Типовые решения ViPNet для Электроэнергетики

Карантаев Владимир / к.т.н. / Член РНК СИГРЭ
Менеджер
Отдел развития продуктов
Vladimir.Karantaev@infotecs.ru

Регламент

Вызовы кибербезопасности Smart-Grid

План доклада

Приветствие

Кибербезопасность АСТУ

Основное время доклада

Ответы на вопросы

Комментарии

Путь поставки электроэнергии

>> ИСТОЧНИК НФОРМАЦИИ «РОССЕТИ»

Перспективные направления развития ЕЭС РФ

- Внедрение технологий Smart Grid.
- Внедрение нового управляемого силового оборудования в ААС.
- Внедрение цифровых ПС с учетом развития цифровой обработки.

«Концепция развития релейной защиты и автоматики электросетевого комплекса», Россети, 2015

Планомерное развитие ЕЭС РФ

- Внедрение подстанций нового поколения.
- Развитие автоматизированных систем технологического управления (АСТУ).
- Переход к необслуживаемым подстанциям.

Вызовы кибербезопасности при развитии активно-адаптивной сети ЕЭС РФ

Вопросы кибербезопасности ИЭС ААС

- Повышение общего уровня информатизации энергетической сферы приводит к повышению риска возникновения ущерба (технического и экономического) от противоправных действий.
- Особенности ИЭС ААС:
- работа в непрерывном активном режиме,
- приоритет задачи сохранения функциональности системы над задачей сохранения ее информационной безопасности.
- Концепция информационной безопасности должна учитывать:
- IEC 62351.
- INL Cyber Security Procurement Language 2008.
- ISO/IEC 27000.

ОСНОВНЫЕ ПОЛОЖЕНИЯ КОНЦЕПЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ ЭНЕРГОСИСТЕМЫ С АКТИВНО-АДАПТИВНОЙ СЕТЬЮ

Вопросы кибербезопасности систем РЗА

- РЗА является ключевым (критически важным) сегментом информационно технологических систем электросетевого комплекса.
- В связи с массовым внедрением МП устройств РЗА, созданием каналов связи и увеличением объема передаваемой и принимаемой технологической информации необходимо обеспечить безопасность работы информационно-технологических систем на энергообъектах, так как они слабо защищены от возможности незаконного вмешательства в работу.

Приложение №1
к протоколу Правления
ОАО «Россети»

от 22.06.2015 № 356пр

КОНЦЕПЦИЯ РАЗВИТИЯ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИКИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА

Источники угроз безопасности устройствам РЗА

- Иностранные разведывательные службы государств, осуществляющих по отношению к нашей стране недружественную политику и имеющих целью нарушения функционирования энергетического комплекса в особый период или в ходе подготовки и ведения войны.
- Террористические организации, криминальные структуры, отдельные лица (хакеры, внутренние и другие нарушители) или группы лиц, реализующие свои корыстные или иные интересы путем деструктивных информационных воздействий на системы оперативно-технологического управления.
- Представителей конкурирующих фирм и организаций, иностранных экономических структур, деятельность которых направлена против интересов.

Экспертное мнение

- Стратегическое направление развития РЗА и ПА должно рассматриваться в совокупности со смежными системами.
- Развитие РЗА и ПА идет по пути реализации преимуществ и широких возможности новой технологии. Будущее за интеллектуальными и многофункциональными устройствами.

- Объединение РЗА и коммуникационных схем призвано в корне изменить как саму систему РЗА, так и её роль в системе управления.
- Успешное внедрение «умных» ЭЭС, глобальных распределенных систем мониторинга, защиты и управления требует решения проблемы кибербезопасности.

