*Электричество, 2020, № 12, с. 14–30* *DOI:10.24160/0013-5380-2020-12-14-30*

# От плана ГОЭЛРО к цифровизации электроэнергетического комплекса страны

**ЛОСКУТОВ А.Б., КУЛИКОВ А.Л.,**
*НГТУ им. Р.Е. Алексеева, Нижний Новгород, Россия;*
**ИЛЮШИН П.В.**
*ПЭИПК, Санкт-Петербург, Россия*

*Принятие плана ГОЭЛРО в 1920 году и поэтапная его реализация позволили удовлетворить потребности страны в интенсивном развитии экономики, обеспечив электроэнергией в требуемых объемах все отрасли народного хозяйства. В настоящее время технологии интеллектуальных электрических сетей (Smart Grid) предоставляют возможность провести их «цифровое обновление» с целью повышения наблюдаемости и управляемости, снижения потерь, а также обеспечения надежного функционирования новых участников рынков электрической энергии – объектов распределенной и возобновляемой энергетики. Интеллектуальные технологии позволяют оптимальным образом интегрировать разнородные источники электрической энергии, магистральные и распределительные сети, а также активных потребителей в единый электроэнергетический комплекс для повышения надежности функционирования, достижения экономических и экологических целей. В статье рассмотрены современные инновационные и перспективные технологии интеллектуальных электрических сетей, а также проведены исторические параллели с планом ГОЭЛРО, определившим курс на электрификацию России.*

Ключевые слова: *план ГОЭЛРО, электроэнергетический комплекс, цифровизация, цифровая электрическая подстанция, интеллектуальные электронные устройства, кибербезопасность, распределенная генерация, возобновляемые источники энергии*

В 2020 г. исполняется 100 лет Плану ГОЭЛРО, реализация которого доказала всему миру высокую эффективность государственного планирования и управления. В нем Г.М. Кржижановский сформулировал основные задачи электрификации России с учетом потребностей экономики страны:

техническое перевооружение всех отраслей народного хозяйства на базе использования электрической энергии;

обеспечение преимущественного роста тяжелой индустрии;

достижение опережающих темпов роста энергетического хозяйства;

строительство крупных современных электростанций;

широкое использование местных топливных ресурсов;

комплексное использование гидроресурсов для нужд энергетики;

строительство линий электропередачи и создание Единой энергетической системы страны;

рациональное размещение энергетического хозяйства.

Безусловно, задачи развития современной электроэнергетики значительно отличаются от задач, стоявших перед страной в 1920 г., однако во многом они и сходны. Авторам статьи хотелось бы вспомнить замечательный план ГОЭЛРО как часть преемственности взглядов электроэнергетиков, уйти от глобальных проблем и рассмотреть перспективные технологии, определяющие дальнейшее развитие электроэнергетического комплекса России [1, 2].

**Программа «Цифровая экономика Российской Федерации».** Программа утверждена 28 июля 2017 г. распоряжением Правительства РФ и предполагает системное развитие и внедрение цифровых технологий во всех отраслях экономики [3]. Цифровая экономика представлена тремя уровнями: 1) организация рынков с взаимодействием поставщиков и потребителей товаров, работ и услуг; 2) цифровые платформы и технологии для функционирования всех отраслей экономики; 3) нормативное регулирование, информационная инфраструктура и кибербезопасность.

Частью цифровой экономики является цифровая энергетика — программа цифровизации всех отраслей топливно-энергетического комплекса, курируемая Минэнерго России. В рамках программы «Цифровая трансформация электроэнергетики России» будут созданы информационная инфраструктура и аппаратно-программные средства технологического функционирования. Таким образом,

электроэнергетика страны переходит к новой парадигме своего развития.

Прослеживается сходство плана ГОЭЛРО с программой «Цифровая экономика РФ», однако программа «Цифровая трансформация электроэнергетики России» несколько оторвана от других отраслей экономики.

План ГОЭЛРО опирался на возможность использования оборудования лучших мировых производителей, однако при этом параллельно шел процесс интенсивной разработки собственных конструкций. Сегодня, в процессе цифровизации в большинстве случаев также применяется оборудование, поставляемое компаниями из различных стран мира. При этом программное обеспечение (ПО) зачастую является открытым и даже не русифицировано, поэтому вопросы обеспечения кибербезопасности цифровых электроэнергетических систем являются чрезвычайно актуальными. Процесс создания собственных разработок отдан на откуп частному бизнесу, прибыль которого либо слишком мала, либо инвестиции в новые разработки слишком рискованны. Даже готовые инновационные разработки научных коллективов не востребованы на рынке по различным объективным и субъективным причинам. В складывающихся условиях частный бизнес не готов идти на такие риски.

В соответствии с Концепцией интеллектуальной электроэнергетической системы России с активно-адаптивной сетью (2011 г.) [4, 5], в рамках дальнейшего ее развития Правительством РФ разработан план мероприятий по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Энерджинет» [6]. Реализация плана мероприятий предусматривает поэтапное с 2018 по 2035 гг. развитие технологий в сфере надежных и гибких распределительных сетей, распределенной энергетики, создание нового оборудования для управления перетоками мощности. Ожидаемым результатом перехода к цифровым технологиям является повышение качества услуг в сфере электроснабжения с появлением и развитием активных энергетических комплексов (активных потребителей), предусматривающих широкое использование интеллектуальных устройств и технологических систем.

Отсутствие нормативно-правового и технического регулирования, необходимых для внедрения интеллектуальных устройств и технологических систем, уже сегодня сдерживает внедрение существующих инновационных разработок и технологических решений. Требуется определение правового статуса функционирования активных энергетических комплексов в составе Единой энергетической системы России. Необходимо создание новых механизмов распределения локальных и общесистемных экономических и технологических эффектов. Следует пересмотреть практику перекрестного субсидирования, а также статус технологически изолированных территориальных электроэнергетических систем. Целесообразна синхронизация процессов внедрения цифровых технологий в различных энергетических компаниях, однако для этого необходимы единые методики, требования и стандарты. В настоящее время такая синхронизация порой невозможна по причине несовместимости информационных форматов и протоколов обмена данными.

Существенная роль в процессе цифровизации технологических процессов в электроэнергетическом комплексе страны отводится АО «Системный оператор Единой энергетической системы» (АО «СО ЕЭС»). Создание активных энергетических комплексов потребует формирования дополнительного сетевого резерва, что приведет к снижению доходности сетевых компаний.

Особая роль отводится развитию технологии управления спросом, которая предполагает объединение потребителей с управляемой нагрузкой (активных потребителей), распределенной генерацией и накопителями электроэнергии с целью снижения электропотребления в часы максимума нагрузки в энергосистеме. Необходима разработка интеллектуальных мультиагентных систем управления, позволяющих в конечном итоге подойти к созданию полноценных «умных сетей» с целью более эффективного управления оборудованием.

Распределительные сети напряжением до 110 кВ с активными и пассивными потребителями, объектами распределенной и возобновляемой энергетики должны стать активно-адаптивными с глобальной информационной средой, в которой интеллектуальные программно-аппаратные средства без участия человека осуществляют энергообмен [7].

Не остаются без внимания и технологически изолированные территориальные электроэнергетические системы, развитие которых невозможно без использования современных гибридных энергетических комплексов и систем управления ими [8].

Очевидно, что существующая система категорирования потребителей по надежности себя полностью исчерпала: требуются разработки новых целевых показателей надежности и средств их достижения.

В отношении основных норм, регулирующих правила использования информационных сетей, необходима разработка новых регламентов и технологий, не применяемых ранее в электроэнергетике.

Статус субъектов распределенной энергетики четко не определен ни на оптовом, ни на розничном рынках, а её прорывному развитию препятствуют сложившиеся правила ценообразования, тарифообразования и технологического присоединения к сетям общего пользования.

Для повсеместного и быстрого внедрения современных технологий требуется широкий спектр унифицированных (стандартных) технических требований, стимулирующих проведение передовых научных исследований. Только в этом случае в России могут появиться научные заделы, в том числе глобальные, которые позволят в долгосрочной перспективе содействовать развитию ее экономики.

Одним из ключевых вопросов является вопрос о совершенствовании систем контроля и учета потребления энергоресурсов, методов управления данными и их восстановления. В результате должны появиться «умные контракты» с подтверждением достоверности данных по объему потребления. В таких условиях потребуется совершенствование правил технологического функционирования и взаимодействия субъектов электроэнергетики.

Электроэнергетика может стать важным социальным и инвестиционным драйвером для развития целых регионов. Например, в регион с достаточными трудовыми ресурсами, но дефицитной энергосистемой практически невозможно привлечь инвестиции для строительства новых или модернизации существующих промышленных производств. Инвесторы чаще всего готовы осуществлять вложения в сферу технологий, в которой они работают. В электроэнергетику инвестируют, как правило, либо сами электроэнергетические компании, либо банки, либо государство. Вспомним, что бурное развитие электроэнергетики в 1950–1960-е годы происходило исключительно за счет государственных инвестиций. Дефицит электроэнергии приводит к сдерживанию инвестиций в регион, а следствием этого является миграция наиболее квалифицированных кадров из депрессионных регионов в интенсивно развивающиеся. Поэтому для построения распределенной экономики в России необходима бездефицитная распределенная и надежная электроэнергетика.

Современная электроэнергетика меняет свой вид: происходящая на протяжении последних десятилетий миграция населения в города требует увеличения в них концентрации генерирующих и электросетевых мощностей с высокой надежностью. Стоимость земли в городах неуклонно растет и становится соизмеримой со стоимостью основного оборудования генерирующих и электросетевых объектов. Поэтому инженеры разработчики и проектировщики ищут новые компактные экологические решения, вписывающиеся в жизнь современного города для удовлетворения постоянно растущего спроса на электроэнергию и социальную стабильность.

