ЕВРАЗ

Защита информации в АСУ ТП

Безопасность технологического сегмента

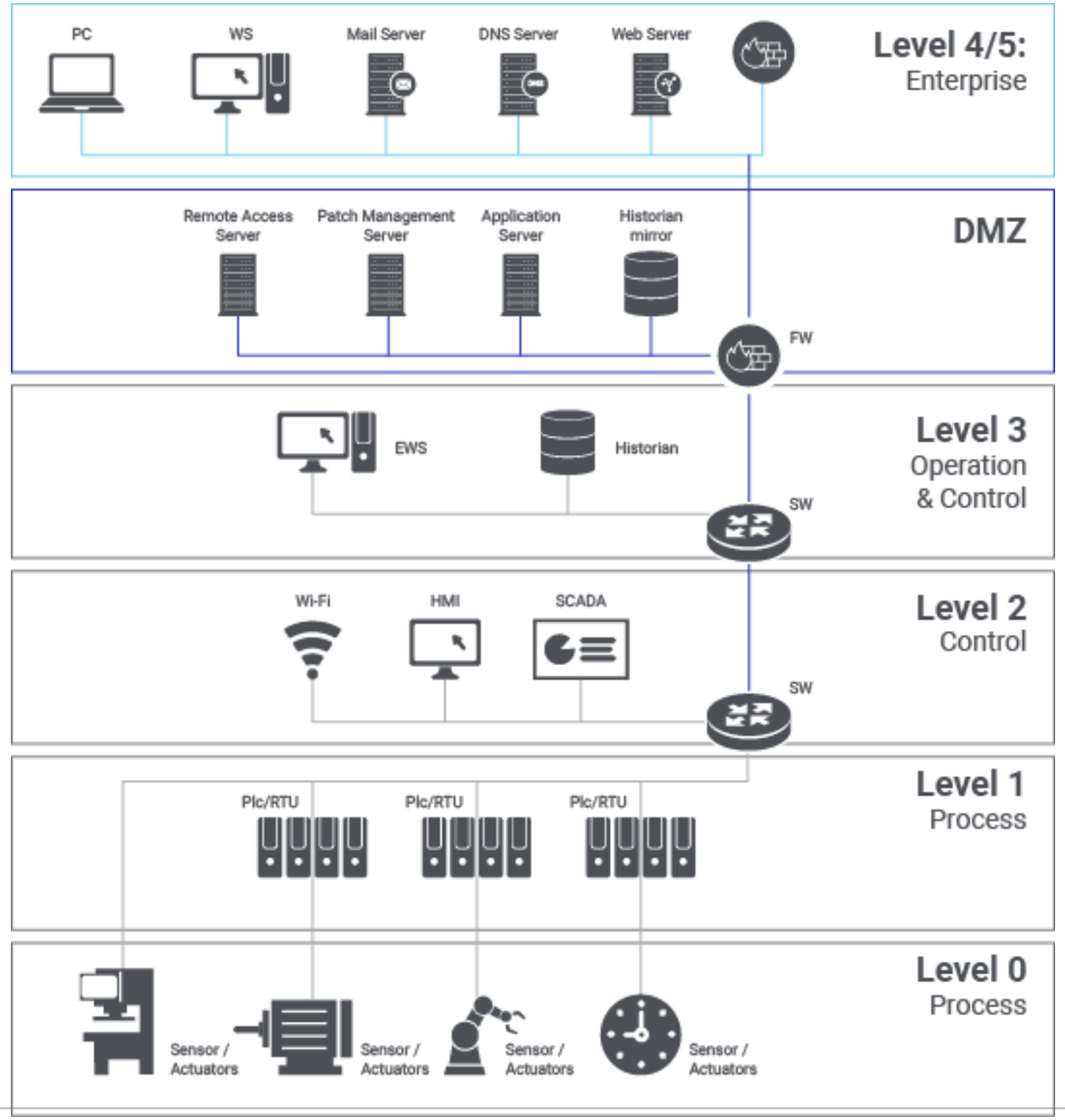
Нуйкин Андрей

03.2023

Немного маркетинга

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.

