cigre Россия

infotecs

«Информационные технологии и телекоммуникации в создании цифровой электроэнергетики: драйверы, решения, возможности и риски с учетом опыта СИГРЭ»

Информационная безопасность и цифровизация отрасли

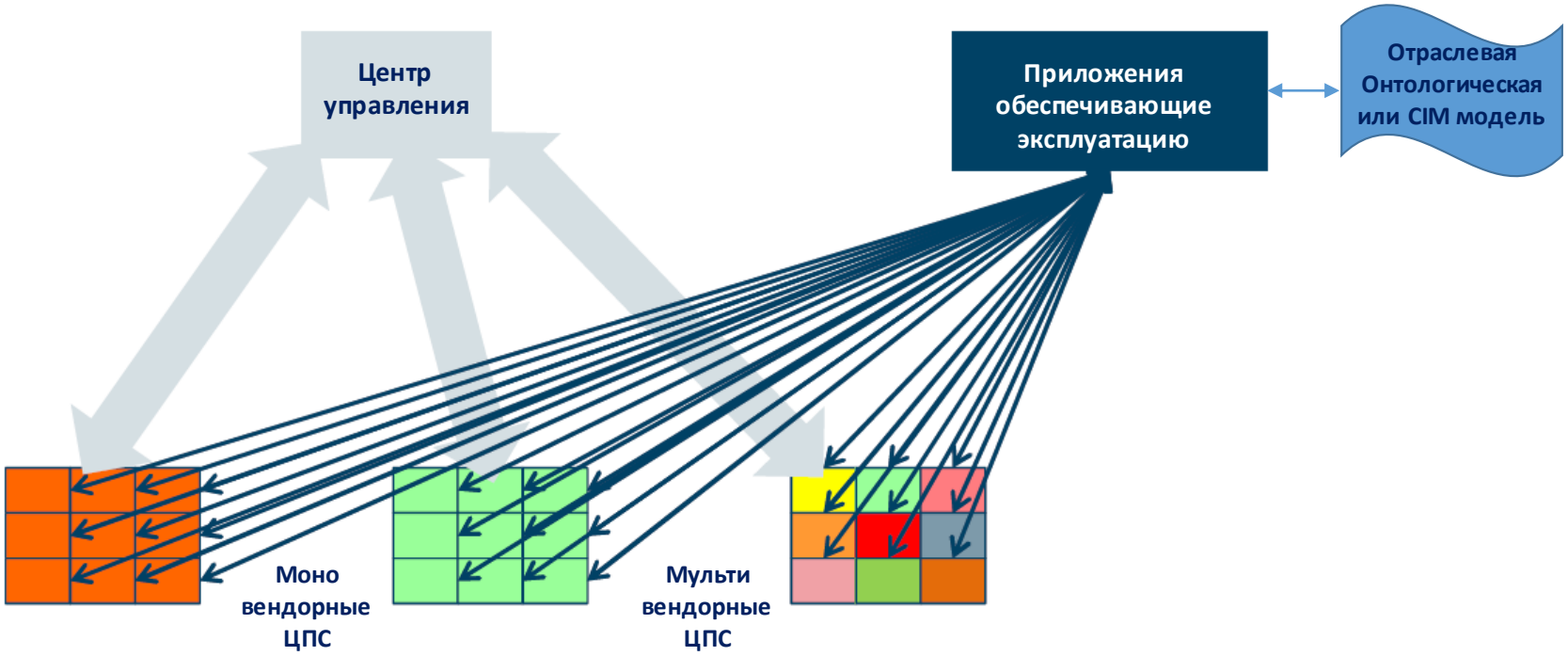
кадровые проблемы и методы их решения в электроэнергетике