**Кибербезопасность.** Указом Президента РФ от 13 мая 2019 г. № 216 утверждена обновлённая «Доктрина энергетической безопасности Российской Федерации», закрепляющая на законодательном уровне следующие основные угрозы и риски [9]:

«противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов топливно-энергетического комплекса»;

«несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков».

Таким образом, Доктрина энергетической безопасности задает направление на дальнейшее развитие импортозамещения в системах технологического управления электроэнергетическим комплексом, объекты которого относятся к критической информационной инфраструктуре [9, 10].

С введением в действие 29 марта 2019 года СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110–220 кВ и узловых цифровых подстанций напряжением 35 кВ» [11] ПАО «Россети» сформировало нормативную базу для создания интеллектуальных электронных устройств и проектирования объектов электрических сетей на новых цифровых принципах.

**Стандарт МЭК 61850 и его развитие в части информационной безопасности.** Цифровые сети с интеллектуальными системами управления становятся неотъемлемой частью электроэнергетического комплекса страны. С появлением группы стандартов международной электротехнической комиссии МЭК 61850 (IEC 61850) возникла иллюзия, что для

их создания все готово. На самом же деле это только начальные документы, определяющие переход к цифровому управлению технологическими и коммерческими процессами.

Международный стандарт МЭК 61850 применяется к системам автоматизации подстанции (*SAS*). В этом стандарте приведены технические определения и описания процессов конфигурации и параметризации функций, требуемых для организации обмена данными между микропроцессорными устройствами на подстанции, а также требования к взаимосвязанным системам. Таким образом, этот стандарт используется для настройки параметров конфигурации микропроцессорных устройств цифровой подстанции с целью обеспечения их функциональной совместимости при обмене данными.

Стандарт МЭК 61850 частично базировался на концепции автоматизации подстанции UCA2.0, разработанной в США под эгидой Электроэнергетического научно-исследовательского института (*EPRI*). Работа над обоими стандартами была развернута в начале 90-х годов прошлого столетия. В 1997 г. *IEEE/EPRI* и МЭК пришли к решению объединить оба стандарта для создания глобальной и уникальной системы промышленной автоматизации. Часть 3 «Общие требования» стандарта МЭК 61850 была опубликована первой в январе 2002 г. После этого были выпущены части, посвященные моделям данных и коммуникационным услугам. А в целом стандарт был подготовлен к использованию в 2004 г. Процесс внедрения стандарта в промышленность занял приблизительно 10 лет, и таким образом около 20 лет прошло с того момента, как рабочие группы впервые приступили к его концептуальной проработке. Очевидно, что дальнейшее развитие и совершенствование стандарта будет продолжаться. Тем не менее, это подтвержденная технология, по которой работают свыше 6000 объектов по всему миру, поддерживаемая приблизительно 300 сертифицированными серверными микропроцессорными устройствами и 16 сертифицированными клиентскими системами.

Согласно СТО 34.01-21-004-2019 [11] ПАО «Россети» уже использует МЭК 61850 в качестве стандарта передачи данных цифровой подстанции (ЦПС) напряжением 6–220 кВ, являющейся единичным объектом автоматизированной системы технологического управления (АСТУ).

На рис. 1 показаны изменения, которые обсуждаются в настоящее время международной группой разработки стандарта IEC 61850-8-1/AMD1 ED2 для внесения в обновленную редакцию. Как можно увидеть (выделено пунктиром), в профиле IEC 61850 появился IEC 62351-6 «Управление энергетическими системами и связанным с этим обменом информацией. Безопасность данных и коммуникаций. Часть 6. Безопасность для IEC 61850». Для потоков данных, выходящих за пределы ЦПС, применение IEC 62351-6 будет обязательным, а внутри технологической вычислительной сети ЦПС – рекомендуемым.

Дальнейшее развитие МЭК 61850 подразумевает встраивание функций информационной безопасности в интеллектуальные электронные устройства (ИЭУ). Большинство выпускаемых ИЭУ для ЦПС, поддерживающих МЭК 61850, не удовлетворяют в полном объеме требованиям IEC 62351-6 и СТО 34.01-21-004-2019 (в части информационной безопасности). Исторически при формировании технических требований к разработке ИЭУ наличие функций информационной безопасности (ИБ) не учитывалось. Встраивание функций ИБ снижает

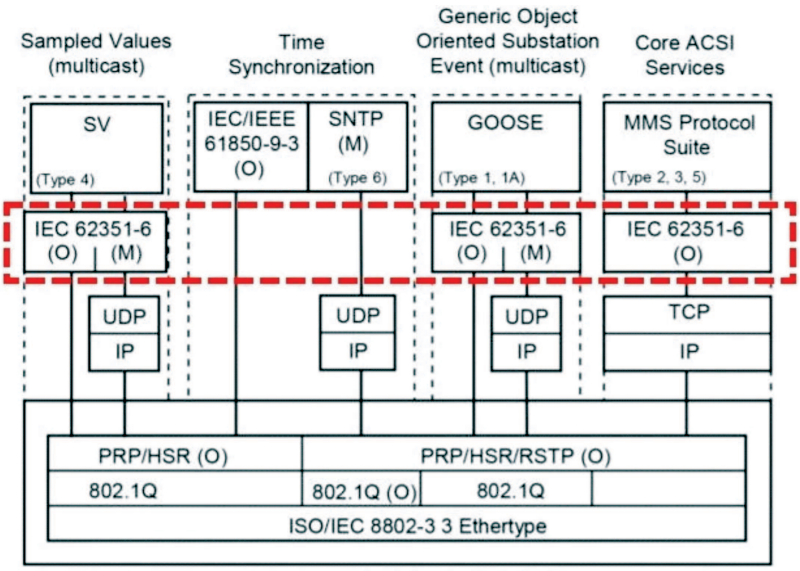


**Рис. 1.** Развитие стандарта МЭК 61850 в части информационной безопасности

быстродействие ИЭУ, что недопустимо, например, для релейной защиты и автоматики (РЗА). Цифровая трансформация электроэнергетического комплекса заставляет искать пути создания новой технологической разработки ИЭУ для ЦПС и РЗА, в частности, лишенных указанных технологических ограничений.

Важно отметить, что стандарт IEC 62351 пока не принят в РФ в качестве национального стандарта, хотя фактически применяется в АСТУ (например, объектов критической информационной инфраструктуры).

**Технология разработки кибербезопасных решений для ИЭУ.** Современное развитие вычислительной техники характеризуется тенденцией удешевления компонентной базы (микропроцессоров, оперативной памяти, систем хранения, интерфейсных микросхем и др.) при росте её надёжности и производительности. В результате этого получили широкое распространение вычислительные средства промышленной автоматизации, выпускаемые серийно и имеющие высокую степень стандартизации. Также сегодня имеется возможность выбора серийно выпускаемых операционных систем для промышленных (космических, военных) условий применения, имеющих развитую систему информационной безопасности, в том числе и сертифицированных Федеральной службой по техническому и экспортному контролю (ФСТЭК).

Технологию разработки кибербезопасных решений рассмотрим на примере кроссплатформенных ИЭУ РЗА. При создании кроссплатформенного ИЭУ выделяют несколько уровней абстракции (рис. 2), часть из которых является доверенной аппаратно-программной платформой, не зависящей от конкретного производителя [12].

Использование доверенной аппаратно-программной платформы обеспечивает информационную безопасность разрабатываемого ИЭУ РЗА в соответствии с требованиями ФСТЭК и одновременно освобождает производителя ИЭУ от трудоемких процессов технического сопровождения (аттестации) аппаратного исполнения. Основные усилия производителя ИЭУ направлены на разработку и совершенствование алгоритмической базы, а также поддержание прикладного функционального ПО устройств, устойчивого к угрозам информационной безопасности.

При реализации кибербезопасных решений ЦПС (рис. 3) в качестве аппаратной составляющей кроссплатформенной РЗА применяются серийно выпускаемые промышленные вычислители, в основе которых лежат микропроцессоры как импортного (*Intel, AMD, ARM*), так и отечественного (Эльбрус, Байкал) производства, что формирует первый уровень абстракции (рис. 2).

На втором и третьем уровнях абстракции используются серийные операционные системы, имеющие соответствующую сертификацию ФСТЭК (*Astra Linux, Alt Linux, Elbrusd,* «Нейтрино», *QNX*). Первые три уровня не зависят от конкретного производителя ИЭУ. Четвертый и пятый уровни абстракции представляют собой кроссплатформенное функциональное ПО ИЭУ и коммуни-


