Обобщение тенденций развития информационных систем и телекоммуникаций в ЭЭ

на основе анализа докладов ИК D2 45-й сессия CIGRE,

25-29 августа 2014 года, Париж (Франция)

Вериго А.Р., к.т.н., РТСофт
по материалам
индивидуального члена СИГРЭ
Данилина А. В.
Генерального директора ООО
«АльтероПауэр»

Основные направления работы ИК D2 в 2015-16г.

Управление

- Новые приложения для управления энергосистемой
- Объединение функций SCADA, EMS, DMS и рыночных приложений
- Приложения интеллектуальных адаптивных сетей для системных операторов и операторов сетей
- Большие данные – приложения и решения

Телекоммуникации

- Беспроводные технологии передачи данных – состав оборудования, приложения, платформы
- Применение общедоступных и частных (закрытых) инфраструктурных решений для организации сети связи
- Мобильные приложения, системы и технологии
- Развитие технологий создания каналов связи

Безопасность

- Анализ влияниея информационной безопасности на автоматизацию в ЭЭ
- Особенности информационной безопасности в сетях smartgrid
- Решения по информационной безопасности в инфраструктуре автоматизации
- Цифровые системы РЗА и ПА – вопросы безопасности

ИК D2: действующие рабочие группы

Консультативные группы

D2.01 Основные бизнес-процессы в информационных системах и сервисах

D2.02 Интеграция с другими исследовательскими комитетами и заинтересованными сторонами СИГРЭ

D2.03 Телекоммуникационные сети, услуги и технологии

Рабочие группы

D2.31 Архитектура безопасности для цифровых систем в электроэнергетике

D2.34 Телекоммуникационные и информационные системы для обеспечения непрерывности бизнеса и аварийного восстановления данных

D2.35 Масштабируемые коммуникационные решения для транспортных оптических сетей

D2.36 Коммуникационные решения для обмена информацией в smart-сетях передачи электроэнергии

Новые рабочие группы

D2.38 Решения для управления электроэнергетикой в ответ на кибер-угрозы, критически влияющие на инфраструктуру

JWGD2 / B2.39 Конструкции, создание и эксплуатация оптических кабелей связи на воздушных ЛЭП ВН

D2.40 Кибер-риски и кибер-безопасность для новых поколений цифровых систем в электроэнергетике

Основные задачи ИК D2 в 2015 - 2016

- Подготовка решений по обеспечению катастрофоустойчивости ИТ в электроэнергетике
- Повышение производительности и обеспечение безопасности ИТ
- Расширение функциональности сетей smartgrid
- Разработка решений для распределенной и возобновляемой генерации
- Подготовка к публикации «Зеленой книги» по информационной безопасности
- Выработка стратегии развития ИТ-инфраструктуры для предприятий электроэнергетики с переходом на облачные технологии
- Подготовка материалов по развитию SCADA/EMS систем и их интеграции с технологиями SMART GRID

Значимые публикации НТД ИК D2 в 2013 - 2014

- **Документ ТВ 588, WGD2.33 «Operations & Maintenance of Telecom Network and Associated Information System in the Electrical Power Utility» (Эксплуатация и техническое обслуживание сетей телекоммуникаций и связанных с ними информационных систем в электроэнергетике)**

Сравнительное исследование задач, средств и опыта эксплуатации / обслуживания телекоммуникационной инфраструктуры энергокомпаний для приложений дистанционного контроля и средств связи для дистанционной поддержки оператора в операционной среде энергосистемы

- **Документ ТВ 603, JWG D2 / B5.46 “Application and Management of Cybersecurity Measures for Protection and Control Systems” (Применение и контроль средств кибербезопасности для систем защиты и управления)**

Исследования применения и управление кибербезопасностью для систем защиты и управления (P & C) в ЭЭ. Обзор угроз кибербезопасности для защиты и управления. Краткий перечень практических решений для реализации кибербезопасности.

Доклады по тематике управления в ЭЭС

D2-102 «Изучение методов комплексной обработки событий с гарантированной доставкой («точно-в-срок») в системах сбора данных»
Ji Ye Wang*, Ning Li*, Ying Xin Xie*, Xiao Zhen Li, Da Peng Wang, Feng Yu Wang,
Beijing GuoDianTong Network Technology Co., LTD., Nari Group Corporation China

D2-105 « Система мониторинга и управления для оценки эффективности инвертора для солнечных источников электроэнергии »
R. GUEVARA*, C. TELLO, J. RODRIGUEZ,
Instituto de Investigaciones Eléctricas, Gerencia de Control Electrónica y Comunicaciones, México

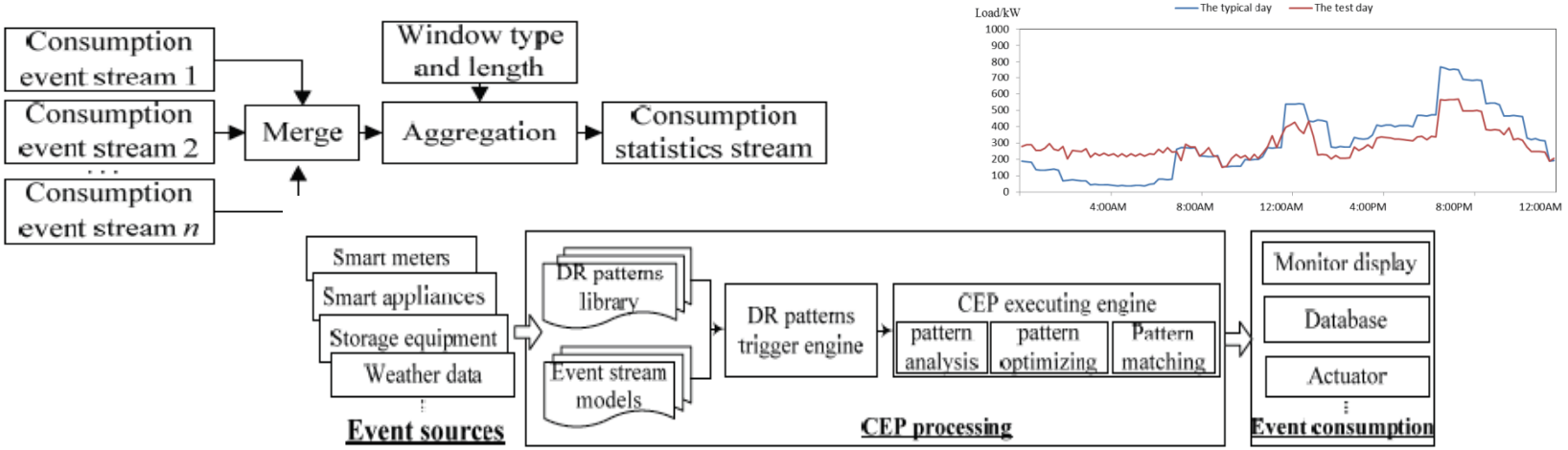
D2-107 «Будущее интеллектуальных систем измерения и управление получаемыми от них данными»
A.I. BATAINEH, NEPCO, Jordan