Современные мировые тенденции развития систем РЗА,

Г.С. Нудельман, 2012

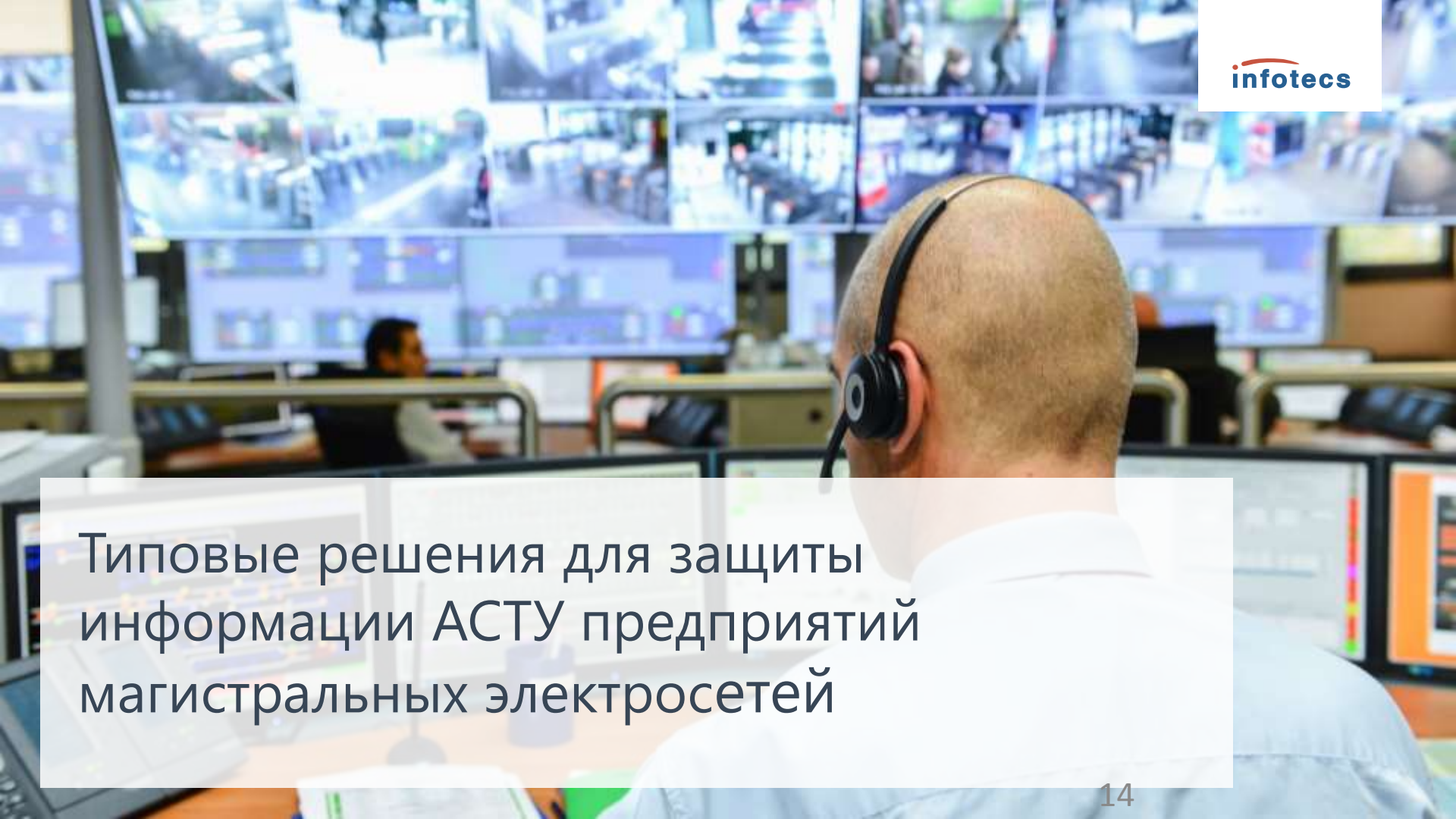
Необычные объекты защиты

А такие последствия возможны?

Экспертное мнение

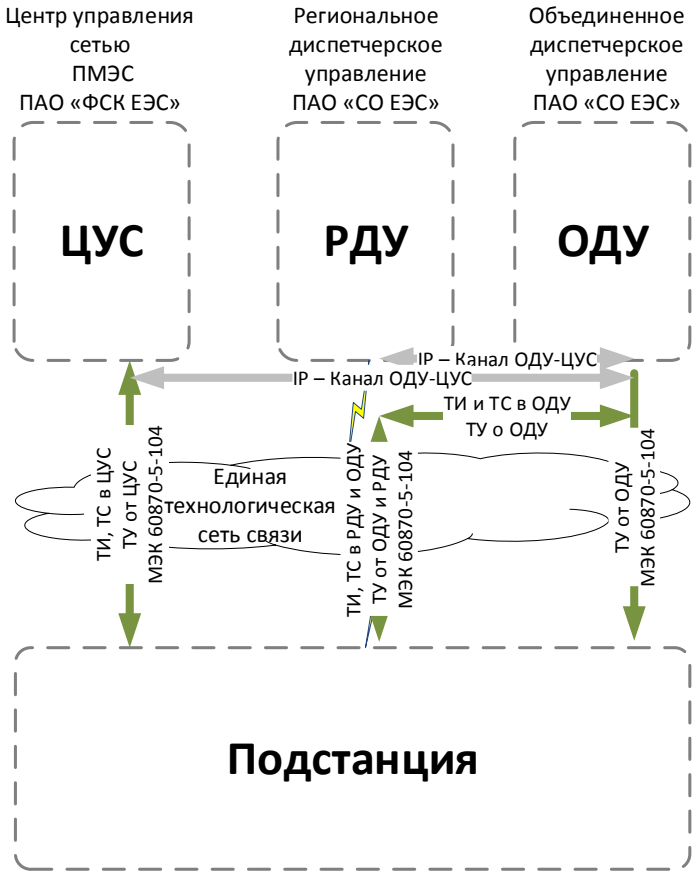
- Стратегическое направление развития РЗА и ПА должно рассматриваться в совокупности со смежными системами.
- Развитие РЗА и ПА идет по пути реализации преимуществ и широких возможности новой технологии. Будущее за интеллектуальными и многофункциональными устройствами.
- Объединение РЗА и коммуникационных схем призвано в корне изменить как саму систему РЗА, так и её роль в системе управления.
- Успешное внедрение «умных» ЭЭС, глобальных распределенных систем мониторинга, защиты и управления требует решения проблемы кибербезопасности.

