Kaspersky Industrial Cybersecurity Conference 2023

Кибербезопасное решение по модернизации АСУ ТП зарубежных производителей

Андрей Григорьев,
заместитель директора
департамента технического
маркетинга НПП «ЭКРА»

kaspersky

ЭКРА

Производители из недружественных стран поставлявшие АСУ ТП подстанций в 2000-2020 гг.

SIEMENS

MIKRONIKA

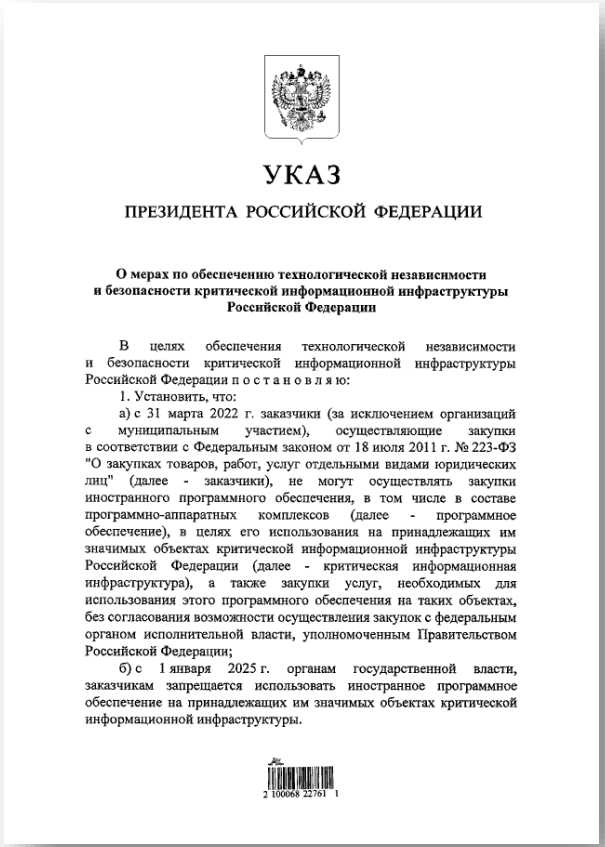
General Electric

ALSTOM

ABB

sprecher automation

Запрет на использование иностранного ПО



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

1. Установить, что:

а) с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее - заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее - программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

2 100068 22761 1

- **с 31 марта 2022 г.** заказчики должны согласовывать закупку иностранного ПО в целях его использования на принадлежащих им значимых объектах КИИ РФ, а также закупки услуг, необходимых для использования этого ПО на таких объектах
- **с 1 января 2025 г.** органам государственной власти, заказчикам запрещается использовать иностранное ПО на принадлежащих им значимых объектах критической информационной инфраструктуры

Указ Президента РФ №166 от 30.03.22

- **с 1 января 2025 г.** органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении РФ недружественные действия