**Рис. 2.** Пять уровней абстракции при создании кроссплатформенного ИЭУ

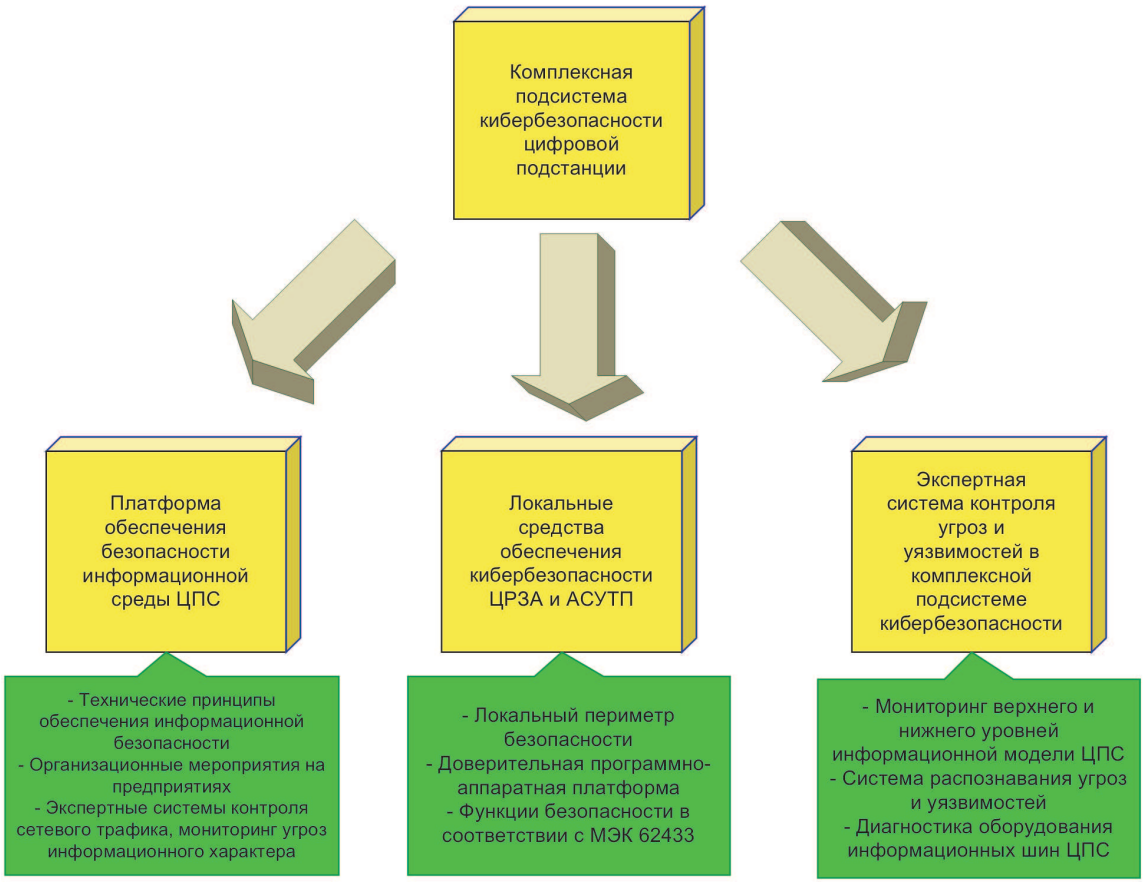


**Рис. 3.** Структура комплексной технологической подсистемы кибербезопасности ЦПС

кации МЭК 61850. Требования по информационной безопасности изначально закладываются в информационную модель МЭК 61850 и ИЭУ при их создании. ИЭУ, созданные с использованием данной технологии, поддерживают:

*SSL/TLS*-шифрование для МЭК 61850-8-1 (*MMS*) между ИЭУ и другими подсистемами ЦПС, а также между центрами управления сетями (ЦУС);

двухфакторную аутентификацию на ИЭУ РЗА и автоматизированных рабочих местах эксплуатационного и оперативного персонала технологической вычислительной сети (шине процесса) ЦПС при удаленном доступе к ИЭУ;

ролевой доступ к элементам интерфейса ИЭУ в зависимости от функциональных обязанностей персонала;

протоколирование событий безопасности на уровне отдельного ИЭУ, ЦПС и ЦУС [12].

Продолжаются работы по реализации (встраиванию) имитовставки в *GOOSE*-сообщения, что также станет частью информационной модели МЭК 61850 кроссплатформенных ИЭУ.

Реализация 5-уровневой модели кроссплатформенного ИЭУ осуществляется с помощью специализированного «Кодогенератора управляющего ПО», который представляет собой инновационный инструмент создания кроссплатформенных решений для «киберзащищенной ЦПС с динамичной архитектурой», где ИЭУ РЗА – один из функциональных элементов (рис. 4).

Кодогенератор включает в себя библиотеку компонентов, с помощью которой специалисты предметной области без программирования в визуальном режиме создают логические схемы ИЭУ, проверяют их корректность, определяют состав групп локального периметра безопасности с правами доступа к элементам интерфейса и функциям ИЭУ. При создании логической схемы Кодогенератор автоматически формирует информационную модель МЭК 61850 ИЭУ, включая атрибуты информационной безопасности, что упрощает создание и конфигурирование файлов по стандарту МЭК 61850. После создания логической схемы можно подать на вход ИЭУ заранее подготовленный Comtrade-файл и проверить корректность работы ИЭУ в различных режимах. После этого Кодогенератор на языке «Си» генерирует программный код, который компилируется для выполнения на перечисленных выше аппаратно-программных платформах. Важно отметить независимость генерируемого программного кода от операционной системы и микропроцессора, его идентичность, а также типизацию и стандартизацию модели ИБ ИЭУ.


**Рис. 4.** Процесс создания кроссплатформенного ИЭУ с использованием «Кодогенератора управляющего ПО»

С помощью Кодогенератора создаются ИЭУ различного функционального назначения (ИЭУ РЗА для ЦПС напряжением 6–220 кВ; ИЭУ АСУ ТП, оперативной блокировки, автоматики управления нормальными и аварийными режимами; ИЭУ технического учета и контроля качества ЭЭ).

Использование Кодогенератора минимизирует количество ошибок при создании ИЭУ, а время его создания в зависимости от сложности и наличия соответствующего математического аппарата (алгоритмической базы) составляет 2–3 недели.

В табл. 1 приведены требования по информационной безопасности, реализованные в ИЭУ РЗА, созданном с использованием Кодогенератора, соответствующие Распоряжению ПАО «Россети» от 30.05.2017 г. № 282р [13].

*Таблица 1*

**Требования по информационной безопасности, реализованные в ИЭУ РЗА**

| Идентификатор | Наименование требования |
|---|---|
| FAU_GEN.1 | Генерация данных аудита |
| FAU_GEN.2 | Ассоциация идентификатора пользователя |
| FAU_SAR.1 | Просмотр журналов аудита |
| FAU_STG.1 | Защищенное хранение журнала аудита |
| FAU_STG.3 | Действия в случае возможной потери данных аудита |
| FAU_STG.4 | Предотвращение потери данных аудита |
| FDP_ACC.1 | Ограниченное управление доступом |
| FDP_ACF.1 | Управление доступом, основанное на атрибутах безопасности |
| FIA_AFL.1 | Обработка отказов аутентификации |
| FIA_ATD.1 | Определение атрибутов пользователя |
| FIA_UAU.2 | Аутентификация до любых действий пользователя |
| FIA_UAU.7 | Аутентификация с защищенной обратной связью |
| FIA_UID.2 | Идентификация до любых действий пользователя |
| FMT_MSA.1 | Управление атрибутами безопасности |
| FMT_MSA.3 | Инициализация статических атрибутов |
| FMT_MTD.1 | Управление данными ФБО |
| FMT_SMF.1 | Спецификация функций управления |
| FMT_SMR.1 | Роли безопасности |
| FTA_SSL.1 | Блокирование сеанса, инициированное функциями безопасности |

В табл. 2 приведена детализация функциональных требований FMT_SMR.1 (Роли безопасности) в этом же ИЭУ РЗА. На рис. 5 представлена кроссплатформенная технология построения ИЭУ РЗА.

**Перспективы развития технологии.** Интеллектуальные электронные устройства РЗА для электрических сетей напряжением 6–220 кВ, созданные по приведенной выше технологии, неоднократно представлялись на отраслевых научно-технических советах, признаны отраслевым профессиональным сообществом и аттестованы в ПАО «Россети».

Технология позволяет расширить область её применения для типизации и стандартизации ИЭУ различного функционального назначения АСТУ ЦПС (рис. 6), т.е. для проектирования ЦПС с заданной степенью централизации/децентрализации и сценариями резервирования в реальном времени

*Таблица 2*

**Детализация функциональных требований FMT_SMR.1 в ИЭУ РЗА**

| Название группы | Функциональные обязанности, роли | Права доступа к элементам интерфейса и функциям ИЭУ РЗА |
|---|---|---|
| Администратор | Представители компании-производителя и/или компании, выполняющей ПНР | Полный доступ к элементам интерфейса и параметрированию |
| Специалист по ИБ | Специалист по ИБ | Управление пользователями |
| Эксплуатационный персонал | Специалисты, отвечающие за эксплуатацию ИЭУ (для ИЭУ РЗА – инженеры РЗА) | Параметрирование с некоторыми ограничениями (калибровка, настройка параметров ЛВС) |
| Оперативный персонал | Специалисты ОВБ, диспетчерский персонал ПС | Ввод/вывод функций РЗА и автоматики, чтение осциллограмм, журнала событий |
| Читатель | Руководящий персонал ПС | Чтение осциллограмм, журнала событий |
| Специалист по АСУ ТП | Инженер по связи, инженер по ИТ | Настройка параметров ЛВС |