Современные мировые тенденции развития систем РЗА, Г.С. Нудельман, 2012

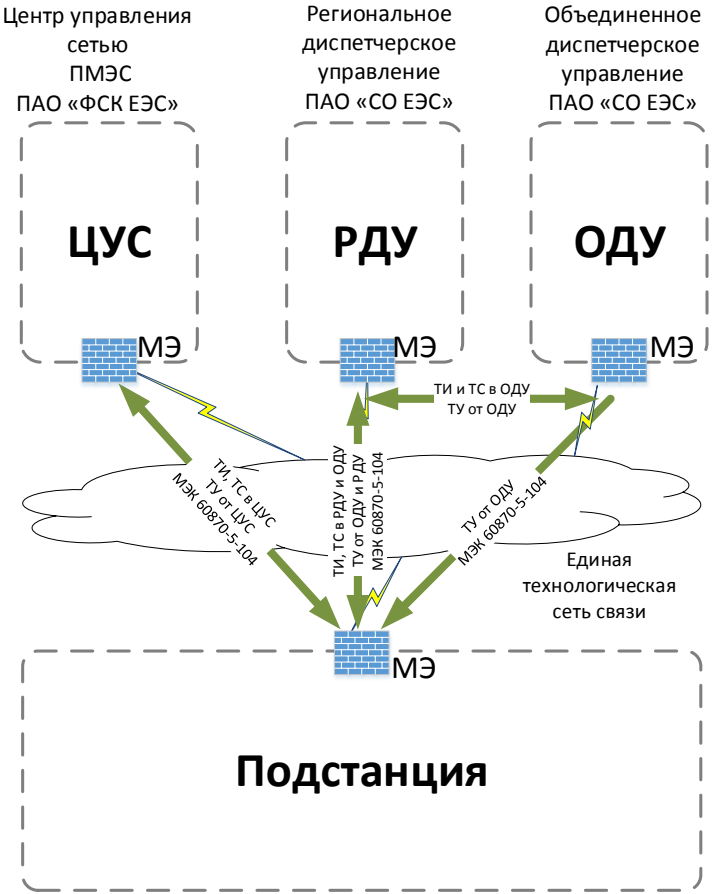


Типовые решения для защиты информации АСТУ предприятий магистральных электросетей

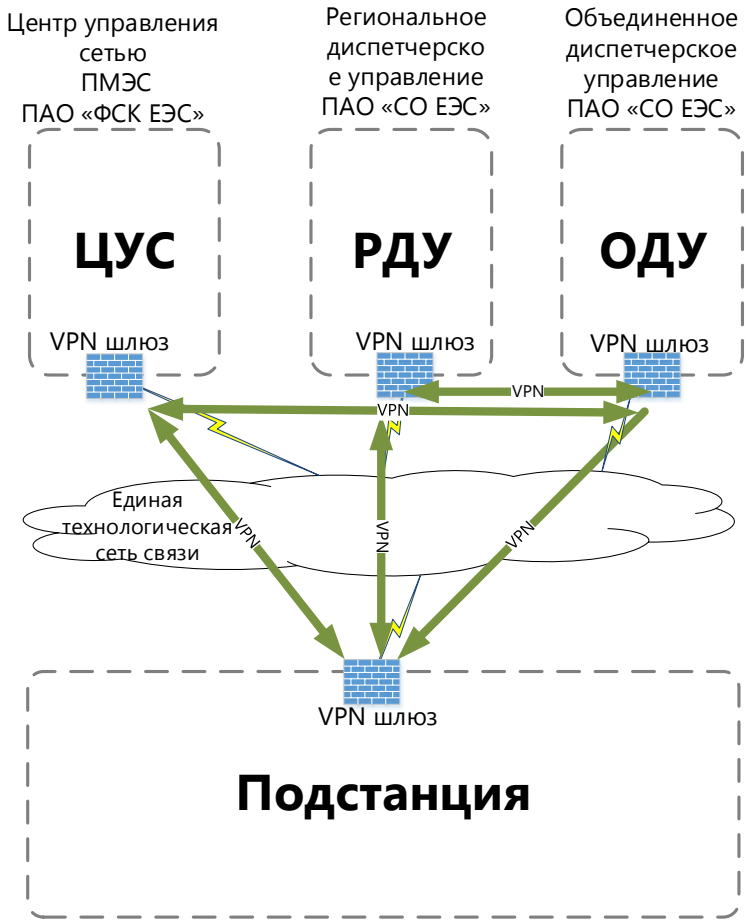
Организация удаленного телеуправления оборудованием подстанции