D2-108 «Применение web-сервисов для обмена данными на европейском рынке электроэнергии»
A. MARTÍN BARBERO E. JIMÉNEZ RAYA J. BEMBIBRE REGUEIRO,
RED ELÉCTRICA DE ESPAÑA, S.A.U., SPAIN

D2 – 307 Smart Grid на основе комплексной SCADA системы (опыт Индии)
K. R. Adisheshan TATA Consulting Engineers Ltd

Управление спросом на ЭЭ

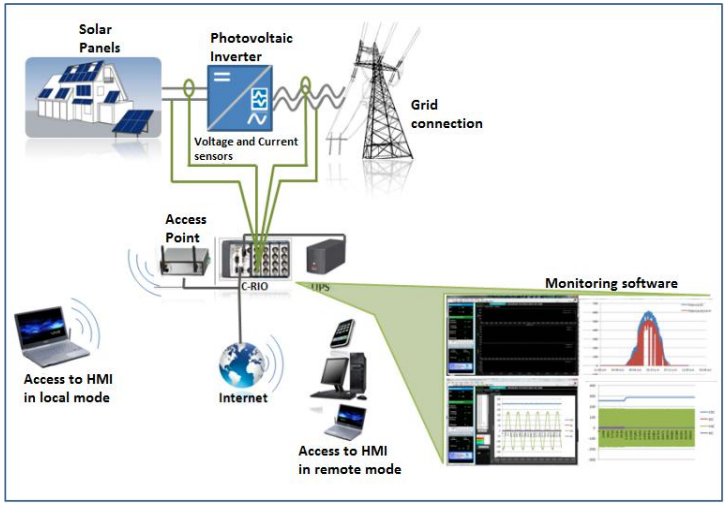
Применение в задачах мониторинга и управления генерацией и потреблением в режиме «по запросу» (On Demand Respond) технологии комплексной обработки событий (Complex Event Processing – CEP).



Технология CEP в реальном времени оперирует дискретными сигналами (или необработанными событиями) и комплексными (обработанными) событиями, являющимися результатом логической обработки. Двустороннее взаимодействие между сетью и потребителями с использованием CEP позволяет решить вопрос пикового спроса на ЭЭ с прогнозируемыми результатами.

Управление инвертером солнечных источников ЭЭ

Особенности настройки инвертора с обеспечением точной синхронизации и управления синхронной работой в реальном времени при подключении к электрическим сетям солнечных панелей.
Возможность получения различных характеристик и параметров работы солнечных источников энергии (гармонические составляющие, коэффициент мощности, форма волны тока и напряжения и др.).



Использование систем «умного» учета ЭЭ для обеспечения управления отключениями и для EMS/DMS-приложений

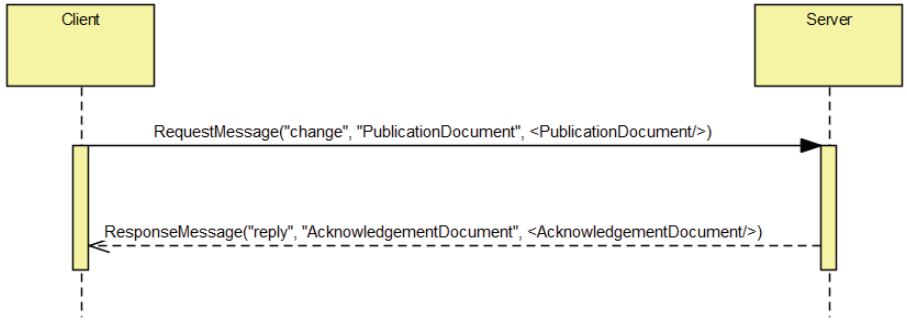
Вариант создания систем автоматизированного сбора показания учета (AMR) и развитой инфраструктуры измерений ЭЭ (AMI) в качестве информационной основы функционирования расчетно-аналитических систем (EMS|DMS) и систем управления отключениями.
Особая роль для реализации системы - интеграции со smart metering и ГИС

Применение web-сервисов для информационного обмена на европейском рынке электроэнергии ЭЭ

Переход от технологий обмена сообщениями в форматах, определенных ENTSO-E, посредством различных транспортных технологий (электронная почта, FTP и др.) к обмену сообщениями, сформированными в соответствие с требованиями стандарта МЭК 61968-100, используя в качестве транспортного механизма реализацию требований стандарта МЭУ 62325-451-n

Стандарт МЭК 61968-100 – для определения структуры сообщения, необходимого для взаимодействия посредством web-сервисов

Использование IEC 61968-100 обеспечивает различные модели отношений при обмене («Простой запрос / ответ»), «Запрос / Ответ с ESB», "События" и т.д.)



В результате - существенное снижение затрат времени и финансов на реализацию взаимодействия

Доклады по тематике технологий связи и ИТ

D2-106 “Стратегический выбор распределительных электросетевых компаний для организации частных телекоммуникационных сетей” G. ROBICHON, Alliander, Netherlands

D2-103 «Коммуникации по ЛЭП для интеграции распределенной генерации» DAVID GIL (DG), ASIER LLANO (AL), FERNANDO CASTRO (FC), JOSE ANTONIO MORENO (JAM), SONIA MARTÍNEZ (SM), TXETXU ARZUAGA (TA)* ZIV CG Automation SPAIN

D2-109 «Опыт использования ВОЛС-ВЛ в Red Electra de Espana» S. KWIK ALLAN*, J.M. DELGADO ÁLVAREZ, Red Eléctrica de España (REE) - Telecommunications Department, Spain

D2-201 «ИТ-платформы японских электроэнергетических компаний» T. YOSHIDA M. KIKEGAWA Kyushu Electric Power Co., Inc. Tohoku Electric Power Co., Inc., R. HOSHIKAWA M. Okamoto Shikoku Electric Power Co

D2-202 «Опыт и практика внедрения управления ИТ в мексиканских электросетевых компаниях» I. PARRA, G. ARROYO*, A. GARCIA, Instituto de Investigaciones Eléctricas, Comisión Federal de Electricidad, MEXICO