Схема защиты от института Пердью



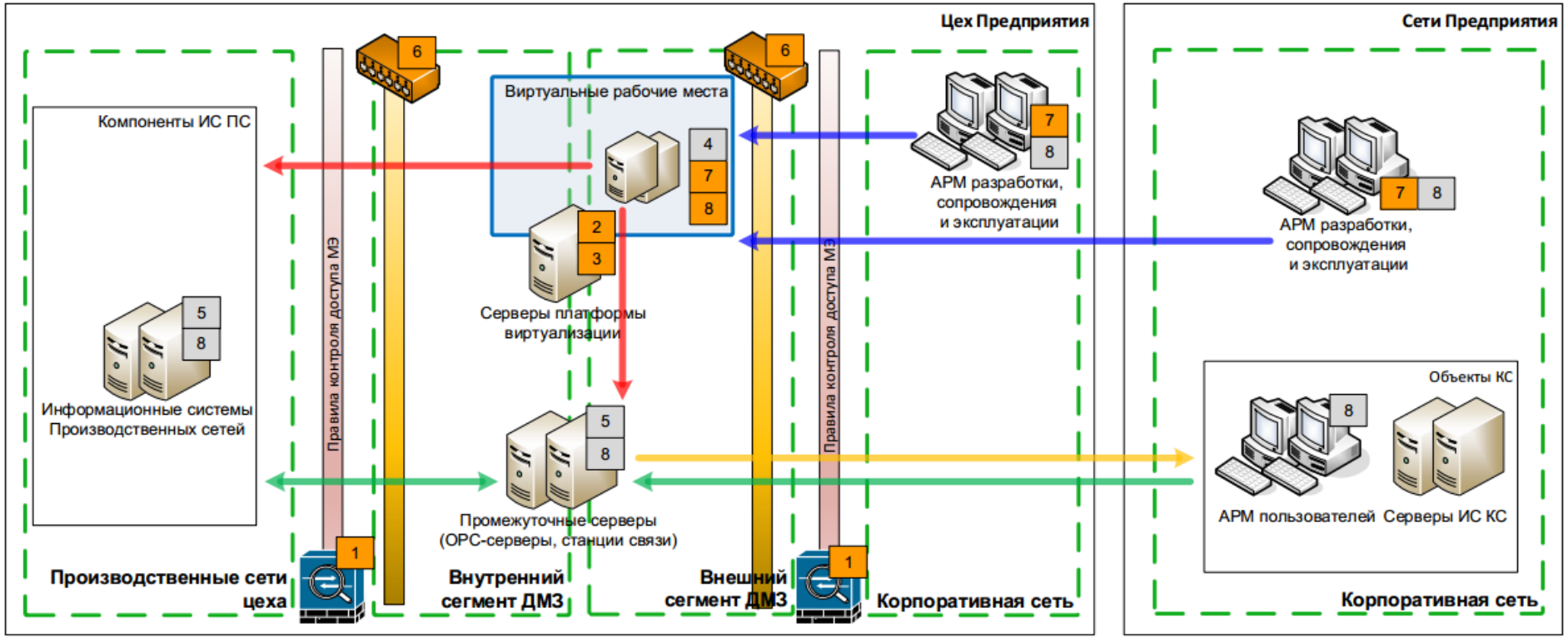
Основные моменты

ЕВРАЗ

- Поддерживать разделение технологической сети от корпоративной. Все что касается АСУТП должно быть в АСУТП.
  - Все, что общается с корпоративной сетью размещаем в DMZ
- Не допускать прямых входящих соединений от корпоративной сети к технологической сети.
  - Связь инициируется только из ТС в КС.
- Поддерживать отказоустойчивость.
  - Разрыв связи с корпоративной сетью не должен сказываться на производстве.
- Входящие данные из корпоративной сети в технологическую сеть передавать через промежуточные серверы.
- Дополнительная аутентификация при входе в технологическую сеть

