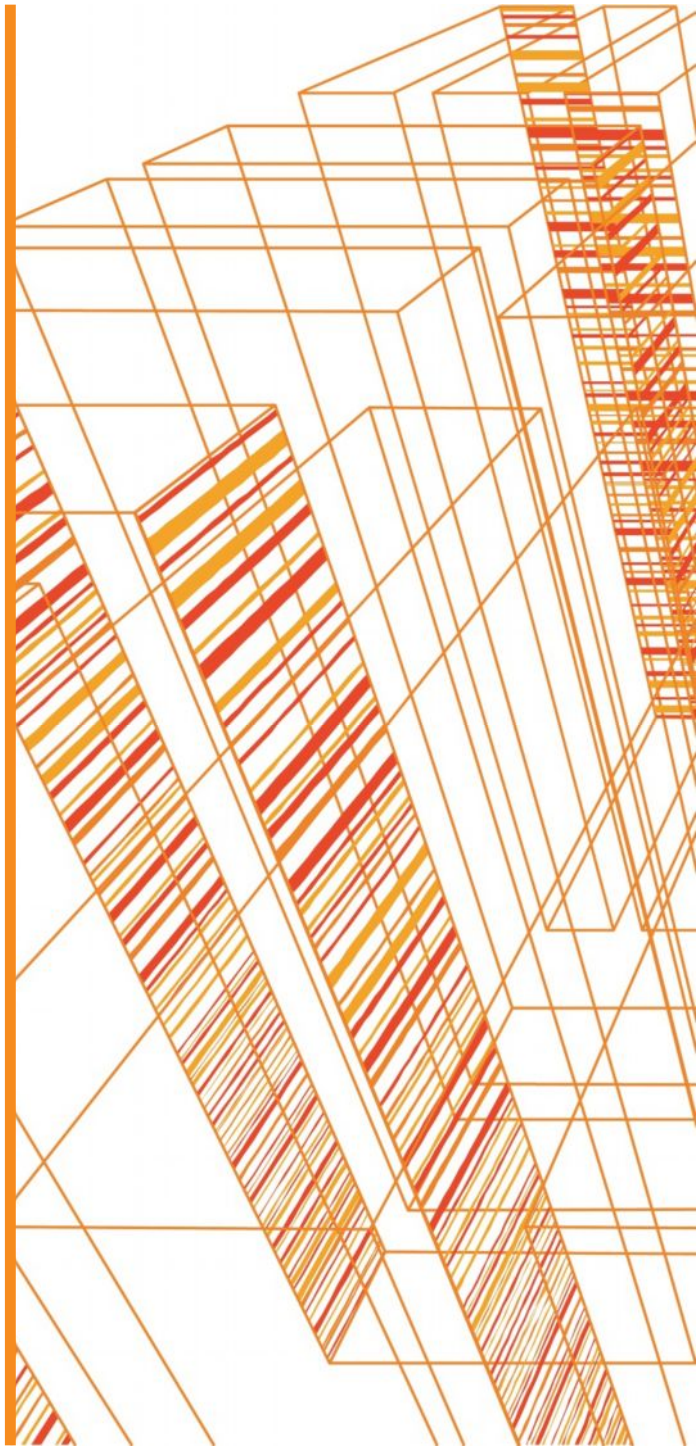
ЕВРАЗ
мы делаем мир сильнее



Безопасность АСУТП

- Разделение корпоративной и технологических сетей

Нуйкин Андрей
CISA, CISM
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:

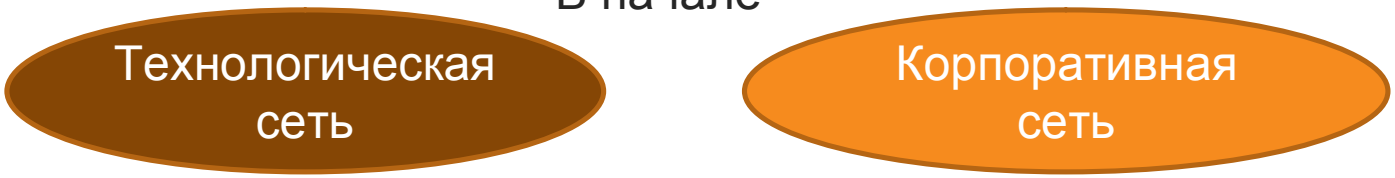
•Производство стальной продукции
•Добыча и обогащение железной руды
•Добыча угля
•Производство ванадия и ванадиевых продуктов
•Торговля и логистика

Как меняется ситуация?

