Защита критической инфраструктуры

Практические аспекты реализации 187-ФЗ на крупных промышленных предприятиях

Игорь Мартыненко

Главный архитектор по защите КИИ

Igor.Martynenko@Softline.com

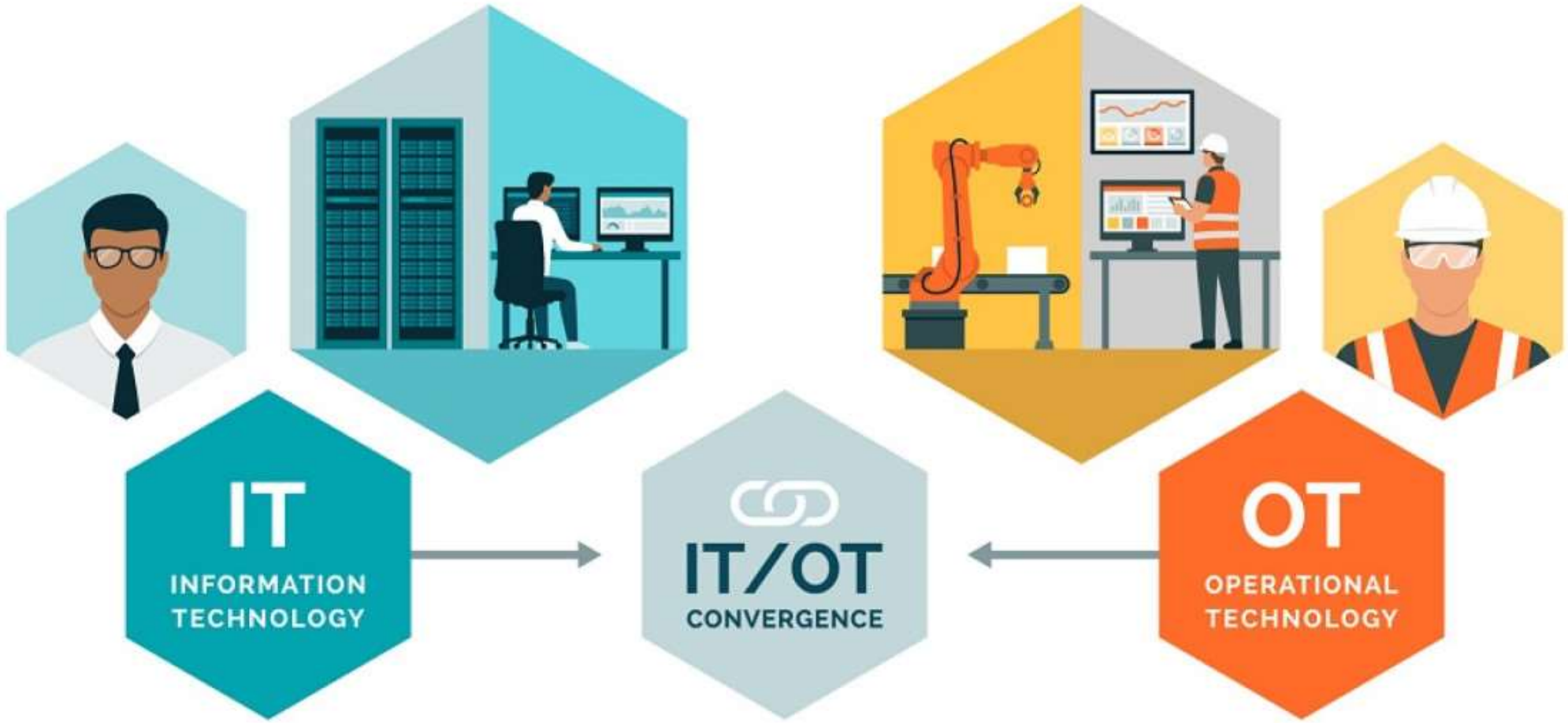
ИТ vs АСУ ТП (IT vs OT)