Концептуальная схема защиты технологической сети

ЕВРАЗ



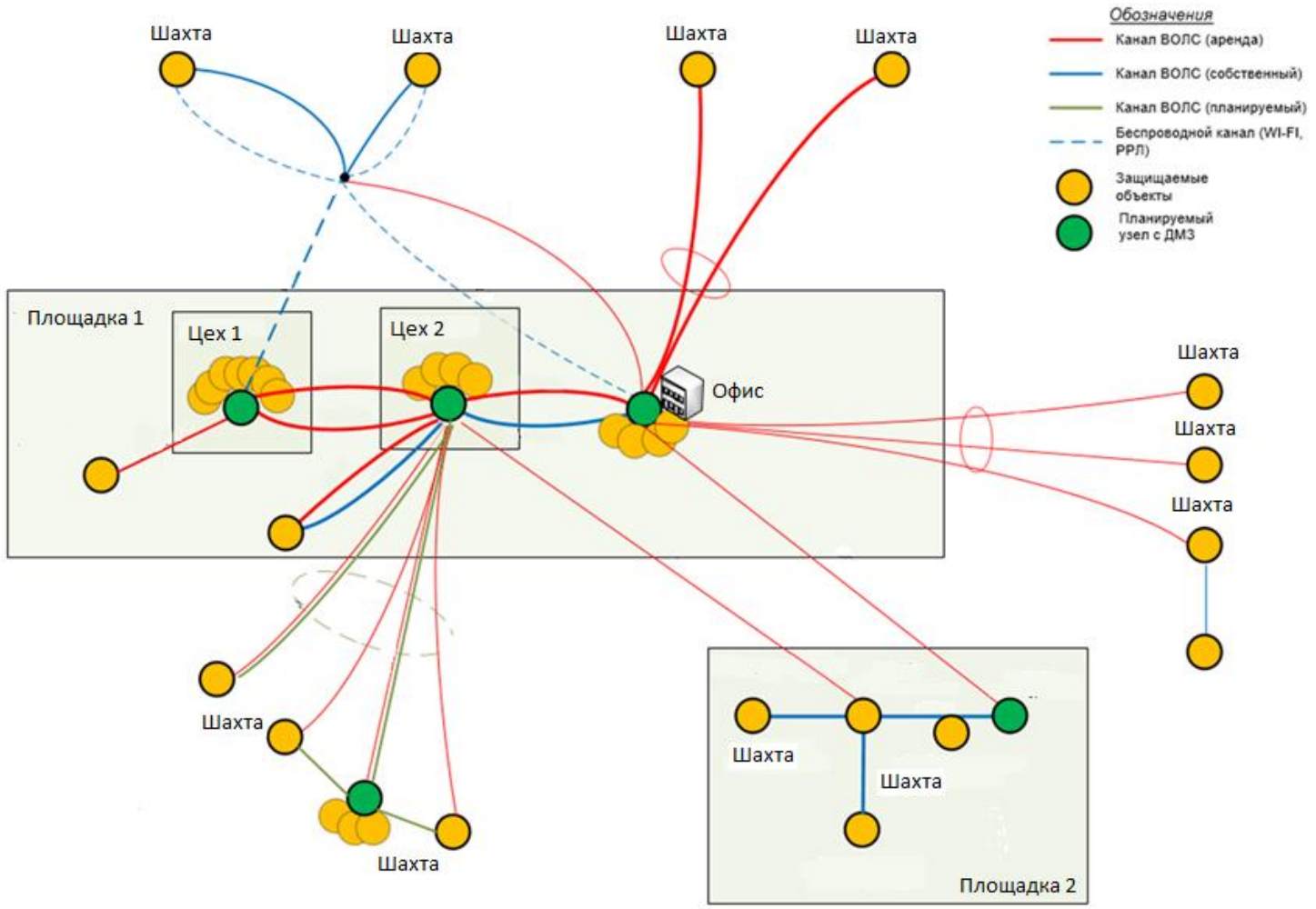
Условные обозначения

1	Средства межсетевого 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
- X — Проектируемые программно-технические средства
- X — Существующие программно-технические средства

