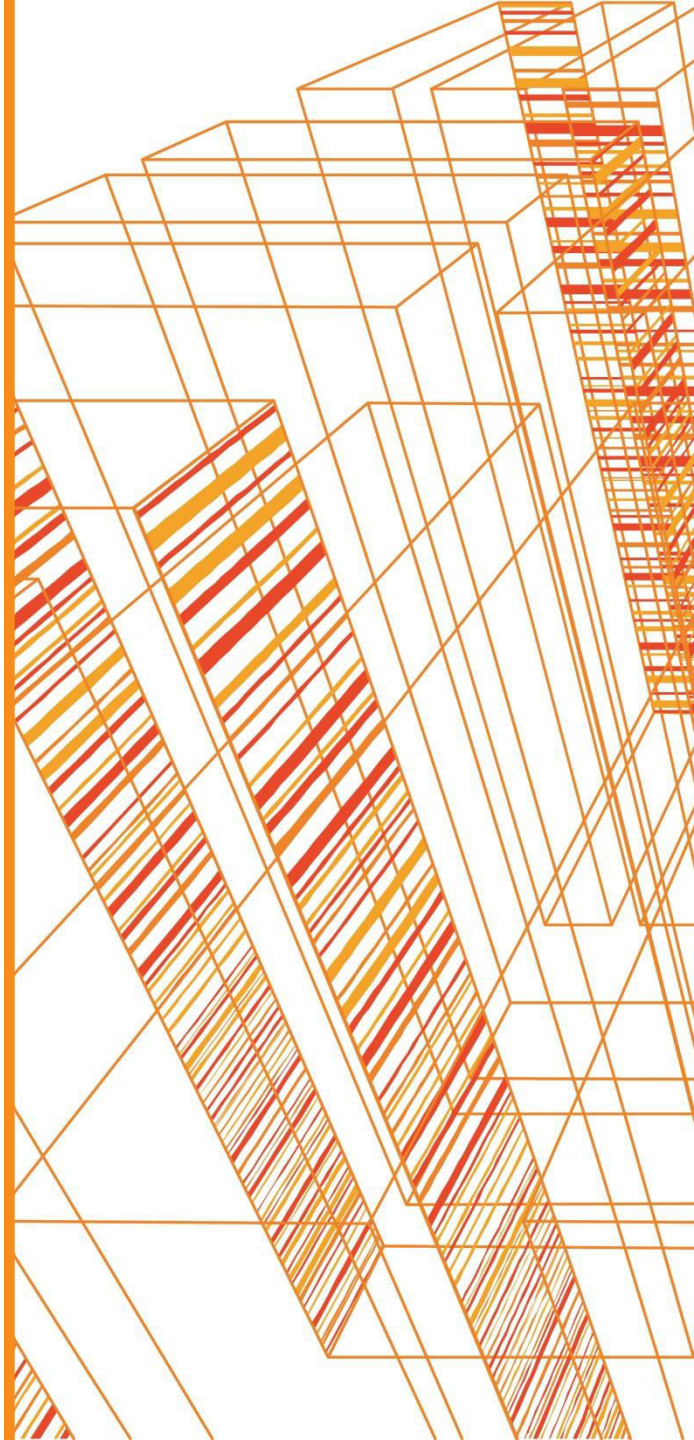
ЕВРАЗ
мы делаем мир сильнее

ТБ Форум 2019

Информационная и компьютерная безопасность объектов промышленности, нефтегаза и энергетики

Опыт разделения корпоративной и технологической сетей

Нуйкин Андрей
ЕВРАЗ



ЕВРАЗ

- Одна из крупнейших вертикально-интегрированных металлургических компаний
- Один из самых низкозатратных производителей стали в мире
- Лидирующий производитель стальной продукции для строительного сектора
- Мировой лидер по производству рельсов
- Один из крупнейших производителей ванадия в мире
- Географически диверсифицированный бизнес

Основные направления деятельности ЕВРАЗа:

•Производство стальной продукции
•Добыча и обогащение железной руды
•Добыча угля
•Производство ванадия и ванадиевых продуктов
•Торговля и логистика

Разделение сетей

Это презентация о пройденных этапах при разделении корпоративной и технологической сети на предприятиях ЕВРАЗ. Частично она основана на предыдущих презентациях, в которых описывались шаги предпринятые в процессе реализации проекта.