Подходы к ИБ

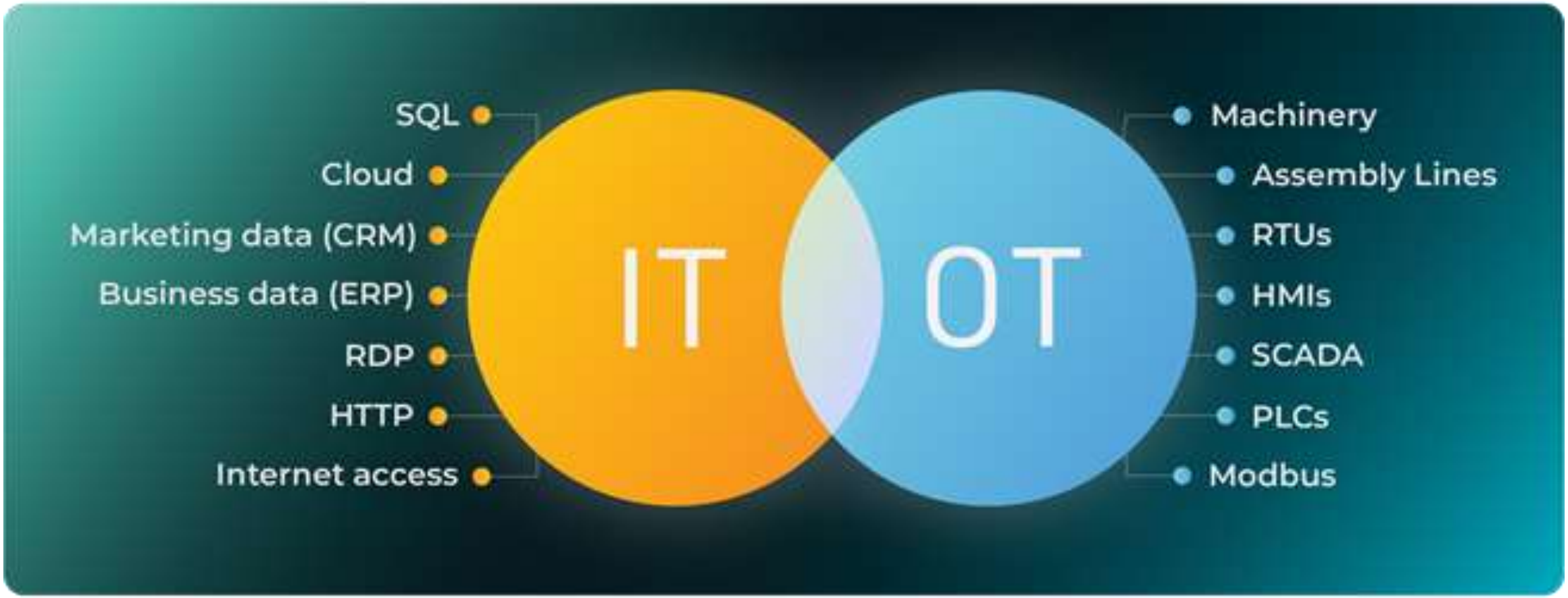
Проблемы безопасности

Примеры проектов

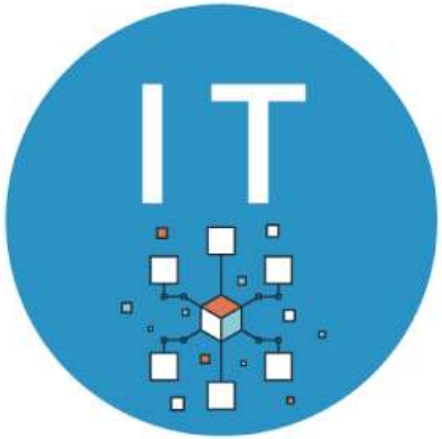
Ландшафт, задачи, инфраструктура, люди



Используемые сервисы и системы



Условия функционирования



- Почти всё ПО и железо стандартизовано
- Автоматическое обновление ОС и ПО
- Отсутствие критичности, в большинстве случаев

- Работает 24ч в сутки
- Максимальная эффективность производства
- Высокая критичность отказов и сбоев

ИТ vs АСУ ТП (IT vs OT)

Подходы к ИБ

Проблемы безопасности

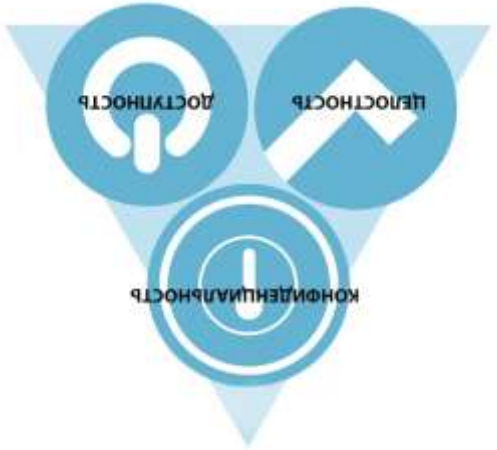
Примеры проектов

Разные приоритеты – разный подход

- **Безопасность ИТ:**
  - Конфиденциальность
  - Целостность
  - Доступность

- **Безопасность ИТ:**
  - Приоритет №1 – Конфиденциальность
  - Фокус – Не допустить разглашения
  - Цель защиты – Сервера, раб. станции
  - Условия – кондиционирование

- **Безопасность АСУ ТП:**
  - Доступность
  - Целостность
  - Конфиденциальность



- **Безопасность АСУ ТП:**
  - Приоритет №1 – Доступность и целостность
  - Фокус – Не допустить простоев и сбоев
  - Цель защиты – Контроллеры, HMI, датчики
  - Условия – агрессивная окружающая среда

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ИТ И АСУ ТП

Методы

- Антивирусное ПО
- Обновление ПО
- Жизненный цикл технологий
- Методы тестирования и аудита
- Управление изменениями

ИТ

- Очень распространено
- Налаженный процесс
- 2-3 года, разные поставщики
- Налаженный процесс
- Регулярные и плановые

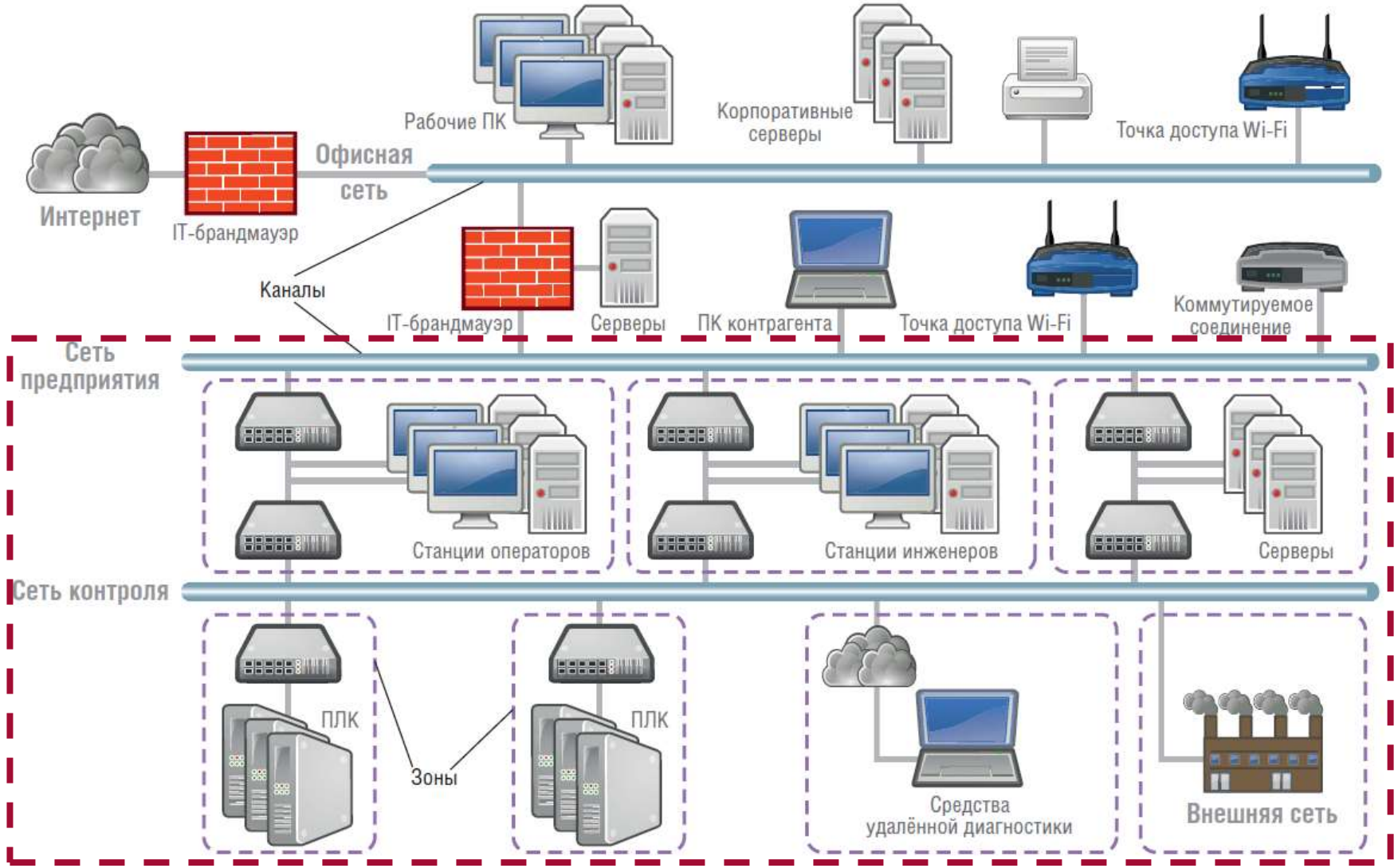
АСУ ТП

- Риск отказа ПО
- Риски деградации производительности
- 10-20 лет, 1-2 поставщика
- Малая применимость
- Долгая плановая подготовка