Вариант организации DMZ для крупного предприятия

ЕВРАЗ



Цифровая трансформация

ЕВРАЗ

Начиная с 2019 года ЕВРАЗ начал цифровую трансформацию.

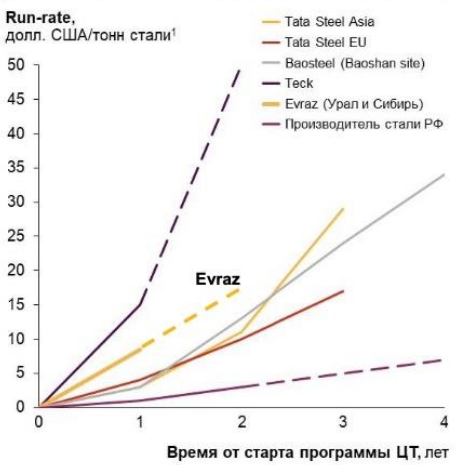
Количество проектов растет и достигает цифры 170 штук.

ЕВРАЗ на уровне мировых лидеров в ЦТ

ЕВРАЗ

- ЕВРАЗ в 2021 ускорил движение в цифровой трансформации и приступил к масштабированию. Цель – создание значительного прямого экономического эффекта в производстве на уровне мировых лидеров ЦТ в промышленности.
  - Определение лидеров согласно McKinsey: «Мировые лидеры – производители стали – достигали результата 3-4 долл. США/т стали после первого года цифровой трансформации и 10-13 долл. США/т стали ко второму году»
- По результатам 2021 года достигнут экономический эффект 150 млн долларов в годовом выражении
- В 2022 году темп сохраняется
- Возникшая в стране нестабильность повлияла на часть эффектов, но основная часть проектов остается актуальной.