Указ Президента РФ №250 от 01.05.22

Срок службы оборудования АСУ ТП подстанции

10 лет

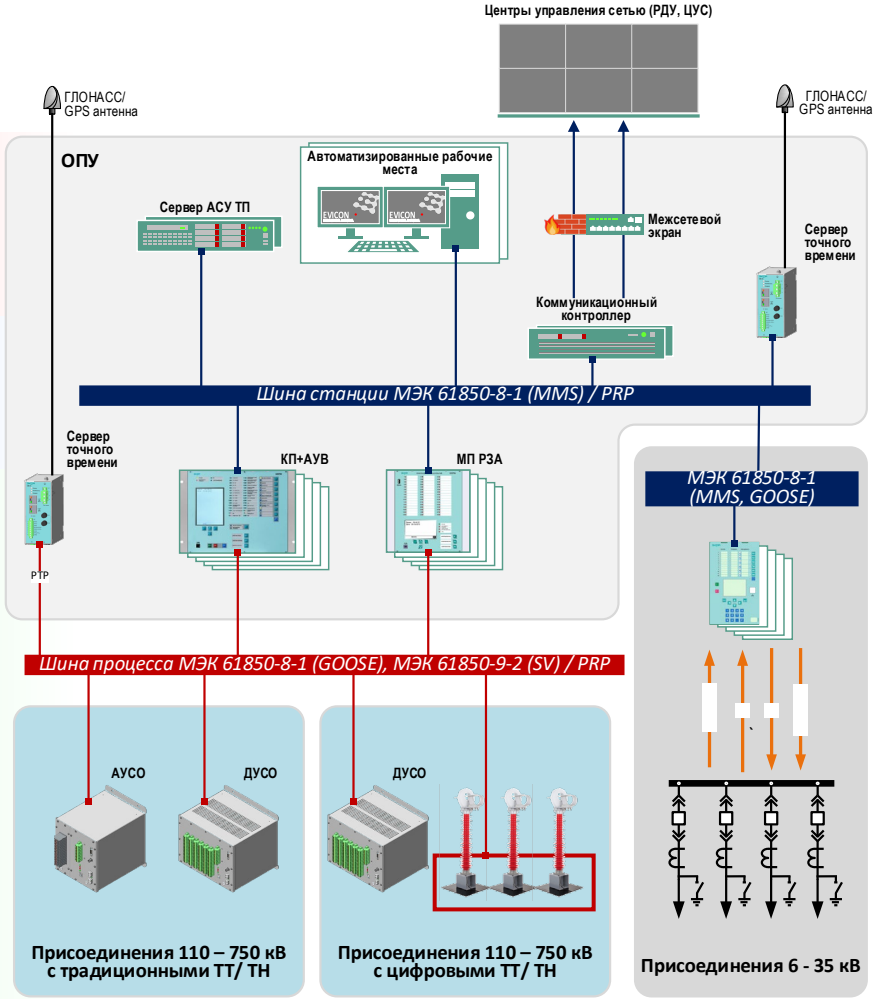
Станционный уровень

15 лет

Серверы телемеханики

20 лет

Уровень присоединения и полевой уровень



1. В период с 2000 по 2020 гг. в РФ внедрено **большое количество ПТК АСУ ТП** производителей из недружественных стран

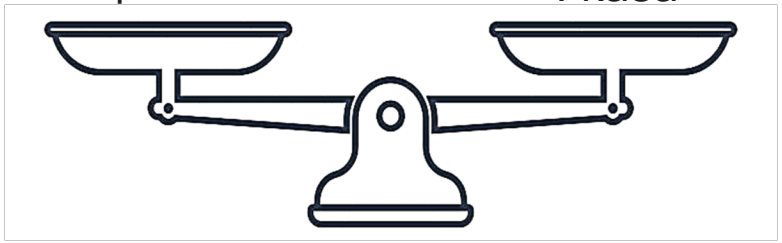
2. Срок службы оборудования верхнего/среднего уровня огромного количества ПТК **закончился или подходит к концу**

3. Большинство производителей из недружественных стран **прекратили поддержку и поставки оборудования и ПО,** закрыли доступ к обновлениям уже поставленного ПО.

4. Действует прямой **запрет на использование иностранного ПО независимо от формы собственности организации** на объектах значимой критической информационной инфраструктуры.

