

Защита информации в АСУ ТП.

Безопасность КИИ — критической информационной инфраструктуры

 Нуйкин Андрей

 15.07.2021

Что такое ЕВРАЗ?



■ ГЛОБАЛЬНАЯ ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности ЕВРАЗа. Компания входит в ведущий индекс Лондонской Фондовой Биржи FTSE-100.

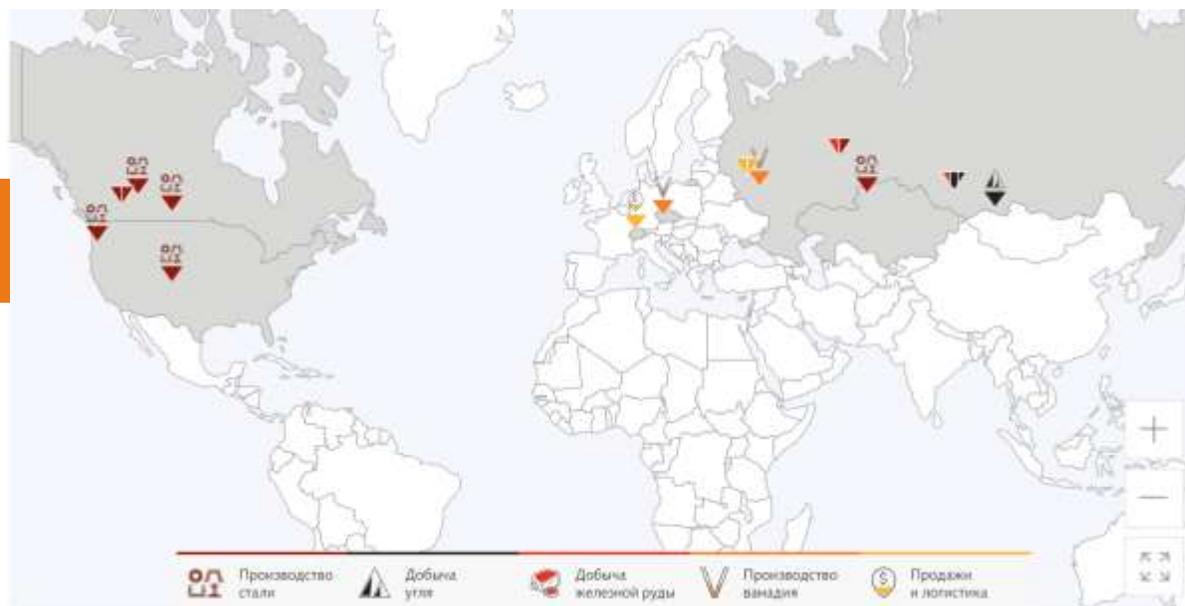
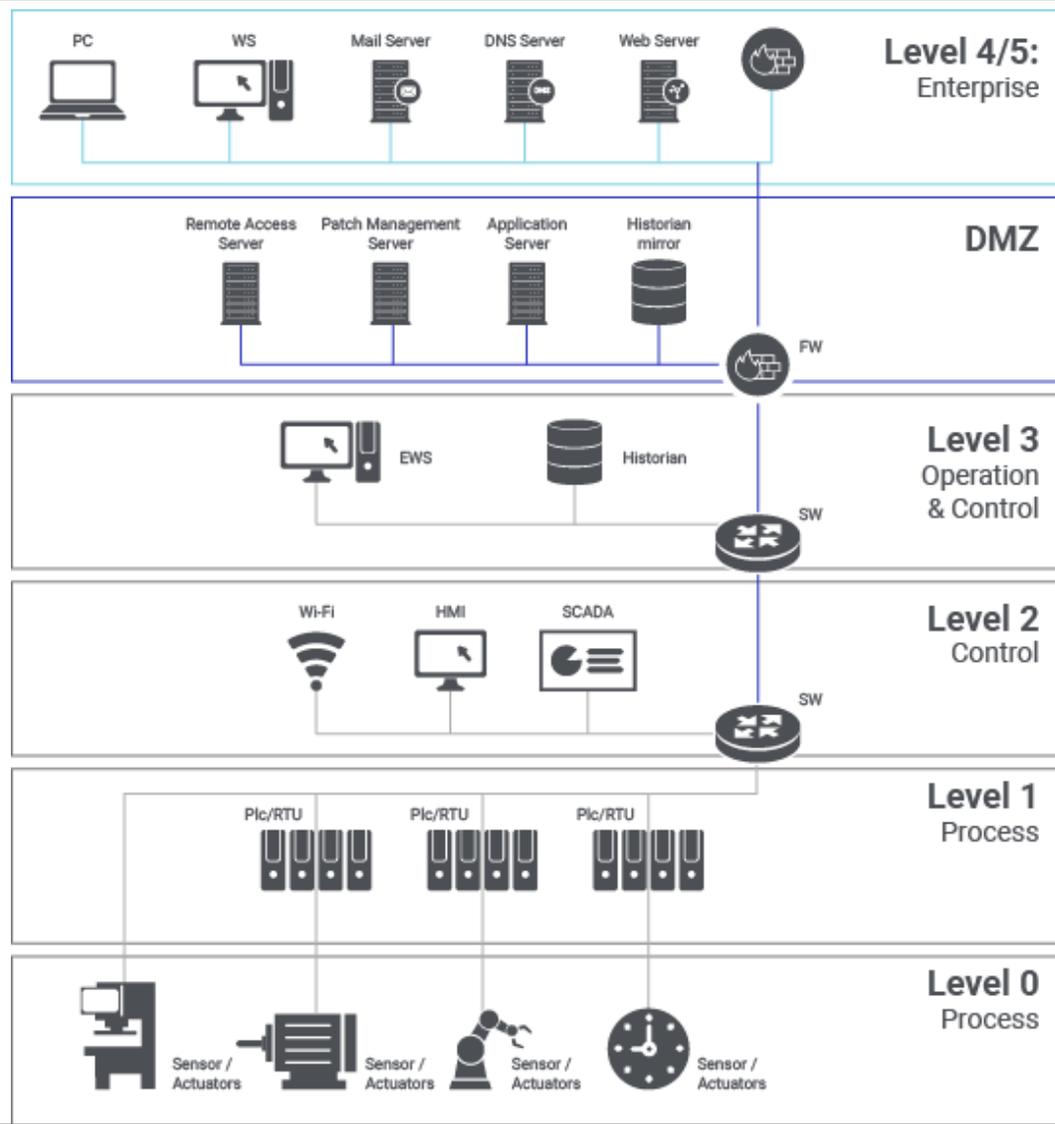
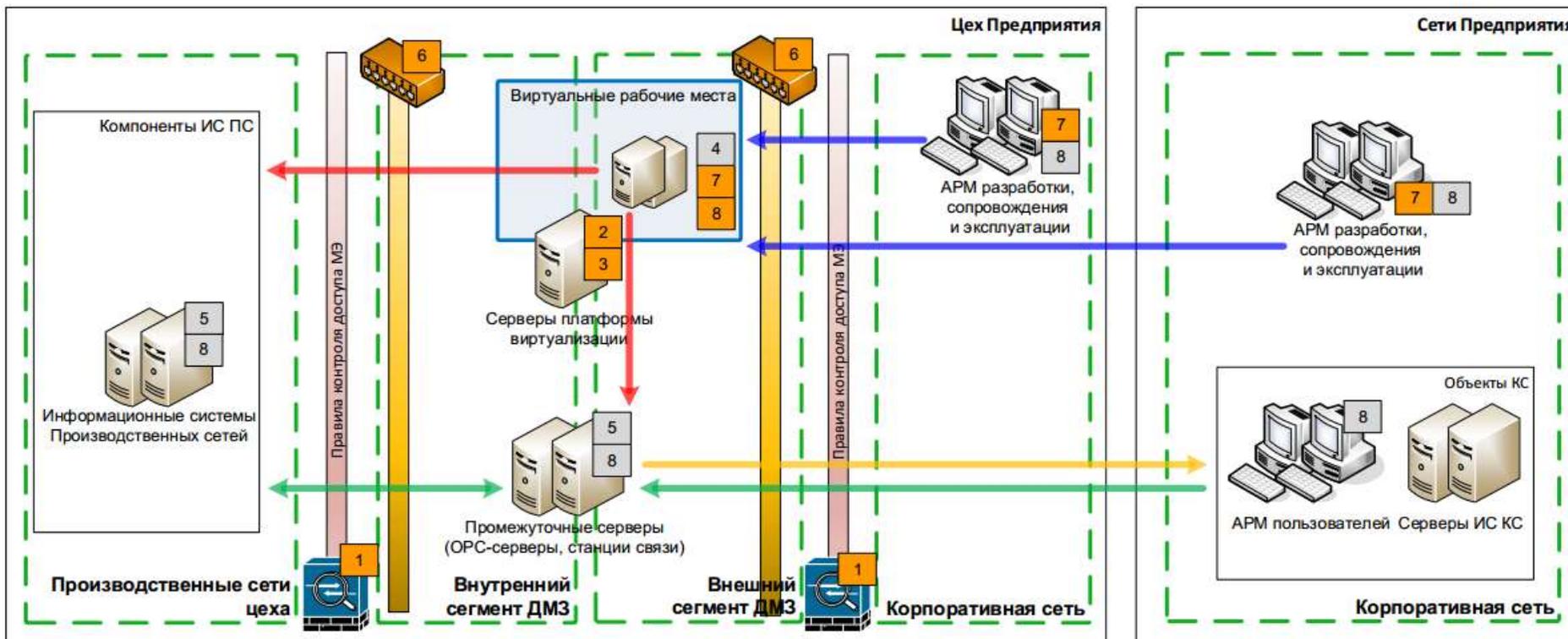