Архитектура АСУ ТП

- **3 уровня:**

- Верхний. Уровень оперативно-производственных служб АСУ (АСУ ТП)
- Средний. Уровень систем автоматического управления (ПЛК)
- Нижний. Уровень автоматизации, датчиков и исполнительных механизмов



ИТ vs АСУ ТП (IT vs OT)

Подходы к ИБ

Проблемы безопасности

Примеры проектов

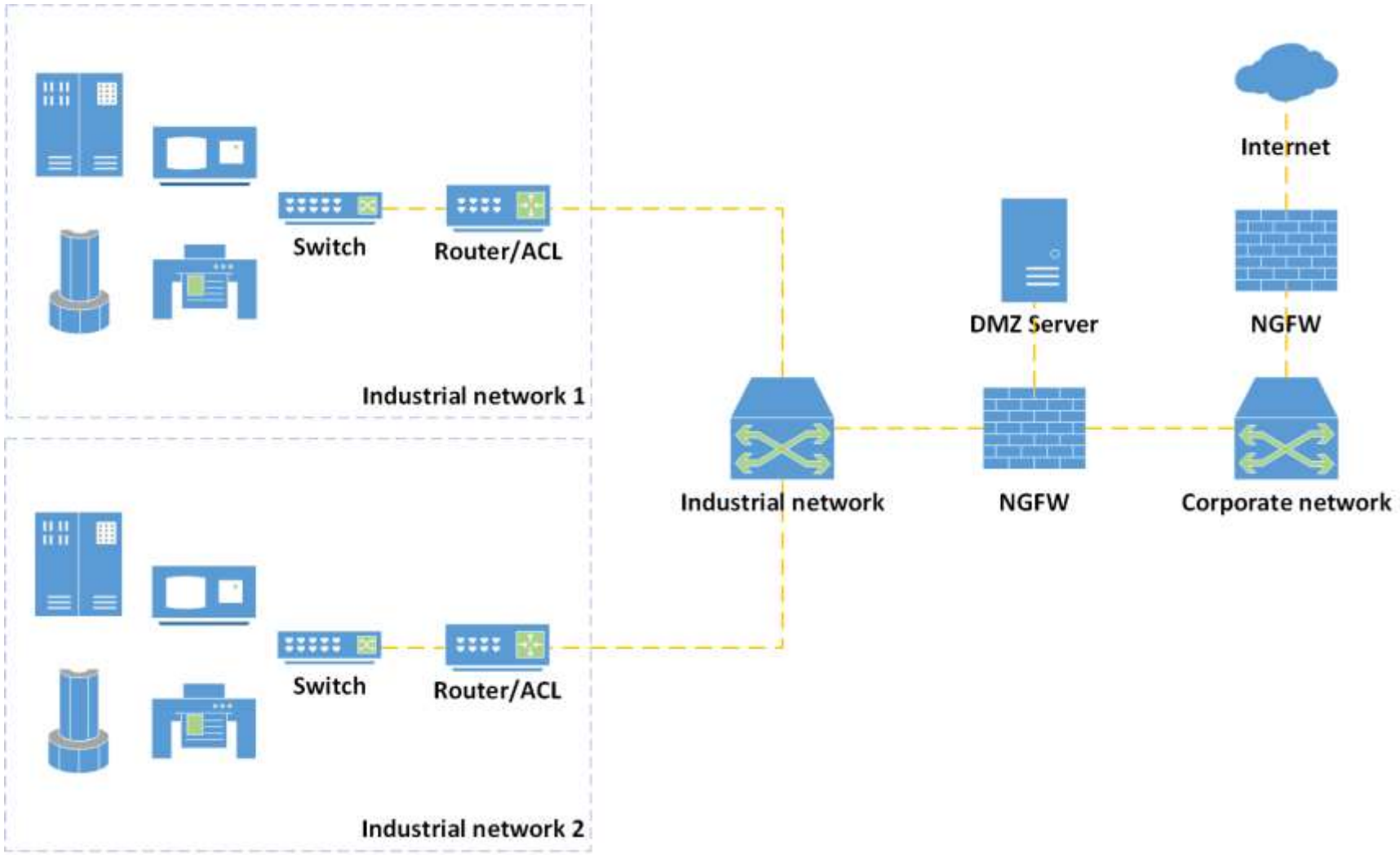
Отсутствие сегментирования сетей и DMZ

Проблема:
Плоская технологическая сеть. Отсутствие сегментирования. Отсутствие DMZ. Отсутствие разграничения доступа

Чем грозит:
- угроза распространения заражения/атаки с КСПД на ТСПД
- быстрое развитие атаки
- компрометация всей сети сразу

Рекомендации:
1. Сегментирование (VLAN)
2. Организация DMZ
3. Оценка взаимодействий между сетями и оптимизация портов
4. Минимизация привилегий пользователей