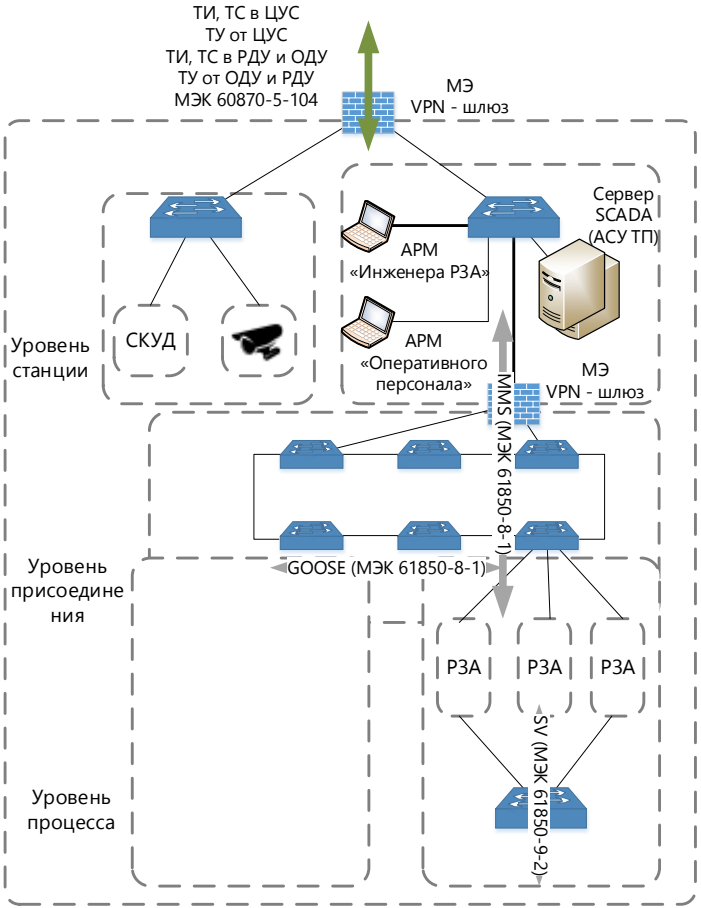
Оперативно-технологическое управление объектами ПАО «ФСК ЕЭС»



