kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Игорь Рыжов

Заместитель директора Центра промышленной безопасности, АО НИП «Информзащита», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Информзащита
Системный интегратор

Проекты по защите АСУ ТП

вчера, сегодня, завтра

www.infosec.ru

Группа компаний «Информзащита»

АО НИП «Информзащита»

Специализируется в
обеспечения безопасности информационных систем

25 лет

является **лидером**
российского рынка ИБ

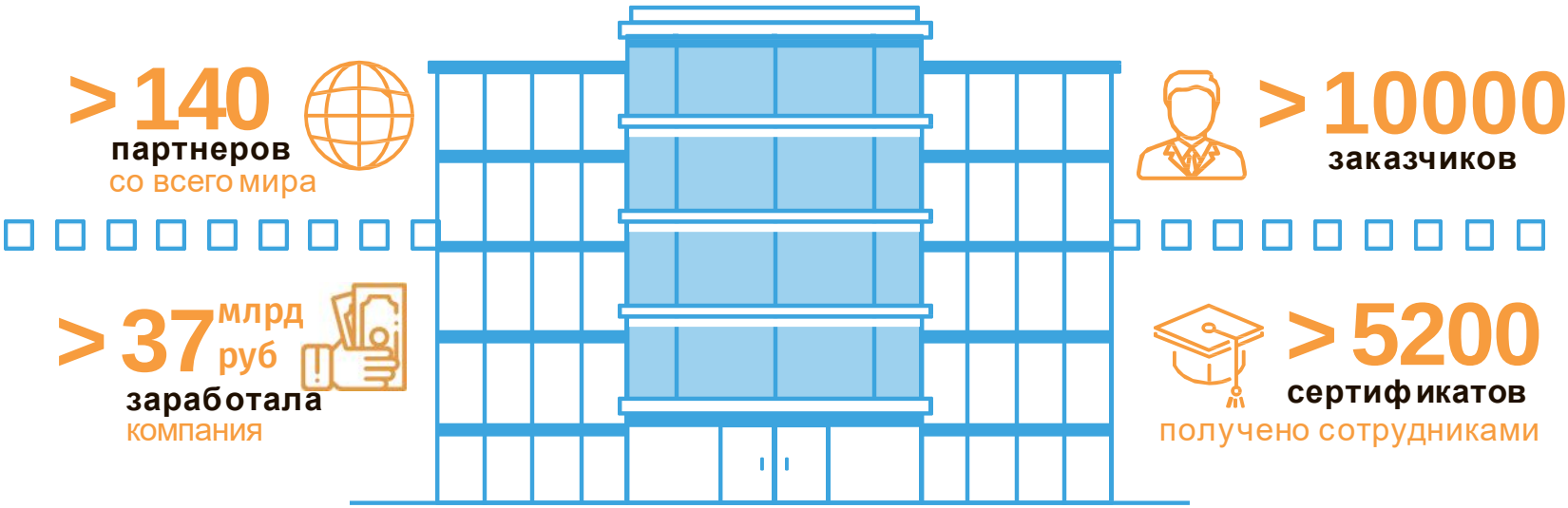
«Информзащита»

За 25 лет

25 лет на рынке ИБ

ТОП-3 российских ИБ-компаний
с 2002 года

лидер
среди российских
интеграторов в сфере ИБ



> 140
партнеров
со всего мира

> 10000
заказчиков

> 37 млрд руб
заработала
компания

> 5200
сертификатов
получено сотрудниками

«Информзащита»

Центры компетенций

«Информзащита»