Сегментирование КСПД и ТСПД



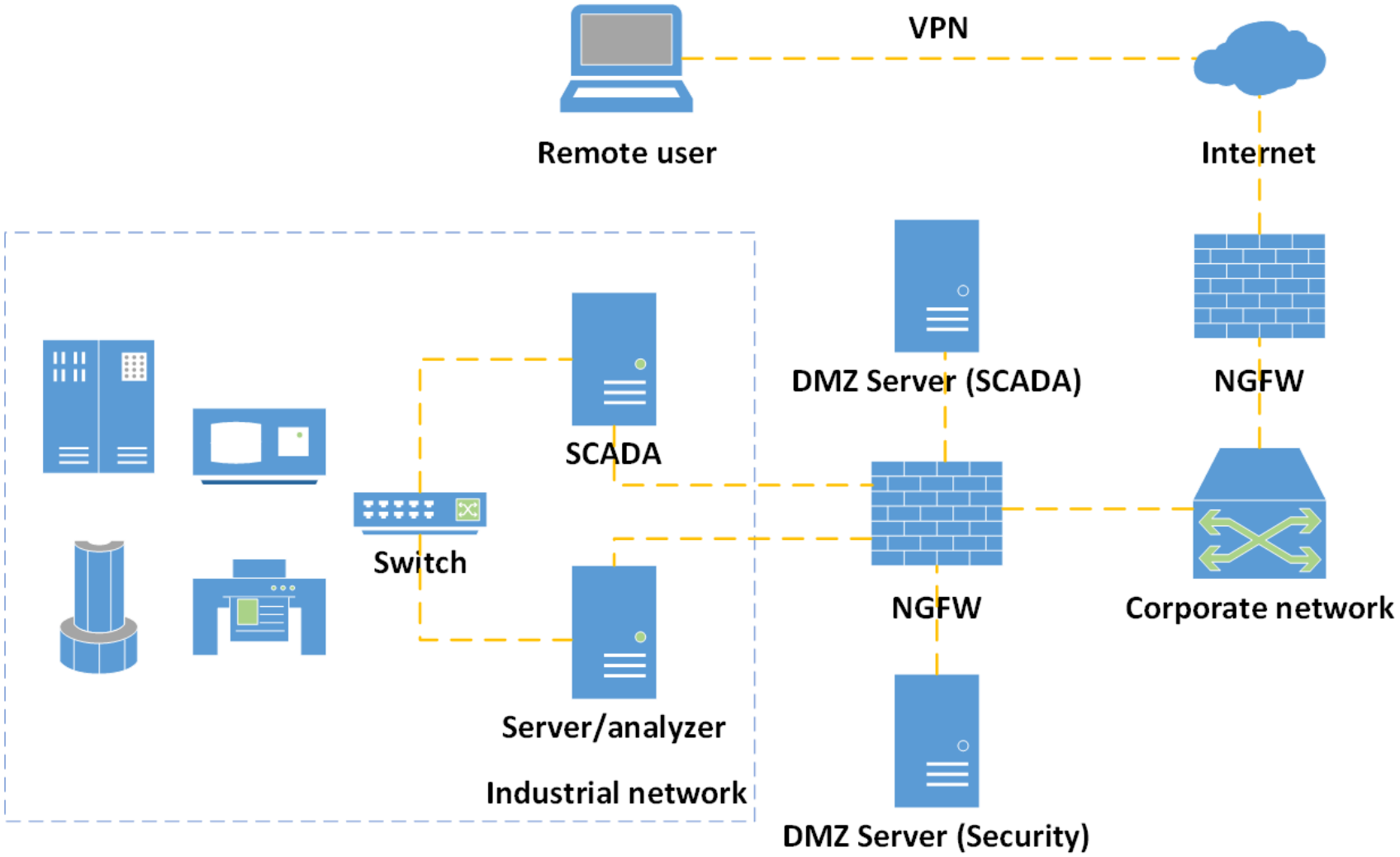
Удаленный доступ к АСУ ТП

Проблема:
Удаленное сопровождение SCADA-систем подрядчиками, прямой неконтролируемый доступ к серверам АСУ ТП со стороны обслуживающих организаций создает потенциальную «дыру» в безопасности

Чем грозит:
- вмешательство в работу АСУ ТП
- при взломе/заражении сети подрядчика под удар попадают администрируемые им объекты

Рекомендации:
1. Оценить необходимость предоставления удаленного доступа.
2. Минимизировать привилегии.
3. Если удаленный доступ необходим – включить в договор на обслуживание требования по обеспечению ИБ и организовать безопасный удаленный доступ:
    - подключение через DMZ;
    - разделение серверов для подключения подрядчиков и серверов для подключения обслуживающего персонала;
    - кроме стандартных средств подключения (VPN) также PIM/PAM-системы и MFA

Удаленный доступ к АСУ ТП



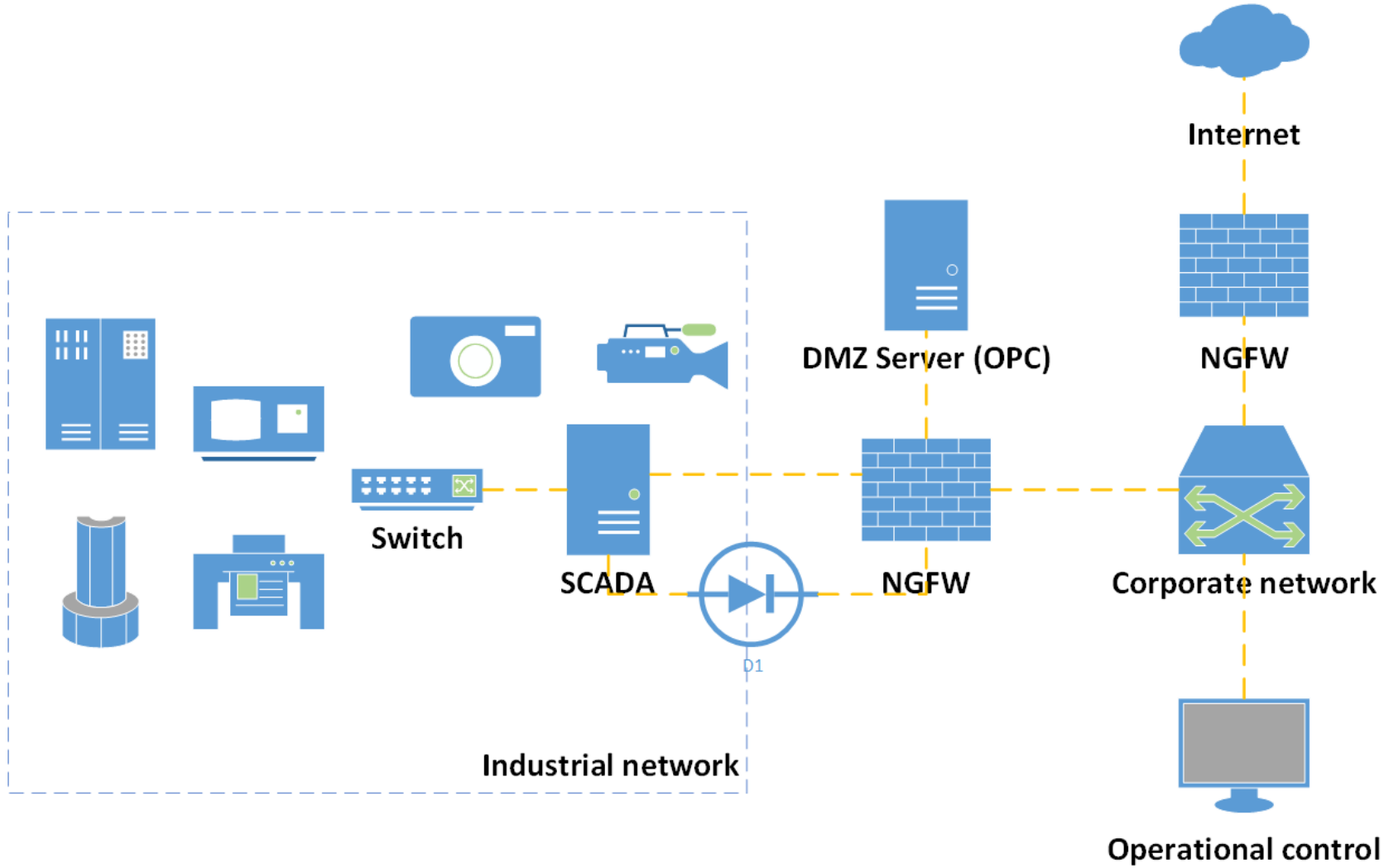
Передача данных из АСУ ТП

Проблема:
Прямая передача данных из АСУ ТП (для мониторинга и аналитики)

