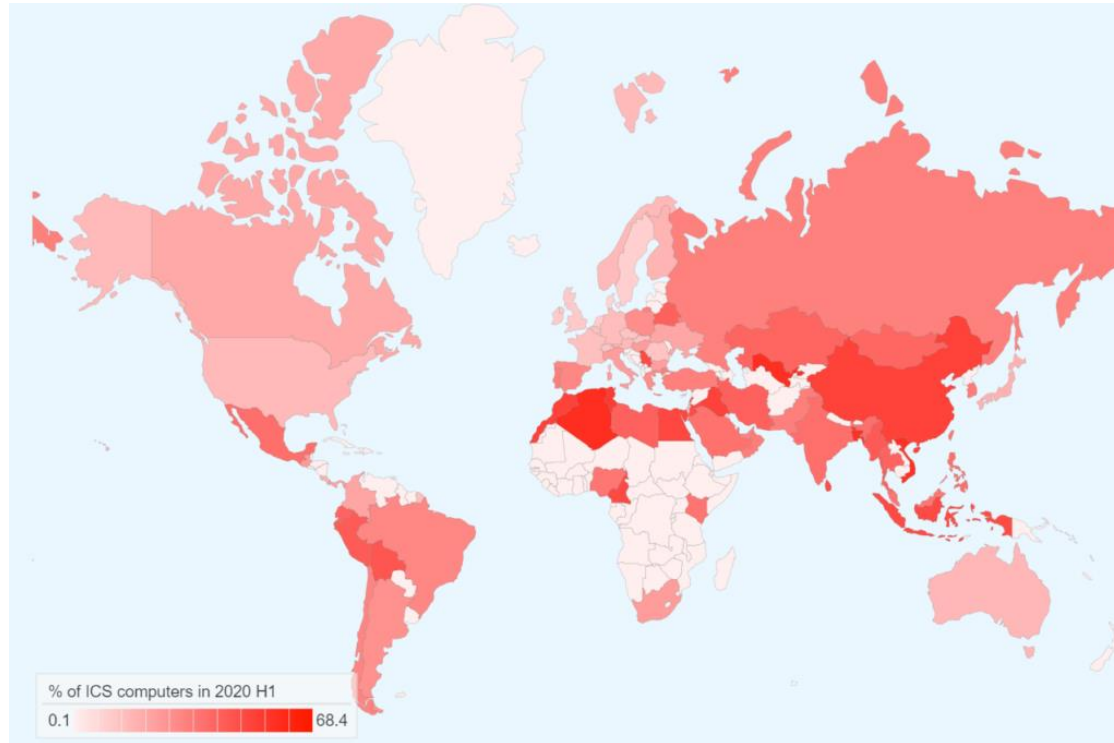


Источники данных

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

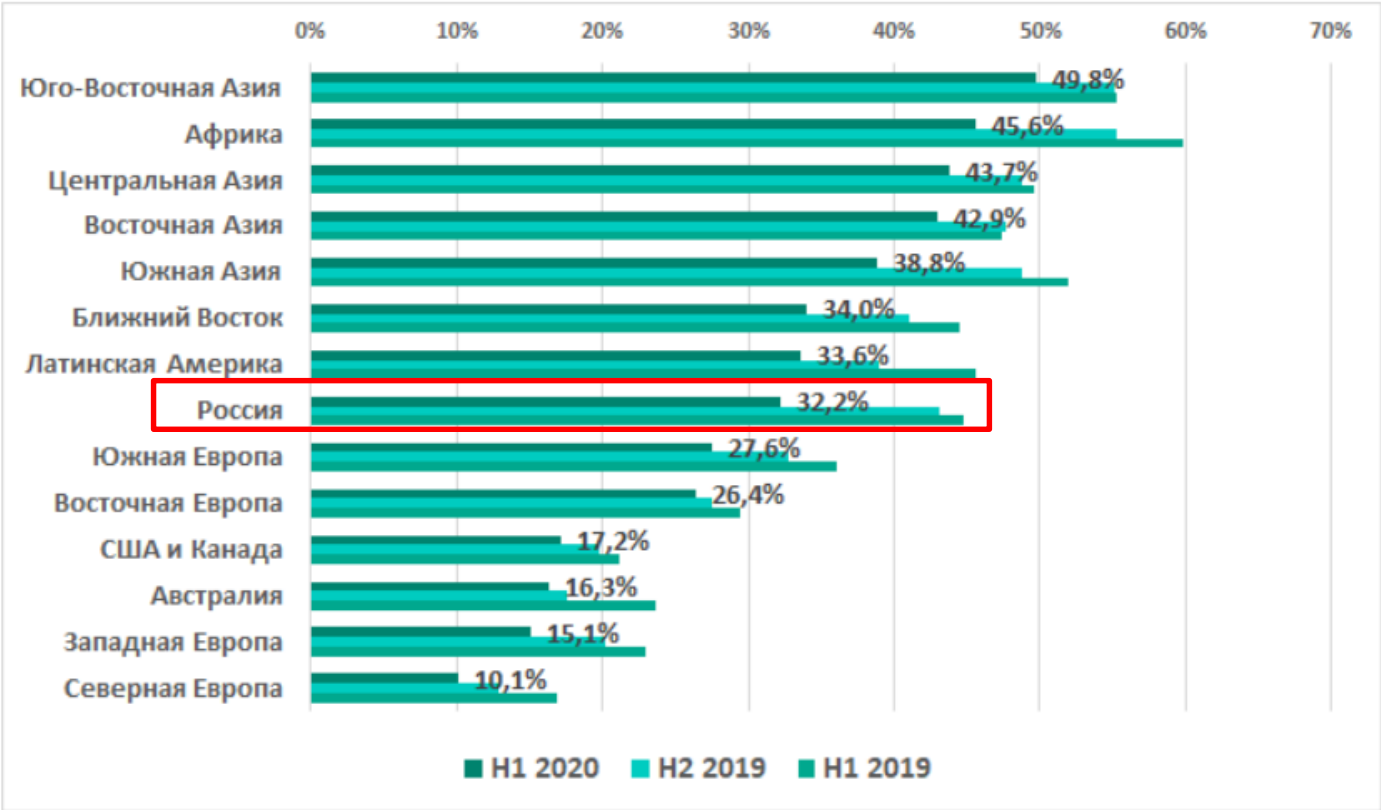
География атак* на системы промышленной автоматизации, 2020