Затраты на модернизацию

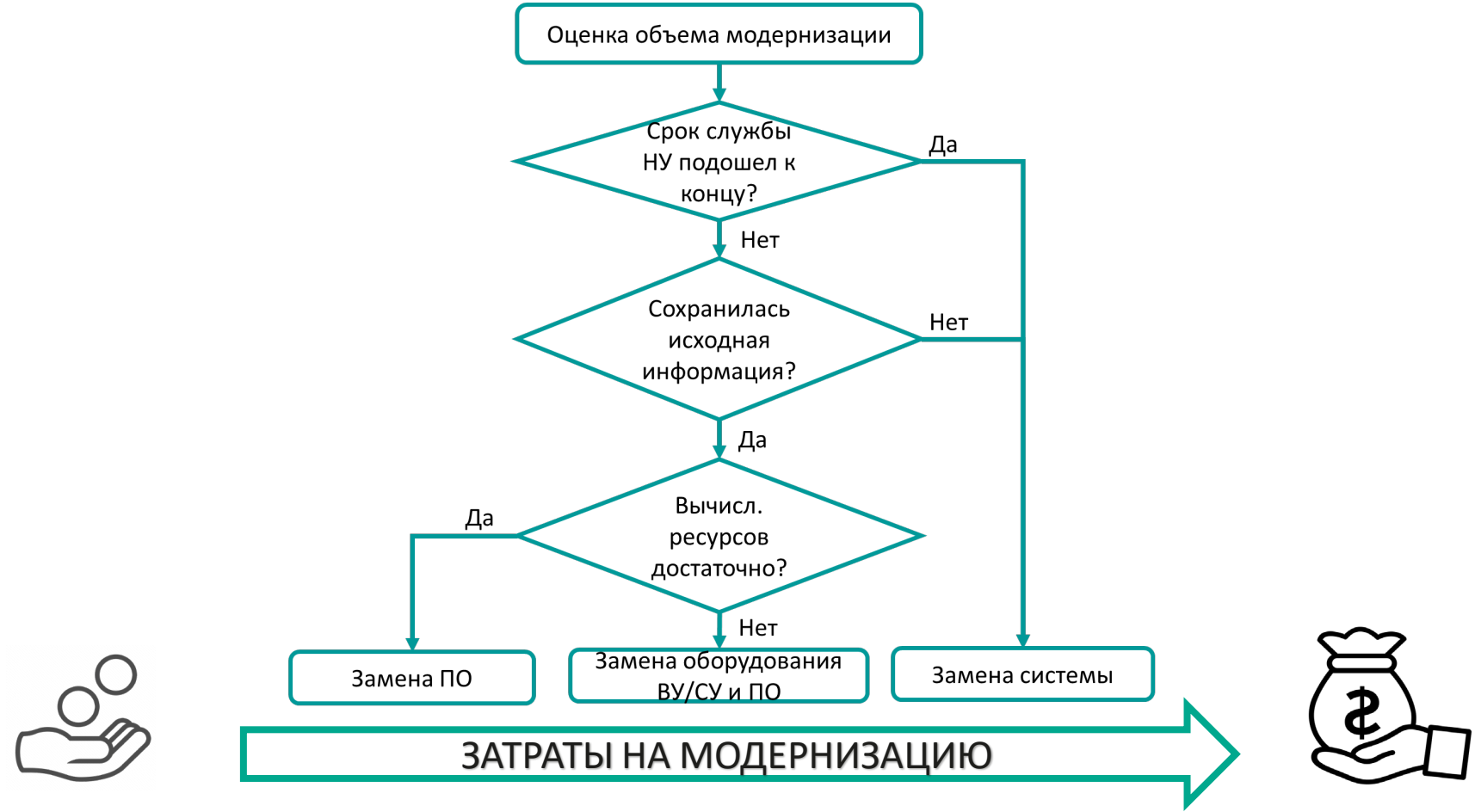
Выполнение требований Указа



Проблемы:

- применение зарубежными производителями проприетарных, нестандартных протоколов связи;
- отсутствие исходной информации (рабочая документация, исполнительная документация, инженерное ПО, конфигурации и др.) по устройствам нижнего уровня (ПЛК, РЗА и др.) позволяющей однозначно идентифицировать сигналы с устройства;
- необходимость приведения модернизируемой системы к актуальным требованиям НТД (в частности требованиям по информационной безопасности).

Как оценить возможность модернизации ПТК?