Краткое содержание предыдущих частей:

2015 год. Проведение комплексного аудита компании состоящий из аудита процессов по ISO 27000 и тест на проникновение. В части процессов были выявлены красные зоны. Тест на проникновение состоял из трех этапов: 1. Из Интернет в корпоративную сеть 2. Из корпоративной сети в информационные системы 3. Из корпоративной сети в технологическую сеть. В ходе теста был получен доступ к информационным системам, в том числе и в технологических сетях. При этом квалификация взломщика могла быть не высокой. По результатам аудита был разработан план мероприятий по устранению красных зон по ISO 27000 и защите технологической сети.

2016 год. Проведены организационные мероприятия по приведению процессов обеспечения ИБ в соответствии с ISO 27000. С помощью специалистов УЦСБ разработан концептуальный проект по отделению технологической сети от корпоративной сети. По итогам концептуального проектирования проведен пилотный проект на двух цехах. Выявлены потоки информации. Построены демилитаризованные зоны. Организовано безопасное взаимодействие корпоративной и технологической сетей. В конце года проведен повторный аудит с тестом на проникновение. Результат аудита: отсутствие красных зон в части соответствия процессов ISO 27000. Тест на проникновение показал, что проникновение значительно усложнилось. Квалификация взломщика должна быть очень высокой и должно быть множество допущений и сбоев. Проникновение в технологическую сеть не произошло. По результатам аудита принято решение тиражировать решение по защите технологической сети на все цеха всех предприятий. Разработан план внедрения решения.

2017 год. Вирус Petya. Остановка многих компаний по миру. Принято решение значительно ускорить внедрение решения по защите технологических сетей. Доработан концептуальный проект для учета MES систем и т.д. Начался большой проект. Одновременно с защитой технологических сетей начаты еще 5 проектов связанных с повышением уровня информационной безопасности.

Постановка задачи

Предпосылки:

Увеличение инцидентов связанных с промышленными предприятиями.
Результаты проведенного аудита.

Задача:

Разделить технологические и корпоративные сети. Максимально ограничить прямое взаимодействие корпоративной и технологической сетей.

Решение:

Организация DMZ на границах сетей

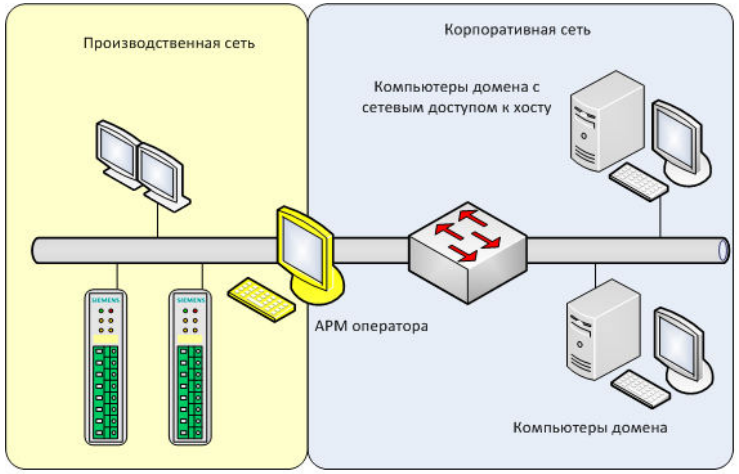
Этапы 2016-2017 гг:

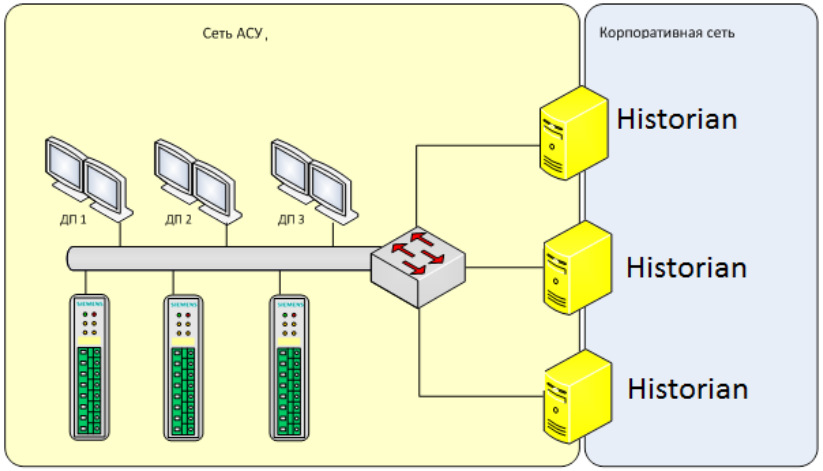
Концептуальное проектирование. Пилотные проекты. Аудит реализованных проектных решений.

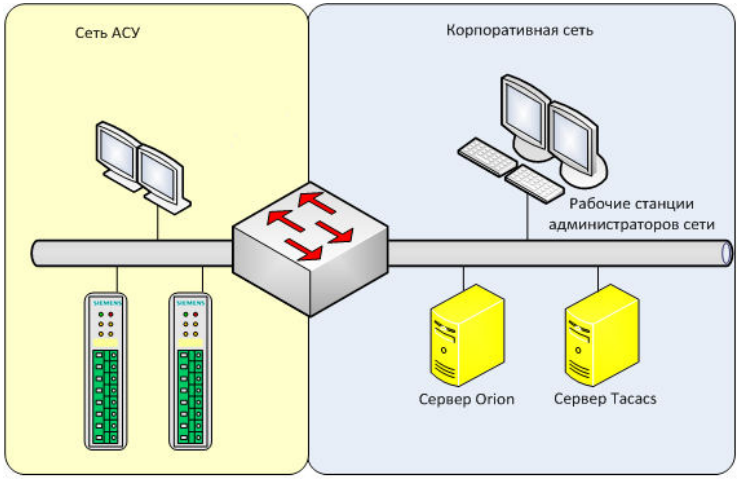
2018 год:

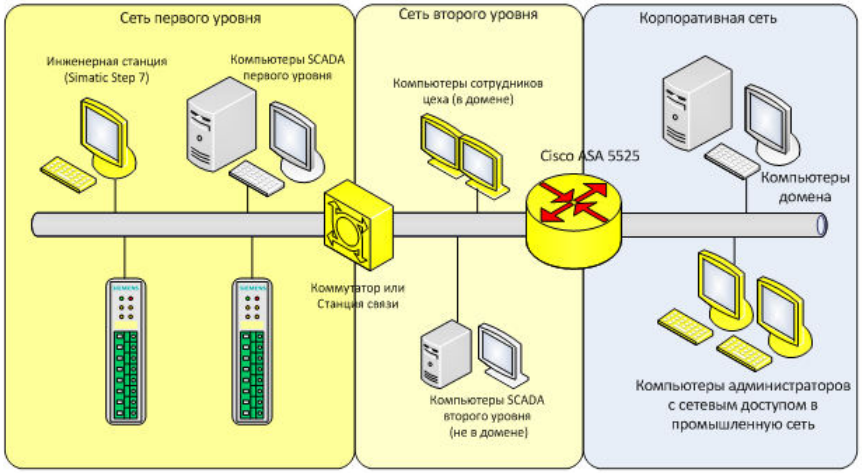
Построение DMZ на всех площадках

Состояние на начало проекта









Что нужно сделать в ходе реализации

- Четко понять какое взаимодействие происходит между технологической и корпоративной сетью

- Полностью отделить технологическую сеть от корпоративной. Все что касается АСУТП должно быть в АСУТП
  - Все, что общается с корпоративной сетью размещаем в DMZ
  - Выделяем административную подсеть

- Обеспечить отказоустойчивость.
  - Разрыв связи с корпоративной сетью не должен сказываться на производстве.