6

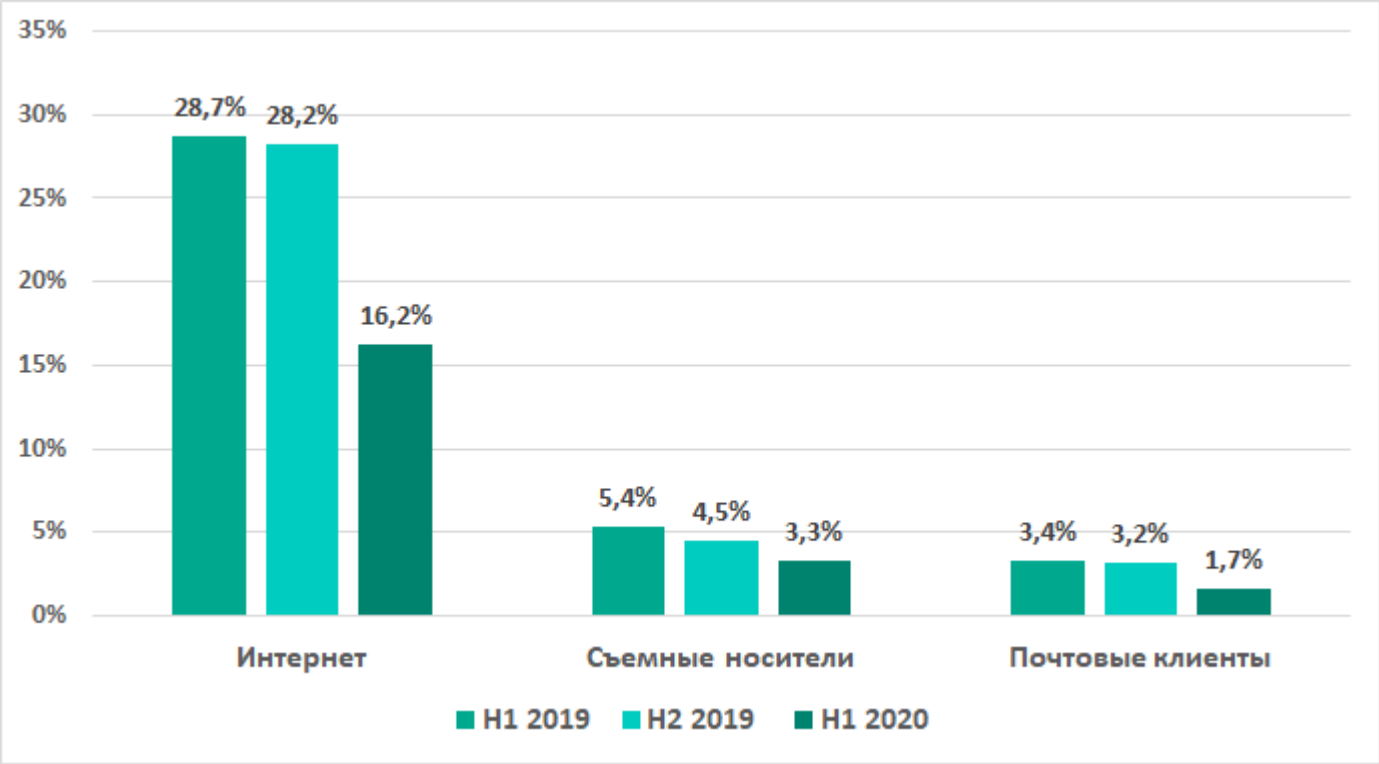


*процент компьютеров АСУ, на которых были заблокированы вредоносные объекты

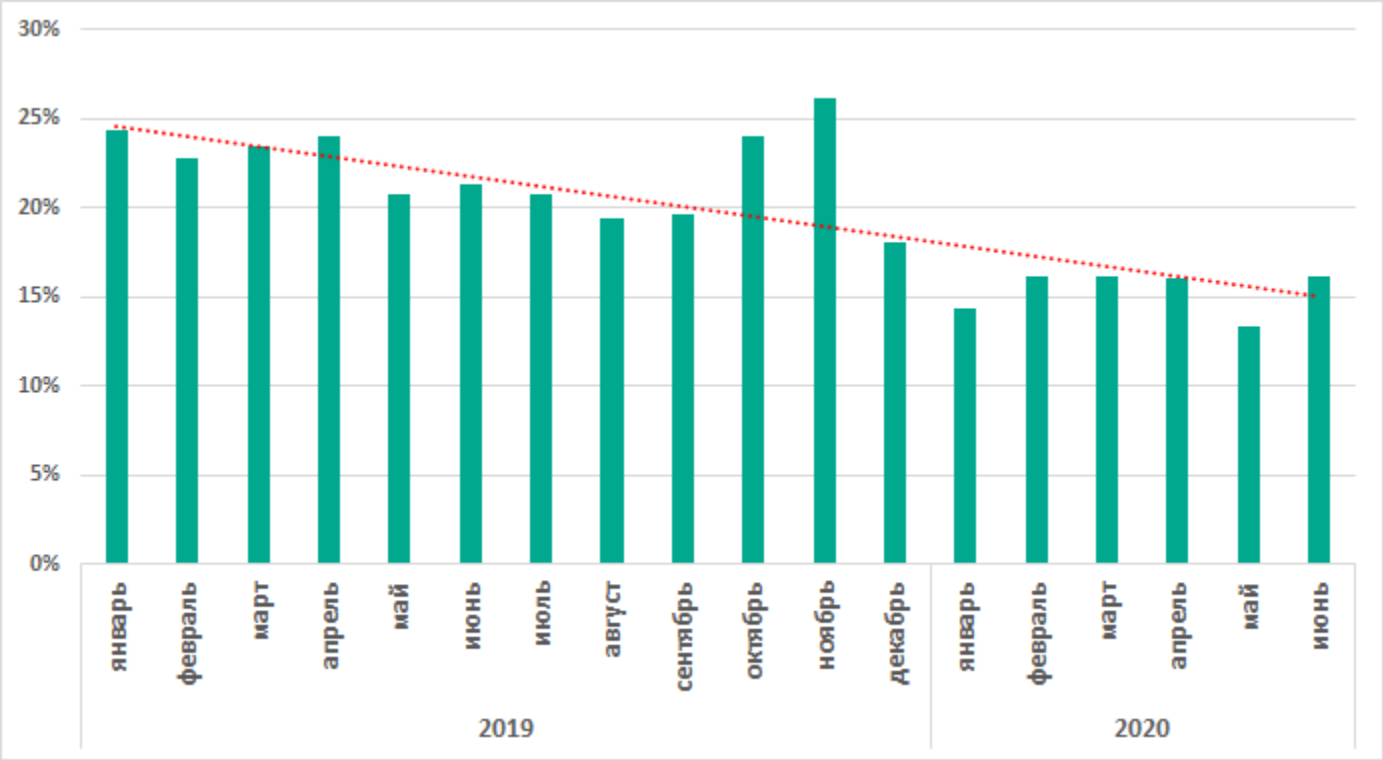
Рейтинг регионов по проценту компьютеров АСУ, на которых были заблокированы вредоносные объекты

