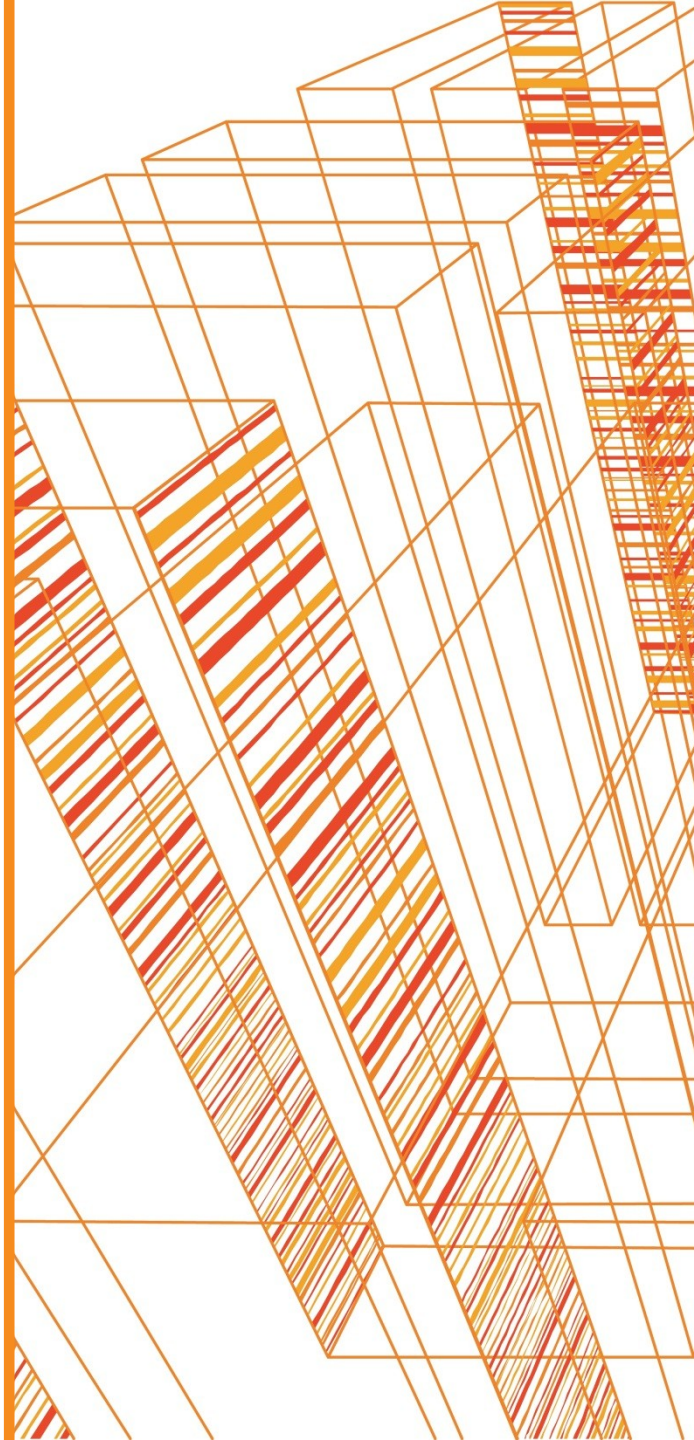
ЕВРАЗ
мы делаем мир сильнее

Безопасность АСУТП

Разделение корпоративной и технологических сетей

Нуйкин Андрей
ЕВРАЗ



Что такое 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

Как меняется ситуация?

