

Организация телеуправления подстанциями без постоянного присутствия обслуживающего персонала. Комплексный подход.

ФЕДОРОВ О.А., НЕБЕРА А.А., ЛИТВИНОВ П.В.
ЗАО «РТСофт»
РОССИЯ
fedorov_oa@rtsoft.msk.ru

КЛЮЧЕВЫЕ СЛОВА

Телеуправление, информационная безопасность, центры управления, релейная защита, технологические блокировки.

1 ВВЕДЕНИЕ

Обеспечение возможности надежного и безопасного телеуправления (ТУ) оборудованием подстанций является необходимым условием для использования современных методов и средств управления электрическими сетями с целью повышения эффективности их функционирования.

В ряде стран уже накоплен достаточно длительный (15-20 лет) опыт эксплуатации подстанций без постоянного присутствия обслуживающего персонала с обеспечением удаленного управления переключениями из диспетчерских центров. В последние годы традиционный состав задач телеуправления расширяется за счет реализации функций телерегулирования, автоматизированного управления вводом-выводом функций и групп уставок РЗА [3].

В российских сетях широкое применение ТУ до недавнего времени сдерживалось, в основном, более длительными процессами перехода к использованию коммутационных аппаратов и РУ повышенной надежности, создания телекоммуникационной инфраструктуры и развития нормативной базы. По мере решения этих вопросов обеспечение ТУ в рамках перехода к подстанциям нового поколения без постоянного присутствия обслуживающего персонала становится все более актуальным.

При этом основными целями реализации ТУ являются:

1. снижение количества технологических нарушений, связанных с ошибками оперативного персонала ПС при производстве переключений;
2. повышение оперативности выполнения оперативных переключений;
3. создание условий для использования современных алгоритмов и средств управления, реализуемых в составе современных программных комплексов диспетчерского и оперативно-технологического управления и обеспечивающих:
 - автоматизацию управления переключениями с контролем допустимости их выполнения;
 - повышение эффективности функционирования сетей, сокращение технологических потерь электроэнергии за счет оптимизации электрических режимов.

В настоящем докладе предлагается комплексный подход к организации телеуправления, обеспечивающий необходимый уровень функциональности, а также технологической и информационной безопасности.

2 КОМПЛЕКСНАЯ ОРГАНИЗАЦИЯ ТЕЛЕУПРАВЛЕНИЯ

2.1 Постановка задачи

Новые Правила переключений в электроустановках [1] вводят понятие подстанций нового поколения, допускающих эксплуатацию, в т.ч. выполнение переключений, как в

присутствии, так и без постоянного присутствия обслуживающего персонала. Отличительными признаками подстанции нового поколения согласно [1] являются:

1. дистанционное управление всеми коммутационными аппаратами и заземляющими разъединителями первичной схемы электрических соединений с АРМ АСУТП ПС и контроллеров присоединений оперативным персоналом подстанции с возможностью дистанционного управления с АРМ персонала центра управления сетями (ЦУС);
2. наличие программной (логической) оперативной блокировки, реализуемой на серверах и контроллерах АСУТП ПС;
3. применение элегазовых, вакуумных выключателей или КРУЭ;
4. наличие блокировки, исключающей возможность одновременного управления оборудованием объекта электроэнергетики с АРМ оперативного персонала подстанции, АРМ оперативного персонала ЦУС, АРМ персонала диспетчерского центра (ДЦ), с контроллеров присоединений;
5. применение микропроцессорных устройств РЗА.

Подстанции нового поколения или РУ подстанций должны обладать всеми указанными выше свойствами.

В целом состав основных задач ТУ может быть структурирован в виде двух групп:

1. Реализация функций централизованного («вертикального») ТУ. Выполнение этих функций может производиться как из диспетчерских центров/центров управления сетями, так и с уровня АСУ ТП смежных подстанций, в случае соответствующей передачи прав управления (например, при организации постепенного перехода к необслуживаемым ПС):
 - Управление коммутационными аппаратами ПС (выключатели, разъединители, заземляющие ножи, выкатные тележки РУ, переключатели во вторичных цепях ТН);
 - Передача команд управления переключением отпаяк РПН, БСК, управление уставками СТК, СТАТКОМ, УШР;
 - Управление вводом-выводом функций и переключением групп уставок РЗА.
2. Реализация функций «горизонтального» ТУ для поддержки средств децентрализованного управления. В целом они могут быть отнесены к перспективным, хотя специальные возможности прямой передачи команд управления между ПС уже давно применяются в РЗА (алгоритмы ДЗЛ, телеускорения и др.). Можно ожидать развития «горизонтального» ТУ в рамках разработки и применения алгоритмов WAPS, мультиагентного управления и др.