Евгений Генгринович
эксперт

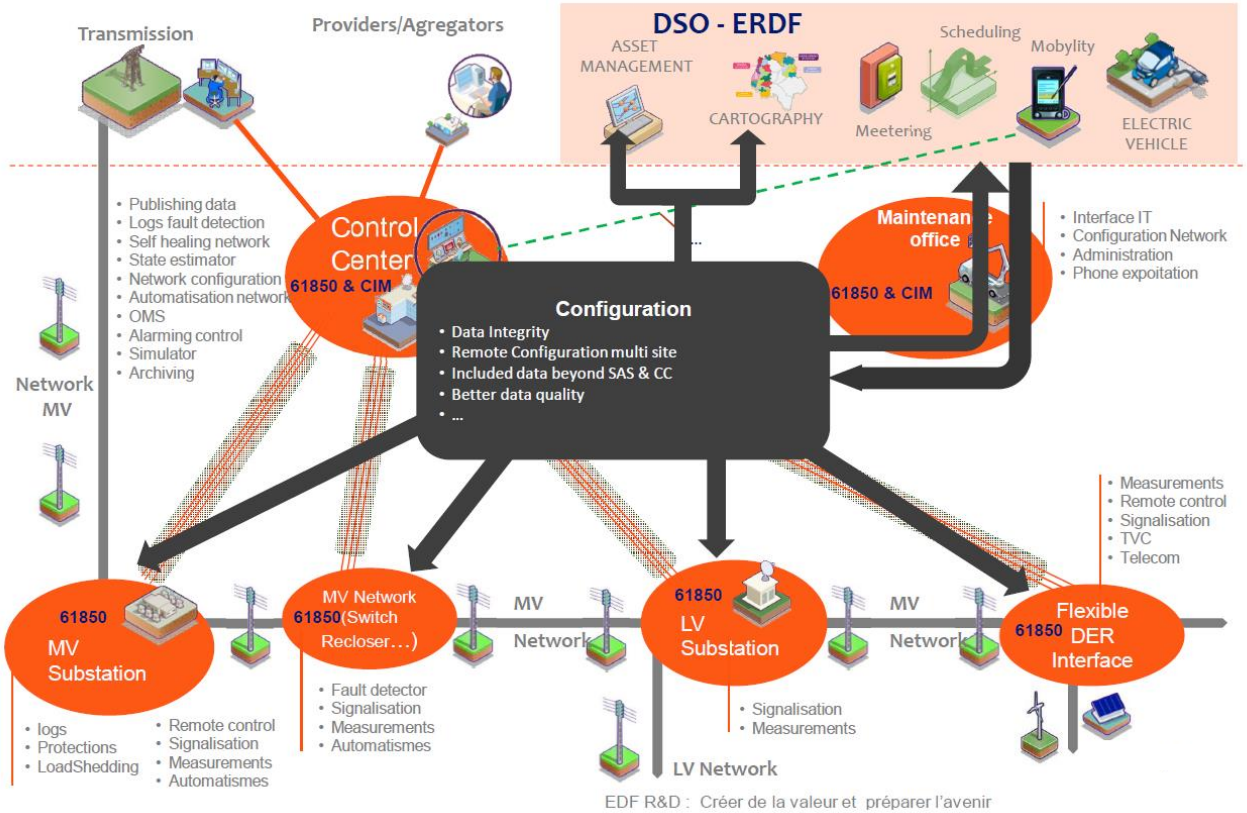
Тренды в создании цифровой электроэнергетики

- Переход на автоматическое удаленное управление подстанциями.
- Цифровые терминалы РЗА станут одним из элементов удаленной системы управления, с постепенным выносом алгоритмов на более высокие уровни управления.
- Возврат инвестиций будет сильно зависеть от того, насколько эффективно будут использоваться растущий объем первичной информации с объекта
- Оптимизация управления инфраструктурой, а не работа каждой подстанции в отдельности, является реальным драйвером для развития цифровизации электроэнергетики.

Структура информационных потоков



Пример интегрированной инфраструктуры (ERDF)



Актуальные вопросы

- Новые технологии и идеи требуют выстраивания новых процессов или наоборот?
- Методологии тестирования и проверки (против чего?).
- Значимое влияние на управление активами:
  - Требует появление новых навыков, ресурсов и обучения.
  - Изменение подходов к обслуживанию и ресурсам.
- Контроль «аппетита к риску» - сбалансировать преимуществ и последствий:
  - Информационная безопасность.
  - Регулирование.
  - Увеличение уровня автоматизации и целостности сети.