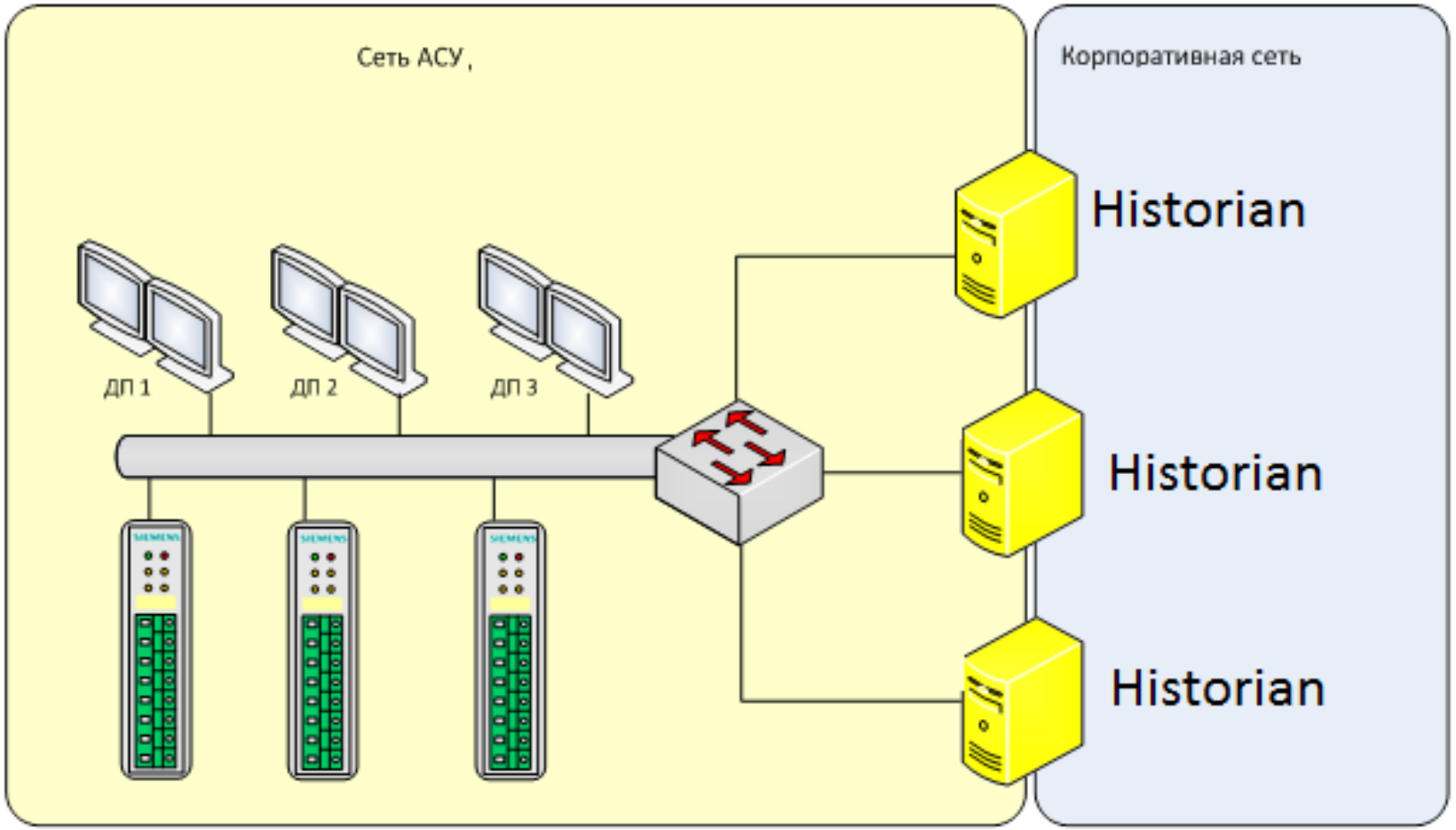
- Все большее использование Ethernet/IP в технологических сетях
- Все больше стирается грань между технологическими и корпоративными сетями
- АСУТП строилась давно. Первоначально вопросы безопасности не стояли так остро
- Постоянное появление новых угроз для технологических сетей
- Появление нормативных актов регламентирующих защиту АСУТП

Предпослыки

- В 2015 году проведен аудит текущего состояния. В ходе аудита проведен тест на проникновение, в том числе и технологической сети.
- В результате теста на проникновение получена информация по векторам атаки и уязвимостям.
  - Основной вектор атаки администраторы и разработчики, имеющие доступ из корпоративной сети к ресурсам технологической сети