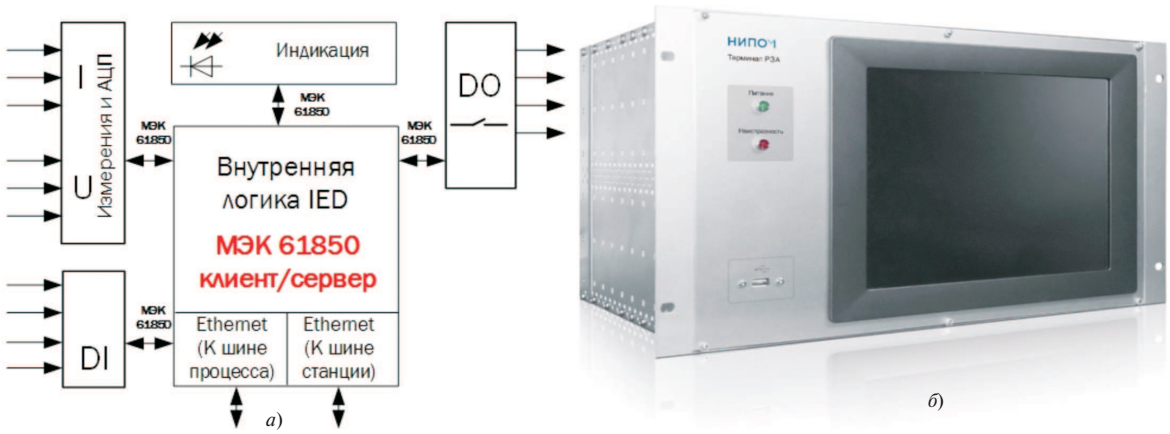


**Рис. 5.** Кроссплатформенная технология построения ИЭУ РЗА: *а* – структурно-логическая схема; *б* – внешний вид ИЭУ

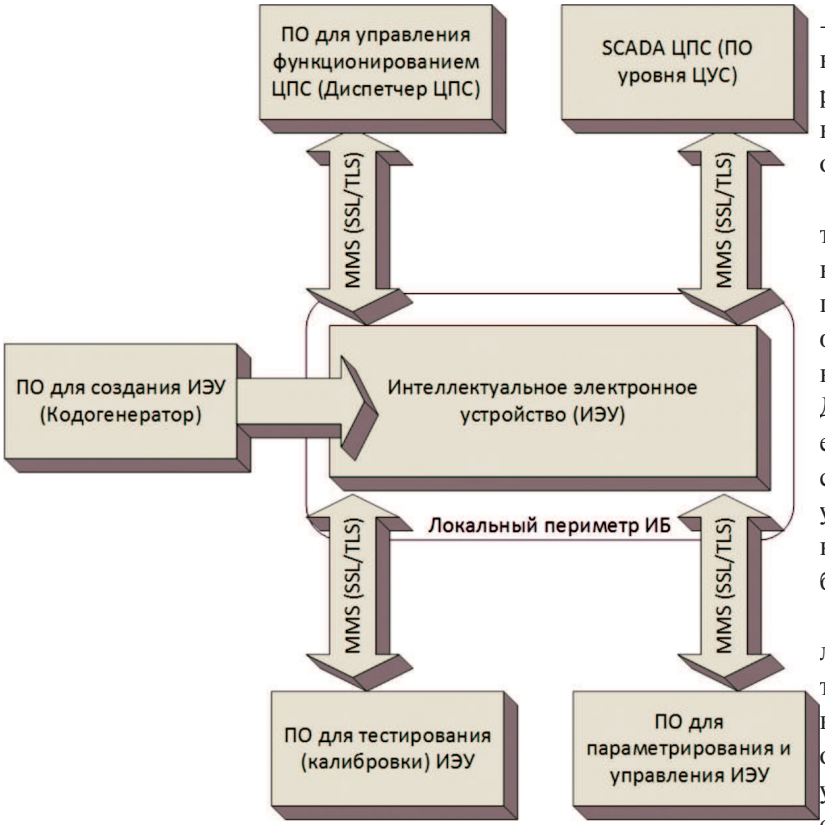


**Рис. 6.** ИЭУ в составе киберзащищенной ЦПС с динамичной архитектурой

– «киберзащищённых ЦПС с динамичной архитектурой». Основными критериями при выборе варианта являются: надежность, стоимость и соответствие отраслевым требованиям и стандартам.

На киберзащищённых ЦПС подсистема информационной безопасности становится полноценной технологической подсистемой объекта критической информационной инфраструктуры (КИИ) наряду с РЗА, АСУ ТП, АИИСКУЭ и т.д. Для каждого ИЭУ АСТУ ЦПС типизируется «локальный периметр безопасности», обеспечивающий индивидуальную устойчивость к киберугрозам и возможным несанкционированным или ошибочным действиям.

Подсистемы РЗА и АСУ ТП ЦПС являются наиболее критичными компонентами при угрозах несанкционированного вмешательства. Одна из точек зрения, основанная на абсолютной изоляции указанных подсистем ЦПС, не соответствует перспективам интеллектуализации современной электроэнергетики. Такой

подход фактически препятствует дальнейшей оптимизации электроэнергетических систем и формированию технологического управления передачей и распределением ЭЭ, которое должно учитывать растущую долю распределенной генерации и микрогенерации. Предпочтительным является вариант создания комплексной системы кибербезопасности, структурные компоненты которой учитывают индивидуальные для ЦПС функциональные особенности и правила противодействия киберугрозам.

Технология разработки кибербезопасных решений для кроссплатформенной РЗА с последующим расширением области её применения на типизацию и стандартизацию ИЭУ позволяет создавать «киберзащищённые ЦПС с динамичной архитектурой». Использование доверенной аппаратно-программной платформы, базирующейся на отечественных микропроцессорах и сертифицированных операционных системах предпочтительно для снижения технологической зависимости электроэнергетического комплекса России и минимизации угроз и рисков, изложенных в обновлённой «Доктрине энергетической безопасности РФ».

**Состояние российского энергетического машиностроения, электротехнической промышленности и научных исследований.** Продолжает ухудшаться состояние российского энергетического машиностроения, электротехнической промышленности, инжиниринга и др. Доля выпускаемого российскими предприятиями на мировом рынке современного энергетического оборудования, в том числе интеллектуальных устройств и систем управления, составляет менее 1%. Динамика годовых темпов роста сегмента энергетического оборудования по прогнозам не превышает 10% в год. Наблюдается тенденция к занятию отечественного рынка информационно-коммуникационных технологий и систем управления крупными зарубежными компаниями.

Анализируя Постановление Правительства РФ [6], экспертно-аналитический доклад [5] и другие официальные документы, можно сделать вывод о том, что путь цифрового перехода в электроэнергетике базируется на копировании опыта ведущих мировых электроэнергетических компаний и производителей оборудования. С таким подходом трудно не согласиться, но «подводные камни» на этом пути могут приостановить движение вперед. Это и кибербезопасность, и санкции, и закрытые коды программного обеспечения, и еще многое другое.

Большинство научных коллективов в России сегодня работают разрозненно, в инициативном порядке, сами ставят себе задачи и сами их каким-то образом решают. Многие научные задачи решаются стереотипно без серьезных инноваций в технических и технологических решениях. Сложившуюся ситуацию можно исправить, если глубоко сегментировать направления научных исследований и ориентировать их на достижение конкретных результатов с заданными показателями и параметрами, соответствующими лучшим мировым образцам. Необходима новая отечественная научная концепция цифрового перехода в электроэнергетике. Миссию по разработке новой концепции может на себя взять только большой коллектив квалифицированных в области проектирования, эксплуатации, в научных исследованиях электроэнергетиков.

В соответствии с «Концепцией интеллектуальной электроэнергетической системы России с активно-адаптивной сетью», разработанной в 2011 г., и концепцией «Цифровая подстанция», получившей статус национального проекта в 2018 г. требуется создание технологической, нормативной и производственной базы с целью массового внедрения в энергетическую отрасль инновационного высокоэффективного продукта – необслуживаемых модульных самодиагностируемых электрических подстанций и станций (ЦПС), в том числе с применением централизованных, децентрализованных и гибридных принципов построения систем защиты и автоматики.

Как уже было рассмотрено выше, в основе проекта «Цифровая подстанция» лежит управление и информационный обмен между элементами по стандарту МЭК 61850 [11]. Архитектура ЦПС подразумевает наличие устройств, реализующих функции измерения, аналого-цифрового преобразования и формирования потоков SV, обмен сообщениями по МЭК 61850 по шине процесса, учет электроэнергии, РЗА, сигнализация, регистрация, управление выключателями. К этим устройствам относятся устройства уровня присоединения (контроллеры присоединения). Функции централизованной РЗА и управления ЦПС, связь с контроллерами нижнего и верхнего уровней осуществляется устройствами (контроллерами) среднего уровня.

Российские производители устройств РЗА и АСУ ТП используют исключительно импортные компоненты, доля которых составляет не менее 56%. С учетом дальнейшего развития цифровых подстанций и интеллектуализации электрических сетей в России разработка технических решений для контроллеров присоединения и контроллеров среднего уровня ЦПС на отечественной элементной базе с применением МЭК 61850 является актуальной задачей, способствующей повышению информационной безопасности энергетических объ-

ектов и снижению затрат на последующее сопровождение ПО.

**Перспективные решения в области защиты и управления энергосистем.** Стремительное развитие коммуникационных технологий позволяет реализовать широкомасштабный обмен информацией. В связи с этим возникло понятие *централизованной защиты участка электрической сети* (*ЦЗУ, Wide area protection* (*WAP*)). Основой такой системы стал вариант построения защиты на переходных процессах, предложенный в 1996 г. [14], в котором синхронизация во времени с помощью *GPS* играет главную роль [15]. Централизованная защита участка сети с применением новых алгоритмов реализуется на основе измерений от несколько информационных точек (рис. 7), способна обеспечить быстрое, надежное и точное обнаружение повреждений. В последние годы ЦЗУ является широко обсуждаемой темой, по которой проводятся научные исследования и публикуются полученные результаты.

*Интегрированная защита.* С развитием цифровых технологий все большее количество функций реализуется внутри одного терминала защиты (линий, трансформаторов, генераторов и т.д.) для достижения определенной степени интеграции. Например, цифровая РЗА линий электропередачи (ЛЭП) может иметь дистанционную или дифференциальную токовую защиту в качестве основной, направленную или ступенчатую токовую защиту в качестве резервной. Современные разработки в микропроцессорных элементах и коммуникационных технологиях открыли новые возможности для РЗА [16, 17]. В отличие от централизованной защиты участка сети (ЦПС) интегрированное решение не просто объединяет аппаратную и программную часть защитных реле, но и основывается на разработке новых алгоритмов с учетом множественных измерений (избыточности), позволяя улучшить характеристики защиты.