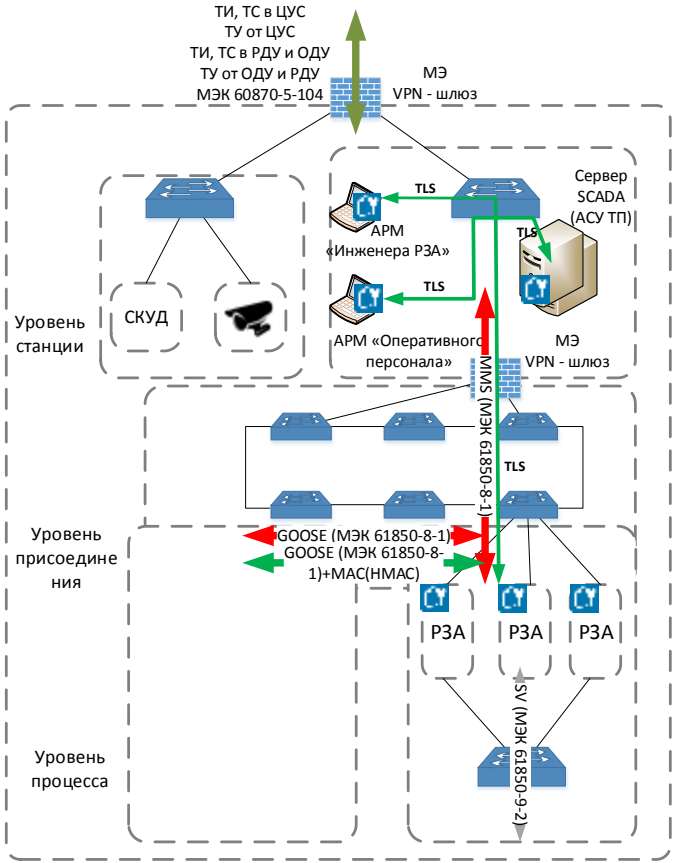
Использование VPN при защите ETCC

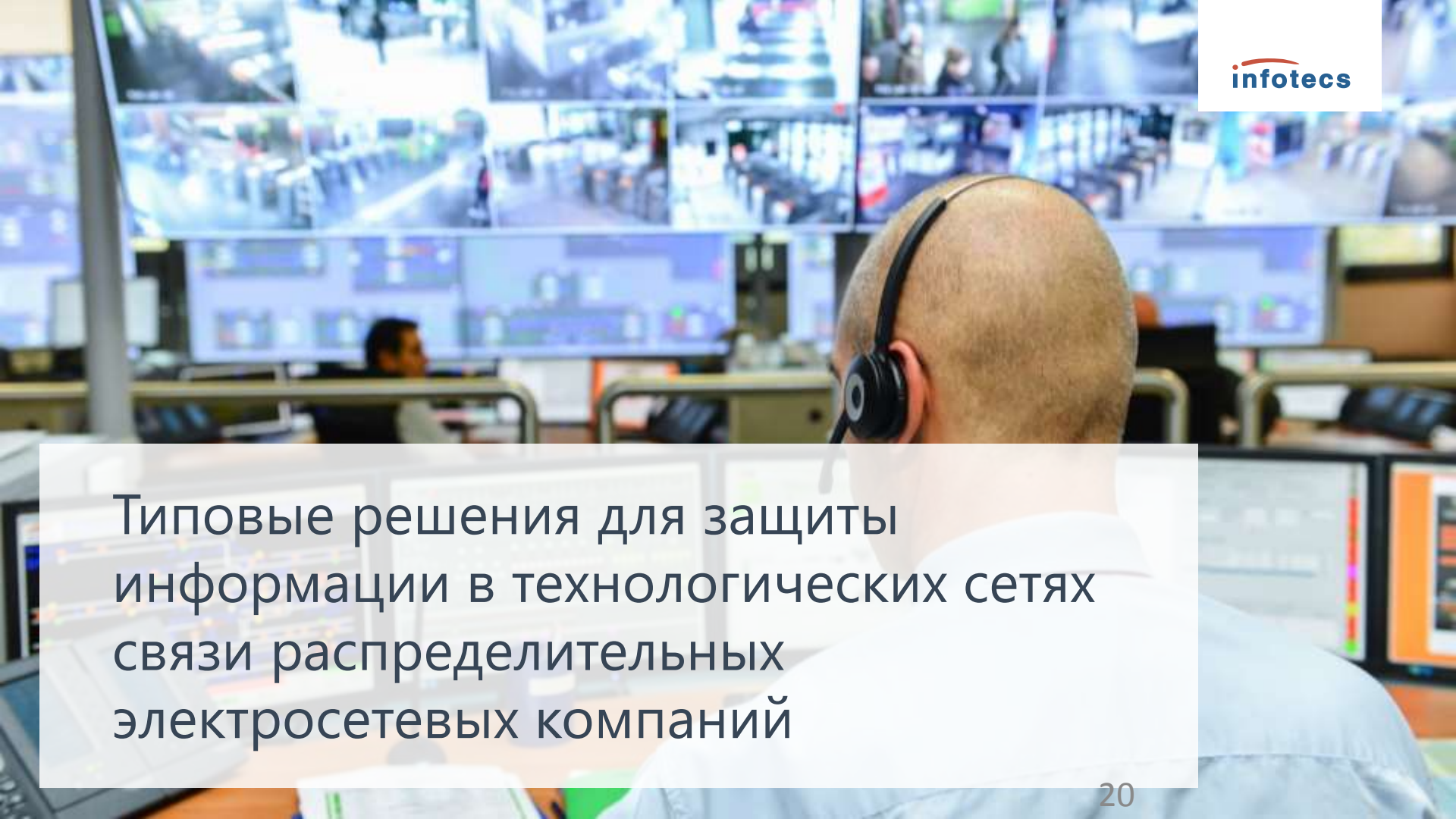


Реализация Киберзащищенной ПС



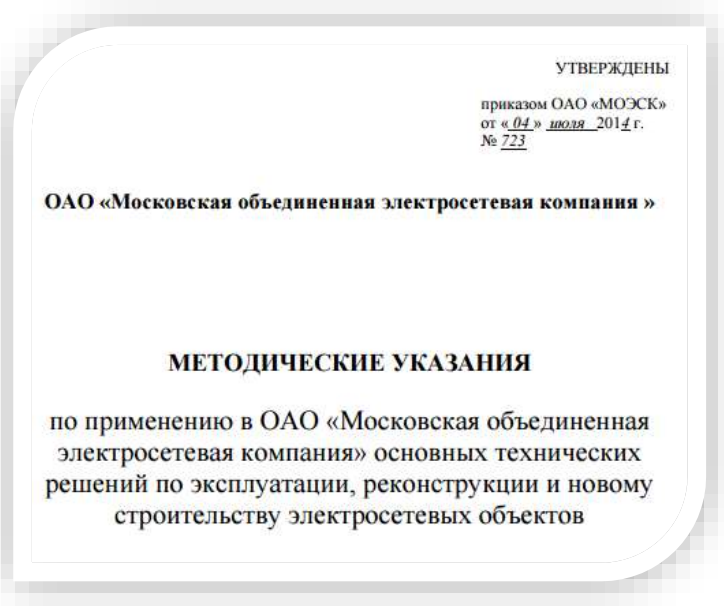
Построение подстанции нового поколения в киберзащищенном виде





Типовые решения для защиты информации в технологических сетях связи распределительных электросетевых компаний

Направления развития АСТУ



УТВЕРЖДЕНЫ

приказом ОАО «МОЭСК»
от «04» июля 2014 г.
№ 723

ОАО «Московская объединенная электросетевая компания »

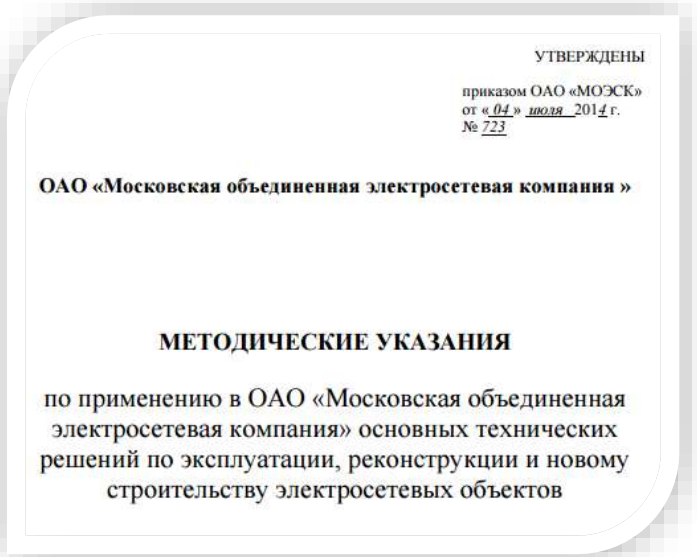
МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по применению в ОАО «Московская объединенная электросетевая компания» основных технических решений по эксплуатации, реконструкции и новому строительству электросетевых объектов