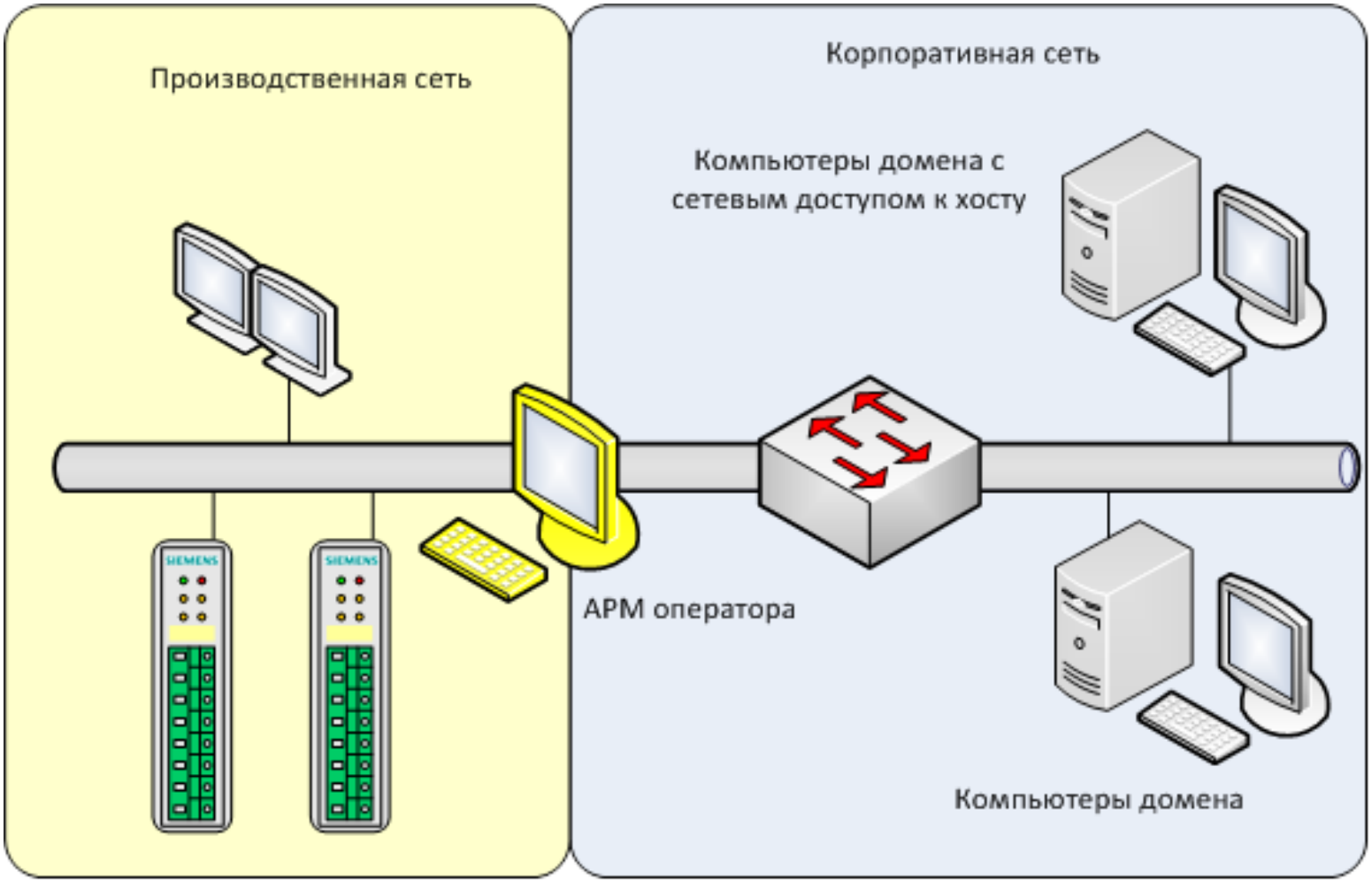
Варианты взаимодействия

Компьютер с двумя сетевыми картами



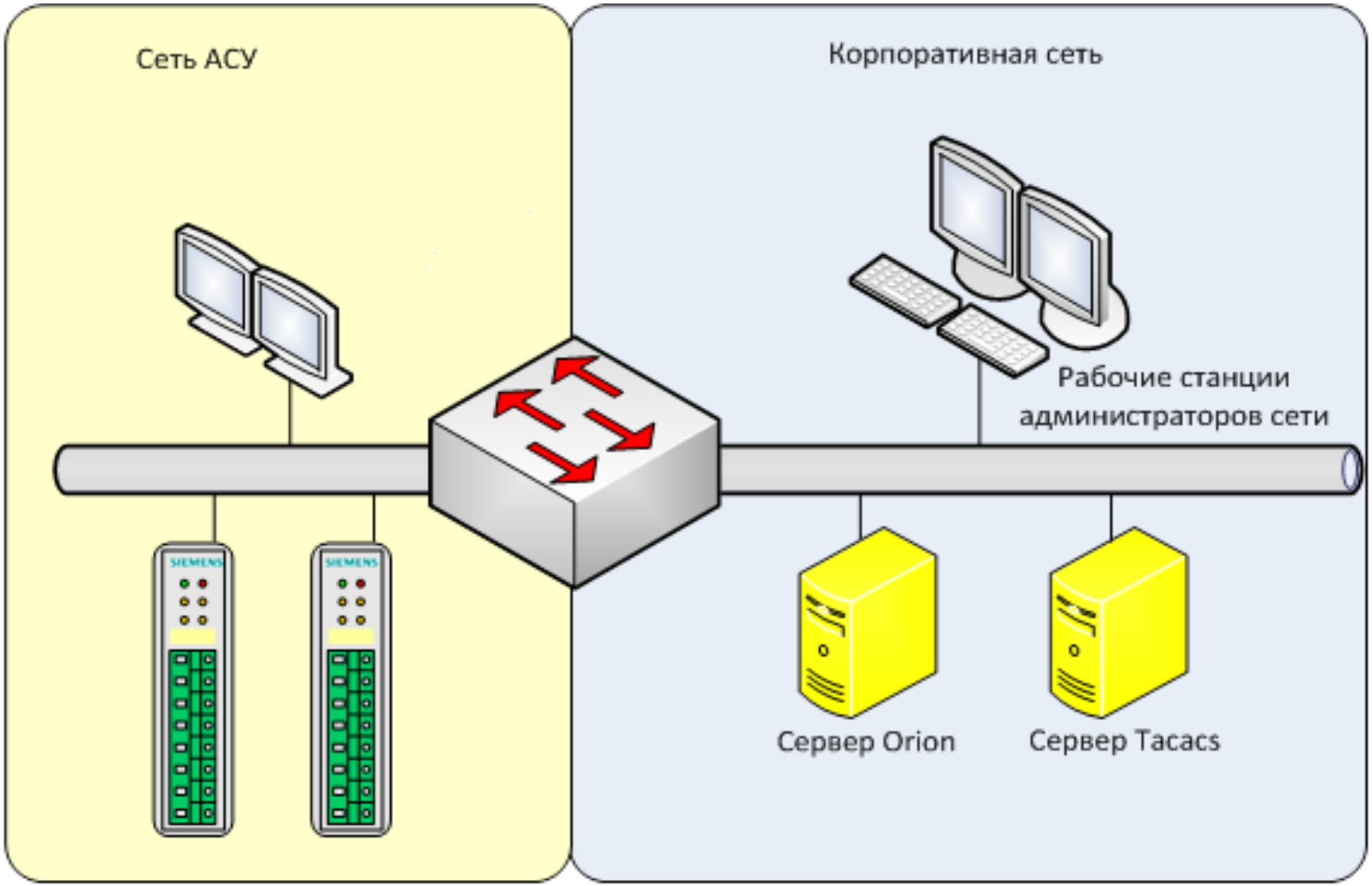
Варианты взаимодействия

Компьютер с двумя сетевыми картами под защитой маршрутизатора с ACL



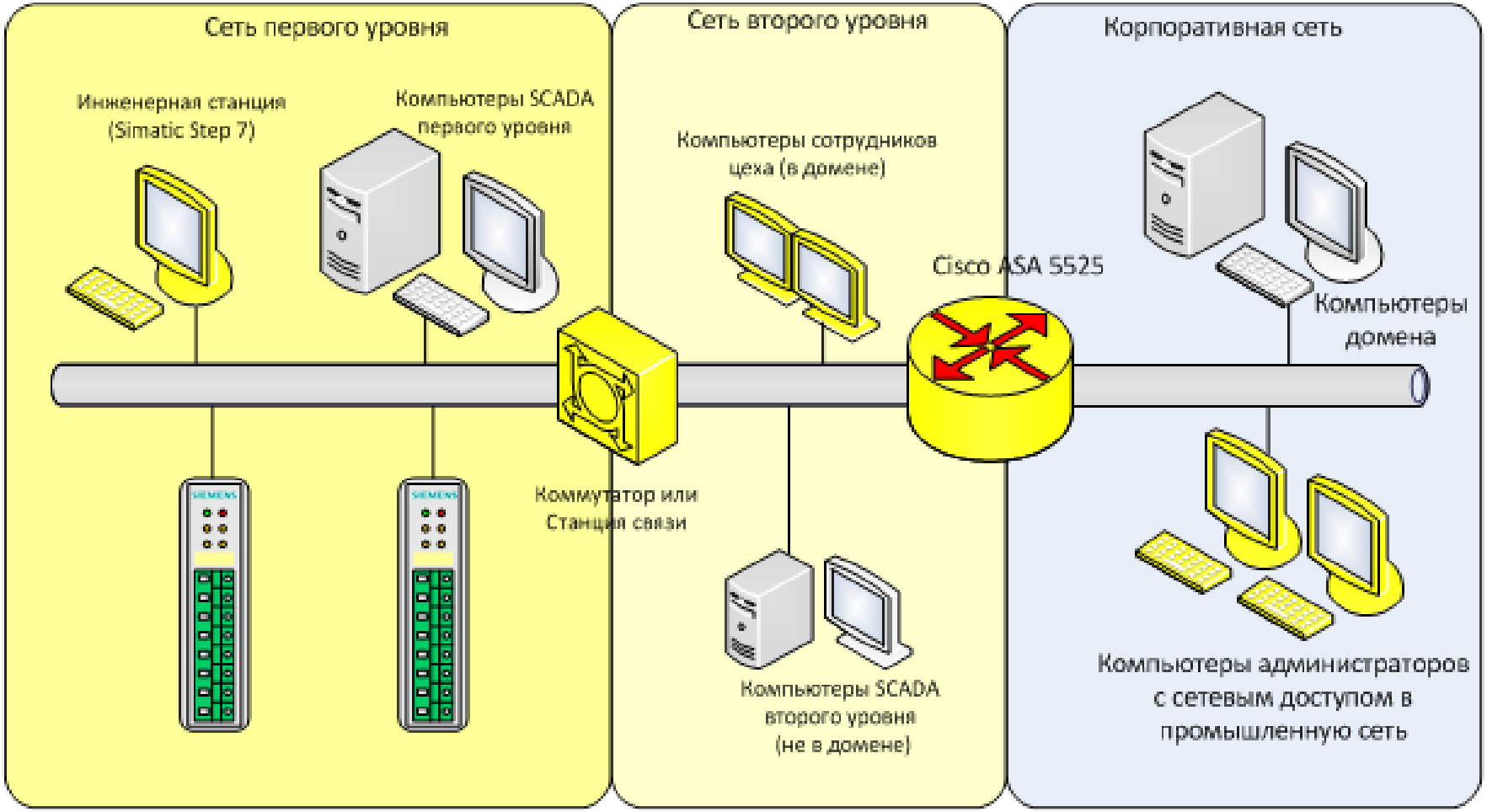
Варианты взаимодействия

Через маршрутизатор с ACL



Варианты взаимодействия

Через межсетевой экран



Недостатки схем взаимодействия

В случае использования компьютера с двумя сетевыми картами:

- Компрометация компьютера связи предоставляет доступ к технологической сети

В случае использования маршрутизатора/межсетевого экрана:

- Компрометация компьютера администратора позволяет получить доступ к технологической сети
- Компрометация маршрутизатора/межсетевого экрана позволяет получить доступ к технологической сети

Существует множество прямых взаимодействий между корпоративными и технологическими серверами:

- Компрометация корпоративного сервера открывает доступ к технологическому сегменту

Что делать?