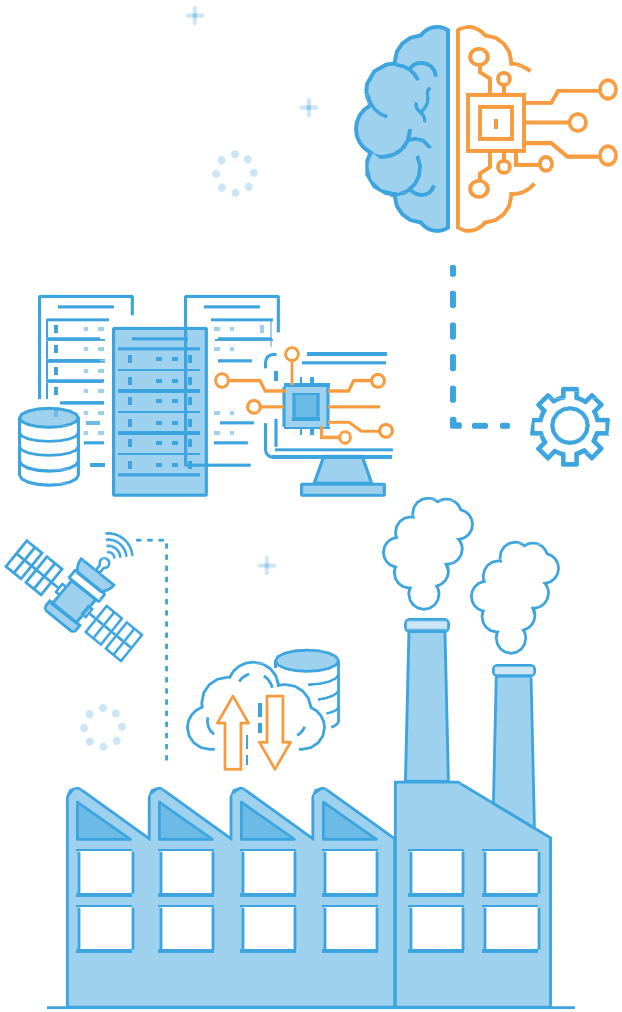
Центр промышленной безопасности

Эксперты с комплексными компетенциями компетенциями в области кибербезопасности, операционных (АСУ ТП) и информационных технологий, функциональной безопасности (ОТиПБ), опытом аудитов и категорирования по 187 ФЗ.

Реализация сложных проектов по защите объектов КИИ, включающих как построение сетей сбора данных, так и настройку продуктов информационной безопасности.

Более 40 отдельных видов работ, а также участие в НИОКР в интересах ФСТЭК, ФСК и других ведомств с целью повышения уровня защищенности промышленных систем и АСУ.

Внедрение решений по информационной безопасности открытого и режимного сегментов сети для обеспечения взаимодействия и стабильности работы сервисов на предприятиях и в организациях.



Обсуждаемые вопросы

- Основные уроки текущих и завершенных проектов по категорированию, проектированию и внедрению комплексных систем информационной безопасности (ИБ) значимых объектов КИИ и не только.
- Развертывание продуктов KICS for Networks, KICS for Nodes в составе перечня средств защиты. Возникавшие проблемы при внедрениях в технологических сетях предприятий, как они были преодолены на конкретных случаях, обобщенные выводы и рекомендации.
- Как построить эффективную ИБ конфигурацию в сложных технологических и организационно-штатных системах реального предприятия. О чем говорят производственники, когда обсуждают с нашими специалистами вопросы ИБ и отказоустойчивость технологических процессов.
- Особенности различных секторов экономики РФ при проектировании ИБ решений.
- Как проекты цифровизации влияют и будут влиять на уровень защищенности технологических сетей. Интернет вещей и 5G сети в промышленности.
- Что в перспективе 2-3 лет придется менять в концепциях защиты АСУ ТП.

Уроки: чем примечателен прошедший год

Информзащита
Системный интегратор

Вопросы года: Как провести инвентаризацию в сетях АСУ ТП? Можно ли применить иностранное решение? в КИИ? Кто «подпишется» за совместимость СЗИ и зарубежного производителя системы АСУ ТП?

- Обследования сетей АСУ ТП. Что важно? Где граница, чья сеть?

- Удаленка, обеспечение доступа. Сеть АСУ ТП изолирована?



Вымогательство – это не только шифровальщики.

«Усредненный» проект ИБ и КИИ :

- Антивирусная защита, впереди EDR
- Сегментирование сетей, микросегментирование, шаблон сегмента
- Межсетевое экранирование, создание DMZ для тех сегмента
- Система обнаружения вторжений, система инвентаризации
- Контроль привилегированных учетных записей, что мешает централизации
- Двухфакторная аутентификация, хорошо бы единая
- Создание центра управления событиями безопасности (SIEM).

Важны детали: Техно-рабочий проект или эскизный проекты – все смешалось из-за требований по ускорению внедрений. Реновации АСУ ТП – реалии производственных площадок.

Мнения в процессе проектирования и внедрения меняют все – Заказчик, Производитель, Подрядчик. Бизнес. Это выливается в корректировки решений. Управление изменениями – постоянная работа всей команды внедрения, РП и АП. Точки контроля во времени. SCAD.

Мир АСУ ТП намного больше чем кажется

Информзащита
Системный интегратор

Разные годы ввода объектов в эксплуатацию

- инвестиционные проекты
- унаследованные системы
- активно модернизируемые системы
- системы без поддержки и без перспектив развития

Разные архитектуры построения технологических сетей

- объединенные сети АСУ ТП, спасибо диспетчеризации
- локальные АСУ ТП, не имеющие сетевых соединений, это надо увидеть глазами
- ПАЗ агрегата зачастую расположен рядом с АСУ ТП агрегата и напрямую связан с ней.

Что влияет на ИБ АСУ ТП

Различия в функциональности оборудования различных производителей

- поддержка зеркалирования трафика, «открытость» Интернета
- пилоты по цифровым двойникам
- связь с облаками производителя
- собственные системы самодиагностики и блокировки

Разные БД угроз, организация обновлений, собственные концепции ИБ

- собственные решения и концепты партнерских решений по АВЗ, МСЭ, УД, идентификации, шифрованию
- движение в ИБ и КБ
- совокупность фидов для СОВ АВЗ