D2-302 «Опыт работы с сетями IP/MPLS» Thomas Leroy, Elia, Belgium

D2-303 «Изменение требований бизнеса Eletrobras Elenorte к телекоммуникациям, управлению и обслуживанию» MARCELO COSTA DE ARAUJO, MARCOS ALVES RODRIGUES Eletrobras Eletronorte, Brazil

D2 – 305 Управление адаптированной архитектурой пакетной сети для сервисов на базе смарт-IP. M. MESBAH, A. MOAINI, V. MENEGUIM, Alstom Grid, France, Brazil

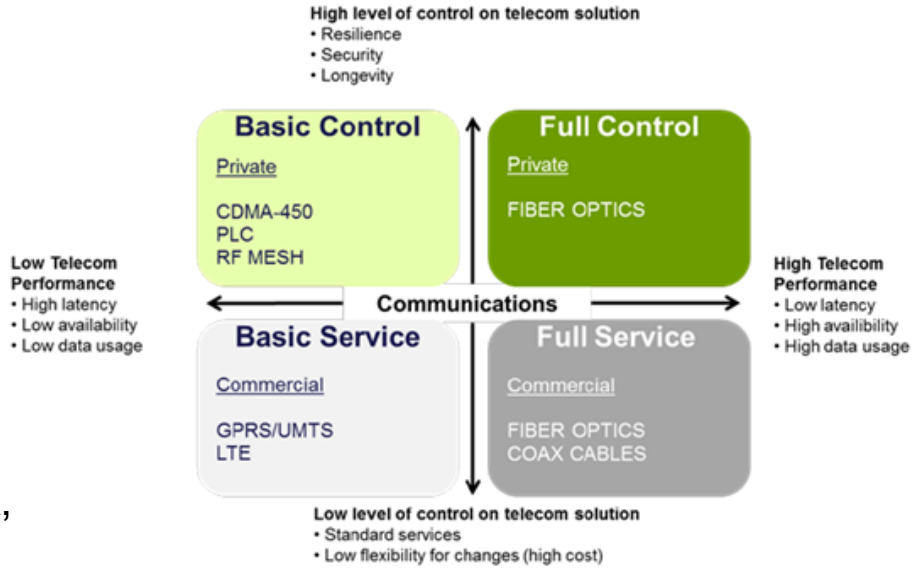
D2 – 306 Проблемы создания крупных сетей связи на основе ВОЛС в грозозащитном тросе (опыт Индии) N.S. Sodha, H.H.Sharan, Sheela Rani, Power Grid Corporation of India

Стратегический выбор: построение собственной сети связи или использование сетей провайдеров

- Серьезные изменения в технической инфраструктуре современной электроэнергетики Европы ведут к глобальному изменению ИТ-инфраструктуры.
- Развитие распределенной генерации, возобновляемых источников электроэнергии, размещение у потребителей интеллектуальных контрольно-измерительных систем - возрастает до критического уровня зависимость от надежности телекоммуникаций и их безопасности
- Анализ требований к телекоммуникационной сети энергокомпании – вывод о целесообразности построения собственных сетей связи.

Рекомендованы технологии для создания собственных телекоммуникационных сетей по комплексному критерию производительность / уровень управления:

- PLC (Power Line Communication) – передача данных по электрической сети
- RF Mesh сети (радиочастотные)
- Частные беспроводные сети, построенные на технологиях типа CDMA, для частотного диапазона 450 МГц



Преимущество отдано технологиям CDMA 450 МГц

Развитие телекоммуникационных сетей на основе ВОЛС по воздушным ЛЭП

- Особенности конструкции волоконно-оптического кабеля (ВОК), интегрированного в фазный провод ЛЭП (*OPtical Phase Conductors,* OPPC).
- Сравнение OPPC с ВОК в грозозащитном тросе (OPGW) – технологии, монтаж, эксплуатация
- Исследовательские и экспериментальные проекты с описанием технических деталей ВОК и использования сопутствующих эффектов – применение свойств ВОК для анализа температуры проводов

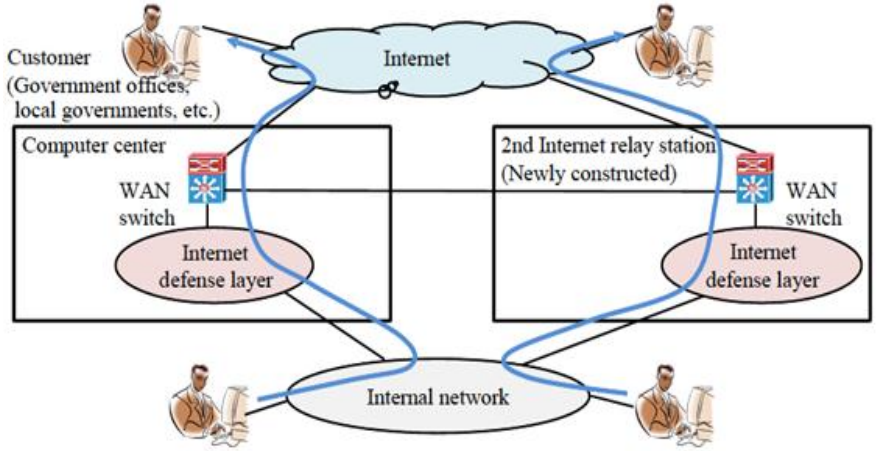
Создание и управление сетями на основе ВОЛС

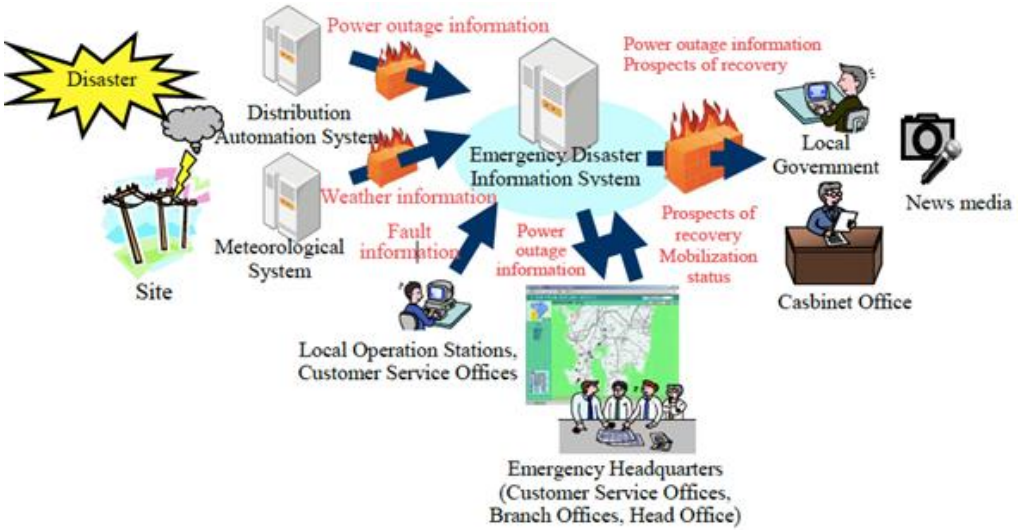
- Опыт создания крупномасштабных (около 9500 км) сетей телекоммуникации на основе ВОЛС с применением OPGW на ЛЭП высокого напряжения для различных приложений (SCADA / EMS, голос, WAMS и пр.)
- Преимущества использования OPGW, включая монтаж ВОК без снятия напряжения
- Организационные проблемы и решения при массовом развертывании ВОЛС на базе ЛЭП