Ход проекта

Концептуальное проектирование и пилотный проект

Срок проекта: февраль 2016 - декабрь 2016 года

Основной исполнитель: ООО «ЕвразТехника» и УЦСБ

Масштабирование проекта на весь холдинг

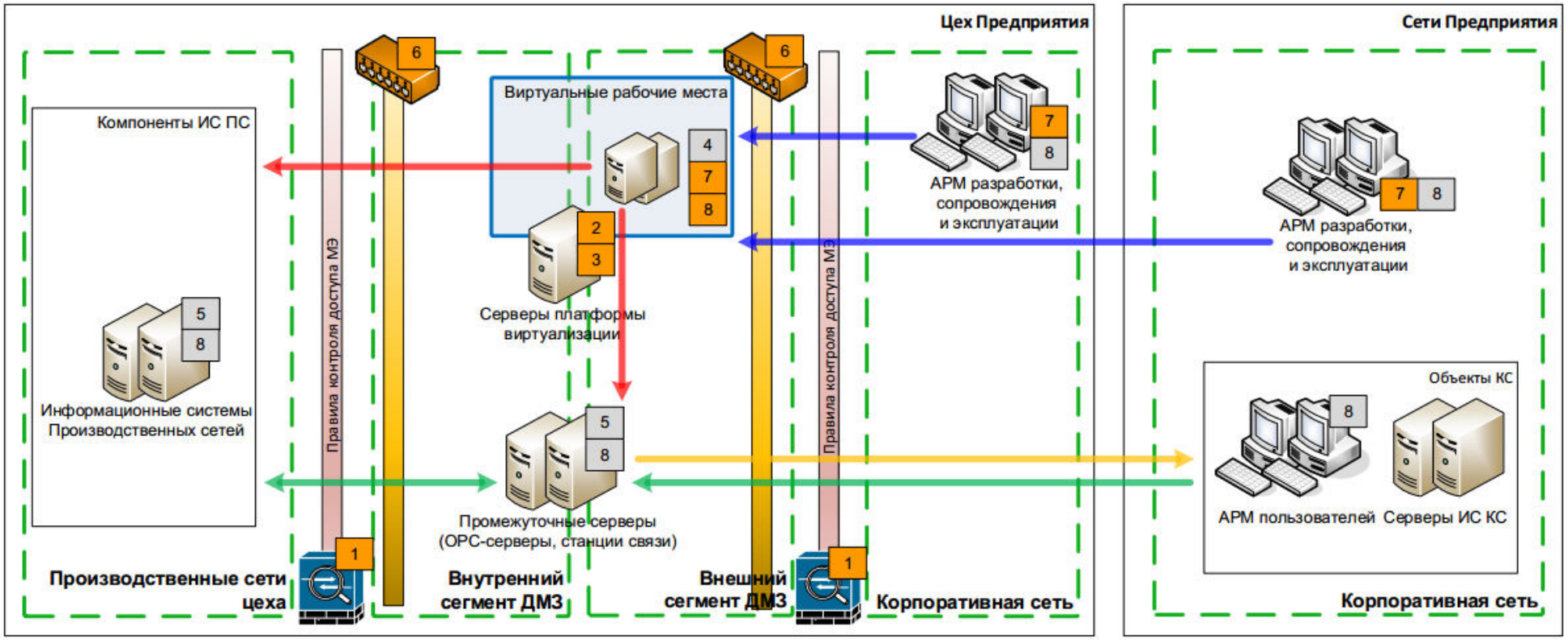
Срок проекта: октябрь 2017 - декабрь 2018 года

Основной исполнитель: ООО «ЕвразТехника»

Основные вопросы возникшие в ходе масштабирования:

- Какое количество DMZ строить?
- Что делать с MES системами?
- Резервирование горячее/холодное?
- Хватит ли ресурсов?