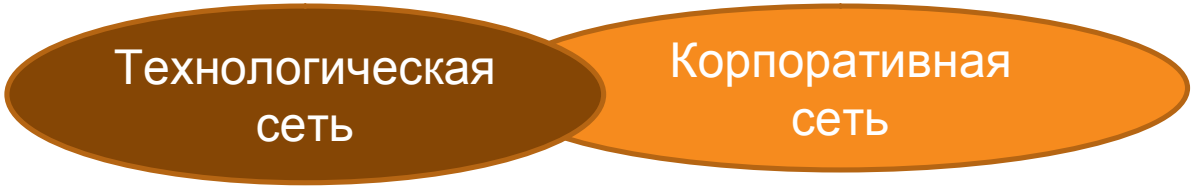
- Все большее использование Ethernet/IP в технологических сетях
- Все больше стирается грань между технологическими и корпоративными сетями
- Первоначально вопросы безопасности не стояли так остро

История взаимодействие АСУТП и корпоративных сетей

В начале



нулевые года

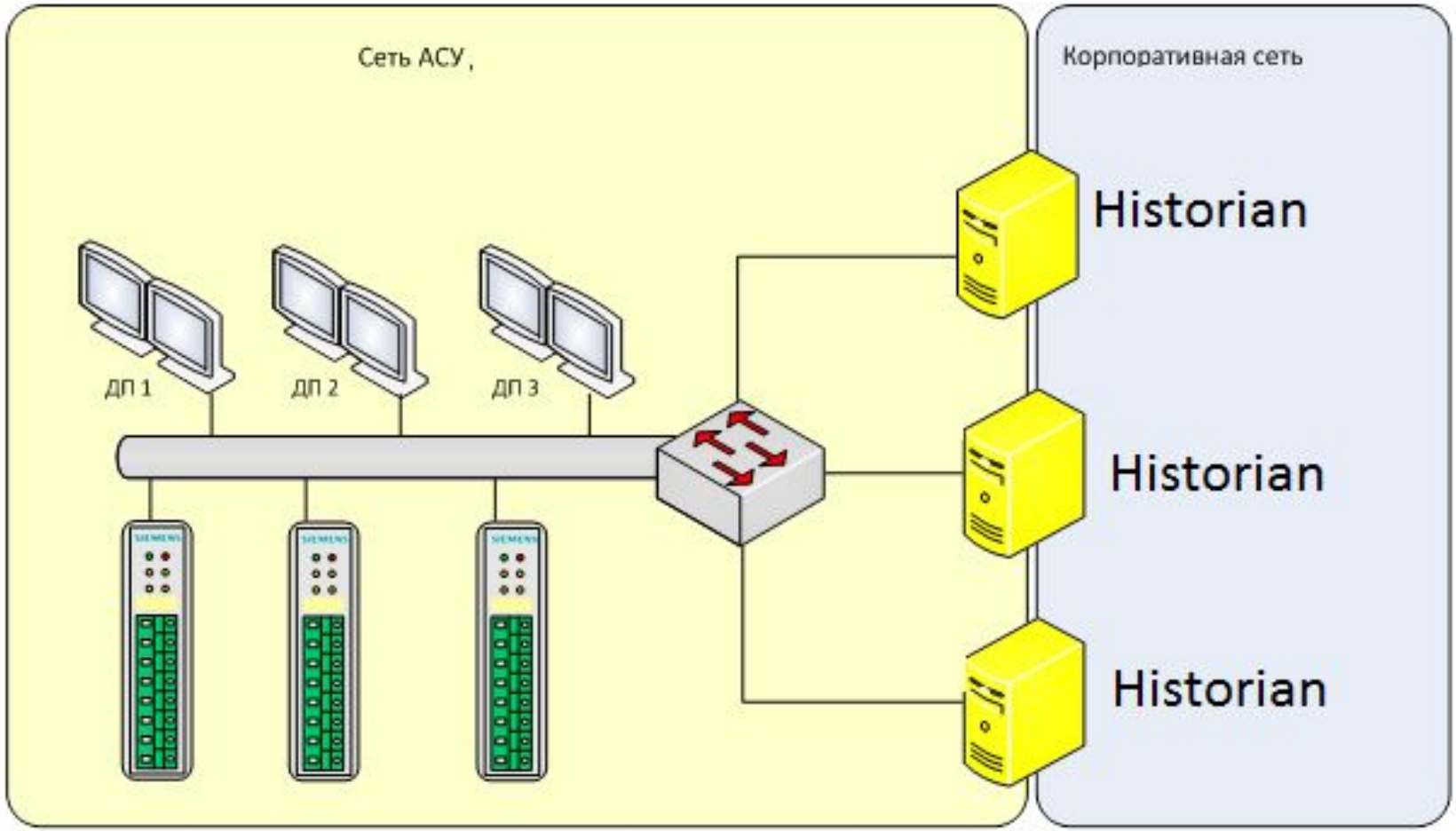


Бывает и такое…

Эталон

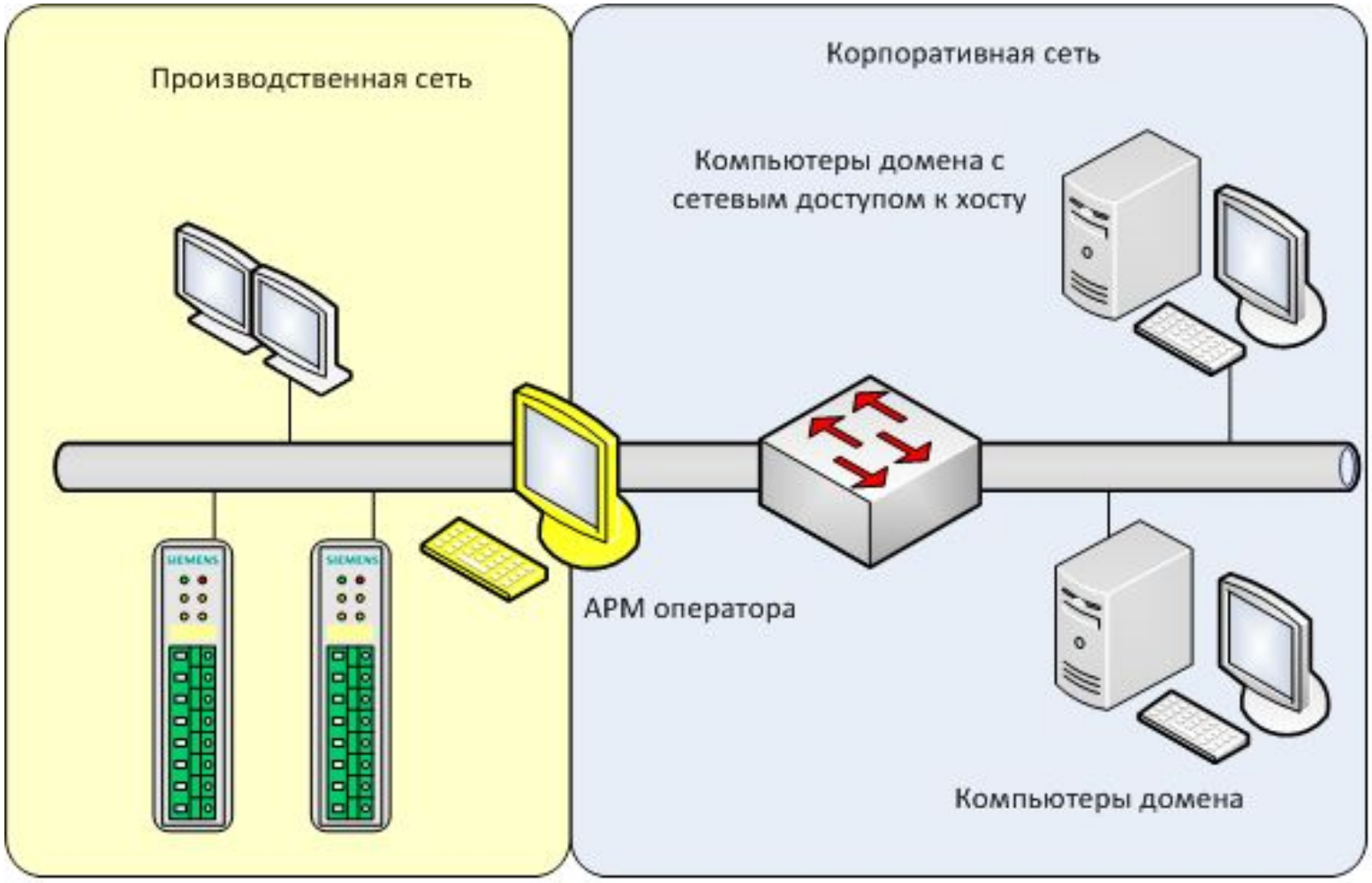
Варианты взаимодействия

Компьютер с двумя сетевыми картами