Далее в основном рассматриваются задачи первой группы в силу большей проработанности и актуальности в текущих условиях.

2.2 Организационные вопросы ТУ

В структуре обеспечения функций телеуправления выделяют два уровня – центр управления и объект управления, а также ряд обеспечивающих систем: ИТ- и телекоммуникационная инфраструктуры, системы обеспечения информационной безопасности.

В качестве уровня центров управления выступают центры управления сетями предприятий магистральных электрических сетей (ЦУС ПМЭС) и диспетчерские центры филиалов ОАО «СО ЕЭС». Специфика организации ТУ в российских электрических сетях в общем случае предусматривает необходимость поддержки многоуровневой передачи и реализации команд телеуправления: ДЦ – ПМЭС – ПС.

Регламентируемая процедура выдачи команд на управление оборудованием, находящемся в диспетчерском управлении и ведении, может вовлекать в процесс сразу несколько ЦУС и ДЦ. Так для организации вывода в ремонт ЛЭП, находящейся в диспетчерском управлении филиала ОАО «СО ЕЭС», требуется обеспечение команд

телеуправления по согласованным программам переключений для двух подстанций, относящихся к различным зонам ответственности двух ПМЭС.

Это накладывает дополнительные требования на техническую реализацию функции телеуправления:

- распределение и согласование прав доступа на ТУ со стороны используемых различных программно-технических комплексов (ПТК) ЦУС и ДЦ;
- автоматизация передачи функции удаленного управления между уровнями центра управления и объекта управления;
- автоматизация формирования, проверки, передачи и принятия к исполнению групп команд на управление оборудованием в составе ПТК ЦУС и ПТК ДЦ.

При этом согласованное управление оборудованием между ДЦ и ЦУС возможно только при синхронизации объектов информационных моделей ПТК, используемых в алгоритмах блокировок, проверок, при формировании групп команд ТУ или последовательностей (программ) переключений.

Отдельной задачей становится автоматизация процесса формирования, передачи и согласований команд ТУ в многоуровневой модели взаимодействия сетевых компаний и ОАО «СО ЕЭС». Плановые операции по управлению оборудованием подстанции могут быть однозначно определены в различных ПТК на основе согласованных и утвержденных типовых программ и бланков переключений. Внеплановые команды на ТУ должны передаваться между ПТК ЦУС и ДЦ для подтверждения и исполнения.

При возникновении условий, препятствующих безопасному телеуправлению на одном из уровней управления, должны передаваться сообщения с указанием причины и источника блокировки. Однозначная и единообразная трактовка сообщений о блокировании телеуправления должна обеспечиваться на всех ПТК ЦУС и ДЦ, с которых производилась трансляция команды.

2.3 Обеспечение безопасности ТУ

Для обеспечения достаточного уровня ситуационной осведомленности оперативного персонала необходимо дополнительно к объему, указанному в СТО 56947007-29.130.01.092-2011 «Выбор видов и объемов телеинформации при проектировании систем сбора и передачи информации подстанций ЕНЭС для целей диспетчерского и технологического управления», собирать и передавать на уровень центра управления:

- результаты оперативно-логической блокировки разъединителей;
- метеорологическую информацию;
- потоки от систем видеонаблюдения;
- данные мониторинга технического состояния основного оборудования и устройств.

На уровне центра управления в ПТК обеспечивается авторизация пользователя с необходимыми правами доступа для функций телеуправления, что обеспечивает разделение в ПТК оборудования подстанций по зонам ответственности и способам управления для групп диспетчеров ЦУС сетевых компаний и ДЦ. Это является одним из базовых методов обеспечения информационной безопасности, более подробно рассматриваемой ниже.

Ситуационная осведомленность диспетчерского персонала обеспечивается не только исчерпывающим объемом предоставляемой информации по объекту управления, но и ее эффективным представлением на автоматизированном рабочем месте. Для обеспечения ТУ должно осуществляться выделение на схемах выбранных для управления объектов и поддержка интерфейса диалоговых окон, предоставляющих варианты команды в зависимости от типа управляемого элемента. Контроль правильности производства переключений реализуется с визуальным отображением новых состояний, условных мнемознаков, соответствующих активным блокировкам телеуправления.