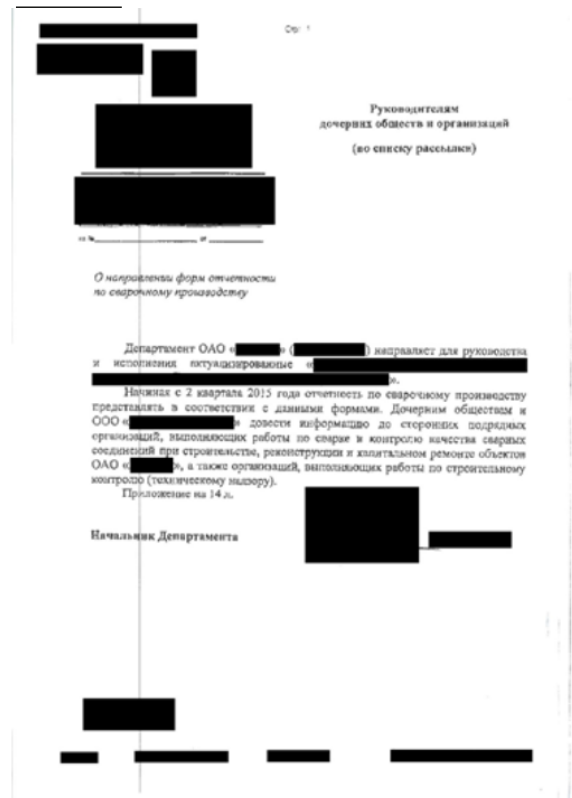


Основные источники угроз

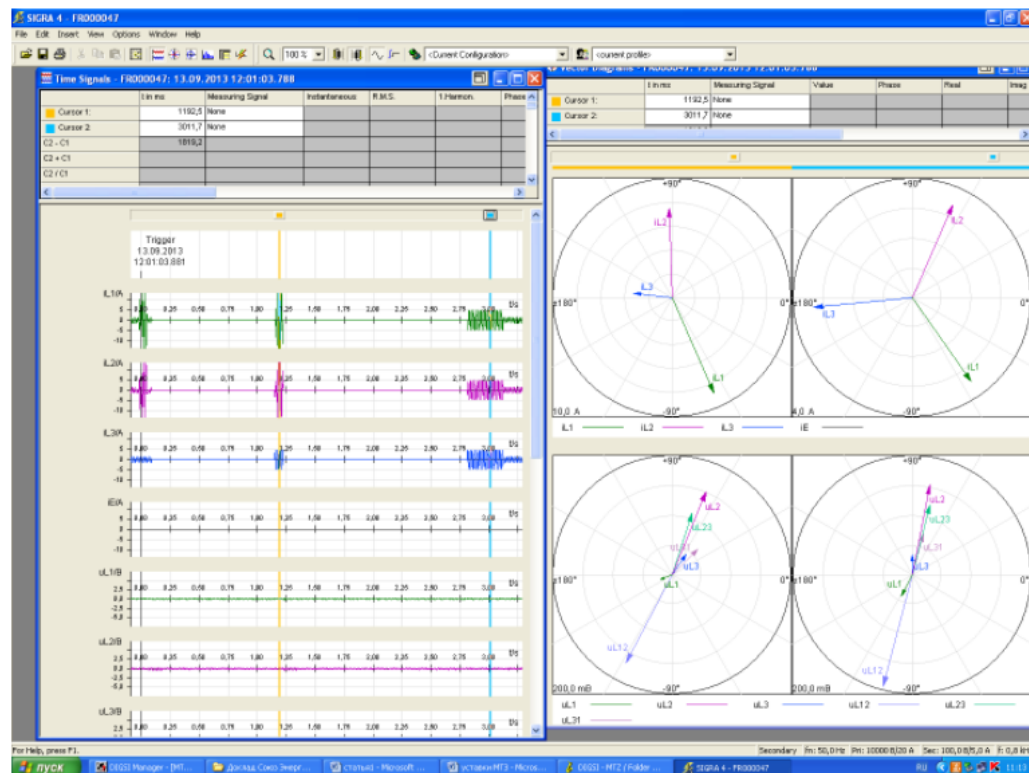


Процент компьютеров АСУ в России, на которых были заблокированы вредоносные объекты 9



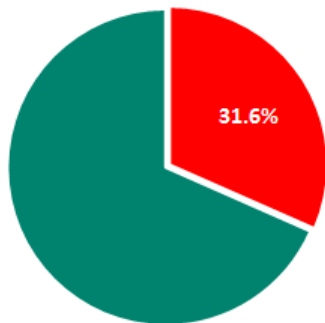


Пример PDF документа с распоряжением для дочерних предприятий, который использовали злоумышленники

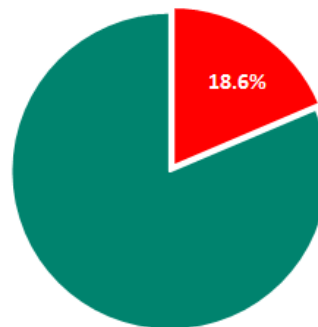


Скриншот векторных диаграмм с осциллограммами

Использование инструментов RAT в АСУ ТП по данным KSN

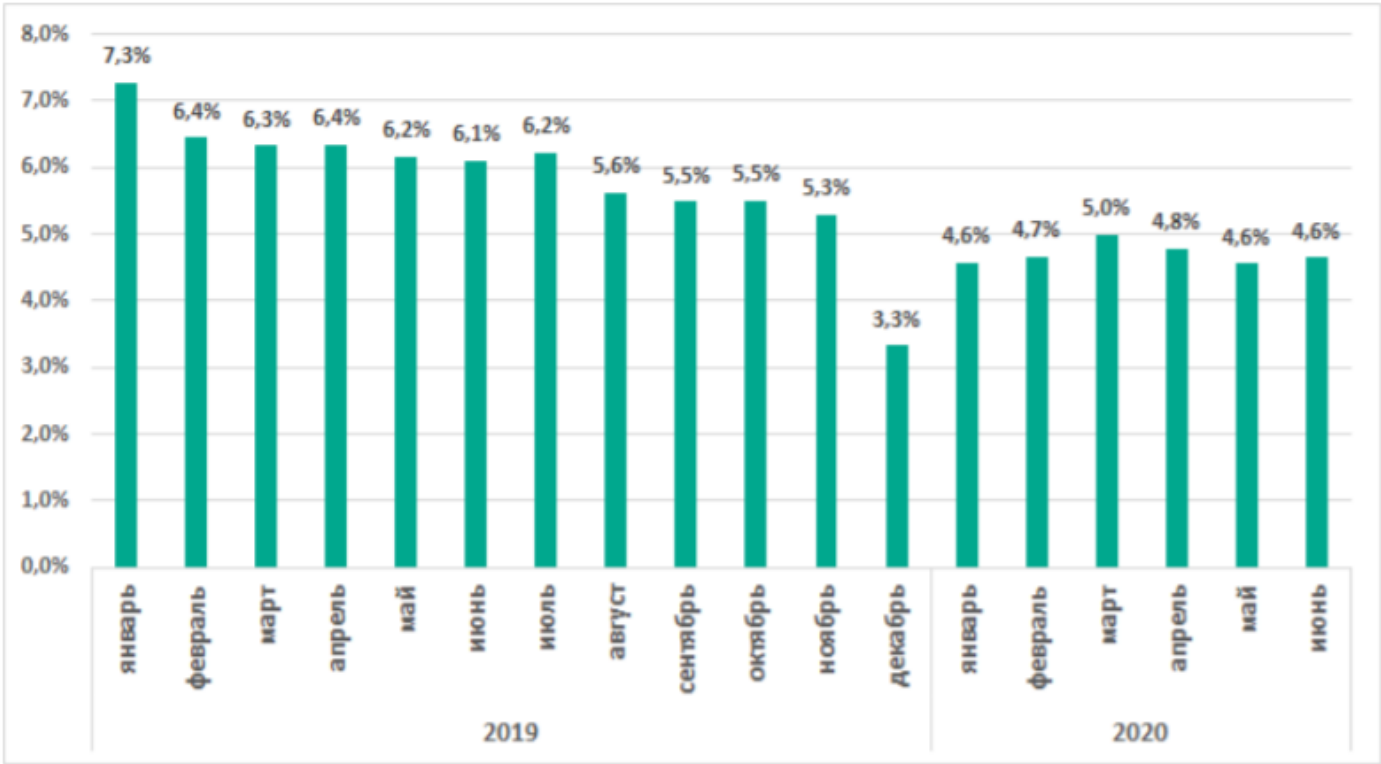


*Процент компьютеров АСУ, на которых
легитимно установлены RAT*



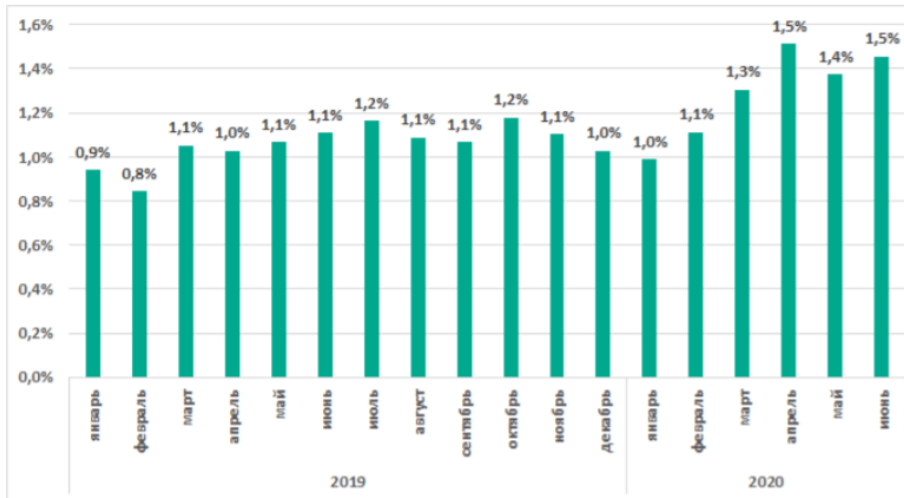
*Процент RAT, установленных вместе с
продуктами АСУ, среди всех обнаруженных
RAT на компьютерах АСУ*