Индустрия 4.0, СЗОКИИ, СБЗОКИИ, СОИБ, КСИБ, КСЗИ, ССАЦБ…

Информзащита
Системный интегратор

Тенденции в кибербезопасности для Индустрии 4.0 в РФ

Тенденции	Последствия
Стремительное увеличение доли интеллектуальных устройств в производстве, мобильные носимые устройства подключенные к ИС. Виртуальные инфраструктуры.	Больше элементов, подверженных киберугрозам. Сложнее мониторинг трафика.
Увеличение доли устройств подключенных к общим сетям связи и задействованных в операциях в корпоративной и технологической сети	Меньше изолированных систем, больше объектов для сетевых атак, больше векторов атак
Объединение отдельных АСУ ТП в технологические маршрутизируемые управляемые сети. Организация доступа для систем цифровой трансформации, подключение к облакам.	Повышение уровня возможного ущерба от компьютерного инцидента и рост числа и направления векторов атак. Повышение киберрисков за счет возможности управлять группами систем и агрегатов.
Интеграция промышленных систем (АСУ ТП) с системами управления производством (MES) и ERP, широкое применение систем диспетчеризации	Новые «вертикальные» векторы атак, больше точек сопряжения с внешними системами и сетями. MES несет в себе разнообразные функции – надо проверять.
Внедрение новых технологий связи в промышленности. 5GR, Wi-Fi 6.	Новые технологии – новые риски, уязвимости и возможности

Риски технического обслуживания и ремонта (ТОиР)

Информзащита
Системный интегратор

Риск	Краткое описание	Последствия	Типовые недостатки СВК – Системы Внутреннего Контроля	Чем поможет ИБ
Некорректный выбор стратегии ТОиР	Некорректное определение целесообразности выбора между ресурсной эксплуатацией и эксплуатацией по состоянию.	Рост общей стоимости владения оборудованием.	Принятие стратегии на основании мнения производственных подразделений без независимого подтверждения расчётов.	- Риск менеджмент - Атифрод как по бизнес транзакциям так и по контролю параметров телеметрии - IDS ка элемент контроля трафика и устройств - Видеоаналитика - DLP, UEBA - Защита удаленного доступа и связи с облаками
Завышение стоимости ремонтов	Внешние подрядчики: оплата работ проводится по актам, предоставляемым подрядчиком. Внутренние подрядчики: завышенное списание материалов на завышенные трудозатраты из-за отсутствия контроля со стороны подразделений-заказчиков.	Потеря денежных средств. Хищения ресурсов. Неэффективное использование персонала.	Неэффективная система бюджетирования (производственные подразделения не заинтересованы в контроле себестоимости, которая складывается, в т.ч. из внутренних заказов на ремонты).	
Недостижение эффективности ремонтов	Ремонты не достигают требуемого эффекта: например, после капитального ремонта внеплановый останов оборудования происходит через несколько месяцев.	Аварии. Срыв выполнения производственной программы. Рост общей стоимости владения оборудованием.	Отсутствие контроля при выполнении ремонтных работ (как внешними, так и внутренними подрядчиками).	
Фиктивное исполнение ремонтов	«Расписывание» (оформление первичной документации) ремонтов без фактического выполнения работ.	Аварии. Срыв выполнения производственной программы.	Оформление всей документации после окончания ремонта. Работающее оборудование (возможно, целый цех), по документам остановленное на ремонт.	
Некорректная отчетность о ТОиР и состоянии оборудования	Значительная часть объема ремонтов классифицируется как аварийные.	Принятие некорректных управленческих решений. Искажение финансовой отчетности.	Несвоевременное формирование и движение первичных документов по ремонту. Отсутствие классификации ремонтов.	

Категорирование и проектирование

Информзащита
Системный интегратор

Что предприятия категорируют и во что это выливается:

- Территориально и функционально выделенные объекты.
- Агрегаты и системы агрегатов, укрупнения, реальная опасность.
- MES, который сами написали и он реально является ядром управления производством – сложность реализации доступа.
- Локальную сеть, внутри которой находится всё – сложно формально соблюсти требования руководящих документов.
- Подали все АСУ ТП, которые сосчитали. Аналог – подали все системы – потому что они все важные.
- Инвестиционные проекты, новые объекты капитального строительства – мы только предполагаем категорию, но бюджетировать и проектировать надо сейчас.
- А можно перекатегорировать?

Внедрения СОВ

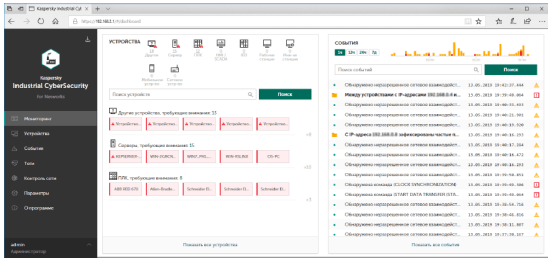
Информзащита
Системный интегратор

- Вне зависимости от категории КИИ всем интересно внедрить у себя в сегменте АСУ ТП свой СОВ.
- Специалисты АСУ ТП не работали раньше с системами зеркалирования трафика, отсутствие актуальной документации.
- Редкая технологическая сеть построена с непересекающейся IP адресацией.
- Технологические сети – какие ситуации типичны: автономны; есть кольцо для управления технологической сетью на оборудовании вендора АСУ ТП, есть план перестроить сеть АСУ ТП; технологическая сеть нового объекта уже спроектирована (про span никто задачу не ставил)
- обьемы хранения и загрузка аппаратных мощностей
- Трафик подан! Что мы в нем увидим.