Чем грозит:
- потенциальная «дыра»
- эксплуатация уязвимости

Рекомендации:
1. Промежуточный сервер OPC в DMZ
2. Скрины (FTP, SMB) в DMZ
3. Системы технологического телевидения
4. Дата-диоды

Передача данных из АСУ ТП



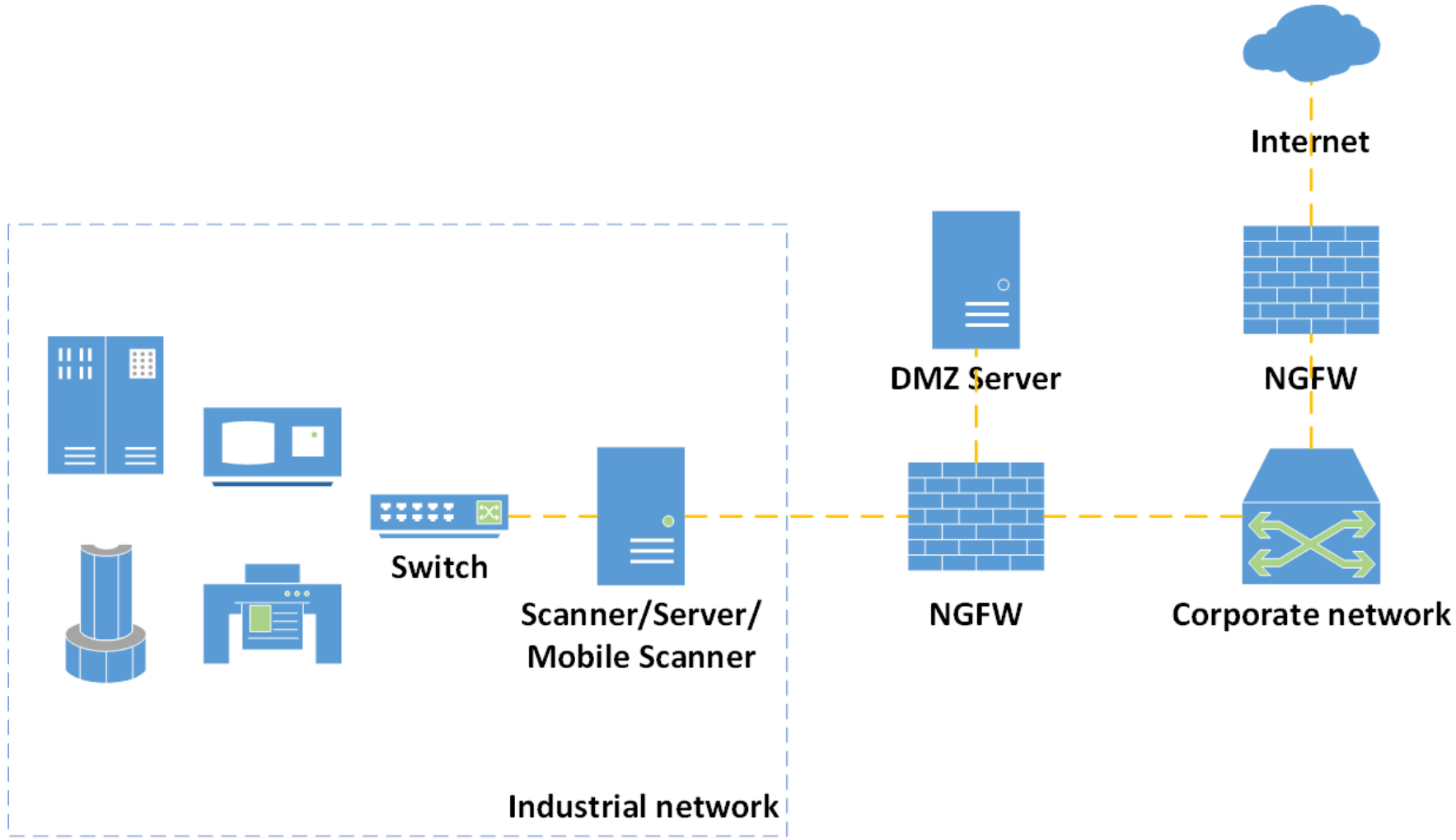
Анализ защищенности и обновления ПО

Проблема:
Со временем накапливается огромное количество уязвимостей

Чем грозит:
Увеличение вероятности компрометации сети

Рекомендации:
1. Своевременное обновление ПО
2. Контроль версий
3. Патч-менеджмент
4. Регулярное сканирование на уязвимости

Анализ защищенности ТСПД



Использование паролей, заданных по умолчанию

Проблема:
Использование паролей, заданных по умолчанию, в SCADA-системах и на сетевом оборудовании

Чем грозит:
НСД

Рекомендации:
1. Реализация парольной политики
2. Обучение работников
3. Аудит безопасности

Подключение недекларированных устройств

Проблема:
Подключение USB-модемов, USB-накопителей, мобильных телефонов и ноутбуков

Чем грозит:
- заражение АСУ ТП вредоносным ПО
- внедрение закладок, в том числе с использованием методов социальной инженерии

Рекомендации:
1. Ограничение доступа на портах
2. Мониторинг подключения новых устройств
3. Обучение работников