Схема защиты от института Пердюю



Концептуальная схема ЕВРАЗ



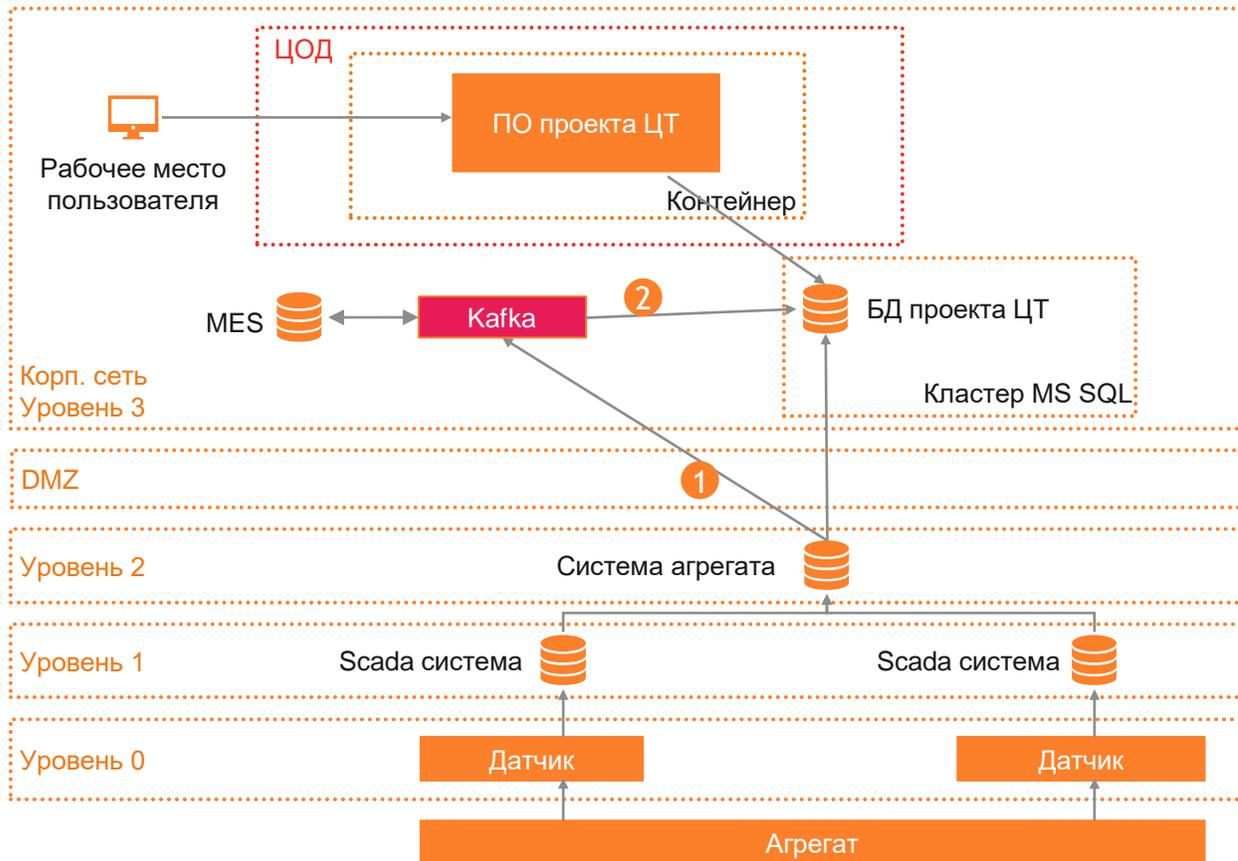
Условные обозначения

1	Средства межсетевое экранирования и предотвращения вторжений
2	Аппаратный сервер виртуализации
3	ПО платформы виртуализации
4	Клиентское ПО сопровождения ИС ПС
5	Специализированное ПО ИС ПС
6	Средства анализа и мониторинга событий ИБ
7	Средства усиленной аутентификации
8	Средства антивирусной защиты