Последовательность выполнения работ при модернизации ПТК

Анализ исходных данных
(предпроектное обследование)

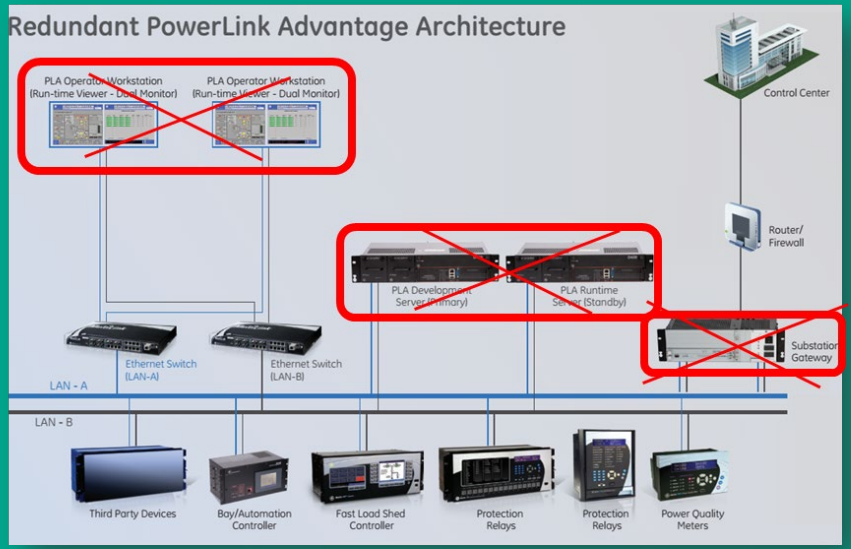
Выбор оптимального технического решения
(проектирование)

Создание SCADA-проекта, настройка оборудования, подготовка к интеграции решения на объекте (заводской этап)

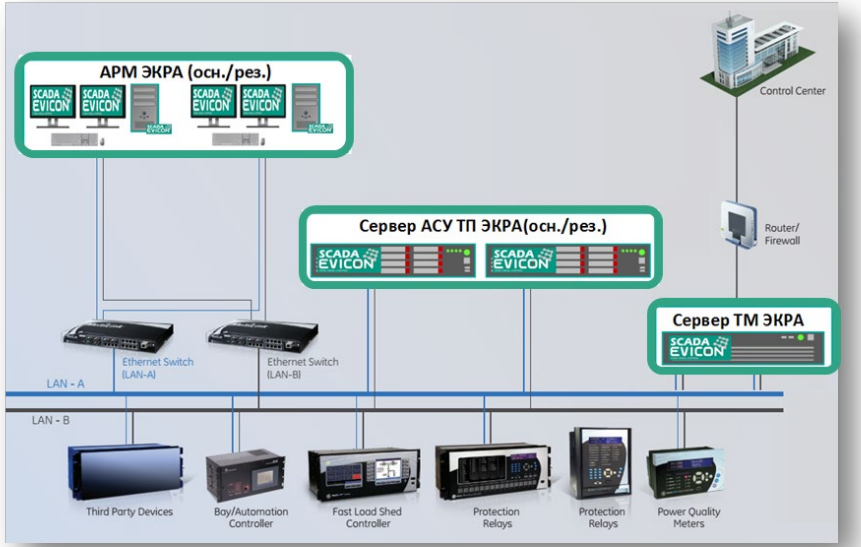
Последовательный запуск и тестирование модернизируемой системы на объекте (параллельная работа старого и нового оборудования и ПО)

Ввод в опытную/промышленную эксплуатацию (отключение старого оборудования и ПО)

Опыт модернизации ПТК. Замена верхнего и среднего уровня

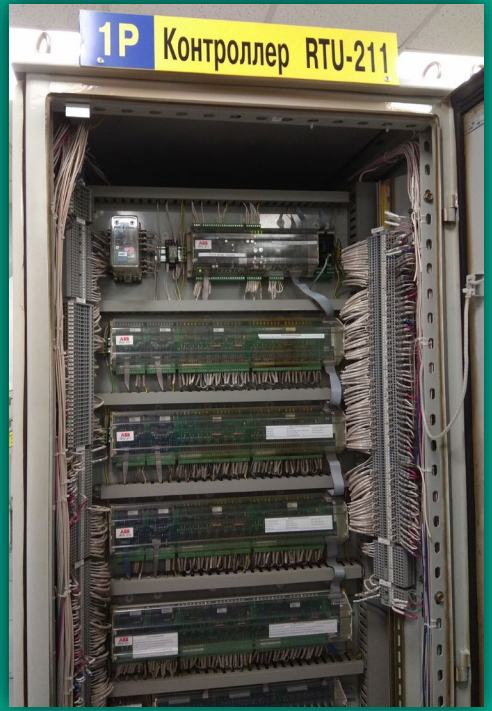


До



После

Опыт модернизация ПТК. Замена нижнего уровня.