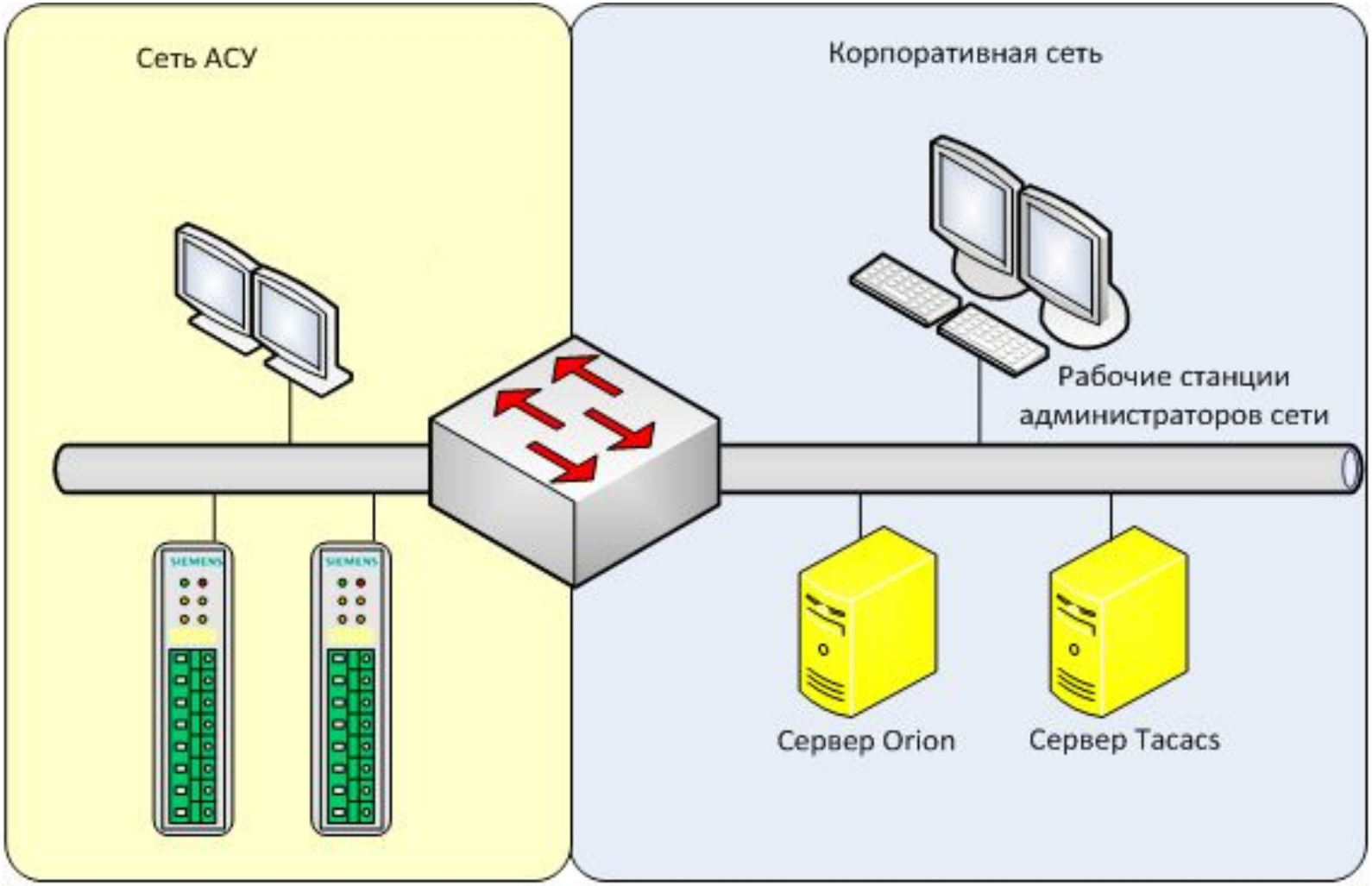
Варианты взаимодействия

Компьютер с двумя сетевыми картами под защитой маршрутизатора с ACL



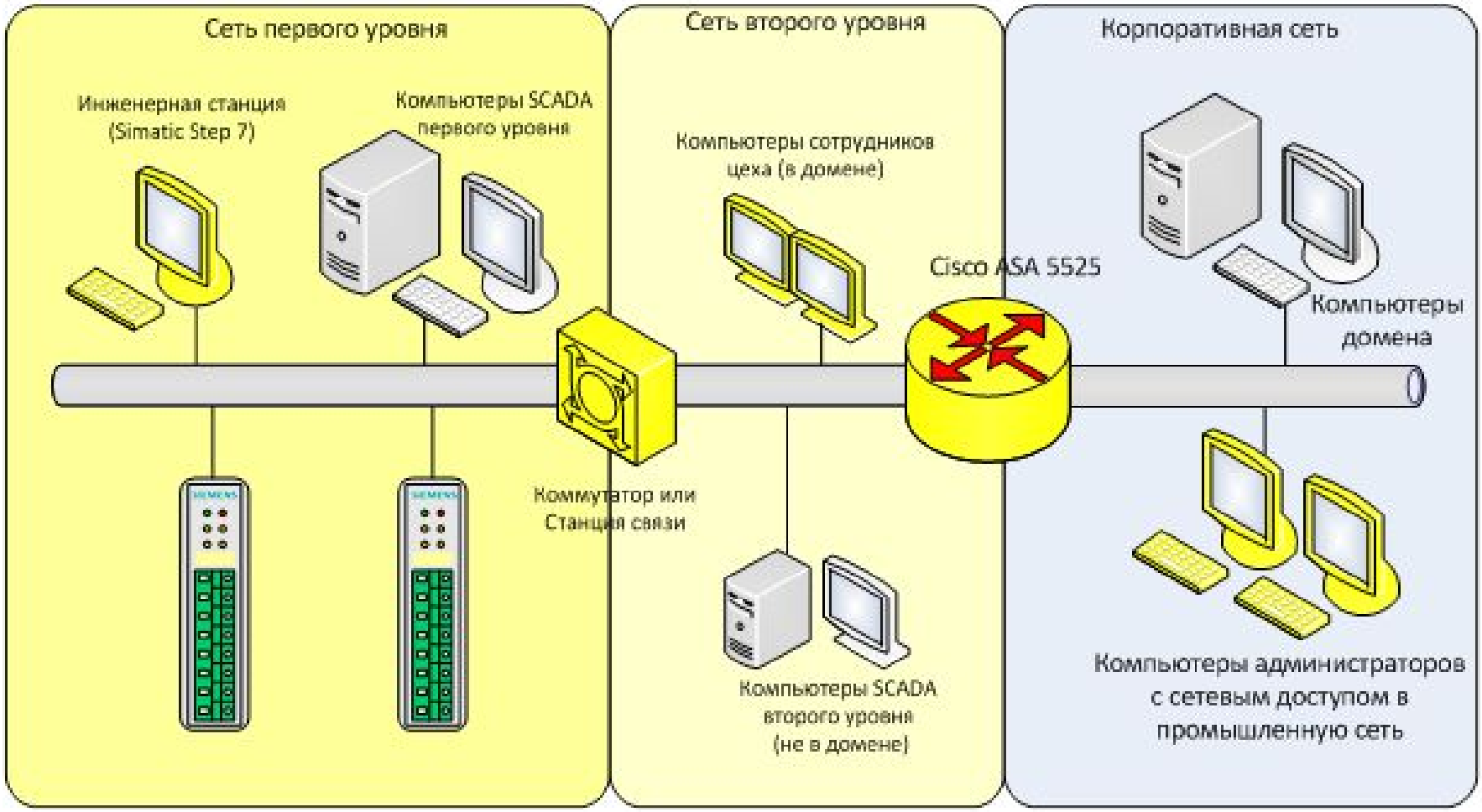
Варианты взаимодействия

Через маршрутизатор с ACL