Kaspersky Industrial CyberSecurity KICS for Networks

Информзащита
Системный интегратор

Решение для мониторинга и контроля в рамках промышленной сети в виде продукта, пассивно подключаемого к сети АСУ ТП:
Преимущества:
• **Обнаружение устройств -** пассивная идентификация и инвентаризация устройств в сети
• **Проверка пакетов -** анализ технологических процессов практически в режиме реального времени
• **Контроль целостности сетей -** обнаружение несанкционированных хостов и трафика в сети
• **Система обнаружения вторжений -** предупреждения о событиях ИБ
• **Контроль команд -** проверка команд, передаваемых по промышленным протоколам
• **Внешние системы -** интеграция через API-интерфейс со сторонними системами обнаружения



• ОС – заказчики волнуются
• что в сигнатурах – заказчики волнуются
• объем трафика большой – заказчики очень волнуются, золотая середина

Внедрения АВЗ

Информзащита
Системный интегратор

- Старые операционные системы, нетронутые с момента внедрения АРМы, слабые технические характеристики.
- Ложное представление об используемых уже антивирусах на АРМах АСУ ТП.
- Собственные разработки в технологических сетях, особенности оборудования сетей АСУ ТП, - ложные срабатывания.
- Режимы блокировки и противодействие специалистов АСУ ТП при внедрении АВЗ.
- А вендоры АСУ ТП не против АВЗ, только сертификация – дорого и недолговечно (обновление версий есть у всех).
- АВЗ и виртуализация.
- А кто этот компьютер вообще обслуживает?

Постоянная защита в технологическом сегменте!!!

Kaspersky Industrial CyberSecurity KICS for Nodes

Информзащита
Системный интегратор

Решение для защиты рабочих мест в рамках промышленной сети, поставляемое в виде программного обеспечения для компьютеров под управлением ОС Windows и Linux

Преимущества:

- **Незначительное влияние на защищаемое устройство**

Минимальное потребление ресурсов

Модульная архитектура решения

- **Высочайший уровень совместимости**

Проверка целостности ПЛК

Проверка целостности файлов SCADA

- **Расширенная защита от вредоносного ПО**

Защита от вредоносного ПО

Защита от шифрования

Анализ журналов

Защита от эксплойтов

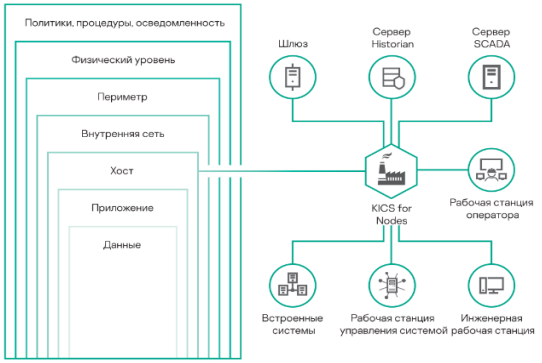
Управление сетевым экраном

- **Контроль среды**

Контроль устройств

Контроль Wi-Fi

Контроль запуска программ



Устройства, защищаемые решением KICS for Nodes

Kaspersky Industrial CyberSecurity
Kaspersky Security Center

Информзащита
Системный интегратор

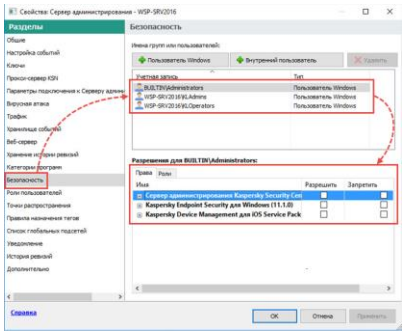
Программное обеспечение для централизованного управления безопасностью
Преимущества:

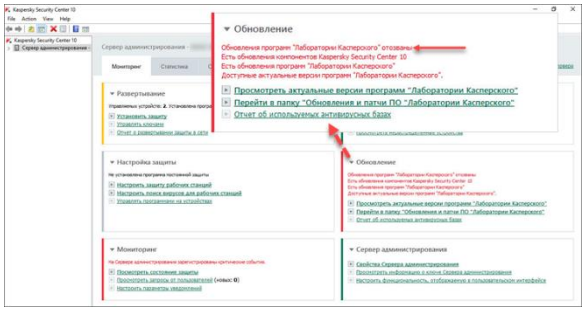
•**Управление системами**
- Централизованный сбор системных данных
- Централизованное развертывание программного обеспечения
- Мониторинг уязвимостей и управление исправлениями
- Расширенные клиентские средства управления

•**Управление политиками**
- Централизованное управление политиками безопасности
- Удаленное планирование и выполнение задач

•**Отчеты и уведомления**
- Журнал событий
- Информационные панели и отчеты
- Уведомления по SMS и электронной почте

•**Интеграция с SIEM-системами**





Предпроектная работа, конкурсы

Информзащита
Системный интегратор

Особенности 2021 года:
- Надо обследовать – там уже обследовали – на до еще раз
- Дальние объекты АСУ ТП, кто будет обслуживать, связь в РФ
- Работа с генподрядными организациями и вендорами АСУ ТП