Процент компьютеров АСУ, на которых использовался RAT

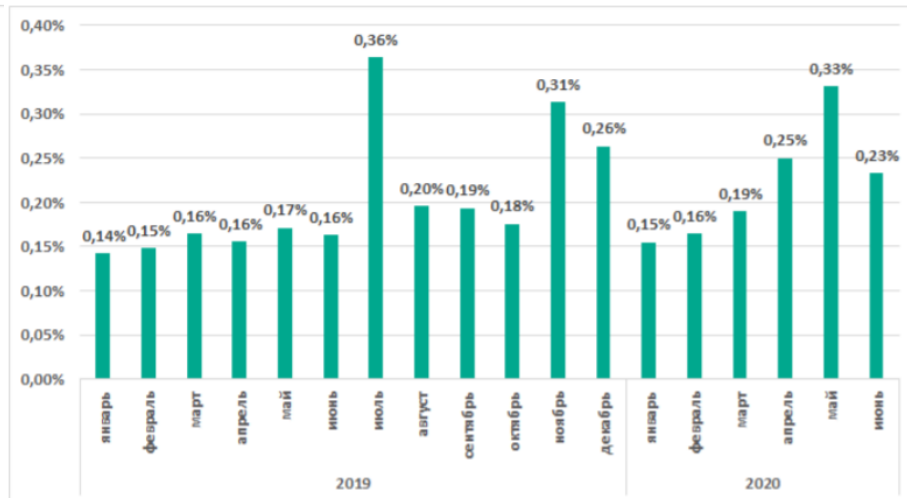


Ландшафт киберугроз для систем промышленной автоматизации 2020

13



Процент компьютеров АСУ, доступных по RDP



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

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

15

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 проведения 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.

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

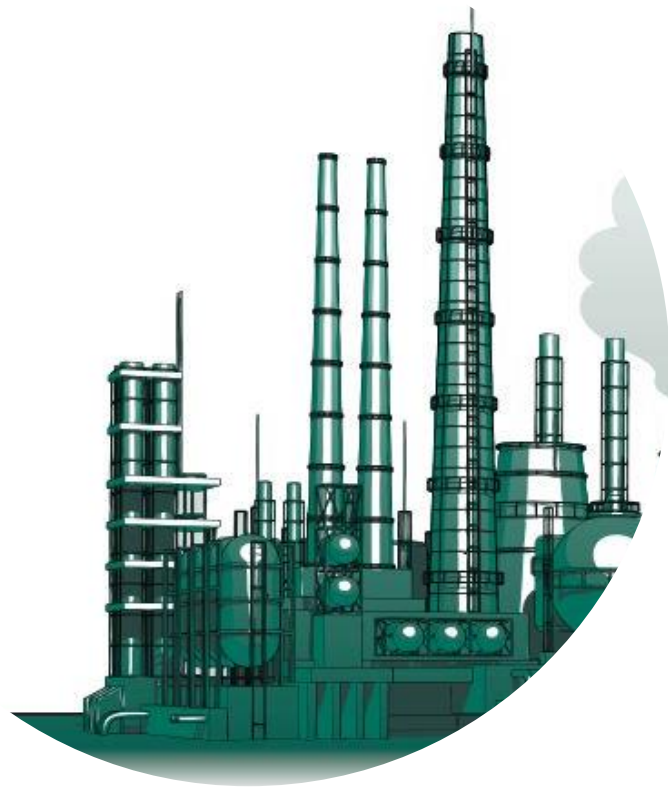
1. Число серьёзных инцидентов уменьшаться не будет.
2. Увеличение срока реакции на инцидент.
3. Увеличение масштаба распространения вредоносного ПО и усугубление последствий киберинцидентов.
4. Пополнение рядов хакеров, подкуп работников предприятий.
5. Новые кросс-платформенные атаки:

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

Прогноз. Случайные заражения и вымогательское ВПО

17

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.

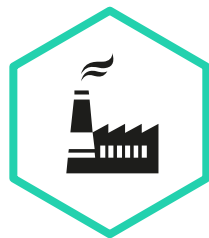




1. Активность группировок будет **коррелировать с локальными конфликтами**: кибератаки будут использоваться как инструмент военных действий наряду с беспилотниками и информационными атаками через СМИ.
2. Более **активные действия**, вероятность **продолжения серии** Stuxnet — Black Energy — Industroyer — Triton.
3. Проблемы с разграничением доступа в ОТ-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.

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

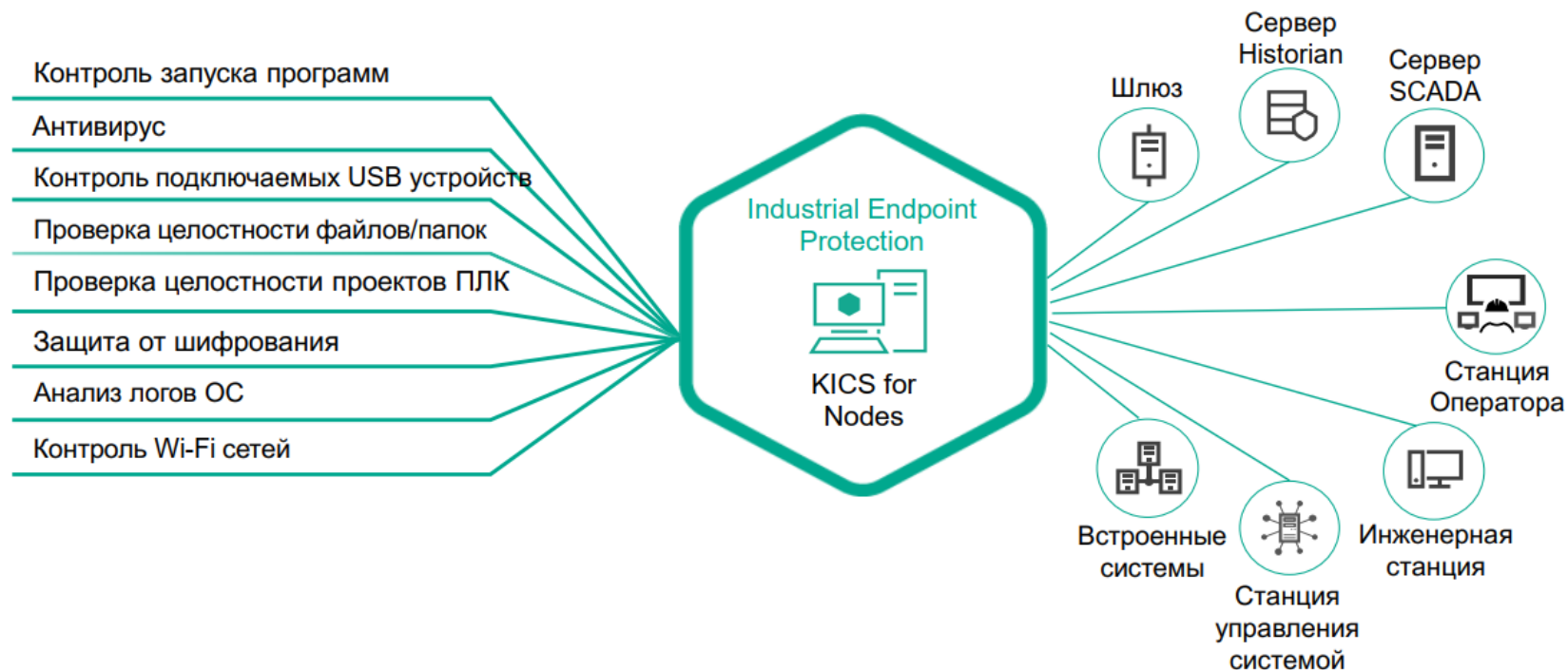
Централизованное
управление
безопасностью