Концепция разделения сетей



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

Выбор варианта организации DMZ

Одна DMZ на всех

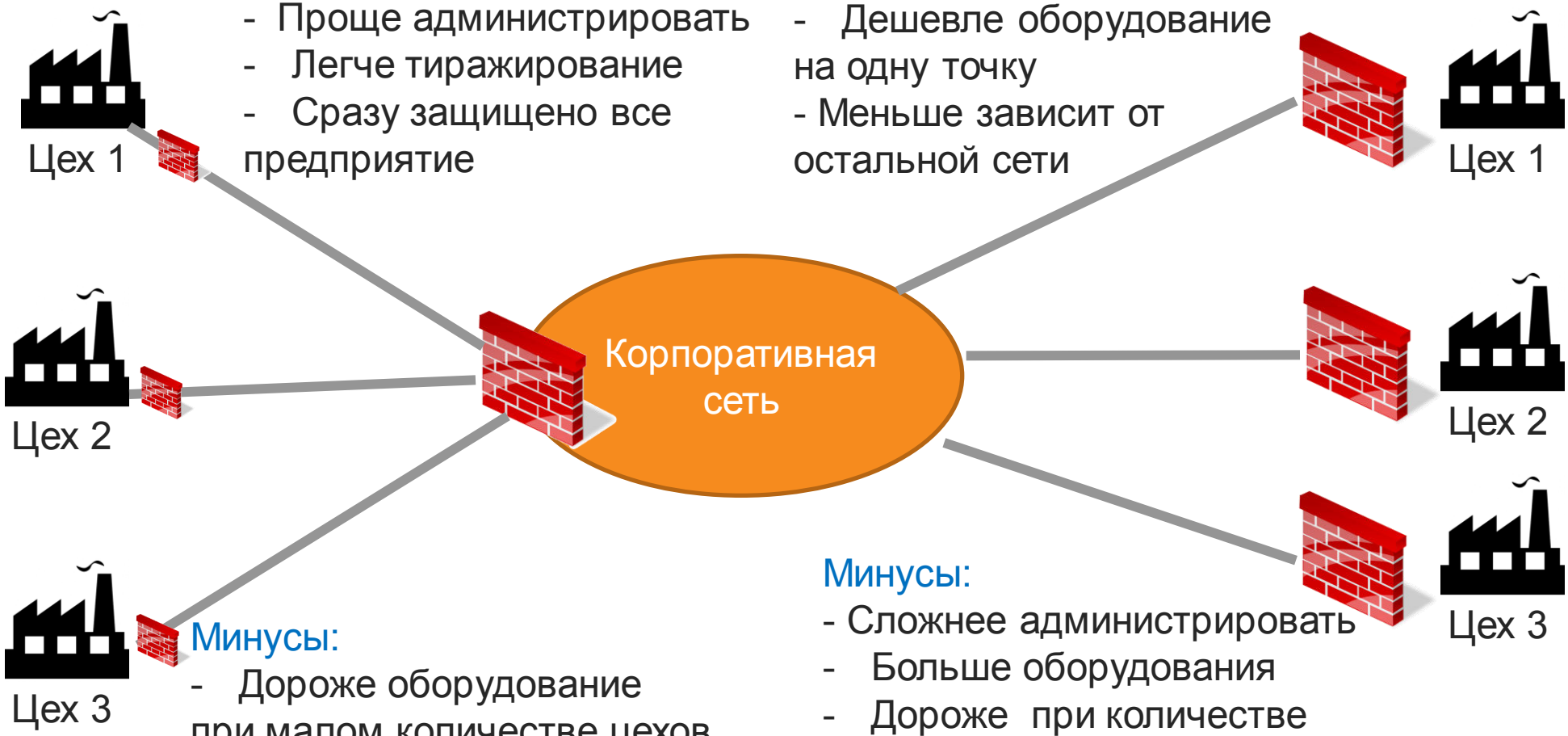
Плюсы:
- Проще администрировать
- Легче тиражирование
- Сразу защищено все предприятие

Минусы:
- Дороже оборудование при малом количестве цехов
- Одна точка отказа
- Зависит от остальной сети