Базовые проблемы ИБ в электроэнергетике

- Специалисты ИБ имеют недостаточно знаний об особенностях обеспечения информационной безопасности в электроэнергетике.
- В отрасли недостаточно экспертов, имеющих практические навыки обеспечения информационной безопасности.
- Большой дефицит квалифицированных кадров.
- Низкая осведомленность персонала в вопросах информационной безопасности.

Дефицит кадров в области информационной безопасности КИИ является глобальной проблемой

- Американский NIST SP 800-181 “National Initiative for Cybersecurity Education” определяет требования к квалифицированной ИБ команде с разбивкой по ролям.
- Последние изменения вышли в январе 2020 года.

Чтобы противостоять новым угрозам, отрасли нужны специалисты ИБ, которые должны:

Обладать знаниями и опытом/
Быть осведомленными об актуальных угрозах/
Уметь работать в команде

NIST NICE Framework

7 Категорий, определяющих функциональные уровни ИБ.


Обеспечение безопасности


Управление& эксплуатация


Требования Регуляторов


Защита


Сбор данных & предотвращение


Анализ

Расследования

33 области специализации, определяющие различные области ИБ.

52 функциональные роли специалистов, определяющие конкретные знания, навыки и способности, необходимые для выполнения задач в рамках данной роли.

Cyber Range платформы

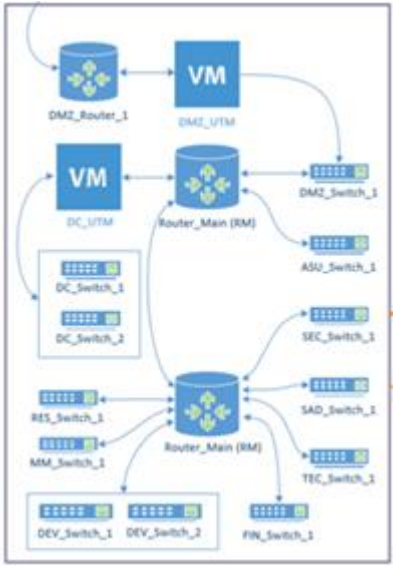
(классификация Гартнер)

Cyber Range

платформы для обучения и тестирования

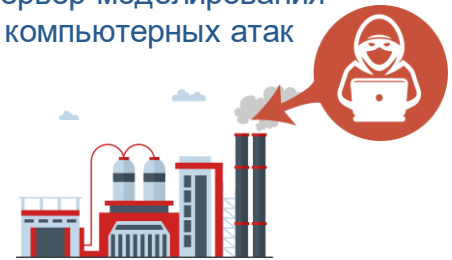
Тренинги для специалистов ИБ на цифровых двойниках корпоративных сетей