Обеспечение устойчивости телекоммуникаций к катастрофам

В основе решения - технологии виртуализации и облачных вычислений

- Дополнительные центры обеспечения связи и телекоммуникаций
- Дополнительные системы мониторинга работы оборудования и ПО

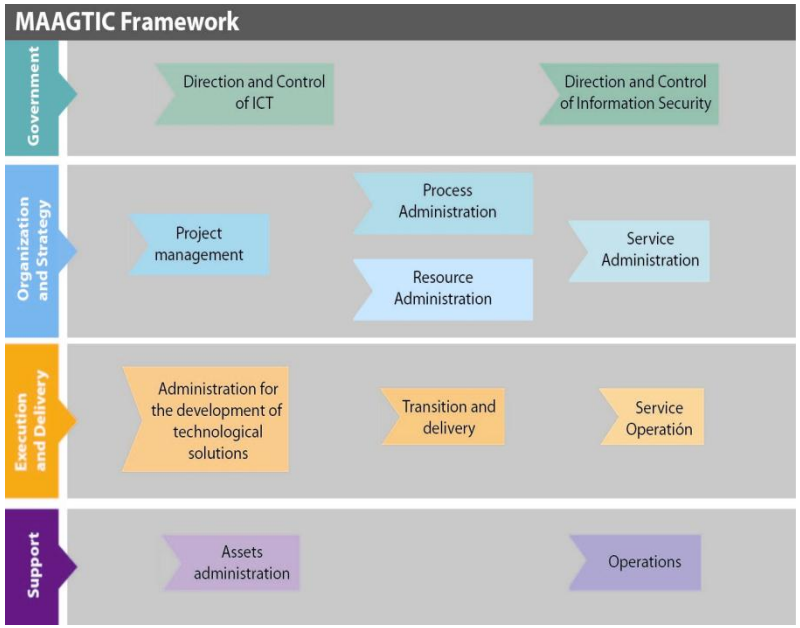


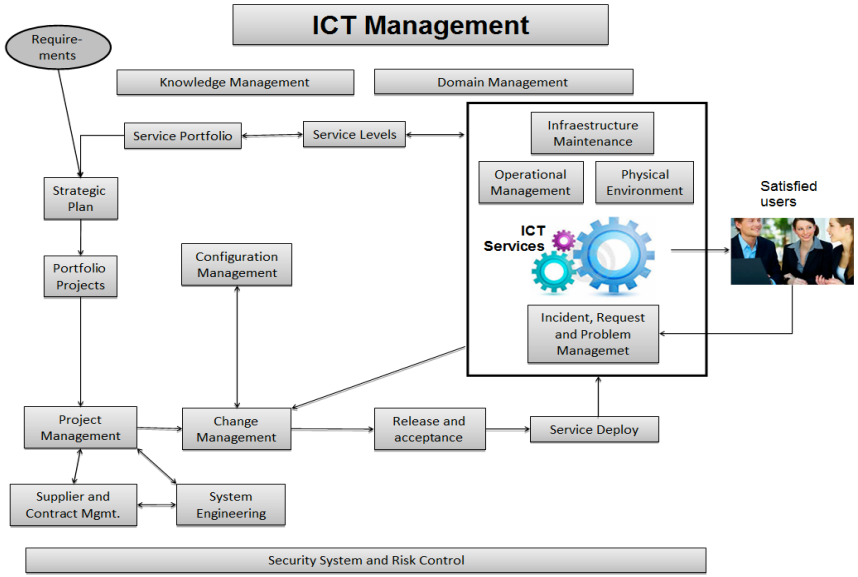


- Создание информационных центров, сообщающих об авариях и бедствиях
- Особые строительные решения (сейсмоустойчивый пол)

Разработка правил по внедрению и сопровождению инфраструктурных и технологических решений в ИТ

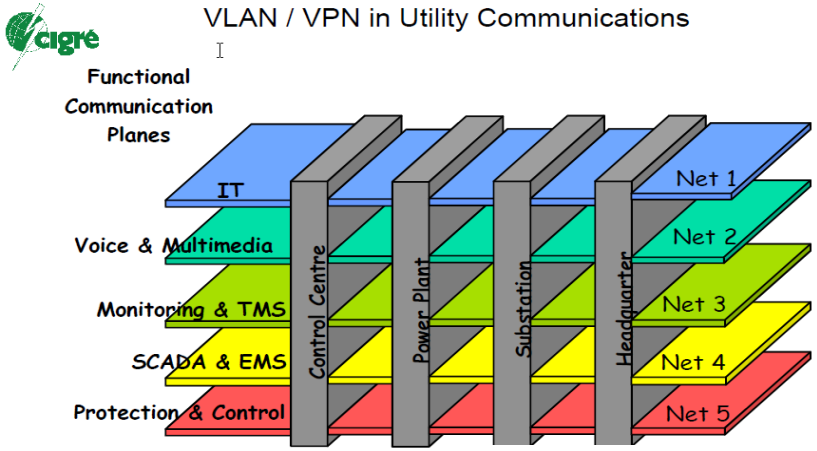
- Фреймворк MAAGTIC-SI на базе ITIL, COBIT, IEC 62351 и ISO 9001 для управления качеством услуг и PMI для проектного управления
- Архитектурно-технические решения на базе методологии TOGAF
- Управление более чем 5000 серверами и около 70 000 ПК, поддержка более чем 400 информационно-технологических и управленческих систем