Для обеспечения безопасности выполнения типовых операций по управлению в нормальных режимах оборудованием в ПТК ЦУС реализуются последовательности или программы переключений, которые поддерживают регламентируемый процесс согласования и утверждения типовых бланков переключений.

Каждый шаг сохраненной в ПТК последовательности переключений, как и отдельно взятая внеплановая команда телеуправления диспетчера автоматически проходит ряд проверок:

- контроль на наличие и нарушение блокировок доступа согласно роли пользователя ПТК и принадлежности оборудования к зонам ответственности;
- контроль на наличие и нарушение блокировок выбора – запрет на одновременную работу с одним и тем же объектом с разных АРМ или разных центров управления;
- контроль на наличие и нарушение топологических блокировок для защиты от коммутационных ошибок;
- контроль на наличие и нарушение параметризуемых блокировок – в виде расчетных формул, результатом которых является логическое значение, указывающее на наличие или отсутствие блокировки.

Для обеспечения функции контроля топологических блокировок в ПТК должен в реальном времени обеспечиваться синтез расчетной топологической модели сети и топологический анализ.

Инициирование запуска контроля на наличие и нарушение топологических блокировок в режиме реального времени происходит по изменению состояния коммутационного аппарата либо по активации команды на телеуправление коммутационным аппаратом.

Помимо контроля целостности и надежности топологии электрических соединений диспетчерский персонал должен иметь возможность оперативно оценивать последствия и степень влияния отдаваемых ими команд – особенно при внеплановых переключениях и изменениях режимов работы оборудования.

Для обеспечения контроля ограничений по ведению режима и надежности сети перед подачей диспетчером команды управления в ПТК в режиме моделирования состояния энергосистемы обеспечивается выполнение следующих расчетно-аналитических функций:

- оценка состояния – формируется расчетная модель сети, которая используется для запуска топологических и режимных блокировок перед выдачей команды управления оборудованием;
- расчет токов короткого замыкания (ТКЗ) в заданном перечне точек и проверка отключающей способности коммутационных аппаратов – перед выполнением команды управления расчет ТКЗ запускается автоматически на основе результатов каждой оценки состояния или моделирования установившегося режима с формированием списка нарушений проверяемых значений отключающей способности силовых выключателей и дополнительно электродинамической или термической стойкости сборных шин;
- анализ вариантов отказов оборудования в моделируемом состоянии после реализации команды удаленного управления – последовательно моделируются режимы сети с поочередным вводом каждого из списка расчетных вариантов нарушений или нормативных возмущений в работе оборудования с оценкой рисков предстоящих команд удаленного управления.

Прием команд телеуправления на уровне объекта управления осуществляется ПТК АСУТП подстанции. Принятая команда телеуправления проверяется на допустимость по следующим критериям:

- наличие права управления у ЦУС ПМЭС;
- контроль качества команды по признакам качества, описанным в МЭК 60870-5-104;
- допустимость выполнения команды по условиям программных - логических и оперативных блокировок АСУ ТП;

При этом в АСУТП ПС реализуется функция передачи функции управления в ЦУС, с возможностью принудительного ее отключения.

На уровне объекта управления устройства РЗА и ПА могут поддерживать переключение групп уставок и ввод/вывод защитных функций из системы АСУТП ПС. Панели и шкафы РЗА и ПА проектируются таким образом, чтобы исключить необходимость ручного оперирования ключами или накладками при изменении режима работы оборудования ПС.

Переход к необслуживаемым подстанциям нового поколения согласно требованиям [1] должен сопровождаться помимо представленных решений организацией технологического видеонаблюдения от подстанционных систем в виде сжатого видеопотока.

При этом будет обеспечиваться визуальный мониторинг состояния оборудования ПС, в том числе – визуальный контроль выполнения оперативных переключений на ОРУ, контроль отсутствия людей в зоне, прилегающей к оборудованию, с которым производятся операции. Передача видео потока инициируется по запросу со стороны персонала центра управления.

2.4 Обеспечение информационной безопасности ТУ

Применение технологий телеуправления невозможно без комплексного решения задач информационной безопасности (ИБ). При этом расширяющийся с каждым годом спектр нормативной документации и многообразие программных продуктов, направленных на обеспечение ИБ, затрудняют однозначный выбор технических решений.