Симуляция корпоративной сети с ИТ и SCADA сегментами

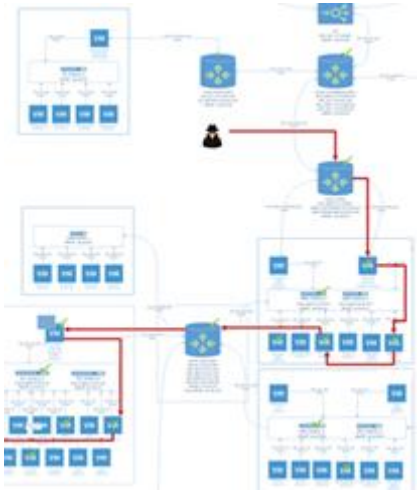


Security Operations Center

Сервер моделирования компьютерных атак

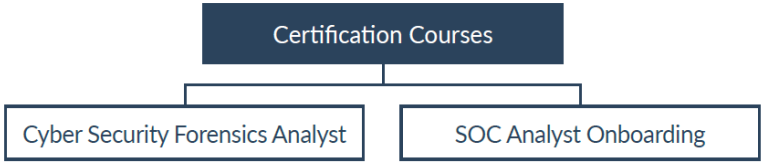


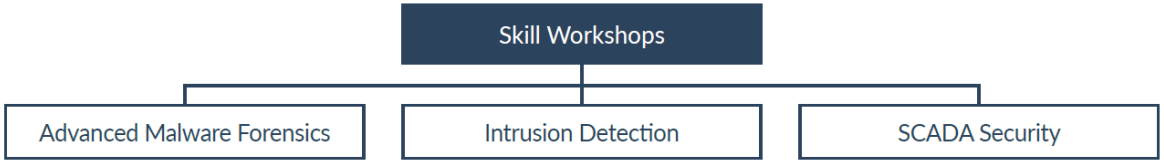
Готовые шаблоны сетей и сценарии обучения



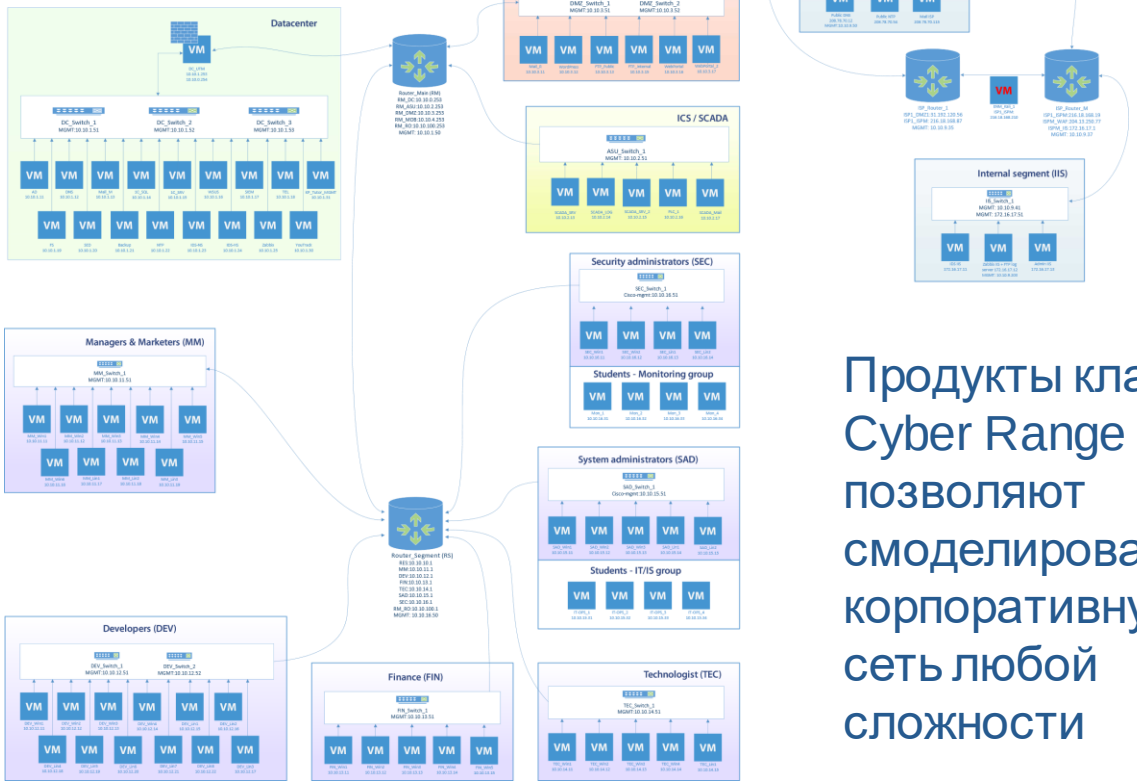
На базе платформ класса Cyber Range проводятся различные курсы и семинары