Задача:

- Максимально ограничить прямое взаимодействие корпоративной и технологической сетей.
- Четко разделить корпоративные и технологические сети

Концепция защиты:

- Организация DMZ на границе сетей
- Организация однонаправленной передачи данных из АСУТП в корпоративную сеть
- Размещение компьютеров необходимых для работы АСУТП в производственной подсети
- Работа администраторов из корпоративной сети через терминальный сервер в DMZ

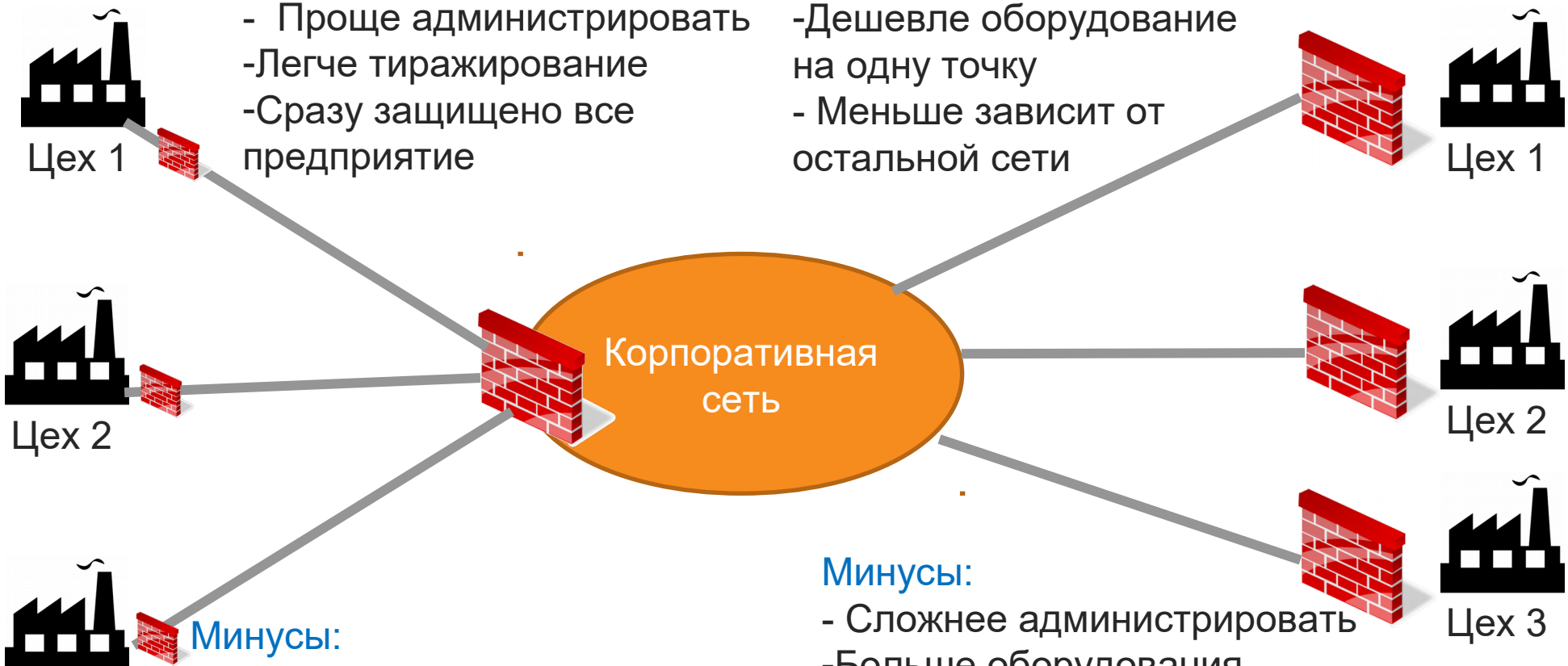
Варианты реализации защиты

Одна DMZ на всех

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

Каждому своя DMZ

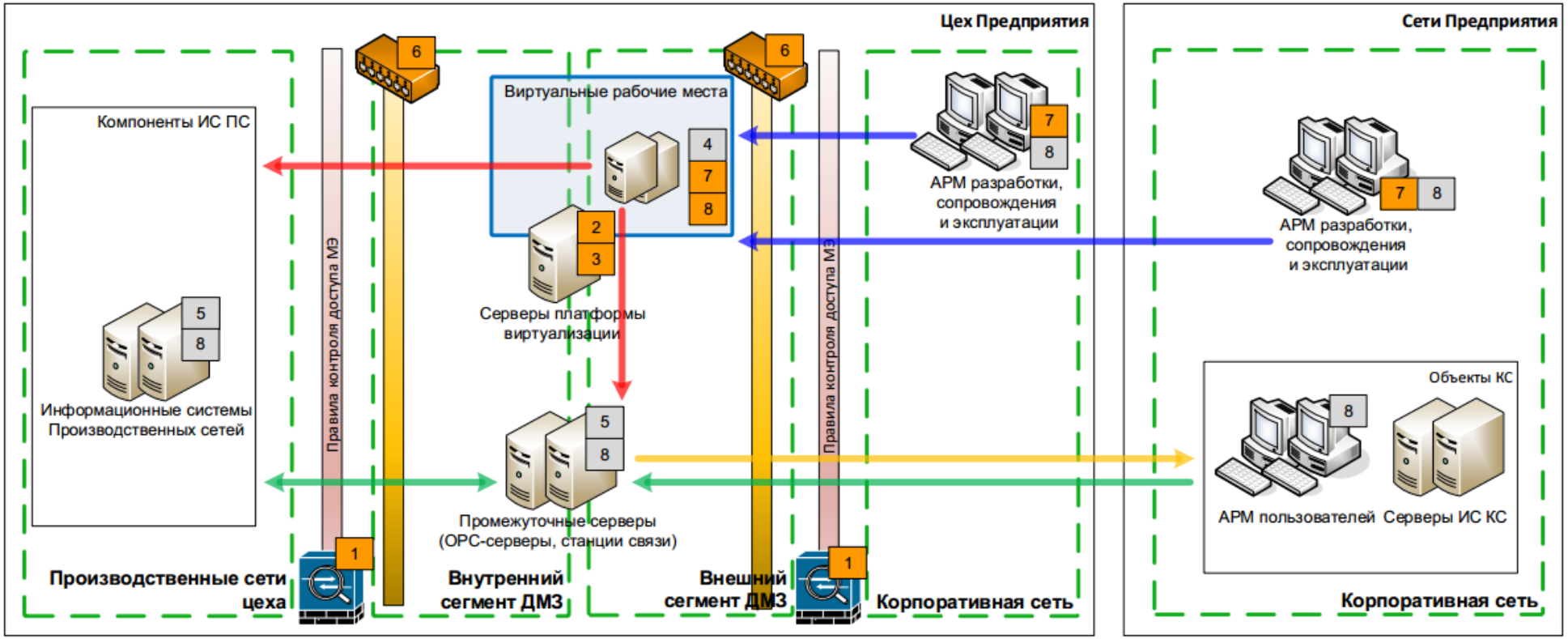
Плюсы:
-Дешевле оборудование на одну точку
- Меньше зависит от остальной сети



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

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

Концептуальная модель 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

Построение пилотной DMZ

Начало проекта 01.2016
Окончание проекта 11.2016

Оборудование
- МЭ - Cisco ASA
- IDS - Cisco FireSight
- VDS для администраторов/разработчиков – VMWare
- Двухфакторная аутентификация – SafeNet + eToken.
- Обновление ОС - WSUS
- Антивирус корпоративный
- Сканирование на уязвимости - OpenVas

Подготовка концептуального проекта интегратором
- Время подготовки 4 мес.
- Трудозатраты площадок – 30 ч/дн.