При поиске этих решений предлагается руководствоваться следующими критериями:

- адекватность разработанной модели угроз;
- обеспечение технологически и экономически обоснованного уровня защиты;
- возможность наращивания функциональности в соответствии с изменяющимися условиями, угрозами и требованиями;
- комплексная и эшелонированная система активного и пассивного противодействия угрозам;
- совместимость с существующими решениями;
- ориентация на мировой опыт и лучшую практику.

Удачная иллюстрация многообразия стандартов и их взаимного позиционирования относительно энергетического сектора была представлена в докладе ESCoRTS Consortium [5] (см. рисунок 1).

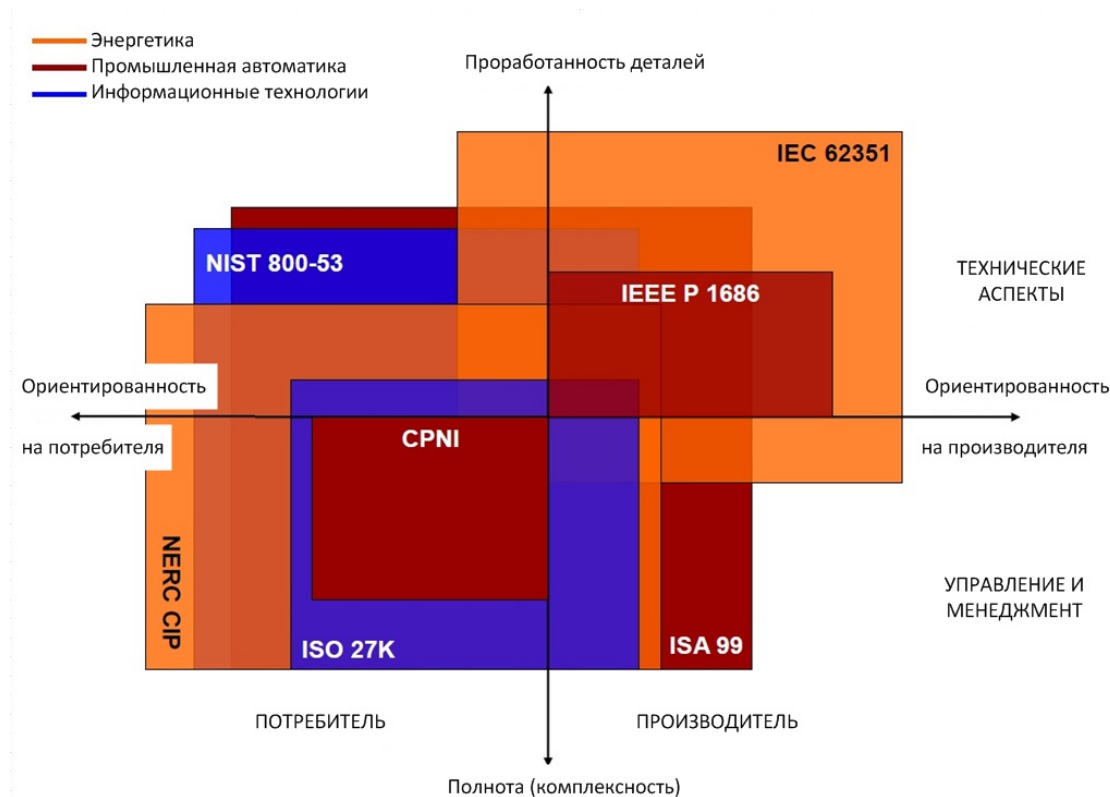


Рис. 1 Графическое представление объема и полноты отдельных стандартов ИБ

Авторы в ходе работы над статьей при выборе информационных источников ориентировались в поиске на самые последние тексты стандартов, не обращая внимания на статус draft. Это разумно, поскольку большинство стандартов для России несут только

информационно-справочный характер, а в последние годы состав и спектр угроз значительно изменился и расширился.

Тезис об увеличении угроз имеет статистическое подтверждение из самых разных источников, и это не удивительно, поскольку реализуются следующие объективные причины:

- Увеличивается количество подстанций и вообще оборудования нового поколения с возможностью доступа и управления по IP.
- Большинство удаленных соединений для сбора информации, управления, диагностики технического состояния и обслуживания в настоящее время не безопасны (без шифрования и / или механизмов аутентификации).
- Стандартизация используемых технологий. Все больше людей вооруженных специальными знаниями и инструментами, специализированных для выполнения атак на популярные системы.
- Растет доступность технической информации. В сети Интернет злоумышленник может найти подробную информацию и стандарты по созданию и защите критических систем.
- Квалификация, опыт и степень ответственности эксплуатационного персонала не всегда соответствует серьезности решаемых задач.