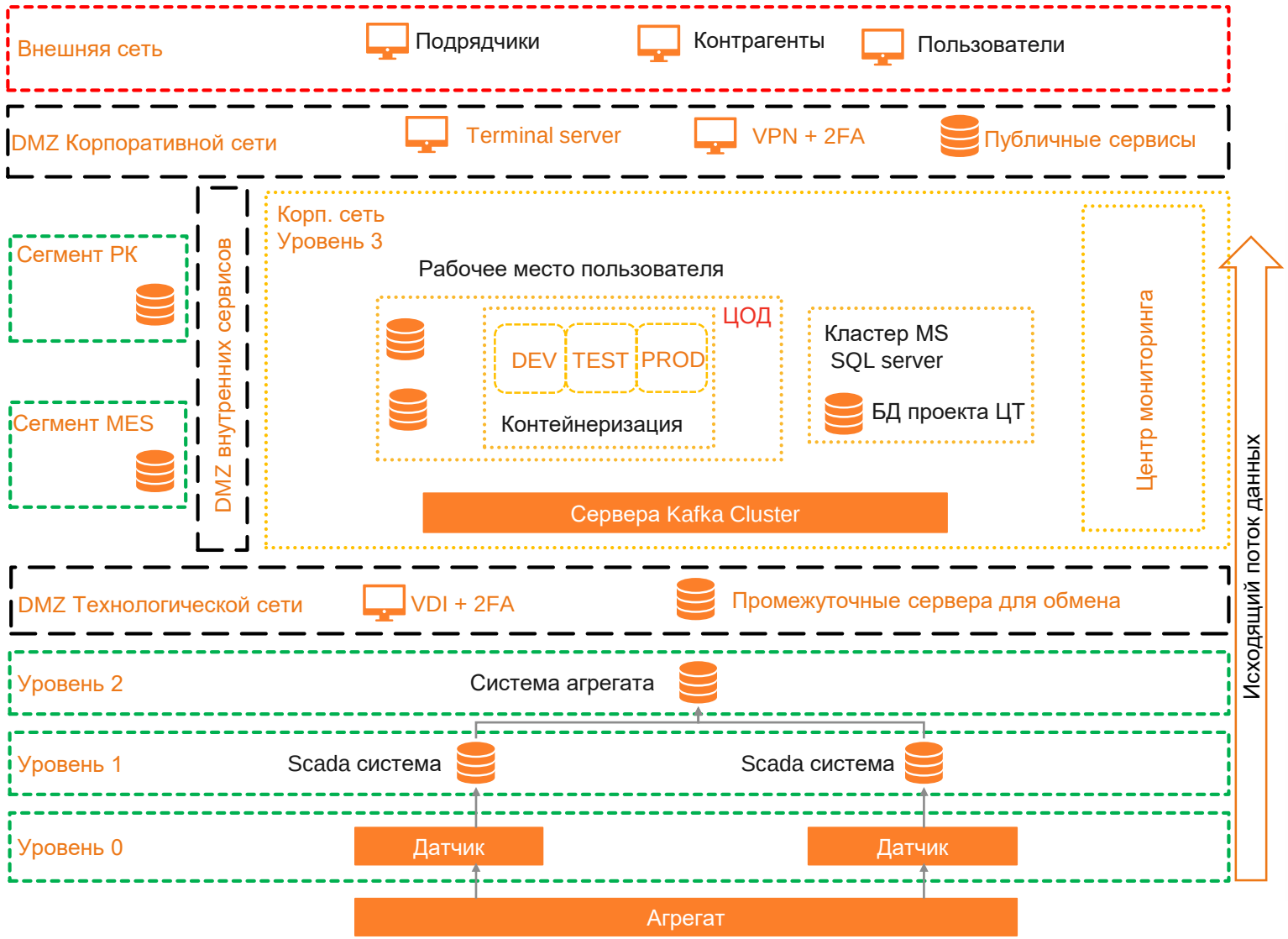
Примеры темпов масштабирования программ ЦТ



Дорожная карта масштабирования цифровой трансформации

Для многих проектов нужны данные из технологической сети

Типовой стандарт разграничения сетей



Ключевые требования

Нет входящих соединений из менее защищенной в более защищенную сеть минуя промежуточные сервера в DMZ