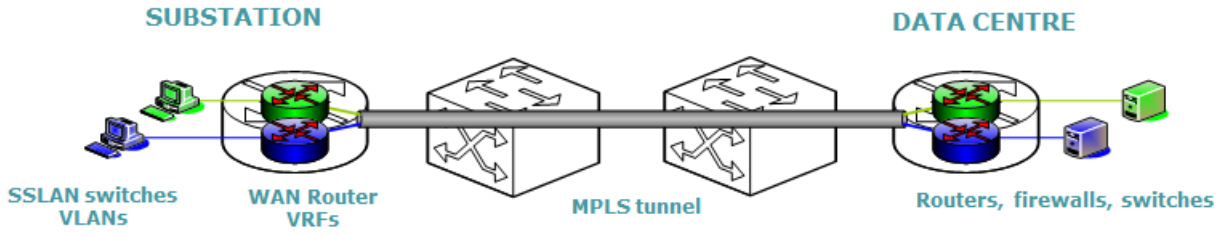
Организация телекоммуникационных сетей на базе парадигмы виртуализации

- Использование технологии IP / MPLS (Internet Protocol / Multi-Protocol Label Switching) в компаниях транспорта ЭЭ при создании Виртуальных частных сетей (Virtual Private Networks) для собственных нужд, а также для безопасного подключения к внешним сетям
- Обеспечение разделения собственного трафика и изоляция потоков с внешними сетями



Эффекты внедрения:

- Большая пропускная способность для приложений различных классов
- Классификация трафика и управление качеством передачи
- Интеллектуальное управление трафиком (Traffic Engineering)
- Поддержка VPN



Телекоммуникации при создании решений Smart Grid

Стандартизация и классификация сетей телекоммуникаций:

- HAN (Home Area Network): объединяют устройства в рамках одного здания или дома (интеллектуальные счетчики).
- NAN (Neighbourhood Area Network): включают коммуникации между зданиями и сооружениями потребителей и вторичными подстанциями.
- UAN (Utility Area Network): сети, охватывающие подстанции и центр обработки данных электросетевого предприятия

Рекомендации по характеристикам сетей для каждого вида сервисов

Service	Topology	Capacity	Latency	Availabilyty	Integrity
Telecontrol	H&S (1) Symetrical	Very low (<10 kbps)	Medium (<10 s) (2)	High	High
Protection	FM (p2p) Symetrical	High (3) (> 1Mbps)	Very low (< 6 ms)	Very high	Very High (BER<10-6)
Metering	H&S Asymetrical	Medium (< 50 kbps)	Not a constraint	Medium	Low
Distribution Automation	FM Symetrical	High	Very low	Medium	Low
Management	H&S Asymetrical	Medium (<100 kbps)	Not a constraint	High	Low

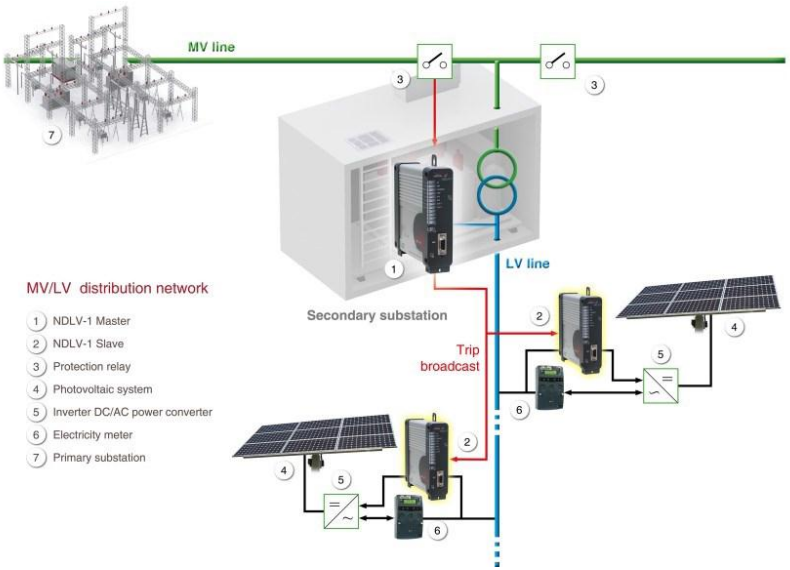
Телекоммуникации при создании решений Smart Grid

Использование PLC-технологии для управления распределенной генерацией

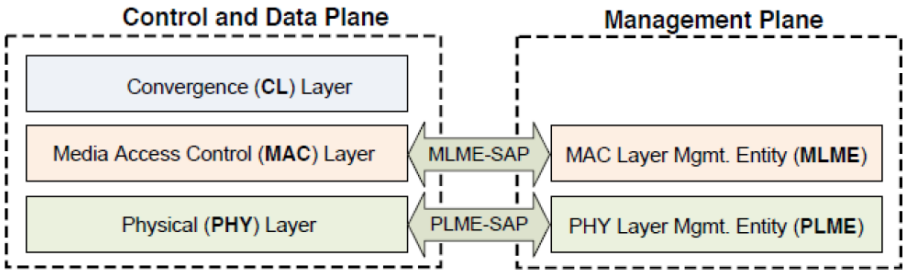
- требование постоянной связи с источниками распределенной генерации (Distributed Energy Resources, DER) на стороне НН и СН для обеспечения управления в режиме on-line
- анализ эффективности использования различных технологий PLC, в частности Powerline Intelligent Metering Evolution (PRIME)
- возможность передачи данных от DER с использованием современных систем учета ЭЭ

Исследованы параметры канала PLC, определяющие качество канала связи:

- шумовые характеристики
- импульсные характеристики
- импеданс



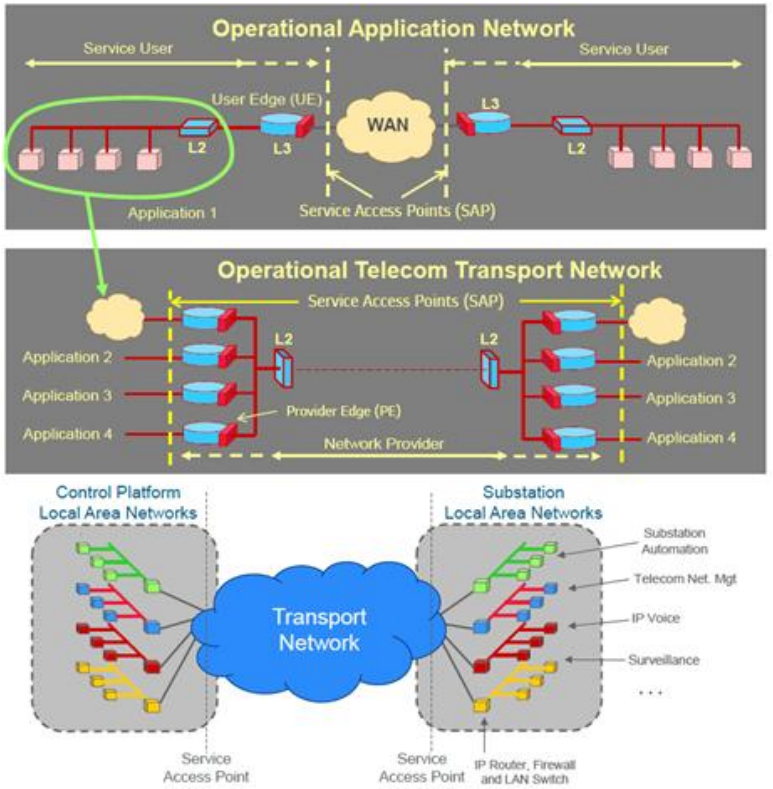
Уровни связи в PRIME:

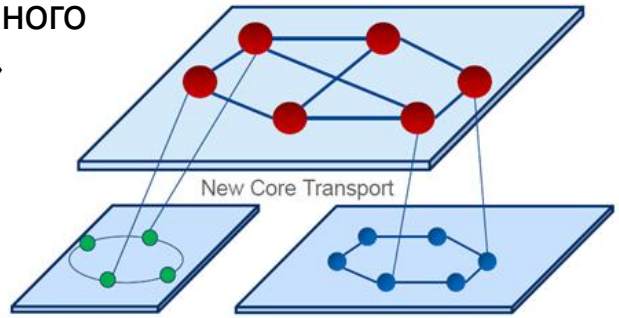


Управление адаптированной архитектурой пакетной сети для сервисов на базе смарт-IP

Анализ адаптированных сетевых архитектур с коммутацией пакетов

- Гибридные иерархические решения (метод наложения) для построения IP-сетей и инструменты управления ими
- Управление сетевыми приложениями с использованием стандарта off-the-shelf IP (расширение Common Industrial Protocol)
- Разделение сетей AN от TN - упрощение архитектуры и эксплуатации телеком-сетей
- Создание транспортной сети независимо от миграции подсети и возможность соединения их в дальнейшем
- Миграция в новую архитектуру по кластерам - возможность «мирного сосуществования» старых и новых подсетей





Доклады по теме ИБ в электроэнергетике

D2-101 «Изучение и практика оценки состояния информационной безопасности в интеллектуальных сетях»

Gao Kunlun, Wang Yufei (China Electric Power Research Institute, China), Xu Ruzhi (North China Electric Power University, China)

D2-104 «Безопасность коммуникаций в задачах контроля напряжений распределённой генерации: анализ воздействия и аномальное поведение»

G.Dondossola, R.Terruggia (Ricerca sul Sistema Energetico – RSE spa, Italy)

D2-203 «Безопасность использования удалённого доступа в электроэнергетических компаниях»

P.Sitbon, C.Poirier (Electricité de France, France), J.Zerbst (Vattenfall, Sweden), D.K.Holstein (OPUS Consulting, USA), M.Scherer (Alstom, France), R.Evans (Snowy Hydro Ltd, Australia), Marc Tritschler (PA Consulting, UK)

D2-304 «Анализ информационной безопасности телекоммуникаций»

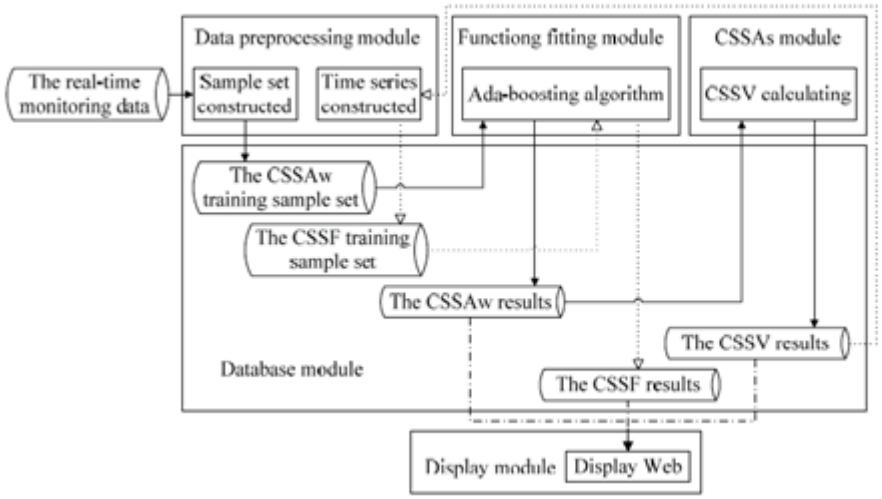
A.Temporal, H.Burle, C.A.Bastos
Companhia Hidro Elétrica do São Francisco, Brasil

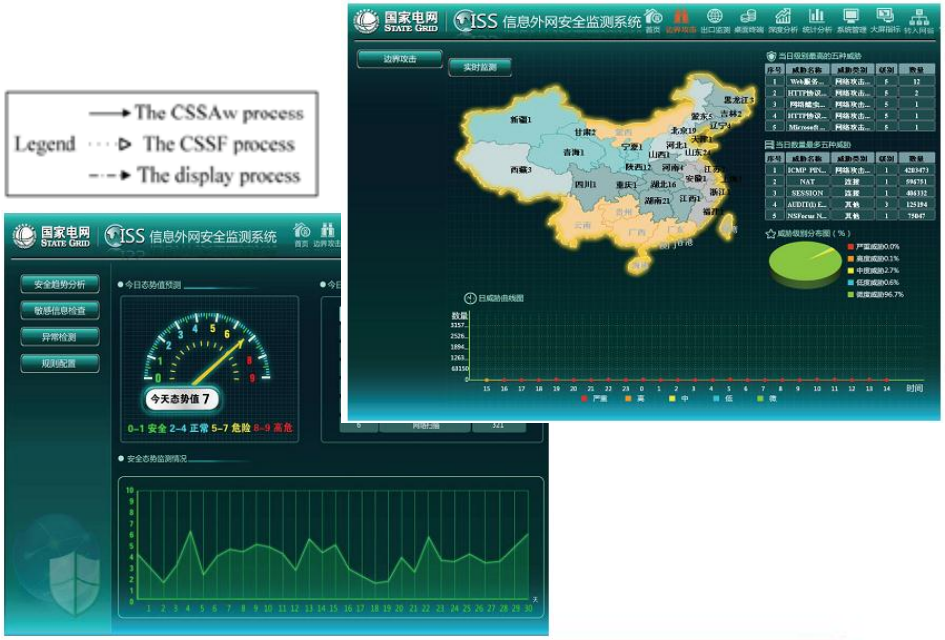
Методы оценки состояния ИБ для сетей Smart Grid