Методология выстраивания защиты от специфических угроз информационной безопасности хорошо проработана в [5-11]. Ниже приводится не исчерпывающий, но достаточно полный перечень технологических приемов:

- Выделение и защита электронного периметра.
- Сегментирование (зонирование), использование межсетевых экранов в том числе с шифрованием (VPN/FW).
- Специализированное ПО – Антивирусное, WhiteListing, инвентаризации программного обеспечения и оборудования.
- Шифрование IPSec, TLS, DTSL, SSL, SSH и др.
- Идентификация и аутентификация с использованием специальных ключей, включая биометрическую, использование электронной подписи.
- Защита удаленного доступа.
- Средства обнаружения и предотвращения сетевых вторжений (IPS, IDS, NIPS, HIPS).
- Технологии Data Loss Prevention (DLP), Security Information and Event Management (SIEM), honeypots и т.д.

Детальные практические рекомендации по обеспечению информационной безопасности в рамках ТУ энергообъектами зависят от актуальной модели угроз, выбранной ориентации на соответствие определенной группе стандартов и выходят за рамки настоящего доклада.

2.5 Прототип системы безопасного ТУ

Для испытаний и комплексного опробования функций телеуправления в рамках интеграции решений от различных разработчиков создан полигон, включающий в себя два уровня – ЦУС и подстанция 220-750кВ. Структурная схема полигона представлена на рис.2.

На уровне ЦУС применяется ПТК *PSIControl*. Подстанционный уровень включает в себя технические решения российских и зарубежных поставщиков оборудования РЗА и АСУТП (РТСофт, Siemens, ЭКРА, Бреслер). В качестве источников телеинформации по энергосистеме для полигона, а также приемников команд ТУ на подстанционном уровне, используются станционные контроллеры (STC), представляющие собой контроллеры SPRECON-E-C и Siprotec 6MD664. Контроллеры имеют встроенный логический переключатель режима ТУ (ЦУС/ПС), управляемый через интерфейс АСУТП SCADA V460. Для отработки функций технологических блокировок в составе полигона предусмотрен сервер с программным обеспечением PowerFactory разработки компании DigSILENT, обеспечивающий возможности моделирования электрических режимов.