Kaspersky
Security
Center

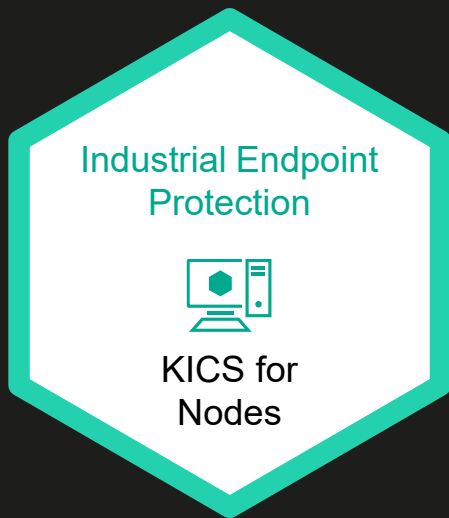
KICS for Nodes

21



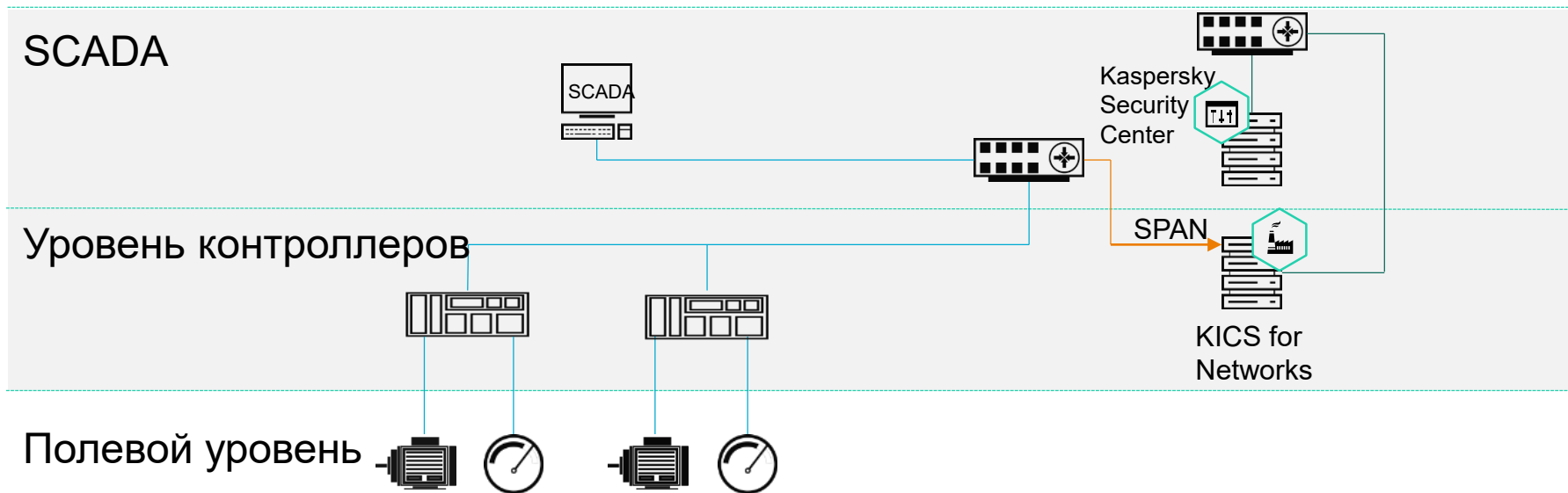


Почему нужно использовать KICS вместо корпоративного антивируса для защиты АСУ ТП?



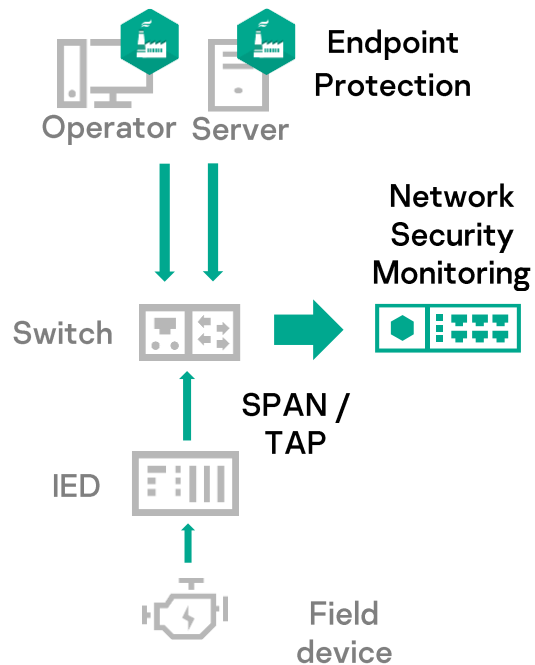
- Уменьшено потребление ресурсов
512 MB Оперативной памяти для Windows XP SP2 / XP Embedded
- Установка / Обновление / Удаление без перезагрузки
- Возможность работы в полностью неблокирующем режиме
- Возможность обнаружения угроз нулевого дня (в том числе в неблокирующем режиме)
Контроль запуска приложений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

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



KICS for Networks

24



- 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**

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

26



SIEMENS



EMERSON

ЭКРА



Ресурсы

Истории успеха **Сертификаты совместимости** Обзор решения

Развитие безопасных сред требует совместных усилий. Именно поэтому «Лаборатория Касперского» все больше взаимодействует с производителями систем промышленной автоматизации. Мы предлагаем наши тесты на сертификацию и интероперабельность, готовим модели возможного взаимодействия, а также интегрируем наши продукты и решения.

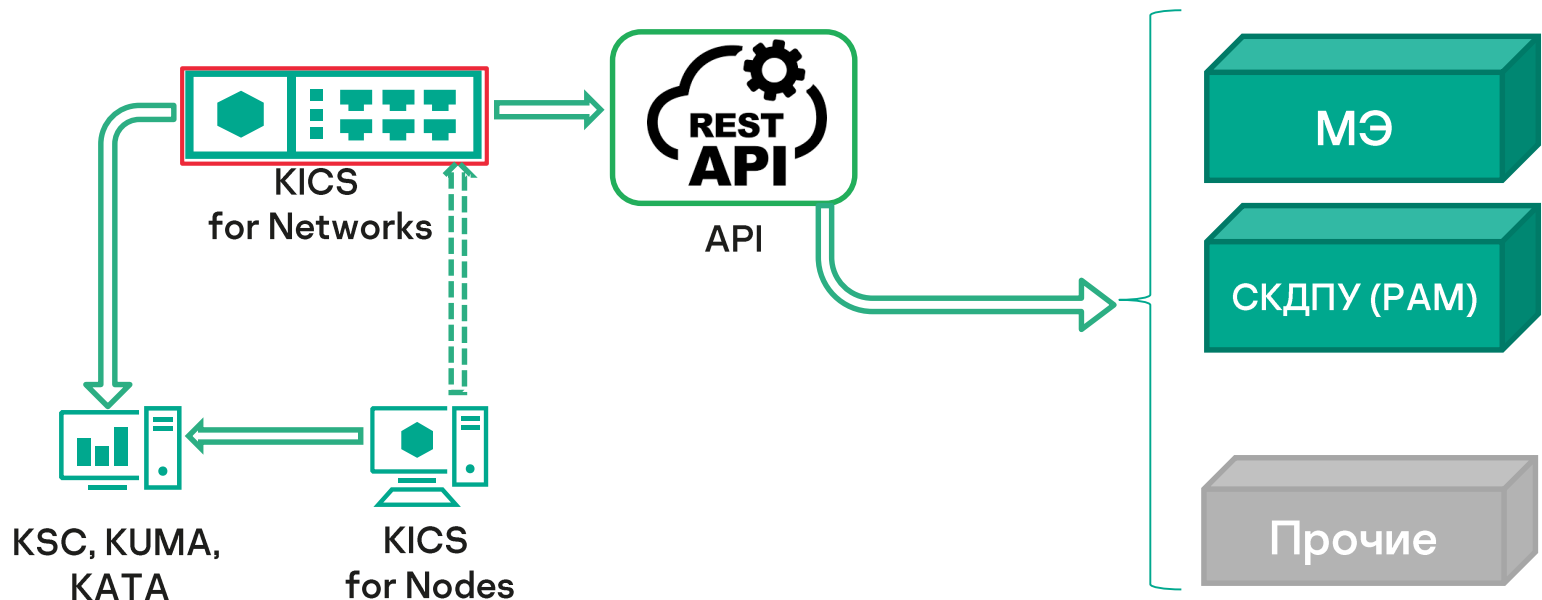
«Лаборатория Касперского» предлагает надежные и проверенные инструменты, которые помогают построить защищенную и гибкую промышленную среду. Наша экспертиза позволяет производителям встраивать передовое защитное решение, полностью соответствующее с требованиями и рекомендациями регуляторов. Результат этого – интегрированное решение, которое полезно не только для защиты конечных пользователей, но и для каждого участника цепи поставок.