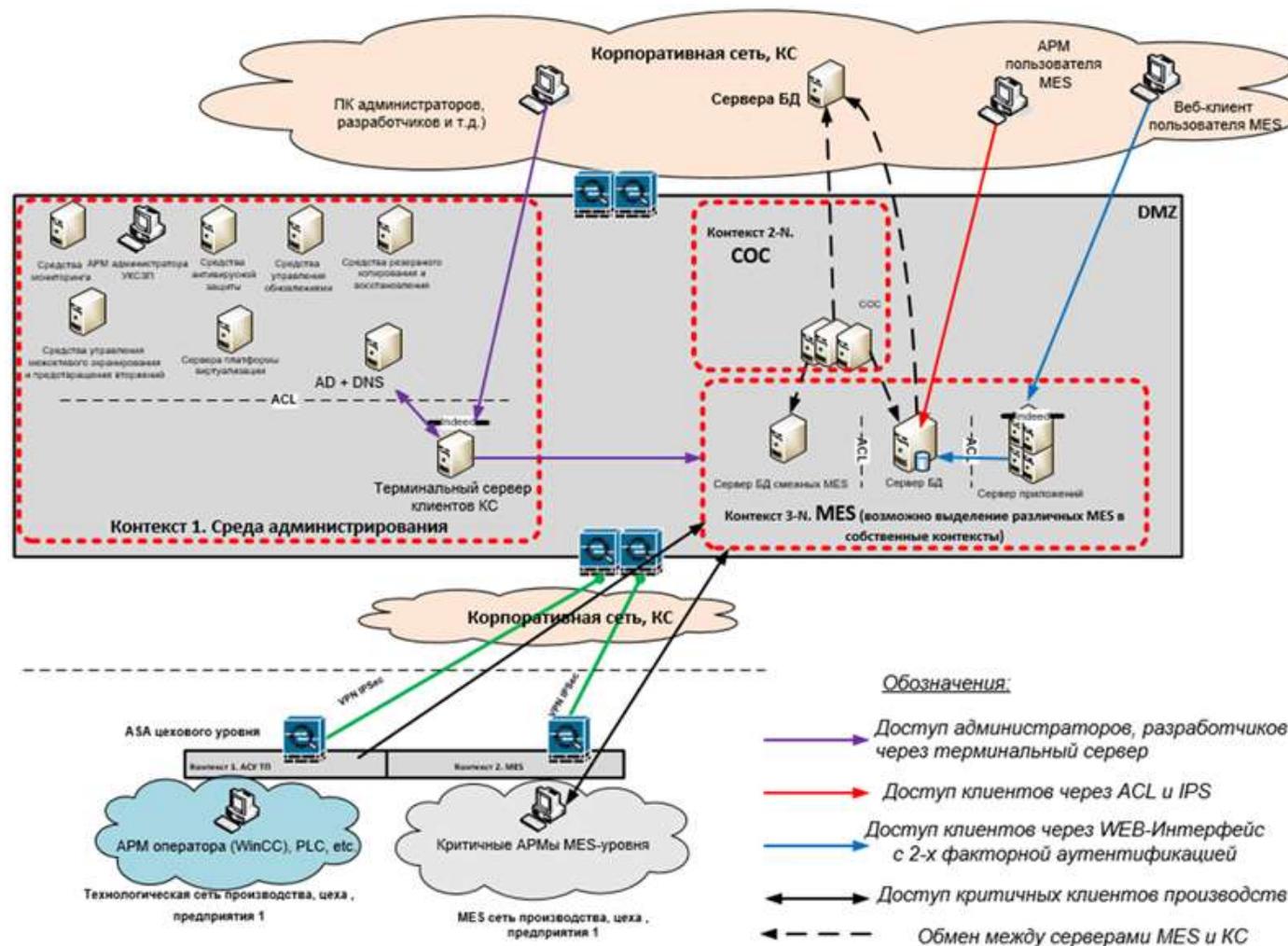
- Опосредованный доступ по протоколу удаленного доступа с применением усиленной аутентификации
- Подключение к компонентам ИС ПС
- Передача данных ИС ПС в ИС КС
- Запрос технологических данных ИС ПС
- Проектируемые программно-технические средства
- Существующие программно-технические средства

- Четко понимать какое взаимодействие происходит между технологической и корпоративной сетью
- Поддерживать разделение технологической сети от корпоративной. Все что касается АСУТП должно быть в АСУТП.
 - Все, что общается с корпоративной сетью размещаем в DMZ
 - Выделяем административную подсеть
- Не допускать (по возможности 😊) прямых соединений между корпоративной и технологической сетью.
 - Связь инициируется только из ТС в КС.
- Не допускать входящих соединений в технологическую сеть.
- Поддерживать отказоустойчивость.
 - Разрыв связи с корпоративной сетью не должен сказываться на производстве.

Использование брокера сообщений **Kafka** – архитектурный стандарт ЕВРАЗа для обмена между приложениями



Данные из АСУТП поднимаются вверх в корпоративную сеть. Обратной связи не предусмотрено.



Проблема в том, что не все системы MES можно разделить на FrontEnd – общение с пользователем и BackEnd – общение с уровнем АСУТП

Спасибо за внимание



+7(495) 363-19-60



Andrey.nuykin@evraz.com



www.evraz.com