- Надёжное телеуправление подстанциями из ЦУС
- Развитие систем сбора и передачи информации
- Создание «цифровых подстанций»

Отраслевые требования

- Должен быть организован удалённый доступ к АСУ ТП ПС с АРМ служб РЗА и АСТУ ЭС ОАО «МОЭСК». При этом должен выполняться комплекс мероприятий по обеспечению информационной безопасности удаленного доступа.
- При использовании арендованных каналов связи (проводных и беспроводных) должны быть предусмотрены сертифицированные средства криптографической защиты информации (ГОСТ 28147-89).
- Система телемеханизации должна в наиболее полной мере соответствовать требованиям по обеспечению информационной безопасности стандартов МЭК 62351.



УТВЕРЖДЕНЫ

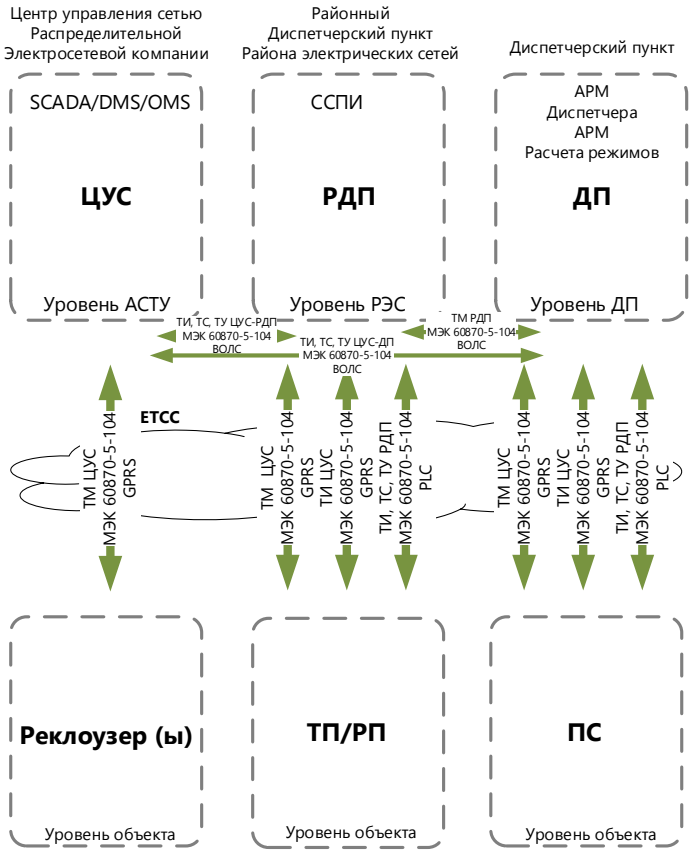
приказом ОАО «МОЭСК»
от «04» июля 2014 г.
№ 723