- 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
- Statement of compatibility with WinCC Open Architecture 3.16 P006 from ETM professional control GmbH, A Siemens Company
- Акт проверки совместимости с UniSCADA от ООО «Ренатамат»

certification

Как с помощью KICS контролировать удаленный доступ?

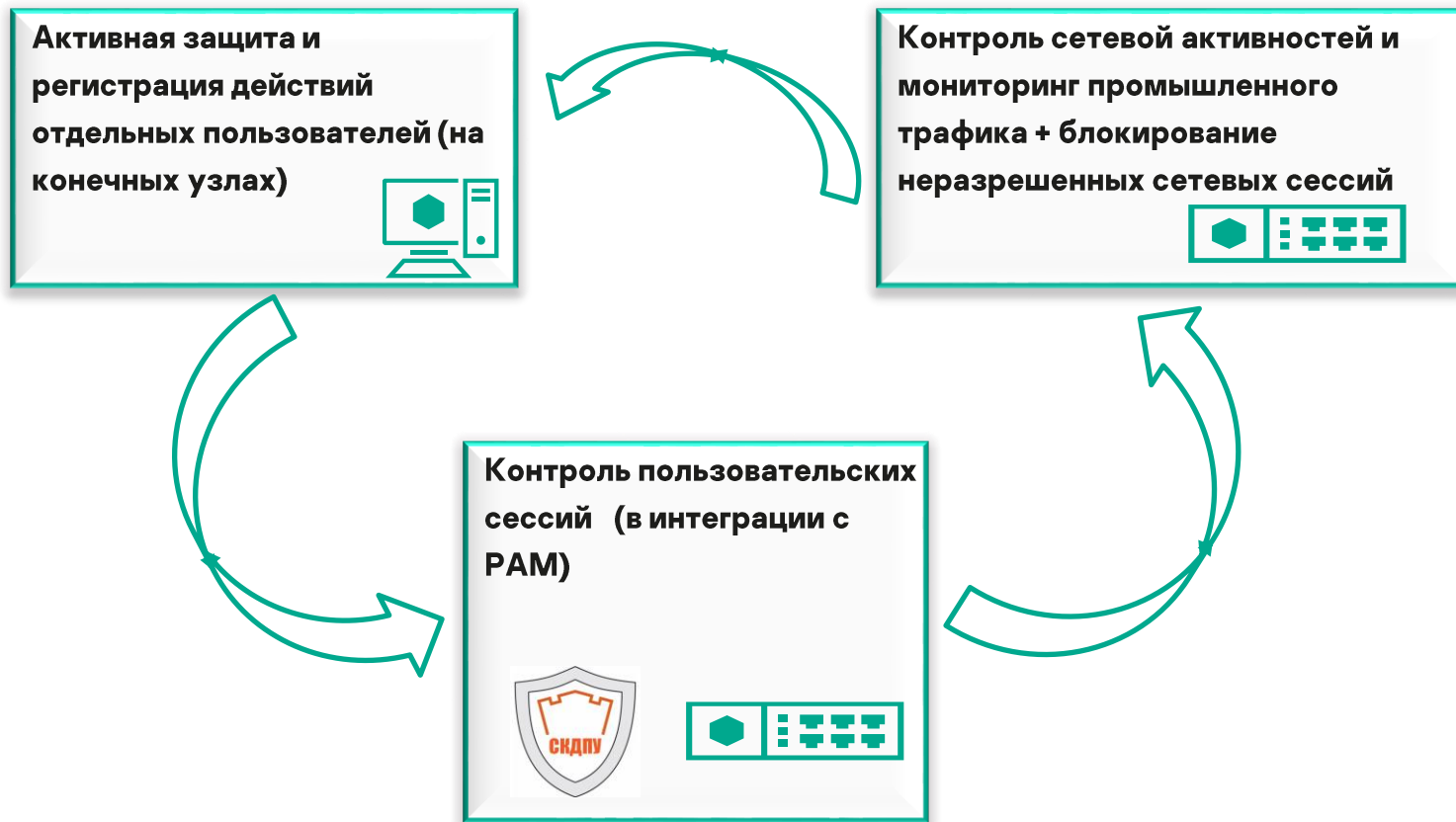
27



KICS позволяет создавать интегрированную экосистему средств защиты информации АСУ ТП

Сценарии защиты удаленного доступа

28





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

События

Настроить таблицу

Обновление таблицы

Важность

Технологии

Период

🕒 ⚠️ 🚫

DPI NIC IDS CC EXT AM

Последние 24 часа

ID

Начало

Технология

Важность

Заголовок

☒	2085	17.04.2019 16:29:58.723	DPI	🚫	Нарушение правила контроля процесса: Уровень LT02_2 вне диапазона
☐	2084	17.04.2019 16:29:55.438	DPI		
☐	2083	17.04.2019 16:29:55.300	DPI		
☐	2082	17.04.2019 16:21:59.443	EXT		

🚫

Нарушение правила контроля процесса:
Уровень LT02_2 вне диапазона

Критические

17.04.2019 16:29:58.723

Описание

Нарушение правила контроля процесса: Уровень LT02_2 вне диапазона. Значения тегов: tag CentumVP-192.168.2.12.LT02_2.PV - значение 7101.42.

Application state:
No problems detected

Total uptime:
00:46:35

Effective uptime:
00:46:35

Since first start:
00:46:35

Tag name	Value	ID	Description
Siemens SIMATIC S7-300.Inte...	0	28	If disabled, the billet falls down off the rota
Siemens SIMATIC S7-300.Item...	184	44	Total items manufactured
Siemens SIMATIC S7-300.Drill...	3	40	Time for tool drive in seconds
Siemens SIMATIC S7-300.start	1	41	marker to start
Siemens SIMATIC S7-300.stop	0	42	marker to stop

STOP PLC command detected

Critical

2020-02-10 16:33:16.938

ID

Status

Technology

Last seen

Total appearances

Monitoring point

Event type

Origin

8251

New

CC (Command Control)

2020-02-10 16:33:16.938

1

mpoint1

4000002602

System

Protocol

Ethernet II / IP / TCP / ISO TSAP / ISO 8073 / Siemens S7comm

Source

IP address

Port number

MAC address

192.168.0.250

2073

8 cab8 00 c9 e6

Destination

IP address

Port number

MAC address

Rack/Slot address

192.168.0.2

102

28 63 36 48 b6 82

2/0

Description

STOP PLC command detected.

Possible reasons:

- Hacker activities and attempts to tamper with the industrial process.

- Authorized change in the industrial process.

- Reconfiguration of the network.

Possible effects:

- Disconnection of assets.

- Reconfiguration of assets.

- Change of industrial process parameters.

Threat elimination measures:

- Identify the event originator based on the address information (IP address, MAC address) and disconnect it from the network if it is an unauthorized connection or does not match the required functions.

- Check the operation of network equipment and information security tools and change their settings if necessary.

- If an event was registered as a result of equipment replacement and the new equipment is permitted for use, create a Network Control rule to allow this system command.

PROCESS_INTERLOCK_DISABLED at tag Siemens SIMATIC S7-300.Interlock - value -1

Critical

2020-02-10 16:34:00.490

ID

Status

Technology

Triggered rule

Last seen

Total appearances

Monitoring point

Event type

Origin

6249

New

DPI (Deep Packet Inspection)

Process_Interlock_Disabled

2020-02-10 16:34:00.490

1

mpoint1

4

User

Protocol

Ethernet II / IP / TCP / ISO TSAP / ISO 8073 / Siemens S7comm

Source

IP address

Port number

MAC address

192.168.0.250

2073

8 cab8 00 c9 e6

Destination

IP address

Port number

MAC address

Rack/Slot address

192.168.0.2

102

28 63 36 48 b6 82

2/0

Description

The process critical interlock has been disabled tag Siemens SIMATIC S7-300.Interlock - value -1 at the. The changes were made from MAC address 8 cab8 00 c9 e6, IP address 192.168.0.250, Port number: 2073, using Ethernet II / IP / TCP / ISO TSAP / ISO 8073 / Siemens S7comm

Caution!!!