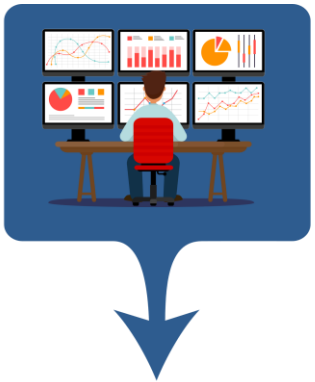
Комбинация теории и практических навыков защиты от различных типов атак на инфраструктуре подобной реальной, позволяет значительно повысить качество обучения специалистов ИБ



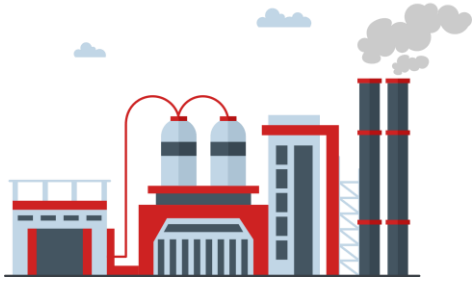


Цифровой двойник корпоративной сети

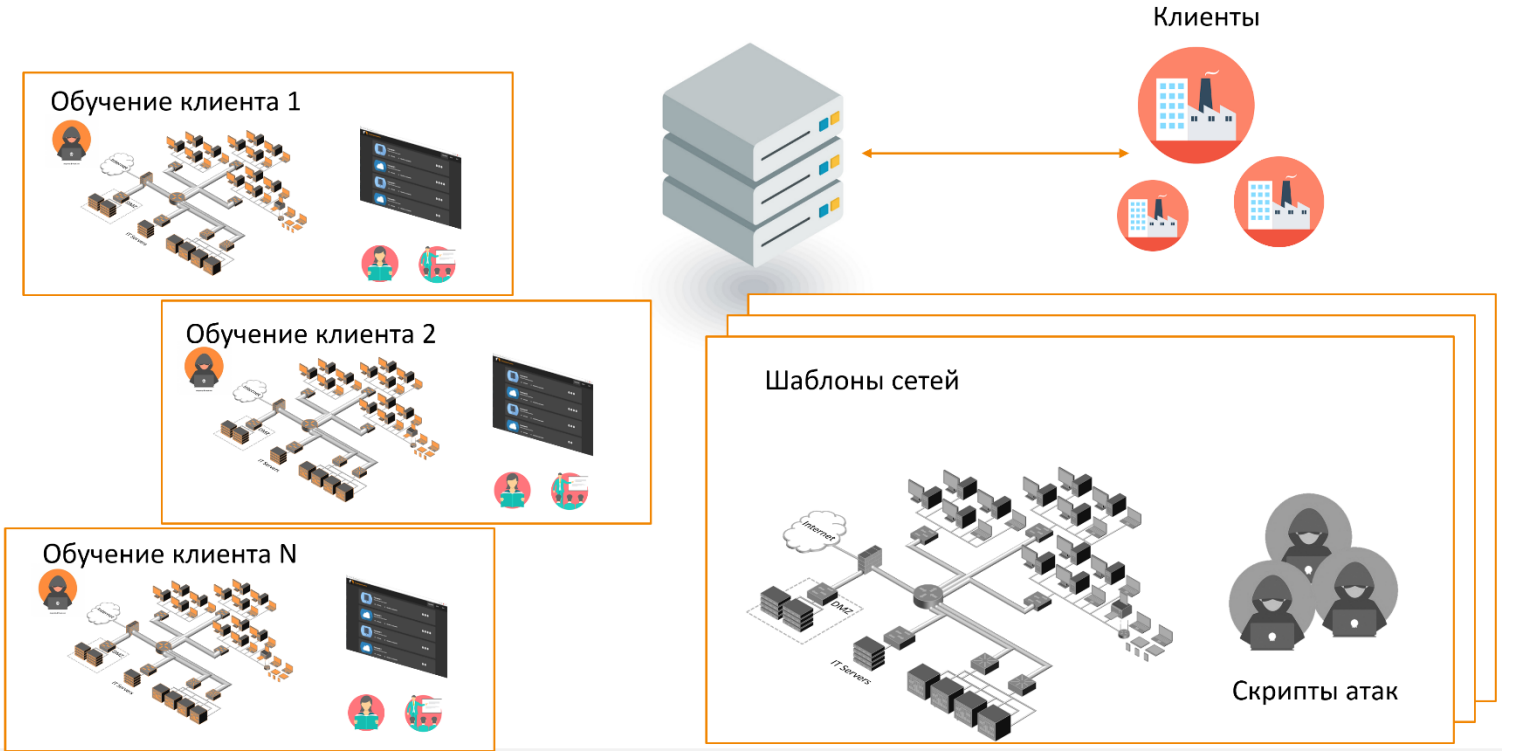




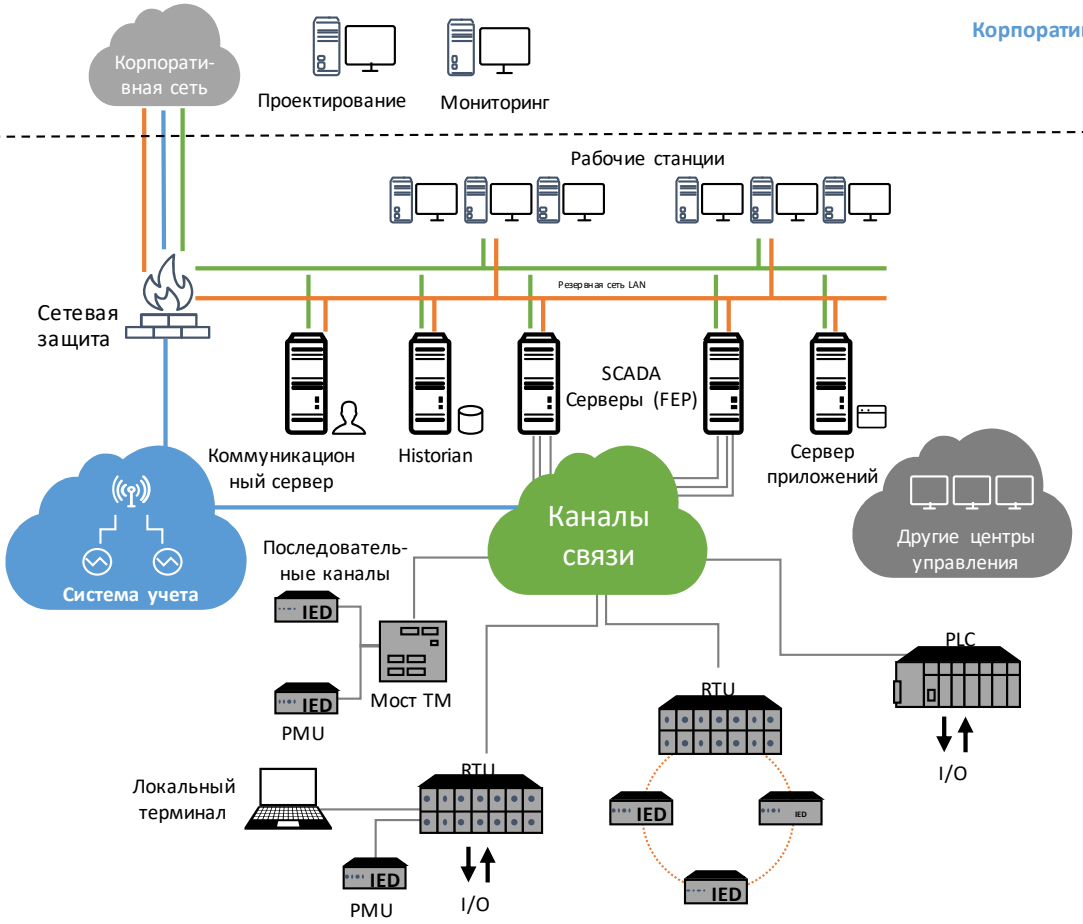
Продукты класса Cyber Range позволяют смоделировать корпоративную сеть любой сложности



Cyber Range позволяют формировать различные шаблоны сетей



Типовая структура сети в отрасли



Корпоративный сегмент сети компании

Офисные информационные технологии (ИТ)

Промышленная сеть (уровень АСУ)

Автоматизированные системы управления производством (АСУ)

Промышленная сеть (объект)

Автоматизированные системы управления технологическим процессом (АСУТП)

Что влияет на безопасность КИИ?