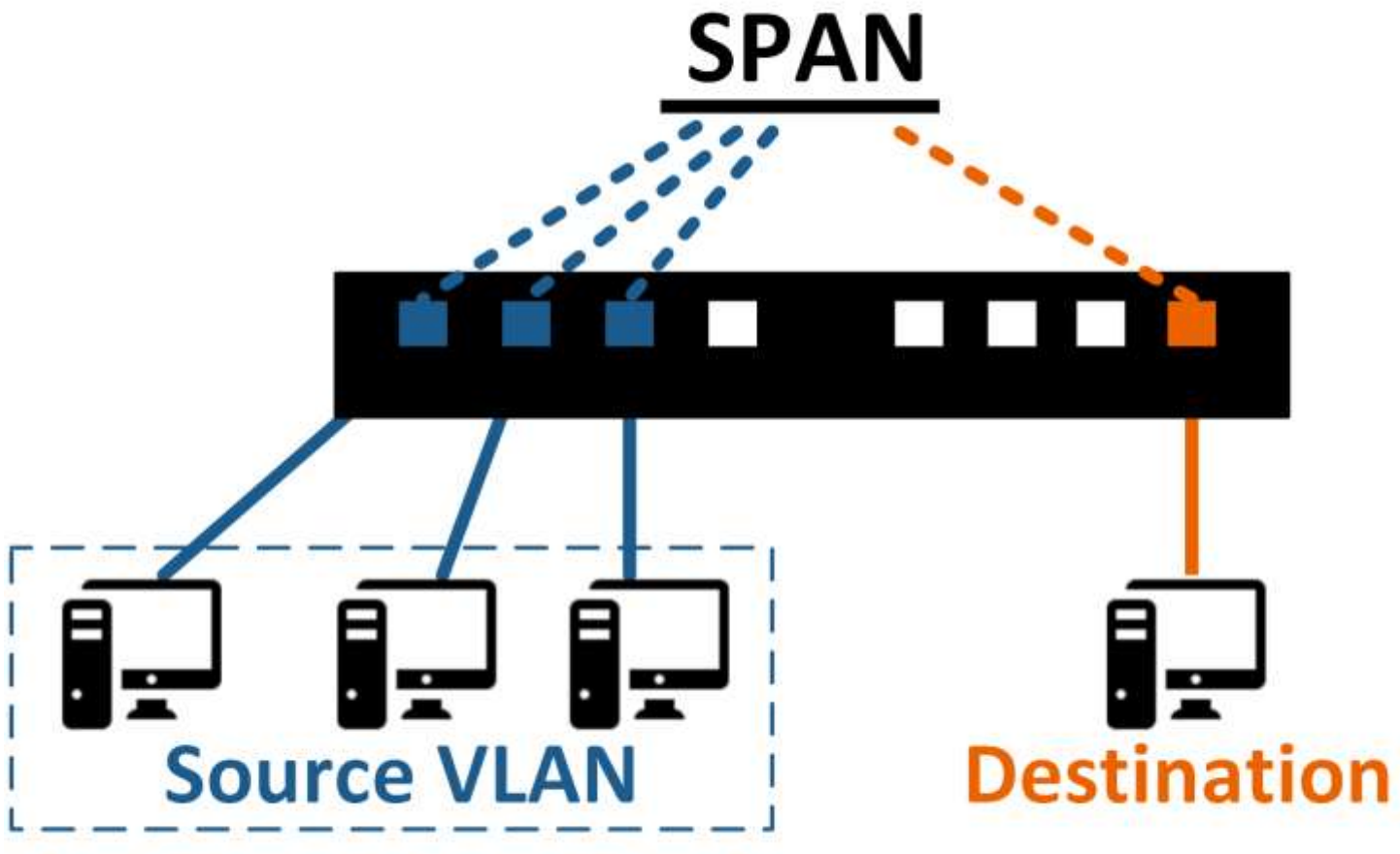
Анализ трафика АСУ ТП

Проблема:
Сбор копии трафика внутри разнородной, распределенной сети. Отсутствие функций зеркалирования

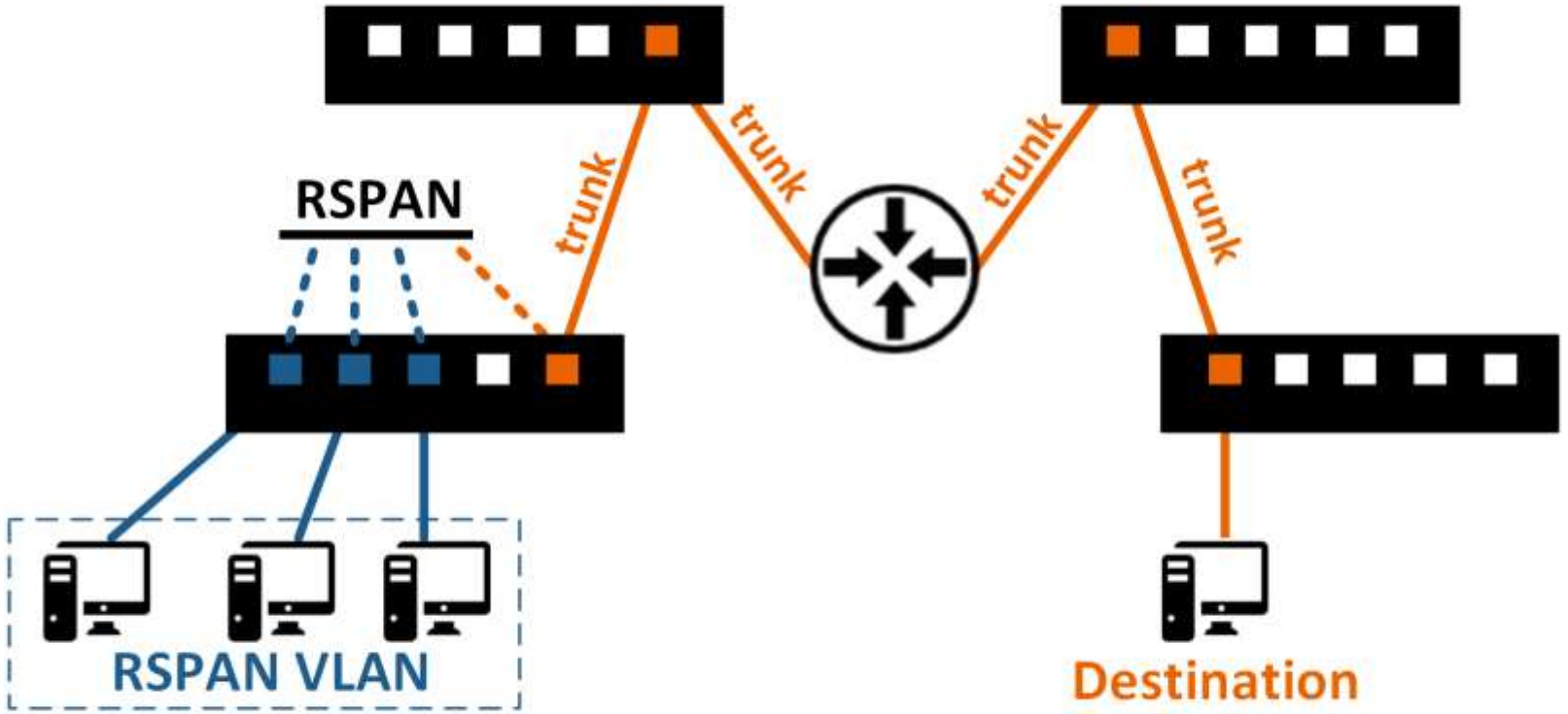
Чем грозит:
При отсутствии контроля, велика вероятность появления в сети не задекларированных устройств