Kaspersky

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

31

Важность

Технологии

Период

DPI

NIC

IDS

CC

EXT

AM

Задать период

От: 01.09.19 14:11:39 до: 24.10.2019 00:00:00

Начало

Заголовок

Важность

23.10.2019 00:10:30

Обнаружена команда (BIND INTERFACE)

25.10.2019 00:07:50

Обнаружена команда (BIND INTERFACE)

24.10.2019 22:31:50

Обнаружена команда (BIND INTERFACE)

24.10.2019 22:22:50

Обнаружена команда (BIND INTERFACE)

24.10.2019 20:32:50

Ошибка (REQUEST NOT FOUND)

24.10.2019 20:32:40

Сработало правило обнаружения вторжений из системног...

24.10.2019 20:31:30

Сработало правило обнаружения вторжений из системног...

24.10.2019 10:21:40

Сработало правило обнаружения вторжений из системног...

23.10.2019 13:38:50

Обнаружена команда (BIND INTERFACE)

23.10.2019 10:04:10

Сработало правило обнаружения вторжений из системног...

23.10.2019 06:39:50

Сработало правило обнаружения вторжений из системног...

23.10.2019 06:38:20

Сработало правило обнаружения вторжений из системног...

22.10.2019 09:45:40

Сработало правило обнаружения вторжений из системног...

Сработало правило обнаружения вторжений из системного набора правил: awp
Критические
24.10.2019 20:32:49.591 – 24.10.2019 20:32:49.591

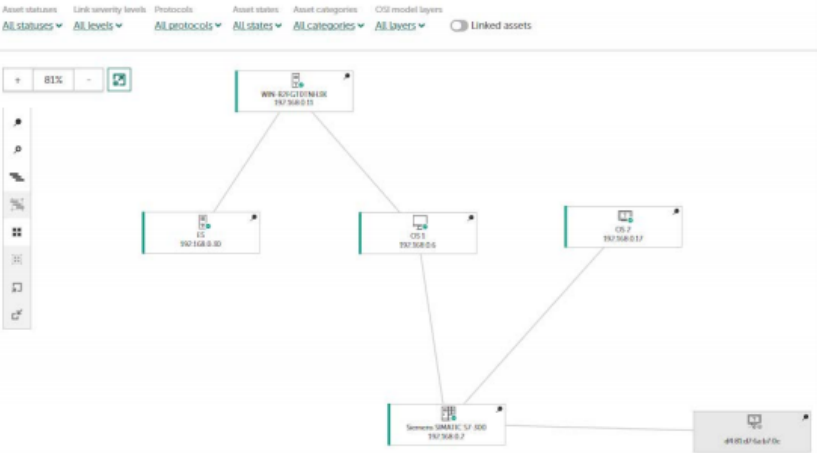
Описание
Сработало правило обнаружения вторжений из системного набора правил.
Класс: Signs of Trojan Activity.
Правило: Exploit.CVE-2010-0022.TCP.C&C.
Приоритет правила: 1
Набор правил: awp.

ID	19111
Статус	Новое
Технология	IDS IDS – Обнаружение вторжений

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

32

Ожидания



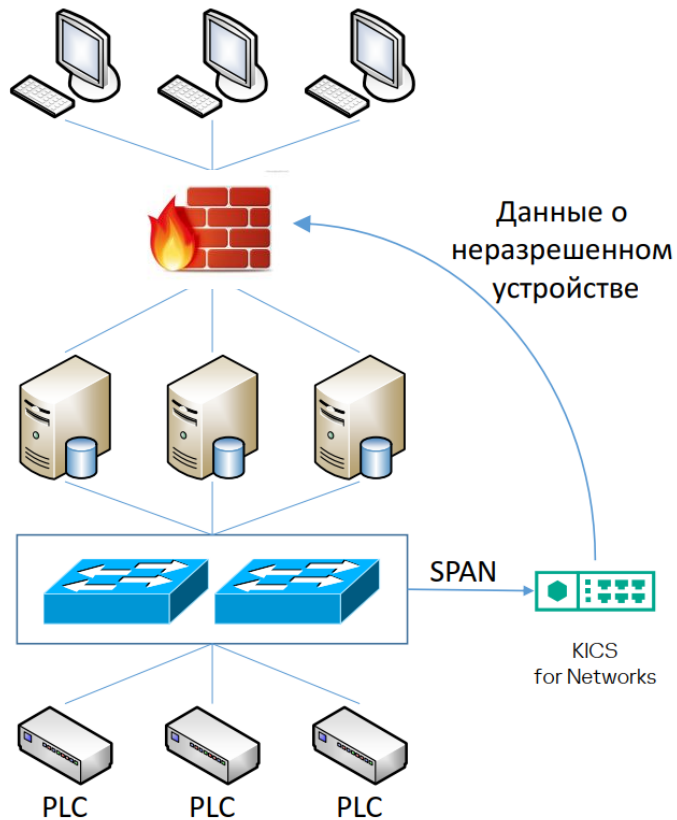
Реальность

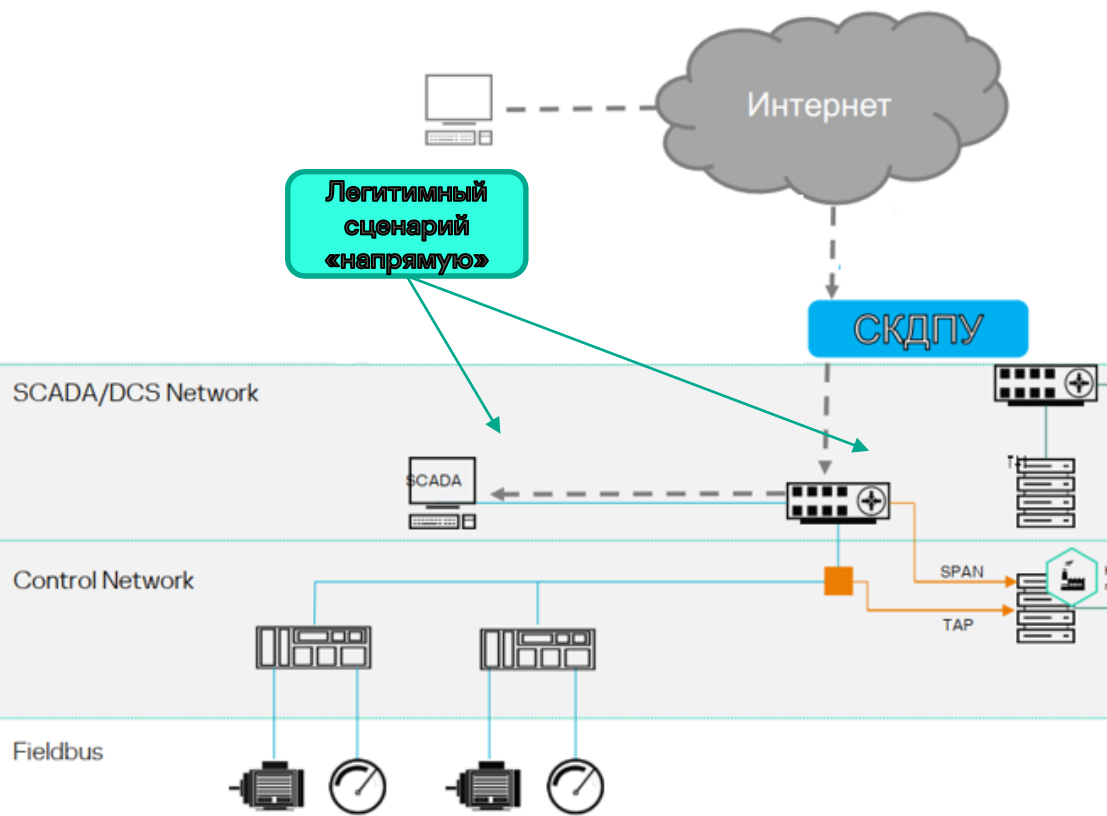
☐ Name	☐ Status	☐ Address information	☐ Category
☐ ES	Authorized	00:0c:29:27:0d:1f; 192.168.0.30	Server
☐ NB3	Authorized	f8:ca:b8:00:c9:e6; 192.168.0.250	Server
☐ OS 1	Authorized	00:0c:29:4a:1d:2c; 192.168.0.6	Server
☐ OS 2	Authorized	192.168.0.17	Other
☐ OS 3	Authorized	00:0c:29:6c:0b:ba; 192.168.0.21	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