С какими отраслями мы взаимодействуем:

- металлургия
- горнорудная
- химия
- энергетика
- нефтегазовая, газовая
- оборонная

Перспективы и бюжеты

Информзащита
Системный интегратор

Рынок разогрет, но компании не готовы финансировать защиту активов в таких объемах

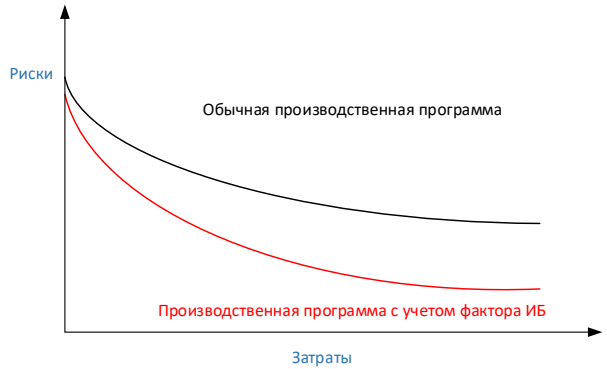
Популярные ответы:

- К нам не придут **- Заплатим штраф –** опыт США **- Укрупним/ сократим объекты КИИ**

Что может ответить СБ

Какие риски действительно волнуют бизнес (суммарно по различным отраслям):

- Хищения, коррупционные сговоры, мошеннические сделки при закупках, отгрузка/ прием продукции
- Физическая охрана периметра, хищения, контроль рабочего времени
- Мошенничество на ремонтах
- Разглашение существенных сведений/ воровство технологий
- Вирусные заражения, остановки производства, вымогательство
- Для отдельных бизнесов – целевые атаки
- Проверки финансовые и экологические, отчасти проверки регуляторов



Учет фактора КБ через технологии ИТ и ИБ дает более сбалансированную производственную политику, снижает ожидаемые риски

АСДУ, ТОиР, ИБ – что общего

Информзащита
Системный интегратор

Непрерывный мониторинг

Для ведения непрерывного мониторинга созданы технические и организационные системы, обучен и назначен персонал, определены показатели и индикаторы, карты реагирования и взаимодействий

Паспортизация оборудования, изменения в инвентаризационных данных

Формирование перечней и иерархии оборудования, схем логической связанности, определения соответствия карт процессов и карт групп агрегатов.

Контроль работ систем, контроль сервисных и подрядных работ

Производство – живой организм. Каждый день есть планы работ. Работы требуют контроля во избежание срыва выпуска продукции, производства брака, отказов смежных систем, возникновения аварийных и чрезвычайных ситуаций

Нормирования, контроль расходования и отклонений, планы обеспечения и замен

Интегрированные подсистемы контроля позволяют обеспечить фиксацию контрольных параметров или операции, заранее определив целевые показатели и допустимые значения

Организация и контроль ППР

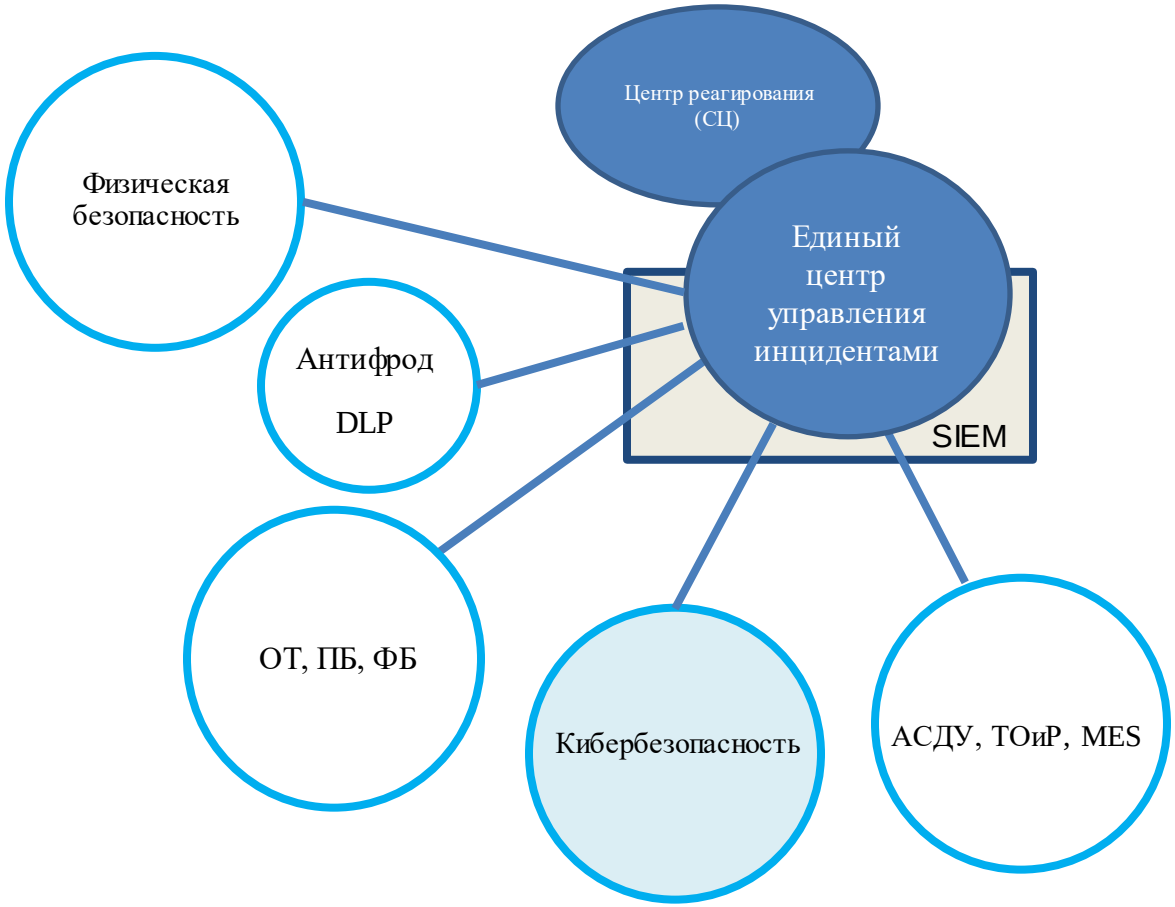
Для ППР: лановые, скользящие, по требованию/ регламенты. Доскональное знание агрегатов/ конфигурации сетей. Контроль отказов, нормированные замены / События ИБ, работа по отклонениям. Планирование заказов на приобретение / анализ трендов, расследования, предикатив