Рекомендации:
1. Port security
2. Ограничение физического доступа
3. Анализ трафика АСУ ТП (специализированные решения)

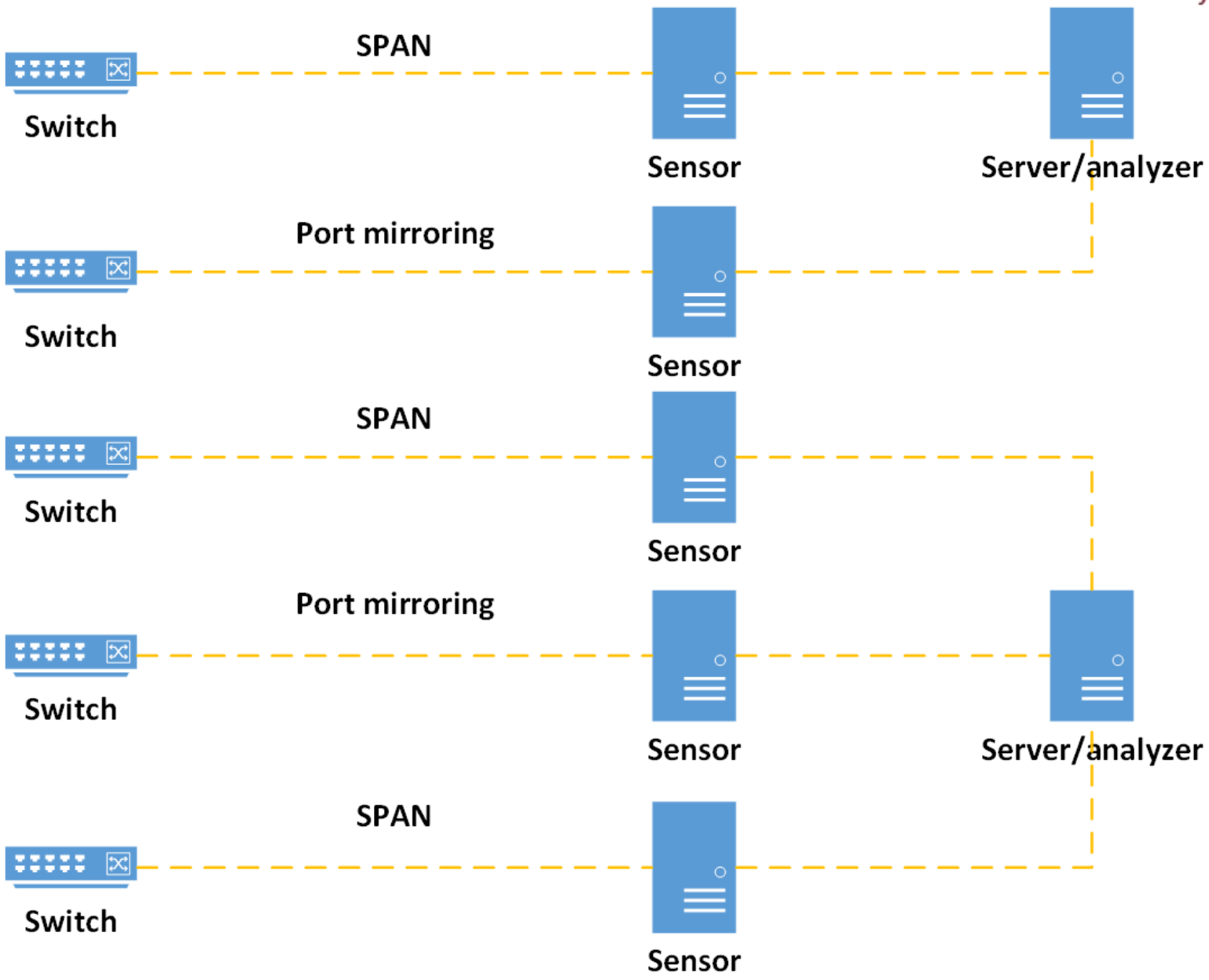
Сбор копии трафика



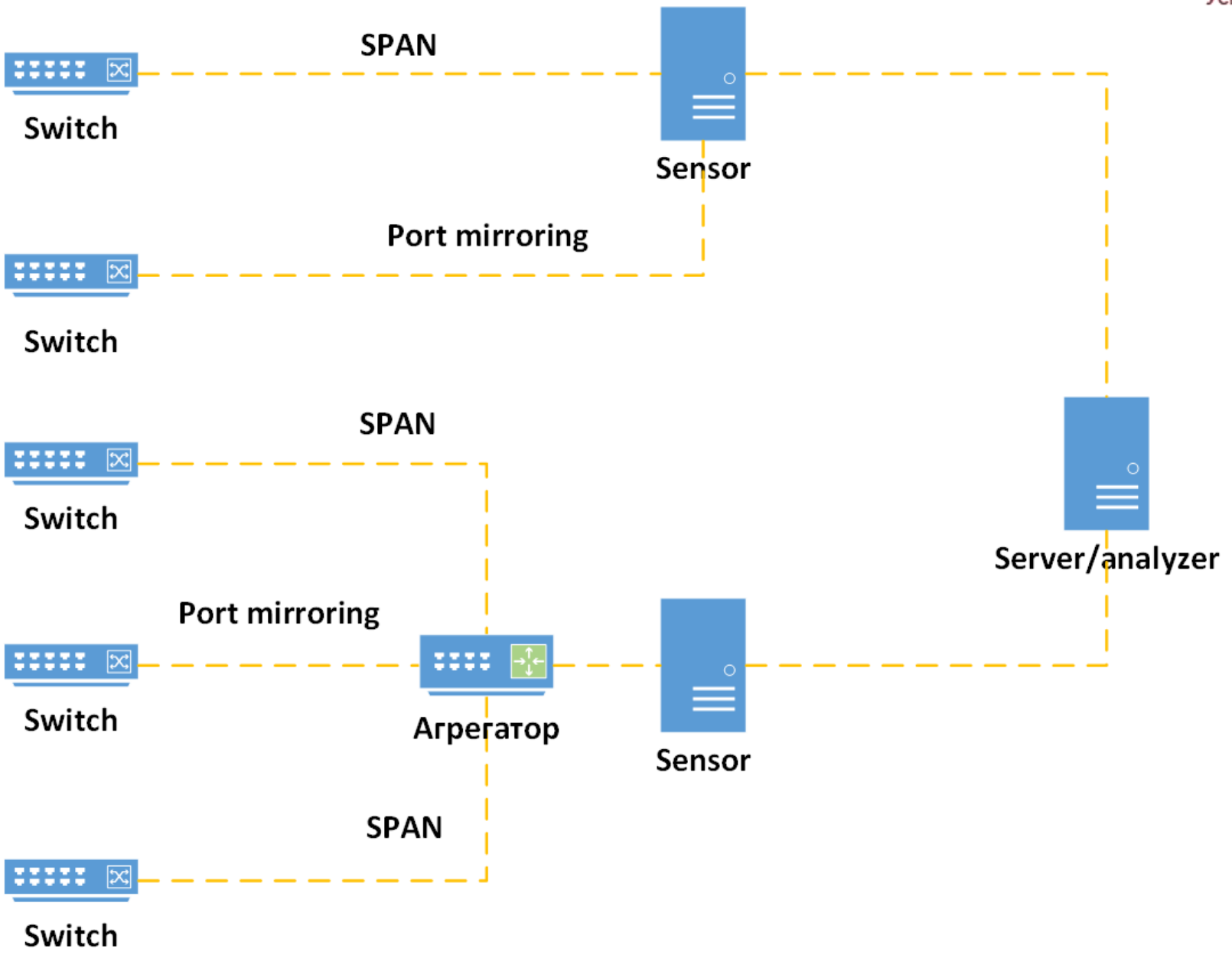
Сбор копии трафика



Сбор копии трафика



Сбор копии трафика



ИТ vs АСУ ТП (IT vs OT)

Подходы к ИБ

Проблемы безопасности

Примеры проектов

Сфера деятельности	Описание кейса
Газодобывающее предприятие (обеспечение ИБ нового месторождения)	Пересмотр проектных решений из-за ошибок сторонних подрядчиков по АСУ, ИТ, ИБ. Взаимодействие с вендорами АСУ ТП. Внедрение комплекса СЗИ АСУ, сегментация и организация VPN между удаленными площадками и центральным офисом. ПНР в условиях крайнего севера. Выстраивание сложных логистических цепочек доставки оборудования и сотрудников. АПКШ Континенты, UserGate, xFirewall, Astra Linux, Efros Access Control Server, Secret Net Studio, KICS for Networks, KICS for Nodes, KES
Металлургическая компания	Проектирование СОИБ ЗОКИИ, проектирование и прокладка ВОЛС, внедрение СЗИ АСУТП, подготовка ОРД, организация взаимодействия с корпоративным SOC, модернизация сетевой инфраструктуры и серверного парка, повышена устойчивость работы всех сегментов. UserGate NGFW + LA + MC, Astra Linux, Red-Виртуализация, КиберБэкап, Efros CI, SNS, KICS for Networks, KICS for Nodes, Kaspersky Endpoint Security, Kaspersky для Виртуализации, PT MP SIEM, xSpider

Сфера деятельности	Описание кейса
Металлургическая компания	Комплексный проект КИИ: Пересмотр проектных решений по обеспечению ИБ ОКИИ производства, внедрение СЗИ, модернизация инфраструктуры и сетевого оборудования. Включение в корпоративный SOC. *CheckPoint SG, Efros CI, СКДПУ НТ, PT MP SIEM, PT MP8, KICS for Networks, КиберБэкап*
Атомное производство	Комплексный проект КИИ: СОИБ АС оперативного диспетчерского управления технологическим процессом переработки ядерного топлива. Категорирование ОКИИ, проектирование СОИБ, подготовка ОРД, внедрение СЗИ АСУТП, заводские испытания. Организация поставки и внедрения как единого пред настроенного ПАК СОИБ. Один из первых крупных проектов с PT Platforma 187. *PT Platform 187 (MaxPatrol 8, MaxPatrol SIEM, PT Network Attack Discovery, PT Multi Scanner, ПТ Ведомственный центр), KICS for Nodes, Secret Net Studio, Red Check, ProfiTAP SPAN Booster*