*Управление участками электрической сети.* Внедрение цифровых синхронных векторных измерений в различных точках электрической сети значительно расширит зону управления, осуществляемого на ЦПС. Такие измерения содержат информацию о комплексах токов и напряжений, синхронизированных с высокой точностью с помощью *GPS*. На их основе могут быть построены системы мониторинга электрической сети, а также различные программные приложения для повышения наблюдаемости и надежности, включающие в себя: усовершенствованную оценку состояния [15], динамические модели онлайн оценки режима, управление перегрузками, оценку стабильности, обнаружения и компенсации межсистемных колебаний [9]. Так-

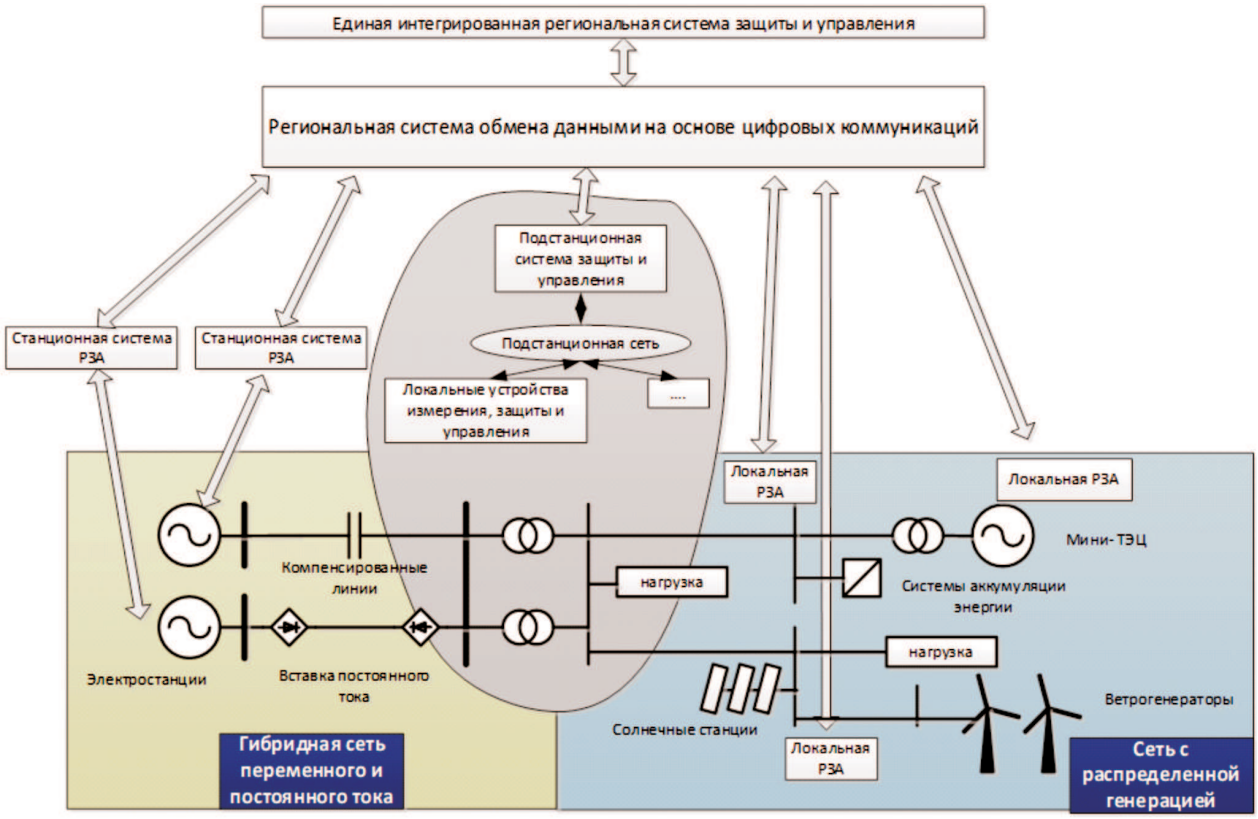


**Рис. 7.** Архитектура интегрированной системы защиты и управления

же проводились исследования в области интегрирования функций защиты и управления [18].

*Концепция интегрированной системы защиты и управления (ИЗУ).* Суть концепции [18] состоит в интеграции функций защиты и управления, в частности на региональном уровне, направленных на предоставление ряда преимуществ для будущей системы. Она предполагает объединение возможностей трех иерархических уровней для предотвращения каскадного отключения электрической сети на большой территории.

Для реализации системы управления разработана специальная синхронизированная быстродействующая система коммуникаций. Ключевым элементом в системе ИЗУ является информационная платформа, которая получает синхронизированные данные в реальном масштабе времени по сети связи. Информационная платформа также поддерживает приложения специально разработанной облачной вычислительной системы для реализации ряда дополнительных функций на уровне ЦПС и систем электроснабжения.

Предлагаемую в [16] региональную систему защиты и управления иллюстрирует рис. 7.

Быстрые и глубокие изменения в системах передачи и распределения электрической энергии, появление нового оборудования, например, управляемых ЛЭП переменного тока, накопителей электроэнергии, возобновляемых источников и др. привели к существенному изменению характеристик и усложнению алгоритмов управления системами электроснабжения. Следовательно, существующие системы защиты и управления не смогут эффективно реализовать заданные им функции. Как показано на рис. 7, система ИЗУ разделена на группы. Ее основными частями являются высокоскоростная коммуникационная сеть и информационная система синхронизации в режиме реального времени. В перспективе функции ИЗУ расширяются для достижения интеграции диспетчерско-технологического управления с релейной защитой и SCADA-системами на региональном уровне.

На локальном уровне предполагается интеграция функций различных устройств. Это относится к следующему оборудованию ЦПС: устройства сопряжения, интеллектуальные терминалы, устройства метрологических измерений, устройства синхронных векторных измерений (СВИ) и РЗА присоединения. Оборудование отвечает за выборки токов, напряжений и других данных в режиме реального времени и отправку информации на уровень шины процесса в систему защиты и управления ИЗУ. Такое оборудование позволит интегрировать цепи первичного силового оборудования и добиться высокой интеграции на уровне присоединения.

На уровне ЦПС интегрируются функции защиты линий, шин, трансформаторов (автотрансформаторов), автоматики управления выключателем, реклоузеров, автоматических оперативных переключений, определения места повреждения, автоматики регулирования напряжения и других функций управления. Для резервирования, автоматического управления доступом на подстанцию и др. используется специальное ПО.

На верхнем уровне ИЗУ интеграция функций РЗА приводит к повышению быстродействия защиты. Кроме того, интегрируются функции определения места повреждения, автоматики регулирования напряжения, контроля напряжения и частоты, обнаружения качаний в энергосистеме и др. В отличие от обычной защиты и управления, разделенных как при проектировании, так и эксплуатации, ИЗУ представляет собой оптимальную комбинированную систему, реализующую функции на региональном уровне.

*Применение облачных технологий.* Основываясь на вышеупомянутой информационной платформе, распределенная система с применением облачных технологий (например, [19]) предназначена для реализации функций ЦПС и на региональном уровне (определение места повреждения, определение поврежденного участка ЛЭП, контроль качества электрической энергии, согласование уставок защит и др.). Расширенные функции также включают контроль состояния первичного оборудования, управление техническим обслуживанием и ремонтом и другие эксплуатационные задачи (рис. 8).

Облачные технологии позволят существенно сократить инвестиции в оборудование общей телекоммуникационной системы. Облако на подстанционном уровне получает данные с уровня процесса, а региональное облако получает данные с информационной платформы. На верхнем уровне реализуются статические и динамические измерения, оценка состояния выключателей, извлечение информации для специальных алгоритмов вычислительных средств и др. Применение облачных технологий позволяет уменьшить нагрузку на каналы связи, обеспечить компактность хранения данных, применить стандартное общедоступное программное обеспечение и получить другие преимущества. Следует отметить, что при использовании облачных технологий вопросы информационной безопасности встают особо остро.

*Распределенные источники энергии.* В соответствии с распоряжением от 8 января 2009 г. № 1-р и постановлением от 28 мая 2013 г. № 449 Прави-