Технология оценки состояния ИБ (ситуационный анализ) на базе алгоритма AdaBoost (Адаптивное усиление классификаторов):

- мониторинг и анализ сетевого трафика в узлах сети
- выявления возможных событий нарушения кибербезопасности
- идентификация различных видов кибератак (CSSE)
- интеграция результатов мониторинга сегментов сети в общую картину безопасности (CSSAs)
- прогнозирование развития опасных ситуаций (CSSF)

Раннее предупреждение об угрозах кибербезопасности в электросетевой компании

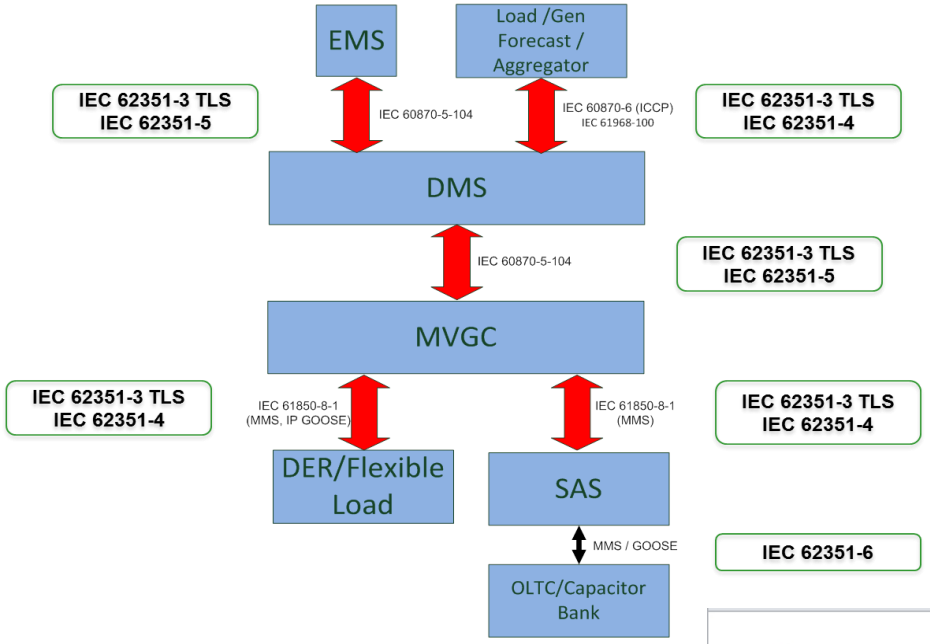




Безопасность коммуникаций в задачах управления распределенной генерацией: критерии анализа рисков

Степень риска	Нагрузка	Потребление энергии	Население	Инфра-структура	Защита информации	Законы и нормы регулирования	Потери для популяции	Репутационные риски	Финансовые риски
КРАЙНЕ КРИТИЧЕСКИЙ	Региональные сети более 10 ГВт	от 10 ГВт/ч	от 50% населения стран или от 25% в нескольких странах	Воздействие на международную инфраструктуру	Не определен	В случае закрытия компании или нарушения залогового обеспечения	Прямые и косвенные случаи летального исхода в нескольких странах	постоянная потеря доверия влияет на всю корпорацию	Пострадавшие третьей стороны
КРИТИЧЕСКИЙ	ЕЭС от 1 ГВт до 10 ГВт	от 1 ГВт/ч до 10 ГВт/ч	от 25% до 50% численности населения страны	Воздействие на ключевую национальную инфраструктуру	Не определен	Временное прекращение деятельности	Прямые и косвенные случаи летального исхода в стране	Постоянная потеря доверия в стране	>=50% EBITDA
ВЫСОКИЙ	Городские сети от 100 МВт до 1 ГВт	от 100 МВт/ч до 1 ГВт/ч	от 10% до 25% численности населения страны	Воздействие на базовую инфра-структуру	Несанкционированное раскрытие или модификация конфиденциальных данных	Тюремное заключение	Прямые случаи летального исхода в стране	Временная потеря доверия в стране	<50% EBITDA
СРЕДНИЙ	Районные сети от 100 МВт до 100 МВт	от 10 МВт/ч до 100 МВт/ч	от 2% до 10% численности населения страны	Воздействие на вторичную инфра-структуру	Несанкциони-рованное раскрытие или модиф-ия персональ-ных данных	Штрафные санкции	Серьезные повреждения	Временный и локальный ущерб, потеря доверия	<33% EBITDA
НИЗКИЙ	Домашние (собственные) сети или сети зданий/сооружения ниже 10 МВт	ниже 10 МВт/ч	ниже 2% численности населения страны	Без воздействия на вторичную инфра-структуру	Персональные и конфиден-циальные данные не повреждены	Предупреждение	Незначительные несчастные случаи	Ограничение во времени & объеме (предупреж-дение)	<1% EBITDA

Обеспечение безопасности управления ИТ- ресурсами



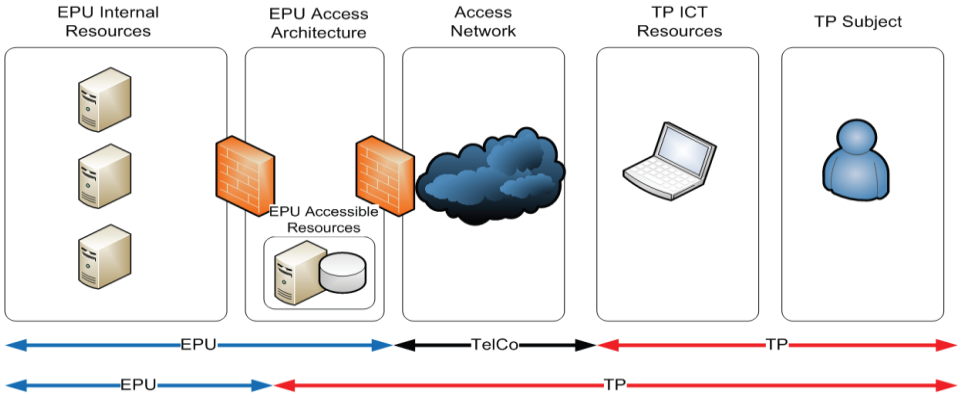
Анализ стандартов по обеспечению ИБ в ЭЭ и область их применения на примере управления напряжением (VC) для распределенных энергоресурсов (РЭР, DER)

Критерии оценки воздействия на информационные активы с группировкой по сценариям атак и типам нарушителей (на примере VC РЭР)