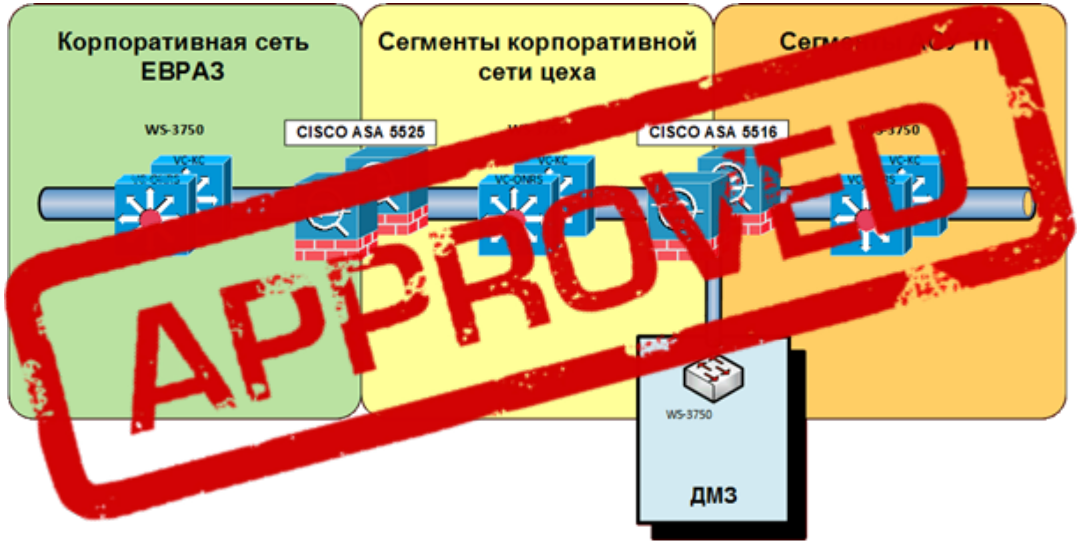
Для реализации проекта были выбраны два цеха на разных площадках
- Время реализации – 6 мес.
- Трудозатраты на реализацию – 180 ч/дн и 169 ч/дн

Что сделано в рамках пилота

- Установлены потоки информации между технологической и корпоративной сетью
- Разработан концептуальный проект разделения технологической и корпоративной сетей
- На границе сетей двух цехов построена пилотная DMZ. В нее вынесены серверы для организации взаимодействия (обновления АВЗ, WSUS и т.д.), виртуальные компьютеры для работы администраторов и разработчиков из корпоративной сети и т.д.
- Технологическая сеть максимально отделена от корпоративной. Все что касается АСУТП - вынесено в сеть АСУТП. Взаимодействие осуществляется через DMZ.
- Ограничено использование протоколов только теми, которые необходимы для работы систем/сетей
- Блокированы сетевые порты, не используемые во взаимодействии систем/сетей
- Работа администраторов и разработчиков с ресурсами в технологической сети производится через виртуальные машины с использованием двухфакторной аутентификации

Результат

- По результатам проекта был проведен аудит информационной безопасности. В ходе аудита проводился тест на проникновение.
- Для аудита привлекался аудитор из BIG4.
- Проверялся доступ из Интернет и корпоративной сети.
- Методика BlackBox и GreyBox.
- Аудит подтвердил безопасность реализованной схемы.
- Принято решение о внедрении решения



Следующие шаги

- Реализация защиты для всех цехов предприятий до конца 2018 г.
  - Построение нескольких DMZ на каждом предприятии. DMZ строятся по производственному или территориальному признаку.
- Углубление в АСУТП.
  - Антивирусная защита, мониторинг, использование принципа наименьших полномочий

Некоторые вопросы возникшие в процессе масштабирования:

•Что делать с MES системами?
•Как связать территориально удаленные цеха с DMZ?
•Что делать с системами, которые не поддерживают работу через DMZ?

Вопросы?

Андрей Нуйкин
Andrey.nuykin@evraz.com