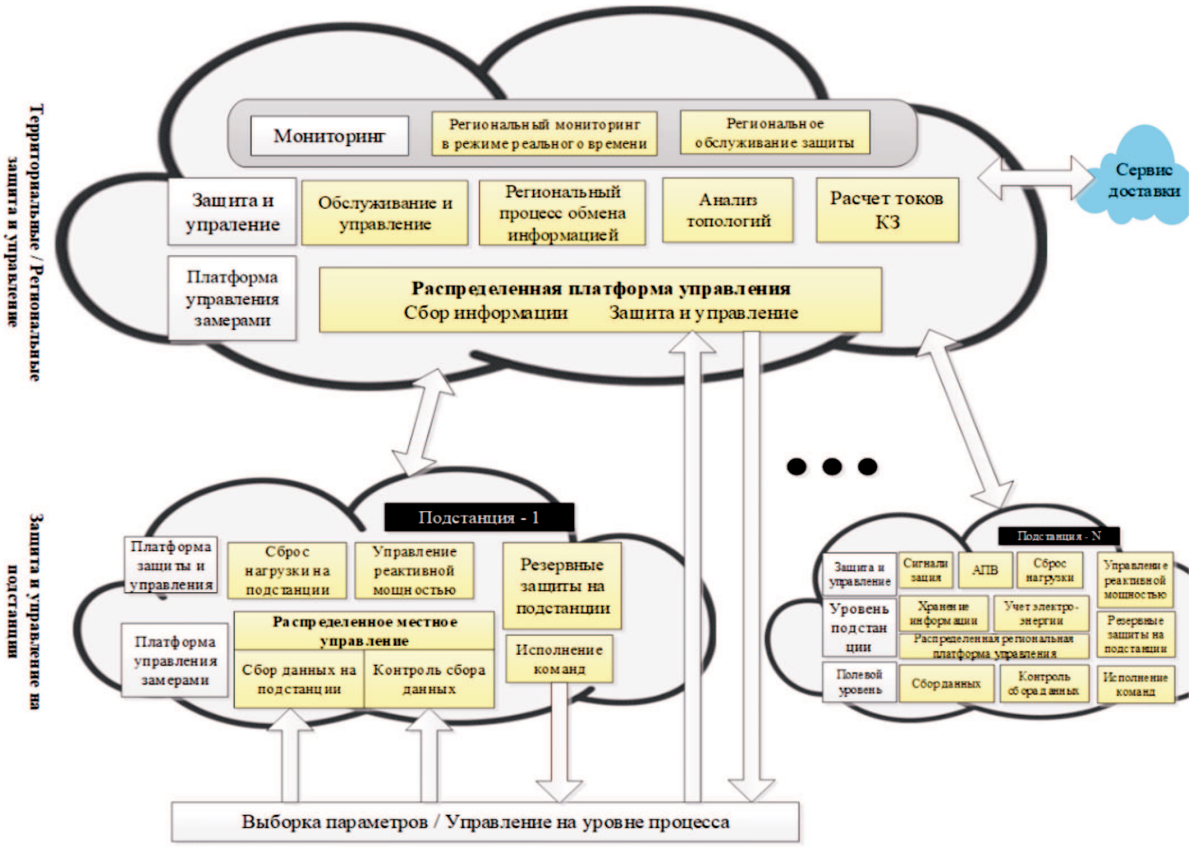


**Рис. 8.** Принцип применения облачных технологий

тельства РФ в России должны быть введены в эксплуатацию ветровые и солнечные электростанции суммарной установленной мощностью 5278,3 МВт [8, 20]. В некоторых энергосистемах доля объектов возобновляемых источников энергии (ВИЭ) в структуре генерирующих мощностей приближается к 15%, что требует корректной оценки их влияния на возможность управления режимами, а также функционирование устройств РЗА.

Вместе с тем, тенденция в отечественной электроэнергетике к старению генерирующего оборудования на традиционных тепловых электростанциях и электросетевого оборудования в магистральных и особенно распределительных сетях повышает вероятность возникновения аварий, приводящих к выделению отдельных энергорайонов в островной режим либо делающих работу особо ответственных электроприемников потребителей невозможной без отделения от энергосистемы.

Необходима трансформация технических требований к устройствам РЗА, обусловленная увеличением скорости протекания переходных процессов, трудностями согласования уставок устройств РЗА и технологических защит генерирующих установок, отклонением показателей качества электроэнергии от нормируемых значений в энергорайонах с распределенными источниками энергии (РИЭ), влиянием РИЭ на алгоритмы работы и параметры настройки устройств автоматики энергосистем и другими факторами.

Технические характеристики РИЭ определяются следующим:

увеличение скорости протекания переходных процессов при возникновении возмущений, что требует повышения быстродействия пусковых органов устройств РЗА;

применение в сетях с РИЭ резервных защит с выдержками времени (ближнее и дальнее резервирование) не позволяет, как правило, обеспечить надежное функционирование РИЭ и электроприемников потребителей вследствие их отключения электрическими или технологическими защитами;

для предотвращения аварий с массовым отключением электроприемников потребителей и РИЭ необходимо применять быстродействующие устройства РЗА и высоковольтные выключатели с меньшим собственным временем отключения с целью снижения глубины и длительности провалов напряжения;

оценка параметров режима в устройствах РЗА должна проводиться с применением методов цифровой обработки сигналов, устойчивых к существенным отклонениям показателей качества электроэнергии;

при технологическом присоединении РИЭ необходимо проводить проверку, а при необходимо-

сти, корректировку существующих алгоритмов работы и параметров настройки устройств автоматики энергосистем, или осуществлять их замену;

в условиях значительных изменений режимов генерации и потребления в течение суток в сетях с РИЭ необходимо внедрение систем автоматического расчета и изменения уставок устройств РЗА в темпе процесса, что требует применения устройств РЗА, поддерживающих данную технологию [21].

*FACTS-технологии.* Гибкие системы передачи переменного тока (*Flexible AC Transmission Systems – FACTS*) [22] включают элементы силовой электроники и предназначены для повышения устойчивости и пропускной способности систем электропередачи. Конструктивную основу *FACTS* составляют четыре типа контроллеров (регуляторов): 1) последовательные, регулирующие уровни напряжения или реактивную мощность ЛЭП (например, последовательный статический синхронный компенсатор); 2) шунтирующие, регулирующие параметры сети в точке присоединения (например, статический синхронный компенсатор); 3) смешанные последовательно-параллельные, используемые в системах передачи с множеством ЛЭП, где реализуют независимую компенсацию реактивной мощности для каждой линии и перераспределяют активную мощность между ЛЭП (например, межлинейный регулятор потока мощности); 4) смешанные последовательно-шунтирующие, представляющие собой комбинацию последовательных и шунтирующих регуляторов (например, унифицированный регулятор потока мощности).

С момента разработки устройств *FACTS* на протяжении более двух десятилетий проходила их успешная эксплуатация на нескольких подстанциях по всему миру. Несмотря на относительно высокую стоимость, такие устройства обеспечивают такие важные преимущества для энергосистем, как регулирование потоков мощности для обеспечения оптимальной нагрузки; увеличение системной устойчивости и надежности, ограничение токов короткого замыкания, управление каскадными отключениями и устранение низкочастотных колебаний; увеличение пропускной способности ЛЭП с одновременным уменьшением перетоков реактивной мощности.

*FACTS*-технологии регулируют передаваемую мощность и пропускную способность ЛЭП за счет управления параметрами ЛЭП. Совершенствование силовой полупроводниковой базы и снижение стоимости *FACTS*-контроллеров открывает возможность широкомасштабного их применения. Предполагается, что эти технологии будут широко использоваться в будущем.

В НГТУ им. Р.Е. Алексеева разработан экспериментальный образец универсального преобразователя напряжения для подключения разнородных источников электроэнергии [23] (работа выполнена при финансовой поддержке Минобрнауки России по теме «Разработка технических решений для создания энергоэффективной системы электроснабжения автономного потребителя на основе комбинированного использования возобновляемых источников энергии и устройств оптимального управления» (ГК №14.516.11.0006 от 15.03.2013)).

Универсальный преобразователь напряжения (УПН) обеспечивает подключение к входным цепям как источников переменного, так и источников постоянного напряжения, формируя при этом на выходе трехфазное напряжение 380 В частотой 50 Гц, удовлетворяющее требованиям ГОСТ 32144-2013 [24]. В качестве базового элемента УПН выбран модифицированный трехфазный инвертор напряжения, работающий как в режиме активного выпрямителя, так и инвертора напряжения. УПН построен по принципу двойного преобразования (*AC*/*DC*; *DC*/*AC*) с промежуточным звеном постоянного тока (емкостным накопителем). Структурная схема УПН приведена на рис. 9.

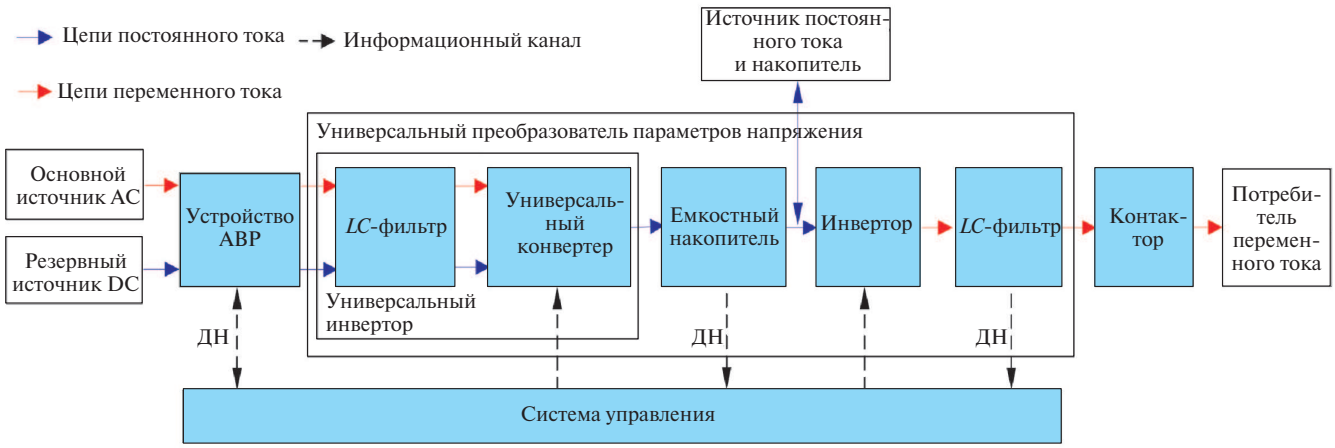


**Рис. 9.** Структурная схема универсального преобразователя напряжений

Схема модифицированного инвертора обеспечивает заряд емкостного накопителя в режимах активного выпрямителя переменного напряжения или конвертера постоянного напряжения в зависимости от типов основного и резервного источников энергии. Базовая схема инвертора работает в штатном режиме, обеспечивая гарантированное питание потребителей стабилизированным напряжением.

*Твердотельный трансформатор.* Твердотельный трансформатор (*Solid State Transformer – SST*) [25, 26] выполняет ту же функцию повышения или понижения уровней напряжения, что и традиционный трансформатор, однако исключает некоторые проблемы, характерные для трансформаторов с железным сердечником.

Высокочастотный преобразователь и трансформатор (рис. 10) составляют сердце *SST*, который выполняется с применением материалов на основе карбида кремния (*Silicon Carbide – SiC*). Главные преимущества *SST* – уменьшенные габариты и вес.