ОАО «Московская объединенная электросетевая компания »

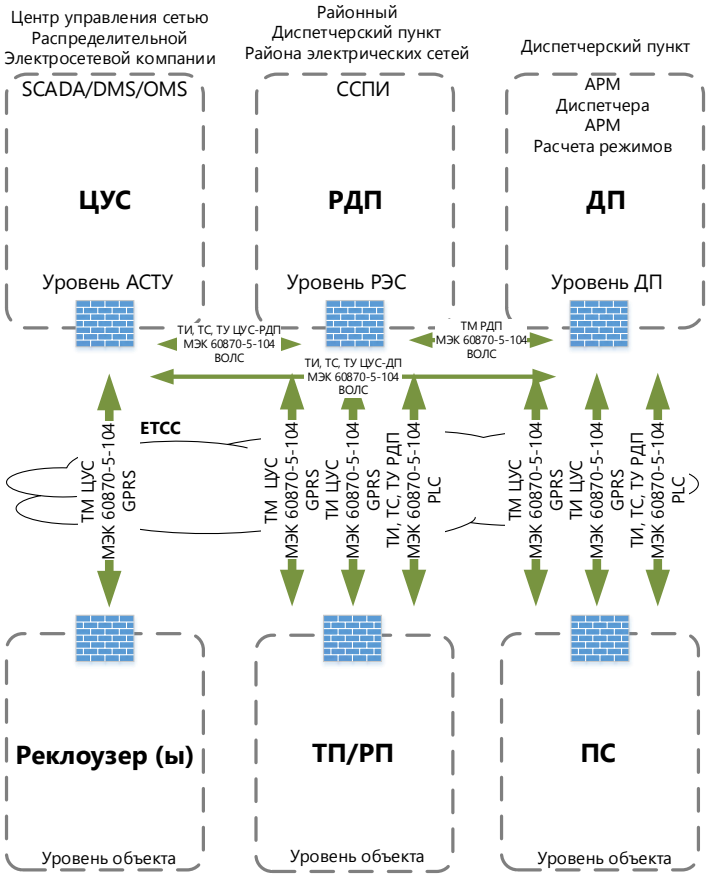
МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по применению в ОАО «Московская объединенная электросетевая компания» основных технических решений по эксплуатации, реконструкции и новому строительству электросетевых объектов

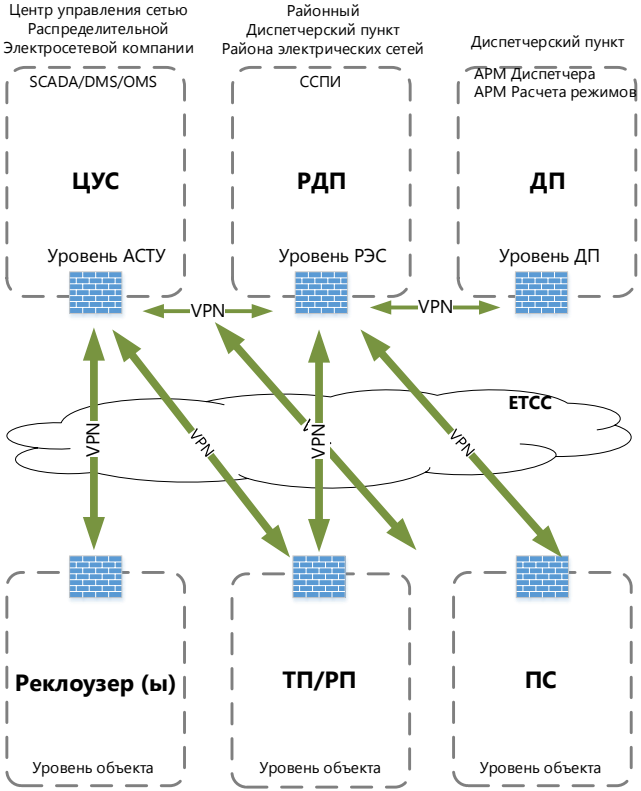
Информационные потоки ТМ в распределительных электросетях