Накопление информации

Оперативная реакция диспетчеров и рекомендации специалистов по технологиям по факту контроля трендов, анализ причин аварийных ситуаций и сбоев. Определения мер повышения качества результатов.

Комплексная безопасность

Информзащита
Системный интегратор



Цели и задачи КБ

- Предотвращение/ минимизация последствий инцидентов
- Сокращение количества и тяжести несчастных случаев
- Отсутствие проблем во взаимодействии с контролирующими органами
- Сокращение дополнительных расходов, связанных с производством и ремонтом

Комплексная безопасность на предприятии

Все стало взаимоувязано, потому что везде компьютеры и сети …

Система контроля и сбора событий от организационных и организационно-технических и инженерных систем жизнеобеспечения предприятия

Система контроля и сбора событий от организационных, организационно-технических и инженерных систем жизнеобеспечения предприятий Компании по направлениям:

- Охрана труда (ОТ),
- Промышленная и функциональная безопасность (ПБ)
- Взрывобезопасность
- Пожаробезопасность,
- Химическая и радиационная безопасность.
- Электробезопасность
- Транспортная безопасность
- Экологическая безопасность

Террористические угрозы

KUMA может стать ответом на вопросы об объединяющей технологической платформе

Система контроля событий от систем физической безопасности (СКУД, PSIM, видеонаблюдение)

Система контроля и сбора событий от технологических систем обеспечения основных производственных процессов (АСУ ТП)

Экономическая безопасность

Медицинская безопасность (медосмотры, Covid)

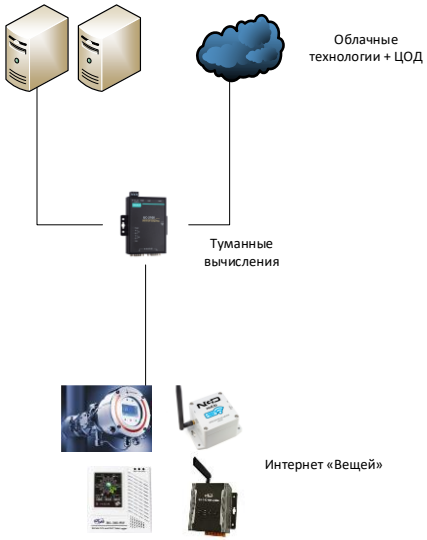
EDGE-устройства и IoT (Internet of Things) (Интернет вещей)

Информзащита
Системный интегратор

Edge-оборудование - это:
- Использование простых интерфейсов (RJ45 для витой пары + WiFi)
- Компактность, позволяющая размещать устройство в разнообразных условияъ
- Низкий уровень шума, чтобы работать возле персонала
- Низкое энергопотребление, потому что постоянным источником электричества может быть батарейка или даже солнечная панель

IoT (Internet of Things) - концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой.