Офисная сеть: шлюзы взаимодействия ИТ/АСУ

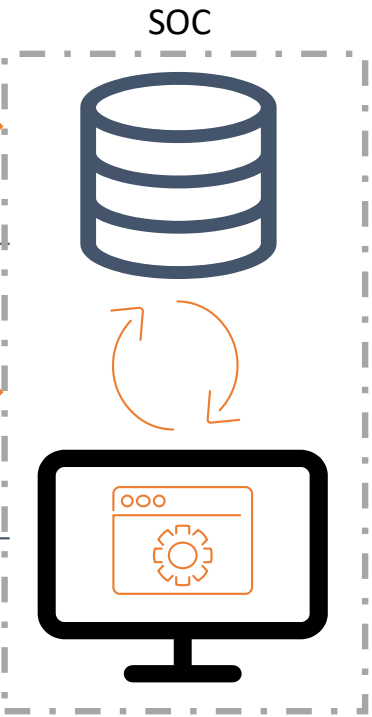
- Сетевые входы и выходы
- Считывание и запись реестров
- Доступ и учет файлов
- Обработка/загрузка DLL
- Доступ к памяти, ввод кода
- Изменение аппаратного обеспечения
- Драйверы

АСУ

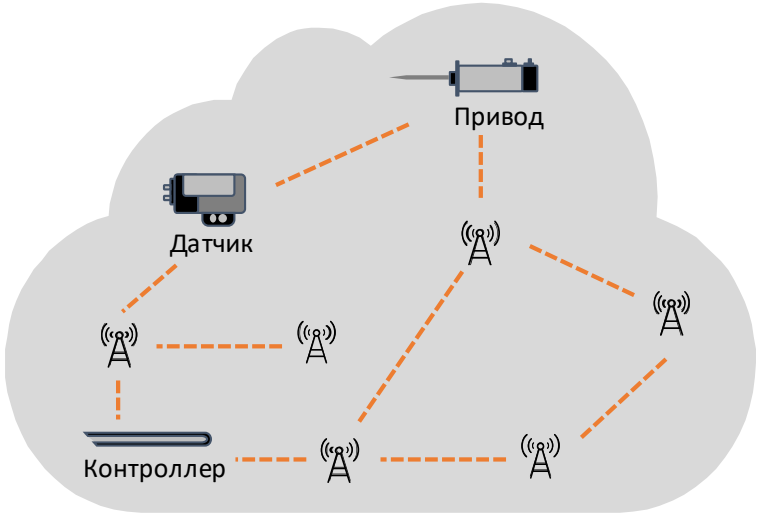
- Сетевые входы и выходы
- Считывание и запись реестров
- Доступ и учет файлов
- Обработка/загрузка DLL
- Доступ к памяти, ввод кода
- Изменение аппаратного обеспечения
- Драйверы
- Поведение программ SCADA
- Разрешения пользователей

АСУТП

- Передачи SCADA
- Команды SCADA
- Уязвимые места SCADA
- Каналы связи SCADA (подключение и взаимодействие)