Сфера деятельности	Описание кейса
Энергосбытовая компания (30 площадок)	Аудит, категорирование ОКИИ, формирование требований, ОРД, проектирование СОИБ ОКИИ, внедрение комплекса СЗИ и проведение ПСИ на 30 площадках. VipNet HW1000, VipNet IG10, Statewatcher, Policy Manager UserGate NGFW, КБ vGate R2, КБ SNS+Соболь, KES, KSWS.
Химическая предприятие (50+ ОКИИ)	Аудит, категорирование 50+ ОКИИ, формирование требований, ОРД, проектирование СОИБ ЗОКИИ 1/2/3кат., внедрение и испытания. Первый этап внедрения: UserGate NGFW, АПКШ Континент КШ+СОВ+СД Второй этап внедрения: KICS for Networks Очередной этап внедрения: PT MP SIEM + VM, Aladdin JAS, UserGate Industrial NGFW, КБ Соболь, KICS for Nodes Подключение СОИБ к корпоративному SOC.

Сфера деятельности	Описание кейса
Группа энерго-добывающих компаний (6 филиалов, 17 площадок)	Обследование, проектирование и многоуровневое согласование расширенного комплекта проектной документации на СОИБ АСУ ТП. Внедрение СЗИ в 6 филиалах и 17 площадках. Произведен перевод на отечественные межсетевые экраны АСУТП. PT ISIM, KICS for Nodes, NGFW, xSpider, Ixia NTO, Натек
Государственная энергетическая корпорация (89 офисов, ~1200 площадок, 1500+ ОКИИ)	Аудит, категорирование 1500+ ОКИИ, формирование требований, ОРД, проектирование СОИБ ЗОКИИ. 89 офисов и ~1200 площадок. Первый этап: КБ АПКШ Континент СД + АП, КБ SN8+SN LSP, KSC, KICS for Nodes, Kaspersky Embedded Systems Security, KES for Windows & for Linux & for Windows Server & for Virtualization, KSMG, PT NAD, PT XDR, КиберБэкап Второй этап внедрения: NextSTage IRP, Infowatch Person Monitor, Efros CI, PT WAF, PT VM, КБ JAS Третий этап внедрения: КБ Соболь, vGate R2, KWTS, Eltex EMS, Safe Mobile, ГАРДА БД, Solar appScreener. Подключение сервисов: Solar webProxy, UTM PTK Солар, корпоративный SOC

ИТ vs АСУ ТП (IT vs OT)

Подходы к ИБ

Проблемы безопасности

Примеры проектов

Игорь Мартыненко

Главный архитектор по защите КИИ

Igor.Martynenko@Softline.com