Варианты взаимодействия

Через межсетевой экран



В случае использования компьютера с двумя сетевыми картами:

•Компрометация компьютера предоставляет доступ к технологической сети

В случае использования маршрутизатора/межсетевого экрана:

•Компрометация компьютера администратора позволяет получить доступ к технологической сети

Варианты защиты

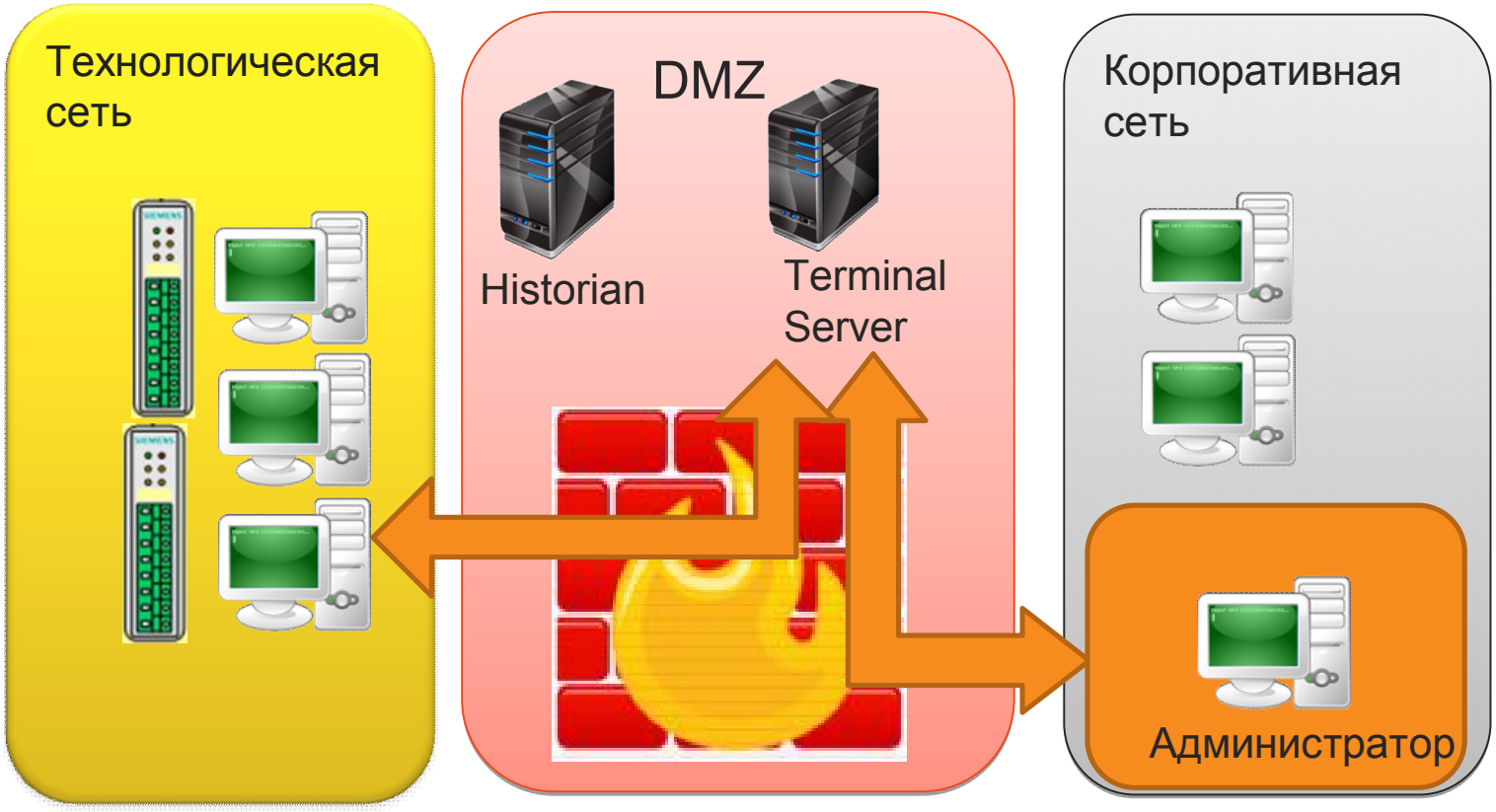
Задача: Исключить прямое взаимодействие корпоративной и технологической сетей