Разрешены исходящие сообщения из более защищенной сети в менее защищенную сеть

Поток данных идет снизу вверх

Центр мониторинга собирает все журналы

Исходный код проектов проверяется на наличие уязвимостей

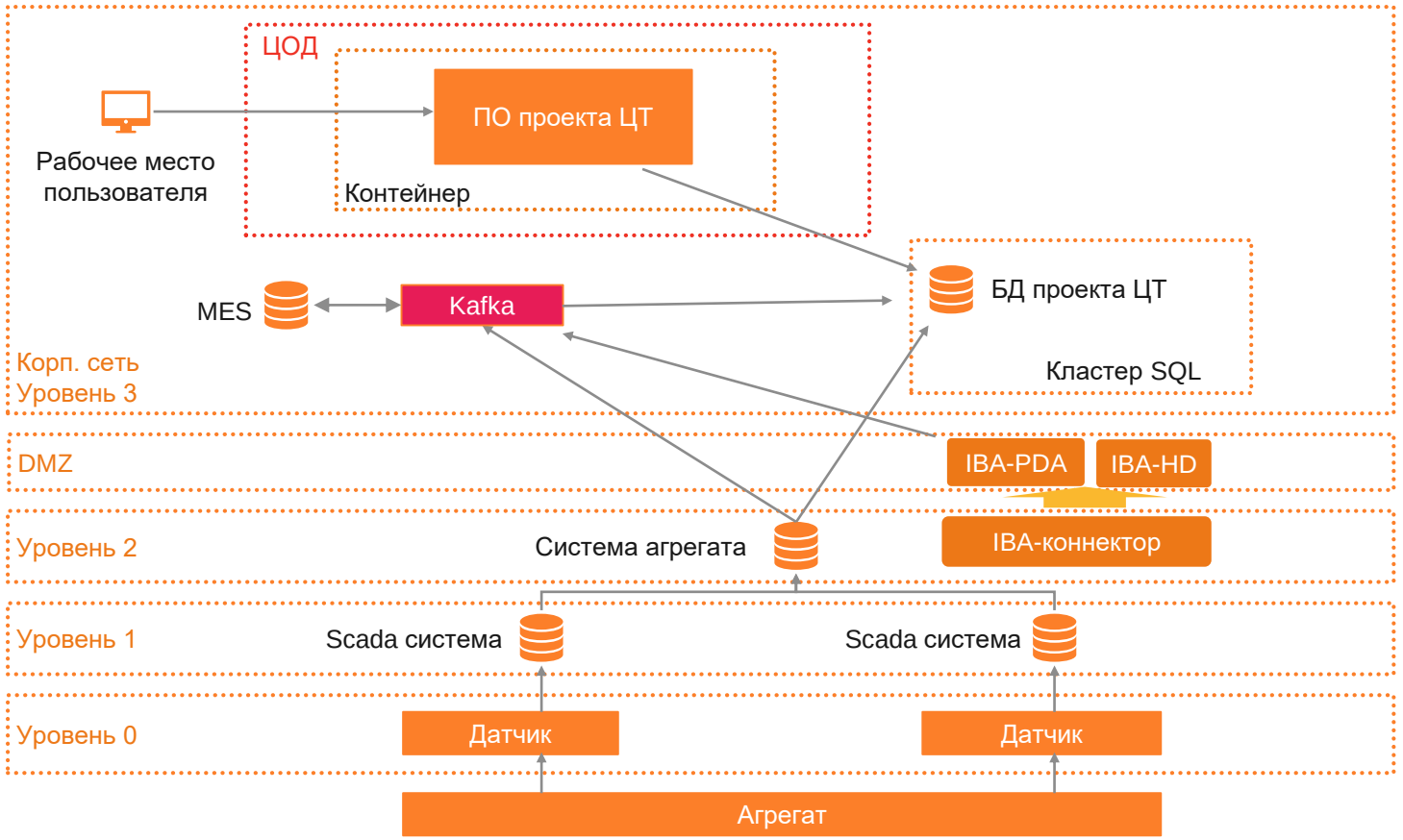
Доступ через VPN при соблюдении требований ИБ и использовании двухфакторной аутентификации (2FA)

Наличие ландшафтов DEV, TEST, PROD

- Защищенная сеть
- Менее защищенная сеть
- Незащищенная сеть

Инфраструктура для передачи данных в Data lake

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



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

Текущая ситуация

ЕВРАЗ

- ИТ динамичная структура.
- Активная цифровизация вносит свои особенности
- Появляются множество цифровых сервисов
- Для разработчиков важна скорость внедрения, а не безопасность
- Бизнесу важно наличие бесперебойного и удобного сервиса

Сделать ИБ частью процессов

ЕВРАЗ

- Общение с бизнесом через Комитет по ИБ
- Включение специалистов ИБ в архитектурные комитеты
- Включение специалистов ИБ в проектные команды
- Интеграция ИБ в DevOps
- Внедрение в компании требований по ИБ
- Проведение аудитов, включая тестирование на проникновение

ЕВРАЗ

Спасибо за внимание

Андрей Нуйкин
CISA, CISM, CRISK
АРСИБ
RuSCADASec Coin #29

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com