33





Инциденты DL-1000192

Назначить мнеНазначить...Закрыть (отработано)3

Редактировать

<>

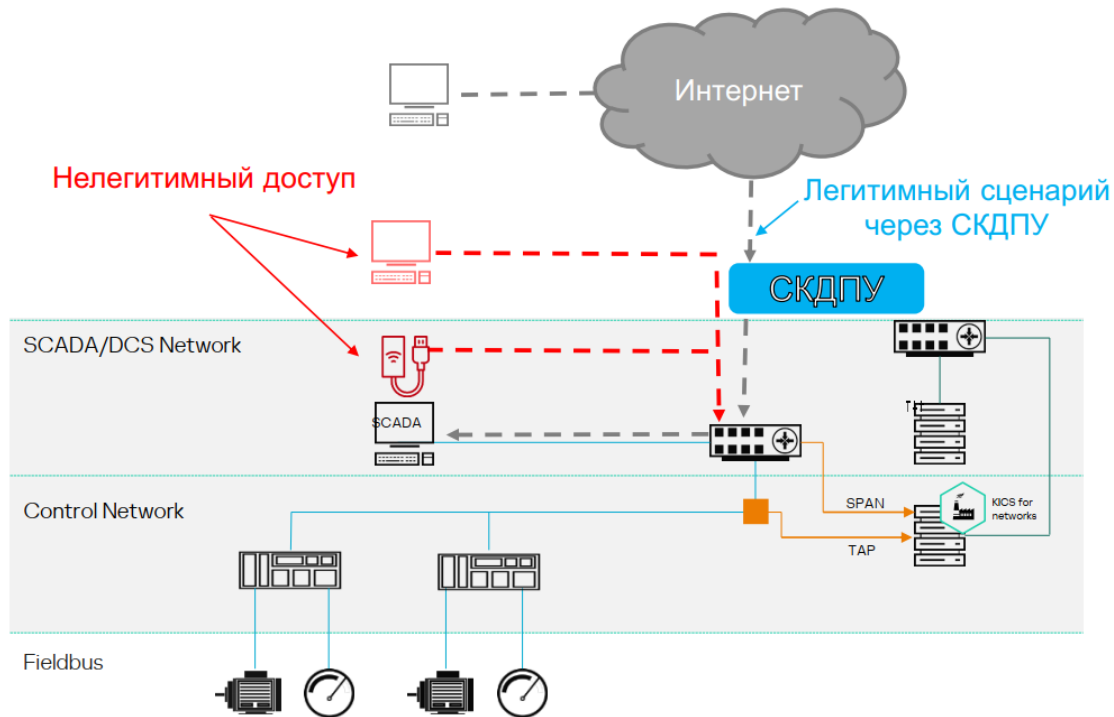
ID	DL-1000192		
Дата регистрации	2020-08-13 16:16:54		
Тип	DIRECT_LOGIN		
Уровень	Высокий		
Статус	Новые		
Назначен	Нет владельца		
Данные	Remote TCP connection from: 172.16.30.63:58349 to: 10.100.101.63:3389		

Подробности:

Дата и время записи	Тип события	Данные	
2020-08-13 16:16:37	DIRECT_LOGIN	src_mac:	64:d1:54:f1:65:fb
		dst_ip_port:	3389
		dst_ip_addr:	10.100.101.63
		src_ip_addr:	172.16.30.63
		ether_type:	1
			-

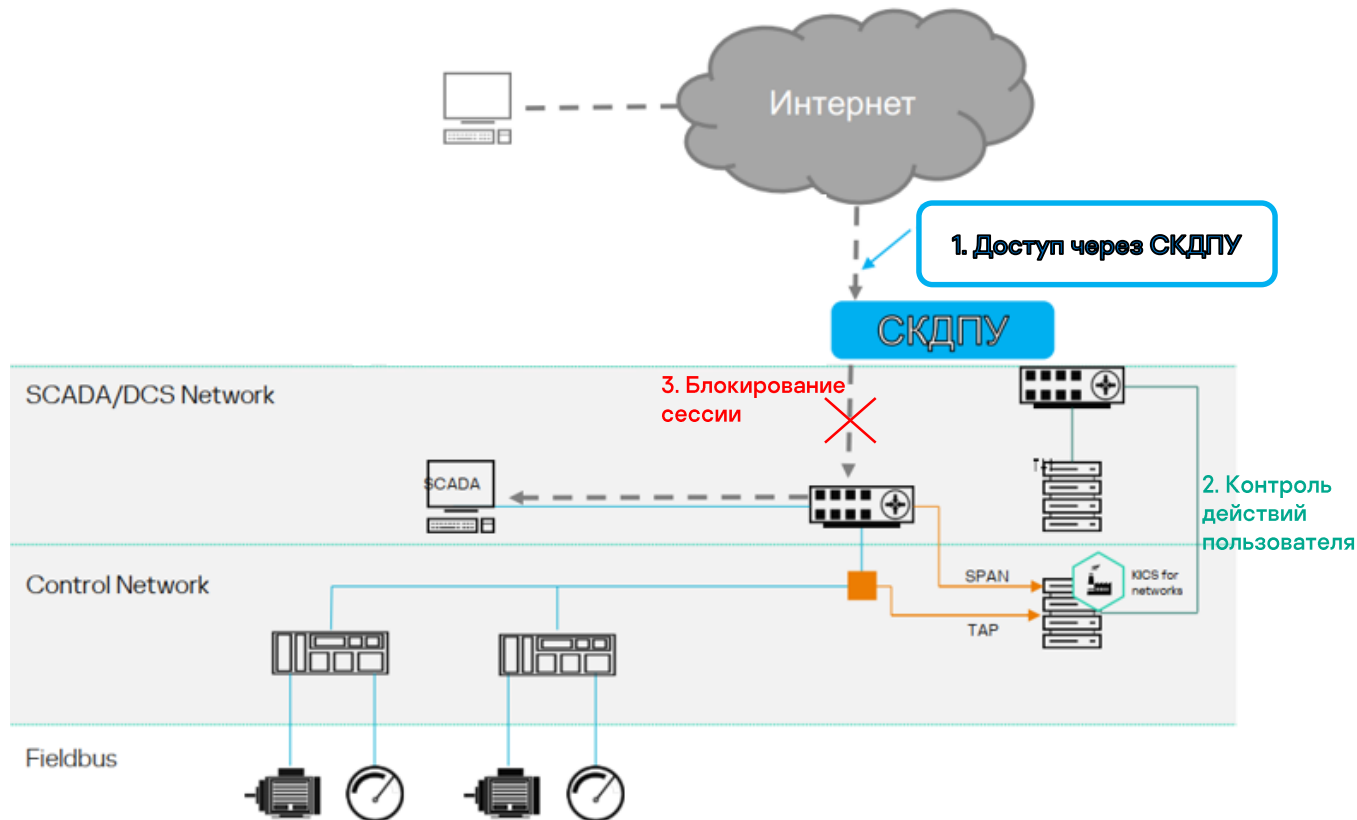
Сценарии защиты удаленного доступа. Контроль пользовательских сессий. Интеграция с СКДПУ. Удаленное подключение

35



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

36



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