До

После

Подсистема сбора данных

- Клиент МЭК 60870-5-101
- Клиент МЭК 60870-5-103
- Клиент МЭК 60870-5-104
- Клиент **DNP3** (распространен в решениях GE, Mikronika)
- Клиент МЭК 61850
- Клиент SNMP
- Клиент MODBUS
- Клиент **JBUS** (распространен в решениях Schneider Electric)
- Клиент OPC
- Клиент **SPA-Bus** (распространен в решениях ABB)
- Клиент СТАРТ
- Клиент СЭТ
- Клиент **нестандартных протоколов**

Подсистема передачи данных

- Сервер МЭК 60870-5-101
- Сервер МЭК 60870-5-104
- Сервер МЭК 61850
- Сервер OPC
- Сервер MODBUS
- Сервер SNMP
- и др.

Второе полугодие 2022

Первое полугодие 2022

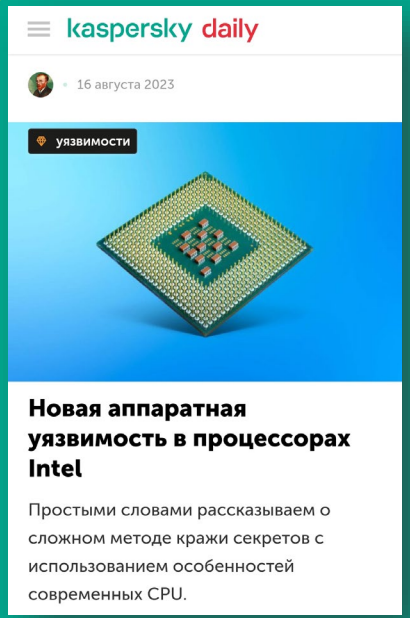
Во втором полугодии 2022 в России отмечено **самое значительное изменение процента атакованных компьютеров в АСУ среди всех стран**. Этот показатель увеличился на 9 п.п. и составил **39,2%**

Встроенные средства защиты информации в EKRASCADA

Защищенные соединения с аутентификацией и шифрованием	Аутентификация и разграничение прав доступа пользователей к функциям EKRASCADA	Идентификация и авторизация пользователей EKRASCADA по учетным данным домена
Ограничение неуспешных попыток доступа пользователей	Блокирование сеанса доступа пользователя при неактивности	Ограничение параллельных сеансов доступа пользователей
Контроль целостности компонентов (во время запуска и работы EKRASCADA)	Журнал событий безопасности с возможностью передачи событий на внешний сервер	Электронная подпись дистрибутива EKRASCADA

Разработка безопасного ПО

Опыт. ПК «EKRASCADA» на аппаратной платформе с процессорами семейства «Эльбрус»



- Доверенная программно-аппаратная платформа "Эльбрус".
- Отечественное решение для АСУ ТП критически важных объектов.

Соответствие требованиям безопасности регуляторов

- НПП «ЭКРА» имеет все необходимые лицензии ФСТЭК / ФСБ для проведения работ по проектированию и интеграции системы обеспечения информационной безопасности;
- «EKRASCADA» и применяемые в решениях программные средства защиты информации входят в единый реестр российских программ для ЭВМ и БД
- «EKRASCADA» поддерживает ОС из реестров МинЦифры и ФСТЭК
- Средства защиты информации прошли испытания на совместимость с ПТК производства НПП ЭКРА, соответствуют требованиям государственных регуляторов