Поскольку в *SST* используются полупроводниковые ключевые элементы, то при их закрывании переменный ток не будет протекать через высокочастотный трансформатор. Таким образом, высокочастотные преобразователь и трансформатор могут функционировать как автоматический выключатель. Площадь подстанции существенно уменьшается благодаря меньшему размеру *SST* (до 75%) и отсутствию автоматических выключателей. Однако важнейшим фактором, сдерживающим применение *SST*, является их высокая стоимость (в 20 раз больше традиционных).

**Заключение.** Масштабы цифровизации и интеллектуализации, глубина преобразований и новизна технических решений, применяемых в настоящее время в электроэнергетическом комплексе России, подобны реализации положений плана ГОЭЛРО.

Как и сто лет назад, в наше время назрела острая необходимость в существенной и радикальной модернизации оборудования электрических станций, магистральных и распределительных сетей, электроприемников потребителей для обеспечения потребностей развивающейся цифровой экономики страны.

Основные возможности для совершенствования электроэнергетического комплекса России предоставляют современные информационные технологии, элементы силовой электроники, а также распределенные источники энергии, в том числе на основе ВИЭ. Определяющим фактором интеллектуализации электрических сетей является разработка и внедрение новых цифровых устройств защиты и управления, выполненных с использованием современной отечественной элементной базы и соблюдением требований по кибербезопасности.

Для принятия оптимальных организационных и технических решений по модернизации объектов электроэнергетики требуется обеспечить правильное сочетание современных технологий и инновационного оборудования. Необходима гармонизация инвестиционных программ, планов по цифровизации, разработка и опытная эксплуатация нового оборудования, а также привлечение к данным работам научно-исследовательских и проектных коллективов.

Цифровая трансформация электроэнергетического комплекса России позволит повысить его надежность, наблюдаемость и управляемость, а также создать условия для развития новых рынков с участием распределенной и возобновляемой энергетики. Последовательное преобразование облика отечественной электроэнергетики необходимо с целью создания необходимых условий для инфраструктурного изменения страны, снятия ограничений в развитии высокотехнологичных отраслей экономи-

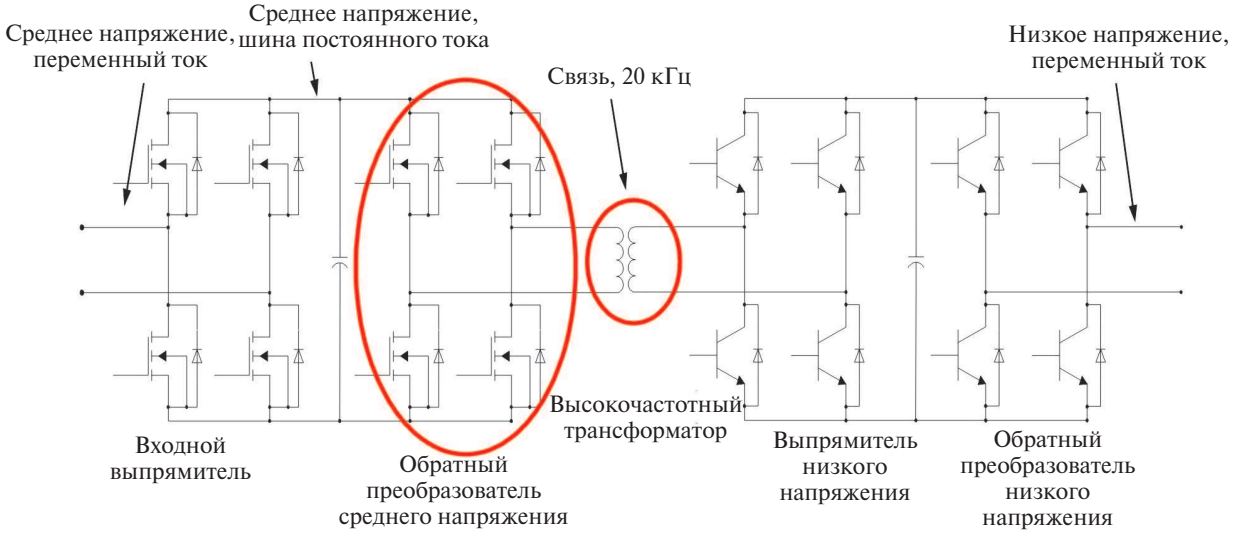


**Рис. 10.** Схемное решение модуля твердотельного трансформатора для одной фазы

ки, решения актуальных социальных, экономических и экологических задач.

СПИСОК ЛИТЕРАТУРЫ

1. **Концепция** «Цифровая трансформация 2030», утверждена Советом директоров ПАО «Россети» 21 декабря 2018 г.

2. **Указ** Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

3. **Распоряжение** Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации».

4. **Лоскутов А.Б.** Проблемы перехода электроэнергетики на цифровые технологии. – Интеллектуальная электротехника, 2018, № 1, с. 9–27.

5. **Цифровой** переход в электроэнергетике России, под общей редакцией В.Н. Княгинина и Д.В. Холкина, – Центр стратегических разработок, Москва, 2017.

6. **Распоряжение** Правительства РФ от 28 апреля 2018 г. № 830-р. «Об утверждении плана мероприятий («дорожной карты») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Энерджинет»».

7. **Шарыгин М.В., Куликов А.Л.** Защита и автоматика систем электроснабжения с активными промышленными потребителями. Н. Новгород: НИУ РАНХиГС, 2017, 284с.

8. **Илюшин П.В. Куликов А.Л.** Автоматика управления нормальными и аварийными режимами энергорайонов с распределенной генерацией. Н. Новгород: НИУ РАНХиГС, 2019, 364 с.

9. **Указ** Президента РФ от 13 мая 2019 г. № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации».

10. **Федеральный** закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

11. **Приказ** ПАО «Россети» от 29 марта 2019 г. № 64 «О введении в действие СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110–220 кВ и узловых цифровых подстанций напряжением 35 кВ», СТО 34.01-21-005-2019 «Цифровая электрическая сеть. Требования к проектированию цифровых распределительных электрических сетей 0,4–220 кВ»».

12. **Куликов А.Л., Зинин В.М., Шарафеев Т.Р.** Формирование новой технологической подсистемы, обеспечивающей кибербезопасность цифровых подстанций. – Цифровая энергетика: новая парадигма функционирования и развития. Сборник статей круглого стола / под ред. Н.Д. Рогалева, 2019, с. 113–124.

13. **Распоряжение** ПАО «Россети» от 30.05.2017 г. № 282р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети».

14. **Bo Z.Q., Wang Q.P., Wang L., Zhou F.Q., Ge S.M., Zhang B.M.** Architecture design for integrated wide area protection and control systems – The 7th Asia-Pacific Power and Energy Engineering Conference (APPEEC 2015), 2015.

15. **Guo Y., Wu W.C., Zhang B.M.** A distributed state estimation method for power systems incorporated with linear and nonlinear models. – International Journal of Electrical Power & Energy Systems, 2015, № 64, pp. 608–616.

16. **Bo Z.Q., Zhang B.H., Dong X.Z., He J.H.** The development of protection intellectuation and smart relay network. – Power System Protection and Control, 2013, № 41 (2), pp. 1–12.

17. **Gao H.L. Liu Y.Q., Su J.J.** New type of substation-area backup protection for intelligent substation. – China Smart Grid Seminar. 2012.

18. **Bo Z.Q., He J.H., Dong X.Z.** Integrated protection of power network. – Relay, 2005, № 33, pp. 33–41.

19. **Bo Z.Q., Wang L., Zhou F.Q.** Substation cloud computing for secondary auxiliary equipment. – IEEE Powercon 2014. Chengdu. 2014.

20. **Илюшин П.В., Березовский П.К.** Подходы к формированию технических требований по участию объектов распределённой генерации в регулировании напряжения в энергосистеме. – Энергетик, 2019, № 3, с. 12–18.

21. **Илюшин П.В., Куликов А.Л.** Трансформация технических требований к устройствам РЗА в условиях массового внедрения распределенных источников энергии. – Электроэнергия. Передача и распределение, 2020, № 2, с. 70–79.

22. **Мисриханов М.Ш. Рябченко В.Н.** Технология и устройства FACTS: учебное пос. Иваново: ИГЭУ им. В.И. Ленина, 2017, 111 с.

23. **Соснина Е.Н., Шалухо А.В., Липужин И.А., Кечкин А.Ю.** Исследование статической устойчивости электротехнических комплексов виртуальных электростанций. – Вестник Самарского государственного технического университета. Серия: Технические науки, 2017, №2 (54), с. 121–129.

24. **ГОСТ 32144-2013** Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения. М.: Стандартинформ. 2014, 16 с.

25. **Samad M.M.** Solid State Transformers: The State-of-the-Art, Challenges and Applications. – Proceedings of the World Congress on Engineering 2019 (WCE 2019), July 3–5, 2019. London, U.K.

26. **Abu-Siada A., Budiri J., Abdou A.** Solid State Transformers Topologies, Controllers, and Applications: State-of-the-Art Literature Review. – Electronics. 2018, vol. 7, No. 11, p. 298.