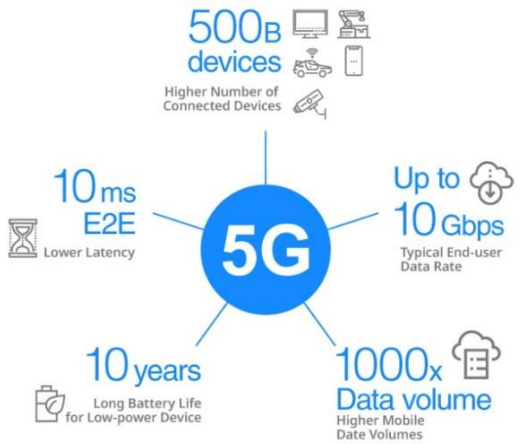
IoT – может ли он быть полезен СБ или это только головная боль для защиты еще одного сегмента



Технологические особенности сетей 5G

Информзащита
Системный интегратор

EDGE-устройства и IoT (Internet of Things) - Интернет вещей приходит на производство



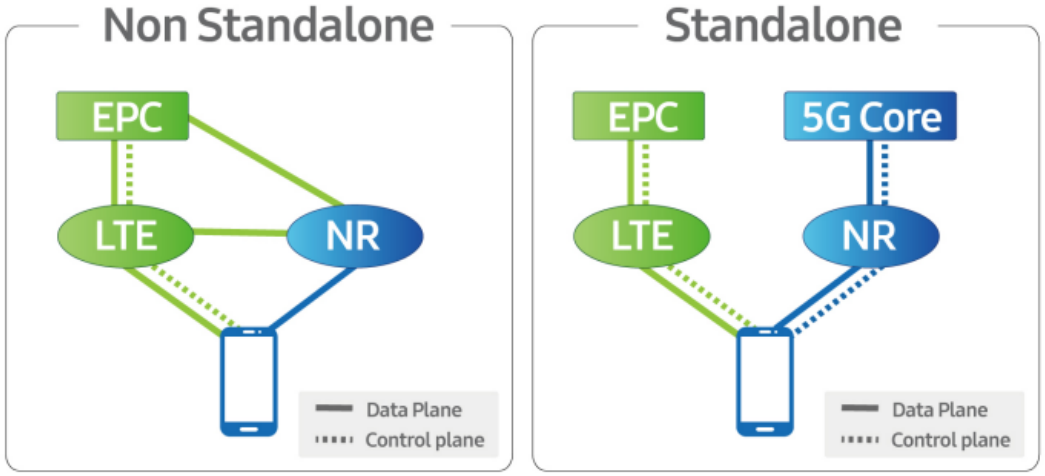
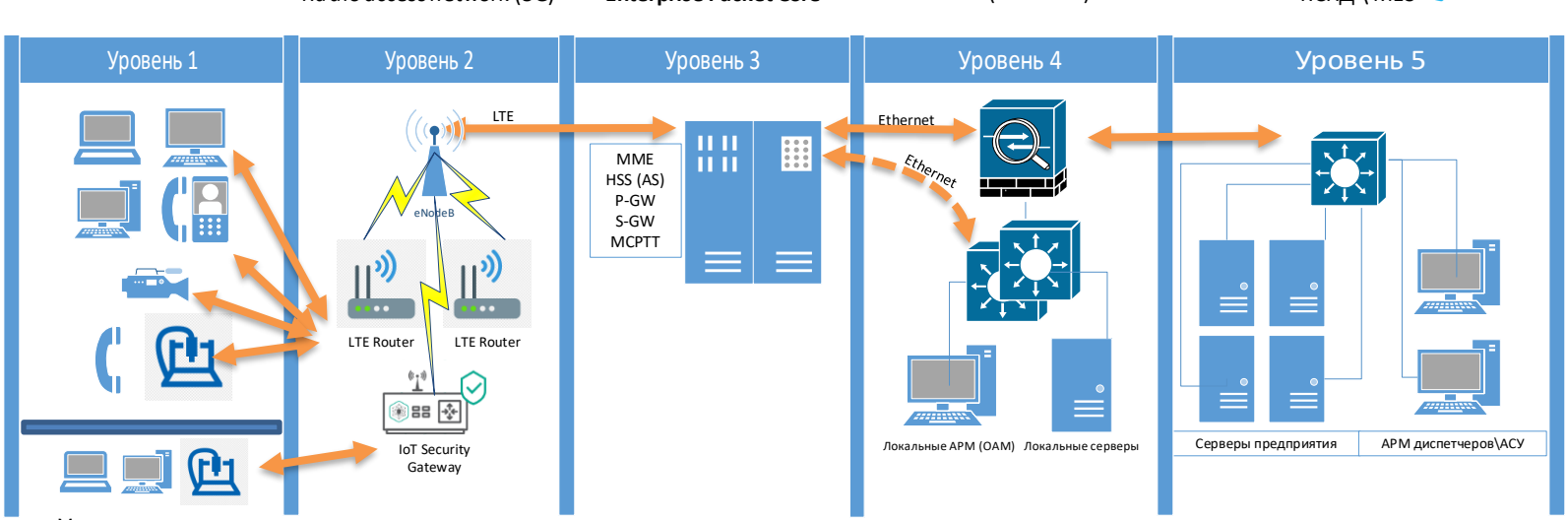


Figure 11 : How NSA and SA work

Объекты защиты проекта

Информзащита
Системный интегратор



Уровень управления и мониторинга:

Центр управления безопасностью, Network management systems (NMS)

Уровень устройств и хостов:

Идентификация, аутентификация и авторизация (IMEI, IMEISV, 5G AKA)

Идентификация, аутентификация и авторизация (Корпоративный AAA)

Регистрация и мониторинг событий безопасности

Endpoint security client

Endpoint security client

Endpoint security client

Резервное копирование и восстановление

Уровень сетей связи:

Network Domain Security (NDS)

Межсетевое экранирование (средствами SEGs EPC)

Межсетевое экранирование (средствами NGFW), **ДМЗ**

Сегментация сети и управление сетевыми потоками (VLAN, Network Slicing, MAC и др. технологии Network Domain Security)

Сегментация сети и управление сетевыми потоками (Firewall, VLAN)

NetGuard Endpoint Security (NES) или иной детектор вредоносной активности в сети

Encryption (IPsec, TLS) средствами SEGs EPC

Encryption (IPsec, TLS) средствами NGFW VPN

Импортозамещение

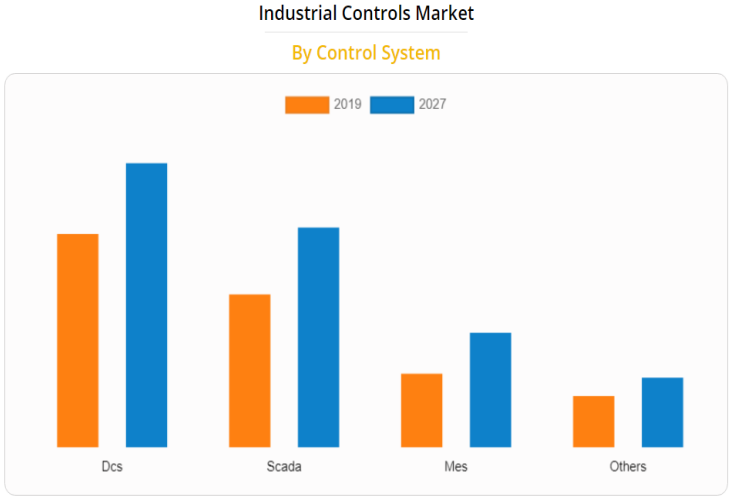
Ведущие ключевые производители на рынке промышленных систем управления:

- Сименс
- ABB
- Омрон
- Emerson Electric
- Rockwell Automation
- Honeywell International
- Yokogawa Electric Corporation
- Schneider Electric

Объединение предприятий ГК «Росатом»
Emerson Process Management
ГК «Текон»
НПФ «Система-Сервис»
ЗАО «Эмикон»
ПАО «Нефтеавтоматика»
ПАО «Нижневартовскасунефть»
ООО «Индасофт»
ООО «Арман»

ISC Security

- ABB Group
- Airbus Group SAS
- BAE Systems PLC
- Baker Hughes, Inc.
- Belden, Inc.
- Check Point Software Technologies Ltd.
- Cisco Systems, Inc.
- CyberArk Software Ltd.
- Cyberbit Ltd.
- Dragos Yachts A.S
- FireEye, Inc.
- Fortinet, Inc.
- Honeywell International, Inc.
- Indegy Ltd.
- Kaspersky Lab
- McAfee
- Nozomi Networks Inc.
- Palo Alto Networks, Inc.
- Rockwell Automation, Inc.
- Schneider Electric SA
- SecurityMatters B.V.
- Sophos Ltd.
- Symantec Corporation
- Waterfall Security Solutions Ltd.



- распределенные системы управления (DCS),
- системы диспетчерского управления и сбора данных (SCADA),
- системы управления производством (MES)
- автоматизированная система безопасности (SIS),
- специализированные (морские, логистические) интегрированные системы управления и мониторинга (ICMS).

Перспективные направления включающие вопросы защиты АСУ ТП

- Ситуационные центры. Интеграция с физической безопасностью (PSIM) и всеми видами ОТ, ПБ, ФБ.

- Системы обнаружения вторжения, интеграция с инвентаризационными и мониторинговыми ИТ системами, интеграция с системами сбора измеренных данных – контроль технологических параметров, АСДУ.

- Контроль сетевой активности. Антивирусы. Ловушки. Киберполигоны.

- Решения для защиты ТОиР систем. Облака. Проверка на НДВ. Упрощение технологий, визуализация.

- Защита в облаке/ защита из облака

- Прозрачность vs защищенность ресурсов.

- Киберразведка и TI – не для всех и не всегда. Создание центров защиты/ восстановления данных.

- Разработка систем защиты сетей pLTE/5G и WiFi-6 для промышленных холдингов

- Антифрод на системах АСУ ТП.

- Роботизация ИБ. ИБ для роботизации и RPA.

- **637:** The number of ICS vulnerabilities disclosed in 1H 2021, almost 200 more than in our previous report covering the 2H 2020
- **61.4%:** The percentage of ICS vulnerabilities remotely exploitable
- **31.6%:** The percentage of ICS vulnerabilities locally exploitable
- **26%:** The percentage of ICS vulnerabilities that went unpatched, or only a partial remediation was suggested
- **65%:** The percentage of ICS vulnerabilities likely to lead to total loss of availability

Biannual ICS Risk & Vulnerability Report

Информзащита
Системный интегратор

Информационная безопасность 24x7x365

Центр противодействия кибератакам IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Сервисный центр

+7 495 981 92 22
support@itsoc.ru
www.itsoc.ru

Пресс-служба

pr@infosec.ru