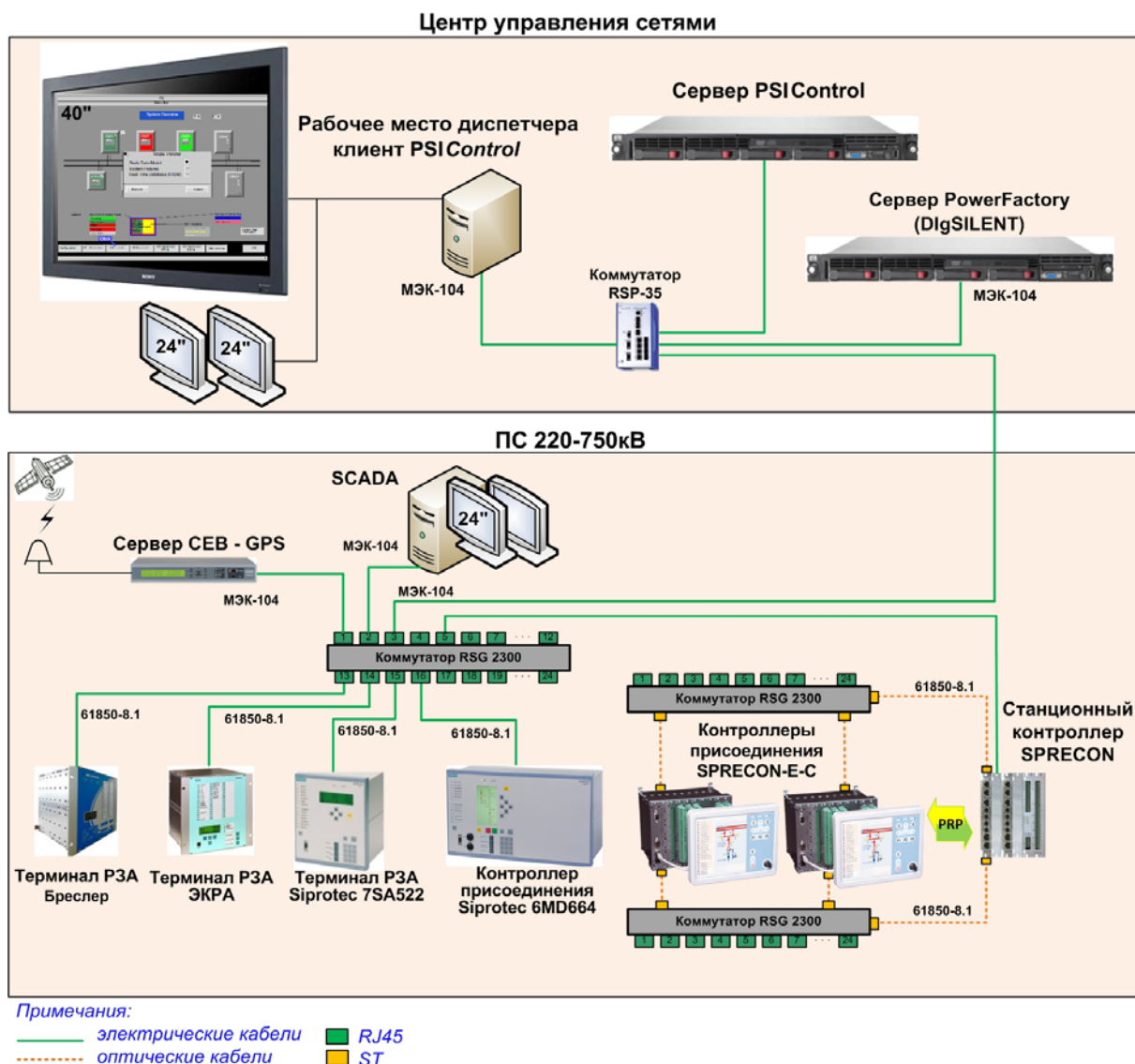


Рис.2 Структурная схема полигона отработки решений безопасного телеуправления.

К моменту написания настоящего доклада на стенде выполнены следующие испытания:

- передача функций управления между ЦУС и АСУТП ПС;
- отработка оперативных, топологических и параметризуемых блокировок на уровнях АСУ ТП и ЦУС;
- прохождение команд ТУ, в том числе последовательности переключений;
- переключение групп уставок терминалов РЗА из ЦУС;
- ввод/вывод защит РЗА.

3 ЗАКЛЮЧЕНИЕ

Организация безопасного ТУ в электрических сетях требует комплексного подхода, учитывающего как вопросы организационного плана, так и необходимость обеспечения технологической и информационной безопасности.

Дальнейшие шаги предполагают развитие полигона как в части отработки практических решений по информационной безопасности, так и в части опробования иерархического взаимодействия между несколькими уровнями управления.

ЛИТЕРАТУРА

- [1] Правила переключений в электроустановках. СТО 59012820.29.020.005-2011.
- [2] МЭК 62351. Вопросы безопасности для профилей протоколов на базе стека TCP/IP.
- [3] N. Schuster, H-J. Herrmann, A. Suhr. Advantages of solutions for remote access in protection and control applications via communication networks, B5-202, CIGRE 2012
- [4] N 256-ФЗ. «О безопасности объектов топливно-энергетического комплекса» от 21 июля 2011 года.
- [5] European Network for the Security of Control and Real Time Systems, «R&D and standardization Road Map», preliminary Deliverable 3.1 Rev, 2010 г.
- [6] ISO/IEC 27002:2005 «Информационные технологии - Методы обеспечения безопасности - Практические правила управления информационной безопасностью».
- [7] Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-82, «Guide to Industrial Control Systems (ICS) Security», 2012 г.
- [8] Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-94, «Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft)», 2012 г.
- [9] Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-53, «Security and Privacy Controls for Federal Information Systems and Organizations» R4, Draft, 2013 г.
- [10] NERC CIP Cyber Security Standards, CIP-003 «Security Management Controls», CIP-005 «Electronic Security Protection», CIP-007 «Systems Security Management», CIP-008 «Incident Response and Reporting».
- [11] BDEW. «White Paper Requirements for Secure Control and Telecommunication Systems», 2010 г.