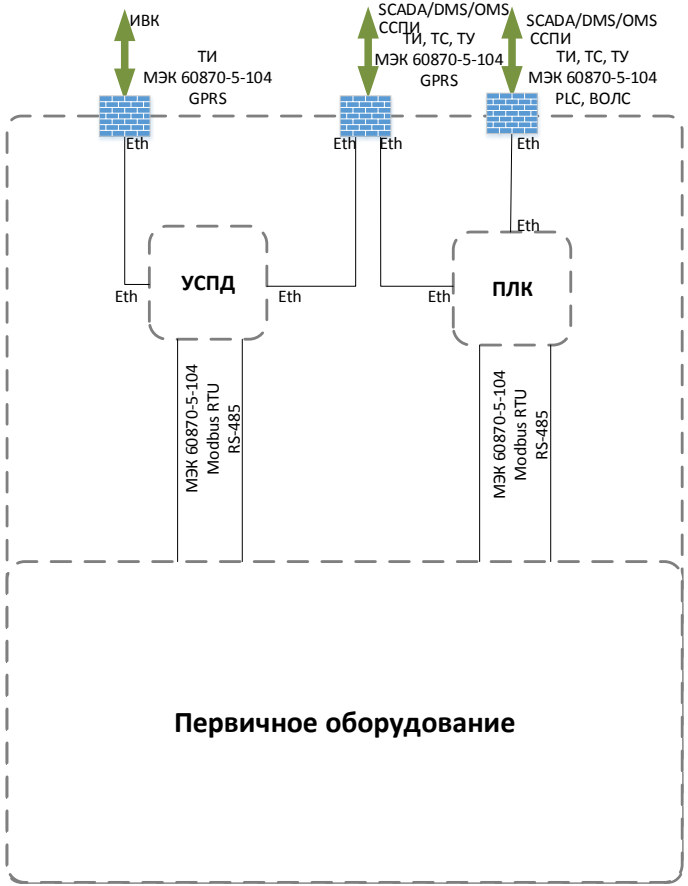
Разграничение информационных потоков ТМ распределительных электросетей



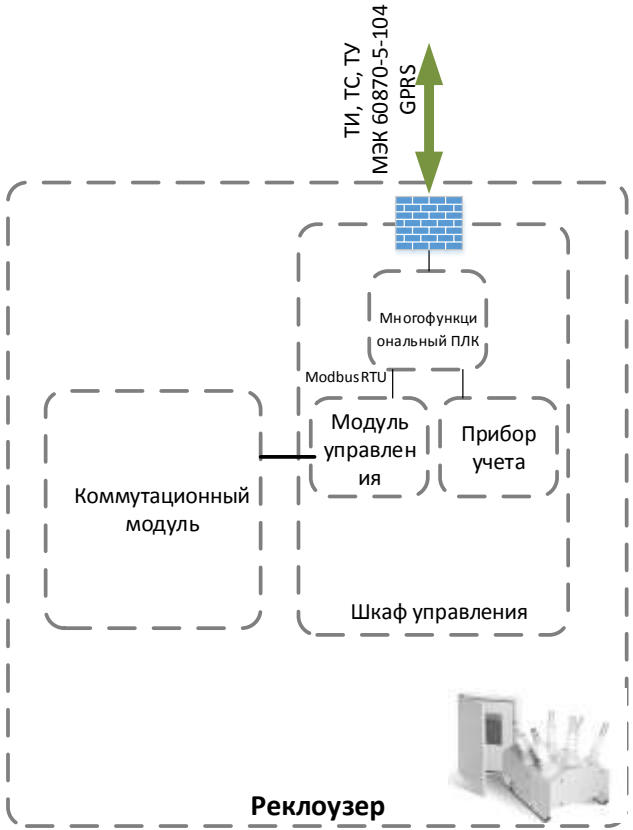
Использование VPN в распределительных электросетях



Организация защищенных каналов ТМ на ТП/РП



Организация защищенного канала ТМ при использовании реклоузеров



Выводы

- Необходимо продолжить формирование отраслевой нормативно-технической базы
- Необходимо осуществлять поэтапное построение системы защиты АСТУ
- При реализации планов перспективного развития ЕЭС РФ необходимо предусмотреть комплекс мероприятий по обеспечению киберзащищенности объектов электросетевого комплекса.
- Создаваемые продукты ИБ должны удовлетворять всему множеству специфических особенностей АСТУ ЕЭС РФ

Давайте пообщаемся!

Карантаев Владимир / к.т.н. / Член РНК СИГРЭ
Менеджер
Отдел развития продуктов
Vladimir.Karantaev@infotecs.ru / +7 915 221 15 96