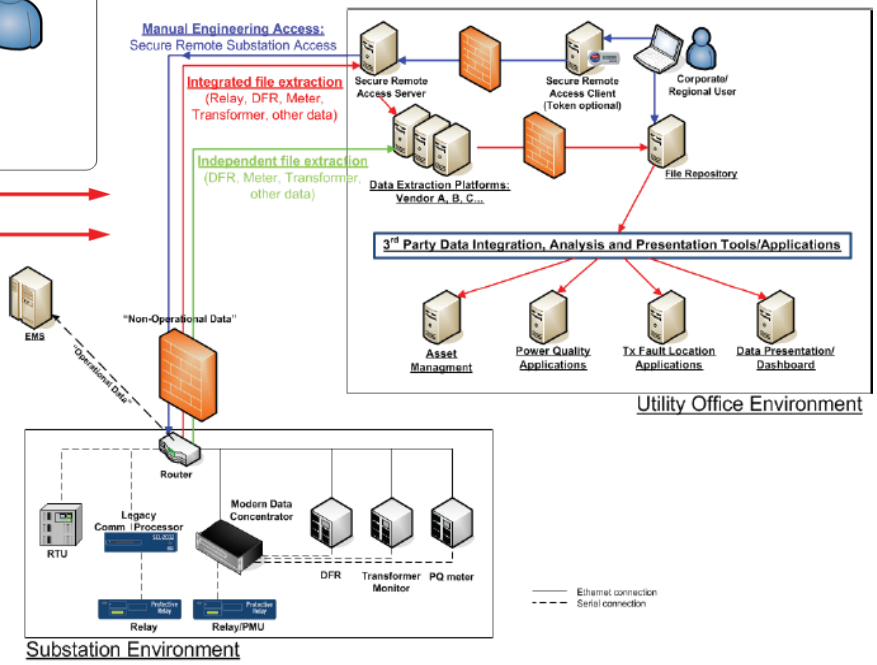
Нарушитель	Тип (направление) коммуникаций		
	ПС - РЭР	ЦУС - ПС	ПС - ЦУС
Нечестный сотрудник **(Admin)**	Очень высокий	Критический	Очень высокий
Нечестный сотрудник **(user)**	Высокий	Средний	Средний
Вандал	Очень высокий	Высокий	Низкий
Хакер	Очень высокий	Высокий	Средний
Террорист	Средний	Очень высокий	Очень высокий

Безопасность удаленного доступа к ИТ- ресурсам

Насущная необходимость обеспечения удаленного доступа к ИТ-ресурсам энергокомпаний для смежных по производственному процессу организаций (потребители, диспетчерские центры) для технического обслуживания или мониторинга



Разработка типовых архитектурных решений для организации удалённого доступа



Безопасность удаленного доступа к ИТ-ресурсам

Цели безопасности на компонентах архитектуры сети для удаленного доступа:

Компоненты Цели	Внутренние ресурсы	Архитектура доступа	Доступ к сети	ИТ/Ком ресурсы третьих лиц	Действия третьих лиц
Строгий контроль доступа на всех: сеть, система, функция, уровень данных	Предпочтение только исходящих потоков	Создание единой DMZ для простоты аудита	Нет прямого подключения к Интернет	/	Именной доступ
		Сегментация по подрядчикам			Удаление аккаунта
					Аутентификация по 2-м факторам
Предотвращение эксплуатации уязвимостей или «задних дверей» на удаленном устройстве обслуживания	Предпочтение только исходящих потоков	Жесткая защита станции управления	Нет прямого подключения к Интернету	Использование выделенного устройства	Обследование сотрудников
	Удаленное управление с помощью одной станции				Обучение сотрудников
	Принцип 4-х глаз				
Сохранение конфиденциальности и целостности данных	/	Сегментация по подрядчикам	Использование криптографии	Использование выделенного устройства	Обследование сотрудников
			Сегментация сети по подрядчикам		Процедуры обработки
			Предпочтение частных сетей		
Протоколирование любых действий дистанционно с помощью техники третьей стороны	Удаленное управление с помощью одной станции	Настройка одной DMZ для простоты аудита	/	/	Именной доступ
Проверка безвредности дистанционного обслуживания для части ИТ-системы	Удаленное управление с помощью одной станции	/	Физическое разделение между сетью на ПС и сети удаленного доступа	Проверка на тестовых платформах до развертывания действующих	Обследование сотрудников
	Принцип 4-х глаз			Предпочтение автоматизированных скриптов	Удаление аккаунтов
Предотвращение утечки данных	Удаленное управление с помощью одной станции	Жесткая защита станции управления	Использование криптографии	Использование выделенного устройства	Процедуры обработки
					Обучение
					Обследование сотрудников

Анализ рисков в телекоммуникационной среде

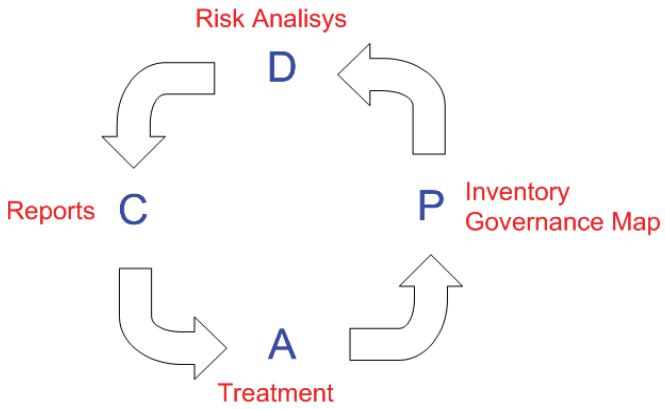
Численное измерение показателей риска ИБ для всех ИТ-активов на основе вероятностей последствий для основного бизнеса компании

Классификация активов по 4-м основным группам формирования рисков:

- человеческие ресурсы
- организационно-экономические процессы
- материальные активы среды передачи
- технологии и оборудование

Разработка политики «ИБ управления телекоммуникационной средой»:

- Управление физическим и логическим доступом
- Резервирование критически важной информации
- Классификация информации и управление активами
- Управление ресурсами для сервисов «по требованию»
- Управление соответствием требованиям ИБ
- Управление непрерывностью бизнеса
- Физическая защита телекоммуникационной среды
- Информация управления инцидентами безопасности
- Изменение и управление конфигурацией
- Управление безопасностью с учетом человеческого фактора
- Процесс управления рисками
- Системы оперативного управления безопасностью



Жизненный цикл управления рисками

Спасибо за внимание

Вериго А.Р., ЗАО «РТСофт»
verigo_ar@rtsoft.msk.ru
тел. +7 (495) 742-68-28, 967-15-05 (доп. 1407)