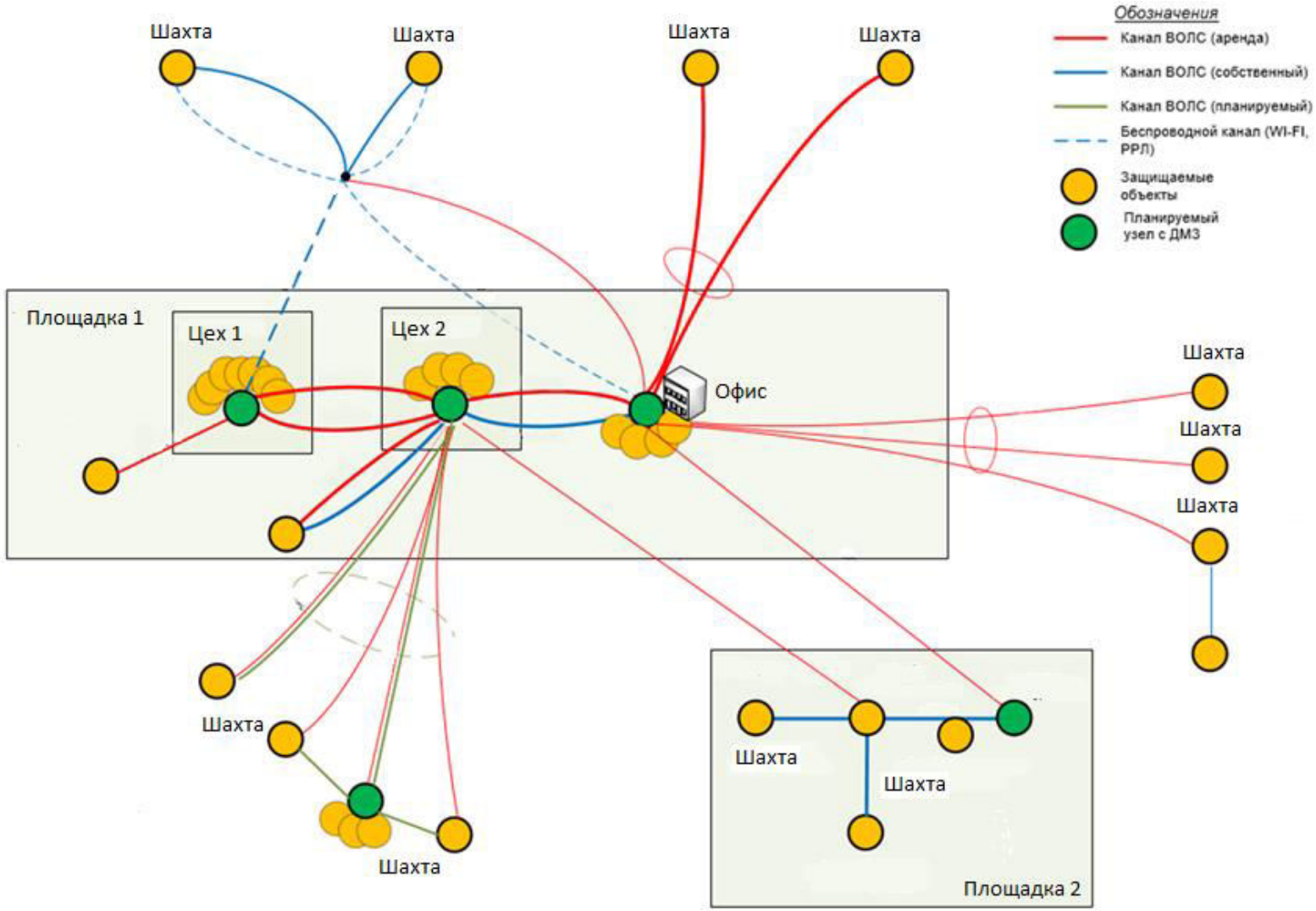
Каждому своя DMZ

Плюсы:
- Дешевле оборудование на одну точку
- Меньше зависит от остальной сети

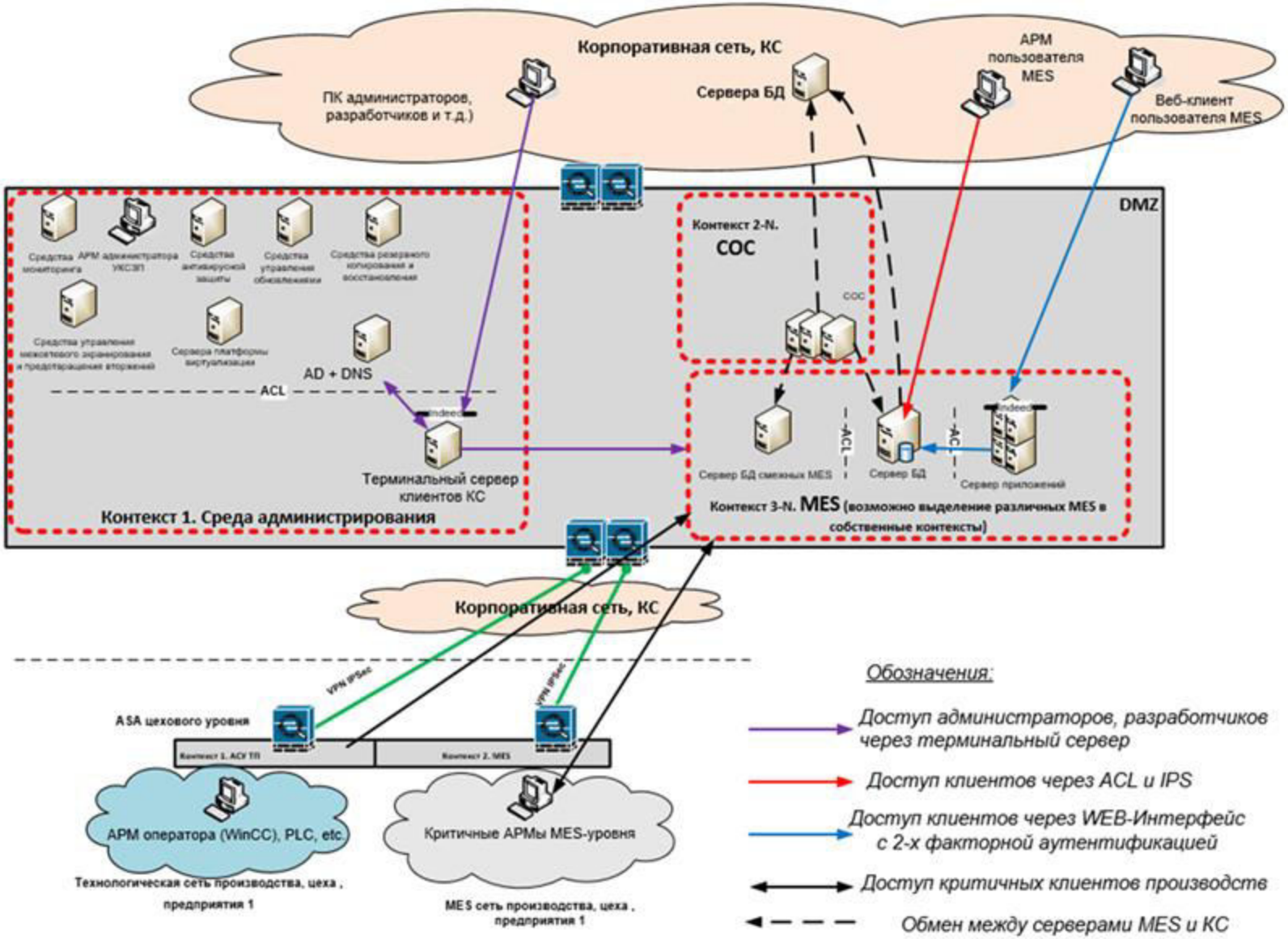
Минусы:
- Сложнее администрировать
- Больше оборудования
- Дороже при количестве DMZ больше 3
- Защищается по мере создания отдельных DMZ



Вариант организации DMZ для крупного предприятия



Вариант защиты MES



Результаты

Основные достижения:

- Построено несколько крупных DMZ
- К DMZ подключены критические производства
- Реализованы меры по защите MES систем

Сложности при реализации проекта:

- Территориальная распределенность промышленных площадок.
- Наличие старых АСУТП. Сложности с их реконфигурацией для работы через DMZ
- Пока нет возможности создать универсальный вариант защиты для MES систем.
- Не все продукты работают так, как заявлено
- Большой объем работ. Необходимость привлечения внешних подрядчиков.

Вопросы?

Андрей Нуйкин
+7 916 124 6287
Andrey.nuykin@evraz.com