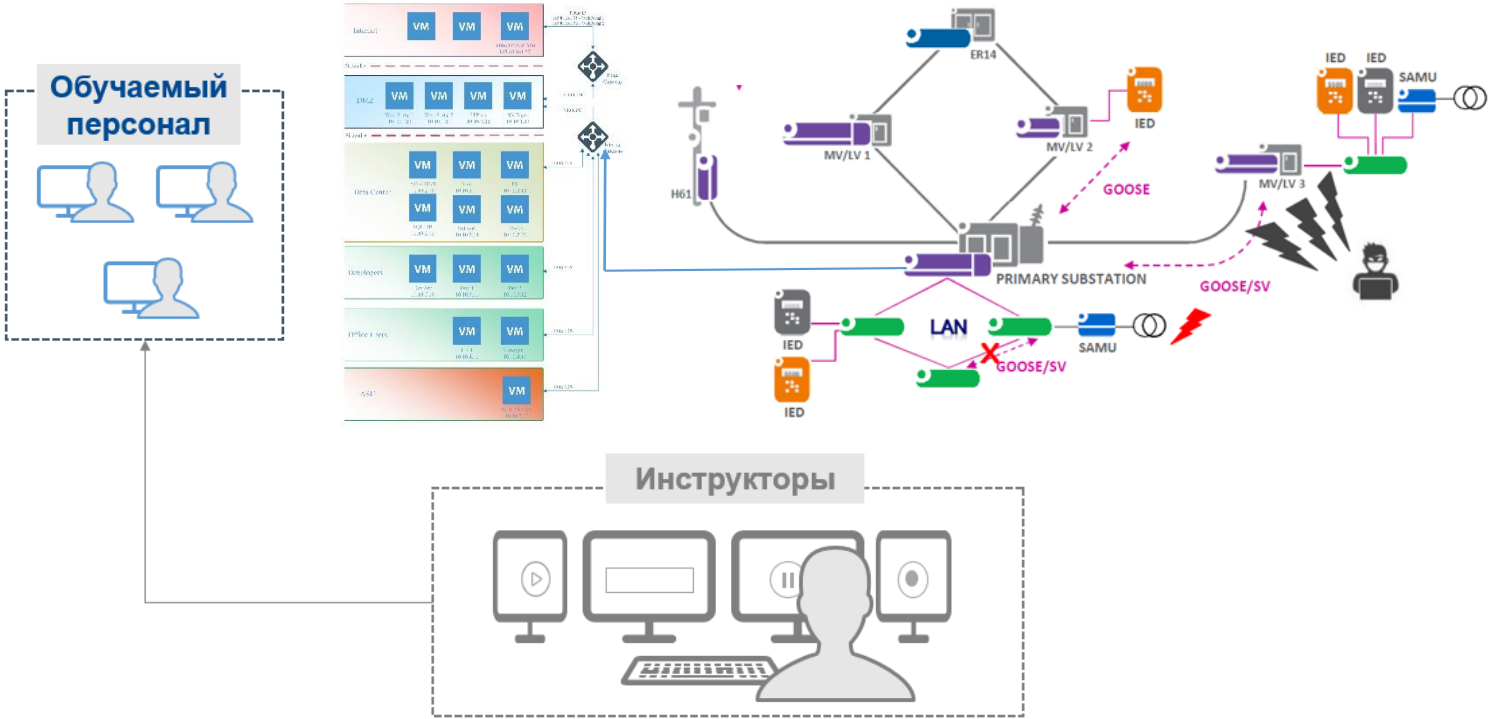


Симуляция кибер-физических систем



Сеть сбора телеметрии

Цифровой двойник сети с ЦПС

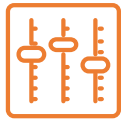


Универсальный испытательный полигон

Построение и проверка сетей с параметрами пользователя

Генерация реалистичного трафика

Комплексные сети и симуляция атак



Высокая гибкость и масшта-бирование

Управляемая испытательная среда

Заключение

- Развитие цифровизации электроэнергетики позволяет решить целый ряд технологических, эксплуатационных и экономических задач.
- В то же время растущий объем первичной информации требует пересмотра сложившихся бизнес-процессов управления и обеспечения их информационной безопасности.
- Формируются новые вектора компьютерных атак, меняются требования к уровню подготовки обслуживающего персонала.
- В расчетах показателей надежности технологических процессов появляется существенная составляющая, связанная с информационной безопасностью.
- Процесс развития цифровизации нельзя ограничить рамками одной или нескольких подстанций, опыт показывает, что это должны быть системные комплексные решения.
- Обеспечение безопасности КИИ влечет за собой появление отдельных обеспечивающих автоматизированных систем по аналогии с управлением эксплуатацией.

Спасибо!