Интегрированное решение для защиты АСУ ТП

Kaspersky Industrial CyberSecurity for Nodes

Инструменты класса
EPP и аудит

- Защита от вредоносного ПО с минимальным влиянием на систему
- Контроль целостности ПЛК
- Противодействие шифровальщикам
- Контроль приложений и устройств

Kaspersky Industrial CyberSecurity

- Единая консоль
- Нативная интеграция
- Кросс-продуктовые сценарии
- Общий kill-chain

Управление рисками и активами

- Пассивное обнаружение компонентов и уязвимостей ОТ
- Дополнительный активный опрос, ориентированная на риск ситуационная осведомленность и отчетность

Kaspersky Industrial CyberSecurity for Networks

Анализ сетевого трафика
(ICS DPI, IDS)

- Обнаружение в трафике передаваемых технологических параметров и их отклонений (промышленный DPI)
- Обнаружение отклонений от базовых параметров в сетевых коммуникациях
- Скоринг рисков событий и узлов
- Инвентаризация активов, включая данные об уязвимостях и состоянии узлов

Опыт частичной модернизации/расширения ПТК АСУ ТП ПС

№ п/п	Объект установки	Производитель модернизируемого/ расширяемого ПТК
1	ПС 500 кВ Хабаровская, ПАО «ФСК ЕЭС», МЭС Востока	PowerLink Advantage (PLA), GE
2	ПС 500 кВ Амурская, ПАО «ФСК ЕЭС», МЭС Востока	PowerLink Advantage (PLA), GE
3	ПС 220/10/10 кВ Латышская, ПАО «МОЭСК»	MicroSCADA, ABB
4	ПС 330 кВ Старорусская, ПАО «ФСК ЕЭС», МЭС Северо-Запада	SYNDIS, Mikronika
5	ПС 500 кВ Дальневосточная, ПАО «ФСК ЕЭС», МЭС Востока	PowerLink Advantage (PLA), GE
6	ПС 500 кВ Барсово, ПАО «ФСК ЕЭС», МЭС Западной Сибири	MicroSCADA, ABB
7	ПС 220 кВ Аэропорт, ПАО «ФСК ЕЭС», МЭС Востока	PowerLink Advantage (PLA), GE
8	ПС 220 кВ Литейная, ПАО «ФСК ЕЭС», МЭС Северо-Запада	Sprecon, РтСофт
9	ПС 330 кВ Тихвин Литейный, ПАО «ФСК ЕЭС», МЭС Северо-Запада	SYNDIS, Mikronika
10	ПС Уссурийск-2, ПАО «ФСК ЕЭС», МЭС Востока	PowerLink Advantage (PLA), GE

Полигон систем автоматизации

- Требуется предварительное обследование объекта КИИ для оценки целесообразности частичной модернизации, т.е. необходимо учитывать специфику каждого объекта;

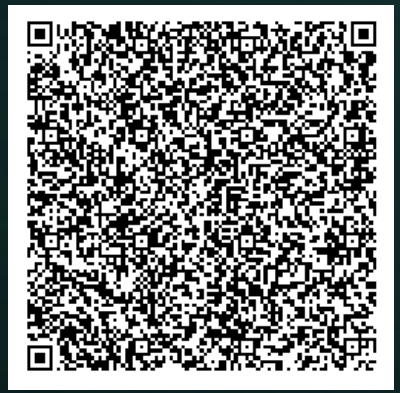
- Полученный опыт позволяет решить ряд организационных и технических сложностей, возникающих при переходе на отечественное ПО связанных с необходимостью поддержки (интеграции) оборудования нижнего уровня иностранного производства;

- Применение в проектах по модернизации АСУ ТП решений KICS позволяет построить комплексную защиту инфраструктуры;

- В целях снижения вероятности внешних угроз, обеспечения технологического суверенитета и безопасности КИИ РФ требуется в минимальные сроки выполнить переход на отечественные решения.

Приглашаем на наш стенд!

Спасибо за внимание!



Контакты:

Андрей Григорьев,
заместитель директора департамента технического маркетинга НПП «ЭКРА»

kaspersky

ЭКРА