Варианты:

- Организация DMZ
- Организация однонаправленной передачи данных из АСУТП в корпоративную сеть
- Размещение компьютеров администраторов в подсети АСУТП
- Работа администраторов из корпоративной сети через терминальный сервер в DMZ
- Выделение подсети администраторов. Исключение одновременной работы в Интернет.

Схема организации взаимодействия

Администрирование из корпоративной сети



Что делать?

- Четко понимать какое взаимодействие происходит между технологической и корпоративной сетью
  - Из технологической в корпоративную (DataDiode и DMZ)
  - Из корпоративной в технологическую (TerminalServer и DMZ)
  - Удаленный доступ (TerminalServer и DMZ)
- Полностью отделять технологическую сеть от корпоративной. Все что касается АСУТП должно быть в АСУТП (AD, VPN и т.д.).
- Разрыв связи с корпоративной сетью не должен сказываться на производстве.

Соответственно:

- Строить DMZ на границе технологической и корпоративной сети, для исключения прямого взаимодействие между корпоративной и технологической сетями
- Все, что общается с корпоративной сетью выносить в DMZ
- Выделять административную подсеть. Ограничивать выход в Интернет из административной подсети
- Для администраторов в DMZ устанавливать VDI машины

Что делать?

- Разделить технологические и корпоративные сети с помощью межсетевых экранов и DMZ
- Максимально ограничить прямое взаимодействие сетей
- Проектировать технологические сети с учетом обеспечения безопасности кабельной инфраструктуры
- Ограничить использование протоколов только теми, которые необходимы для работы систем/сетей
- Блокировать сетевые порты, не используемые во взаимодействии систем/сетей
- Использовать управляемое сетевое оборудование
- Вести мониторинг событий и инцидентов
- Ограничить использование беспроводных сетей
- Разграничить доступ к оборудованию и портам управления
- Проводить обучение персонала по вопросам ИБ

Вопросы?

Андрей Нуйкин
Andrey.nuykin@evraz.com