*[22.10.2020]*

*Авторы:* ***Лоскутов Алексей Борисович*** *– доктор техн. наук, профессор кафедры «Электроэнергетика, электроснабжение и силовая электроника» Нижегородского государственного технического университета им. Р.Е. Алексеева». Докторскую диссертацию защитил в 1994 г.*

***Куликов Александр Леонидович*** *– доктор техн. наук, профессор кафедры «Электроэнергетика, электроснабжение и силовая электроника» Нижегородского государственного технического университета им. Р.Е. Алексеева». Докторскую диссертацию защитил в 2007 г.*

***Илюшин Павел Владимирович*** *– доктор техн. наук, проректор по научной работе ФГАОУ ДПО «Петербургский энергетический институт повышения квалификации». Докторскую диссертацию защитил в 2019 г.*

*Electrichestvo, 2020, No. 12, pp. 14–30* *DOI:10.24160/0013-5380-2020-12-14-30*

# From the GOELRO Plan to Digitalization of Russia's Electric Power Complex

**LOSKUTOV Aleksey B.** *(Nizhny Novgorod State Technical University n.a. Alekseev (NSTU), Nizhny Novgorod, Russia) – Professor of the Department of Electric Power Engineering, Power Supply and Power Electronics, Dr. Sci. (Eng.)*

**KULIKOV Aleksandr L.** *(Nizhny Novgorod State Technical University n.a. Alekseev (NSTU), Nizhny Novgorod, Russia) – Professor of the Department of Electric Power Engineering, Power Supply and Power Electronics, Dr. Sci. (Eng.)*

**ILYUSHIN Pavel V.** *(Federal State educational establishment, St. Petersburg, Russia) –Vice-rector for research, Dr. Sci. (Eng.)*

*Owing to adoption of the GOELRO plan in 1920 and its stage-by-state implementation, it became possible to meet the country's needs for intense development of its economy through providing the required amounts of electricity to all sectors of the national economy. Nowadays, the smart grid technologies open the possibility to carry out «digital updating» of the grids to obtain their better observability and controllability, smaller losses in them, and to ensure reliable operation of distributed and renewable power generating facilities, which have become new participants in the electricity market. The use of smart grid technologies opens the possibility to optimally integrate heterogeneous electric power sources, backbone and distribution networks, and also active consumers into a unified electric power complex for achieving the economic and environmental objectives. The article considers modern innovative and prospective technologies of smart grids and outlines historical parallels with the GOELRO plan, which determined the course for electrification of Russia.*

K e y w o r d s: *GOELRO plan, electric power complex, digitalization, digital electrical substation, smart electronic devices, cybersecurity, distributed generation, renewable energy sources*

REFERENCES

1. **Kontseptsiya** *«Tsifrovaya transformatsiya 2030», utverzhdena Sovetom direktorov PAO «Rosseti» 21 dekabrya 2018 g.* (Concept «Digital Transformation 2030", approved by the Board of Directors of PJSC ROSSETI on December 21).

2. **Ukaz** P*rezidenta RF ot 21 iyulya 2020 g. № 474 «O natsional'nykh tselyakh razvitiya Rossiyskoy Federatsii na period do 2030 goda»* (Decree of the President of the Russian Federation of July 21, 2020 No. 474 «On the national development goals of the Russian Federation for the period up to 2030»).

3. **Rasporyazheniye** *Pravitel'stva RF ot 28 iyulya 2017 g. № 1632-r «Ob utverzhdenii programmy «Tsifrovaya ekonomika Rossiyskoy Federatsii»* (Order of the Government of the Russian Federation of July 28, 2017 No. 1632-r «On approval of the program" Digital Economy of the Russian Federation».

4. **Loskutov A.B.** *Intellektual'naya elektrotekhnika – in Russ. (Smart Electrical Engineering),* 2018, No. 1, pp. 9–27.

5. **Tsifrovoy** *perekhod v elektroenergetike Rossii, pod obshchey redaktsiyey V.N. Knyaginina i D.V. Kholkina. — Tsentr strategicheskikh razrabotok* (Digital Transition in the Electric Power Industry of Russia, edited by V.N. Knyaginin and D.V. Kholkina. — Center for Strategic Research). Moskou, 2017.

6. **Rasporyazheniye** *Pravitel'stva RF ot 28 aprelya 2018 g. № 830-r. «Ob utverzhdenii plana meropriyatiy («dorozhnoy karty») po sovershenstvovaniyu zakonodatel'stva i ustraneniyu administrativnykh bar'yerov v tselyakh obespecheniya realizatsii Natsional'noy tekhnologicheskoy initsiativy po napravleniyu «Enerdzhinet"»* (Order of the Government of the Russian Federation of April 28, 2018 No. 830-r).

7. **Sharygin M.V., Kulikov A.L.** *Zashchita i avtomatika sistem elektrosnabzheniya s aktivnymi promyshlennymi potrebitelyami* (Protection and automation of power supply systems with active industrial consumers). N. Novgorod: NIU RANKhiGS, 2017, 284 p.

8. **Ilyushin P.V. Kulikov A.L.** *Avtomatika upravleniya normal'nymi i avariynymi rezhimami energorayonov s raspredelennoy generatsiyey* (Automatic control of normal and emergency modes of power districts with distributed generation). N. Novgorod: NIU RANKhiGS, 2019, 364 p.

9. **Ukaz** *Prezidenta RF ot 13 maya 2019 g. № 216 «Ob utverzhdenii Doktriny energeticheskoy bezopasnosti Rossiyskoy Federatsii»* (Decree of the President of the Russian Federation of May 13, 2019 No. 216 «On approval of the Doctrine of energy security of the Russian Federation»).

10. **Federal'nyy** *zakon ot 26 iyulya 2017 g. № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii»* (Federal Law of July 26, 2017 No. 187-FZ «On the security of the critical information infrastructure of the Russian Federation»).

11. **Prikaz** *PAO «Rosseti» ot 29 marta 2019 g. № 64 «O vvedenii v deystviye STO 34.01-21-004-2019 «Tsifrovoy pitayushchiy tsentr. Trebovaniya k tekhnologicheskomu proyektirovaniyu tsifrovykh podstantsiy napryazheniyem 110-220 kV i uzlovykh tsifrovykh podstantsiy napryazheniyem 35 kV», STO 34.01-21-005-2019 «Tsifrovaya elektricheskaya set'. Trebovaniya k proyektirovaniyu tsifrovykh raspredelitel'nykh elektricheskikh setey 0,4–220 kV»* (Order of PJSC Rosseti dated March 29, 2019 No. 64 «On the introduction of STO 34.01-21-004-2019 «Digital power supply center. Requirements for technological design of 110–220 kV digital substations and 35 kV nodal digital substations», STO

34.01-21-005-2019 «Digital electrical network. Requirements for the design of digital distribution electrical networks 0,4–220 kV»).

12. **Kulikov A.L., Zinin V.M., Sharafeyev T.R.** *Tsifrovaya energetika: novaya paradigma funktsionirovaniya i razvitiya. Sbornik statey kruglogo stola / pod red. N.D. Rogaleva* (In the collection: Digital energy: a new paradigm of functioning and development. Collection of articles of the round table. Ed. by N.D. Rogalev), 2019, pp. 113–124.

13. **Rasporyazheniye** *PAO «Rosseti» ot 30.05.2017 g. № 282r «Ob utverzhdenii trebovaniy k vstroyennym sredstvam zashchity informatsii avtomatizirovannykh sistem tekhnologicheskogo upravleniya elektrosetevogo kompleksa gruppy kompaniy «Rosseti»*.

14. **Bo Z.Q., Wang Q.P., Wang L., Zhou F.Q., Ge S.M., Zhang B.M.** Architecture design for integrated wide area protection and control systems // The 7th Asia-Pacific Power and Energy Engineering Conference (APPEEC 2015). 2015.

15. **Guo Y., Wu W.C., Zhang B.M.** A distributed state estimation method for power systems incorporated with linear and nonlinear models. – International Journal of Electrical Power & Energy Systems, 2015, № 64, pp. 608–616.

16. **Bo Z.Q., Zhang B.H., Dong X.Z., He J.H.** The development of protection intellectuation and smart relay network. – Power System Protection and Control, 2013, № 41 (2), pp. 1–12.

17. **Gao H.L. Liu Y.Q., Su J.J.** New type of substation-area backup protection for intelligent substation. – China Smart Grid Seminar. 2012.

18. **Bo Z.Q., He J.H., Dong X.Z.** Integrated protection of power network. – Relay, 2005, № 33, pp. 33–41.

19. **Bo Z.Q., Wang L., Zhou F.Q.** Substation cloud computing for secondary auxiliary equipment. – IEEE Powercon 2014. Chengdu. 2014.

20. **Ilyushin P.V., Berezovskiy P.K.** *Energetik – in Russ. (Energetik)*, 2019, No. 3, pp. 12—18.

21. **Ilyushin P.V., Kulikov A.L.** *Elektroenergiya. Peredacha i raspredeleniye – in Russ. (Electricity. Transmission and distribution)*, 2020, No. 2, pp. 70—79.

22. **Misrikhanov M.SH. Ryabchenko V.N.** *Tekhnologiya i ustroystva FACTS: uchebnoye pos. (FACTS technology and devices: textbook). Ivanovo: IGEU im. V.I. Lenina, 2017, 111 p.*

23. **Sosnina E.N., Shalukho A.V., Lipuzhin I.A., Kechkin A.Yu.** *Vestnik Samarskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Tekhnicheskiye nauki – in Russ. (Bulletin of the Samara State Technical University. Series: Engineering Sciences)*, 2017, No. 2 (54), pp. 121—129.

24. **GOST 32144-2013.** *Elektricheskaya energiya. Sovmestimost' tekhnicheskikh sredstv elektromagnitnaya. Normy kachestva elektricheskoy energii v sistemakh elektrosnabzheniya obshchego naznacheniya* (Electrical energy. Electromagnetic compatibility of technical means. Electricity quality standards in general-purpose power supply systems), M.: Standartinform, 2014, 16 p.

25. **Samad M.M.** Solid State Transformers: The State-of-the-Art, Challenges and Applications. – Proceedings of the World Congress on Engineering 2019 (WCE 2019), July 3-5, 2019. London, U.K.

26. **Abu-Siada A., Budiri J., Abdou A.** Solid State Transformers Topologies, Controllers, and Applications: State-of-the-Art Literature Review. – Electronics. 2018, vol. 7, No. 11, p. 298.

*[22.10.2020]*