Александр Агеев, Олег Бочкарев, Евгений Грабчак, Евгений Логинов

Сетецентрическая система повышенной живучести управления энергетикой России в сложнопрогнозируемых критических условиях

УДК: 620.9
DOI: https://doi.org/10.33917/es-3.177.2021.6-17

Энергетика, как и оборонный комплекс, является одной из ключевых отраслей, на которых базируются процессы жизнеобеспечения страны и вытекающая отсюда устойчивость конструкции государства. Мировая практика четко выявила ключевую зависимость внутриполитической и социальной стабильности от надежности и устойчивости энергоснабжения. Многофакторную живучесть энергетической суперсистемы в обычных и критических условиях природного и техногенного характера можно обеспечить за счет формирования сетецентрической системы повышенной устойчивости управления, опирающейся на распределенную сеть межкорпоративных катастрофоустойчивых дата-центров по обработке и хранению сверхбольших массивов данных. Предлагается использование дата-центров как базы для цифровых «двойников» энергетических объектов и процессов с целью итогового выхода на новое качество управления на основе цифровой топологии в рамках единой цифровой модели энергетической суперсистемы с возможностью защищенного сбора, хранения, обработки, обмена данными, необходимыми для управления энергетическими объектами различных отраслевых подсистем ТЭК России, а также для региональных и муниципальных властей. Использование цифровой топологии позволяет при локальных взаимодействиях осуществлять поиск и реализацию решений по продвижению к локальным и сете- и полицентрическим ресурсно-операционным оптимумам для минимизации затрат (ценовой нагрузки на потребителя) отдельных компаний и всей отрасли с целью поддержания надежности и устойчивости энергоснабжения, включая затраты на безопасность систем критической информационной инфраструктуры.

Ключевые слова
Энергетика, управление, сетецентрическая система, дата-центры, информационная система, цифровая топология, защита, устойчивость, чрезвычайные ситуации.

Агеев Александр Иванович — директор Института экономических стратегий, генеральный директор Международного научно-исследовательского института проблем управления, заведующий кафедрой НИЯУ МИФИ, доктор экономических наук, профессор МГИМО(у) МИД России, НИЯУ МИФИ, МГУ имени М.В. Ломоносова.

Бочкарев Олег Иванович — заместитель председателя коллегии Военно-промышленной комиссии Российской Федерации, кандидат экономических наук.

Грабчак Евгений Петрович — заместитель министра энергетики Российской Федерации, кандидат экономических наук.

Логинов Евгений Леонидович — начальник экспертно-аналитической службы Ситуационно-аналитического центра Минэнерго России, дважды лауреат премии Правительства РФ в области науки и техники, доктор экономических наук, профессор РАН, эксперт РАН.

Aleksandr I. Ageev — Institute for Economic Strategies; International Research Institute for Advanced Systems; MGIMO University; MEPhI; Lomonosov Moscow State University.

Oleg I. Bochkarev — Military-Industrial Commission of the Russian Federation.

Evgenii P. Grabchak — Ministry of Energy of the Russian Federation.

Evgenii L. Loginov — Ministry of Energy of the Russian Federation.

Развитие интеллектуальных информационных сервисов, Интернета вещей и цифровизации приводит к тому, что объемы производимой, передаваемой и обрабатываемой информации резко возрастают [1].

Глобальный оборот данных к 2025 г. может вырасти более чем в 5 раз.

При этом аналогично растут стандартизированные потребности операторов и пользователей с повышенными требованиями к скорости передачи и качеству обработки информации [2, 3].

Рост значения информации ведет к росту потребностей, а следовательно, и затрат на безопасность [4].

Лавина информационных трансформаций

Опрос, проведенный в 2020 г. *Dell Technologies Global Data Protection Index*, показал, что совре-

Net-Centric System of Elevated Stability (Survivability) of Energy Management in Russia Under Difficult-to-predict Critical Conditions

Energy sector, like the defence complex, is one of the key industries that serve as a basis for the life support processes of the country and the resulting stability of the state political structure. World practice has clearly demonstrated the key dependence of domestic political and social stability on reliability and sustainability of energy supply. Multifactorial survivability of the energy supersystem under normal and critical conditions of natural and anthropogenic origin can be provided through forming a net-centric system of elevated management stability, based on a distributed network of inter-corporate disaster-resistant data centers for processing and storing extremely large data sets. It is proposed to use data centers as bases for digital "twins" of energy facilities and processes in order to finally achieve a new quality of control based on digital topology within a single digital model of the energy supersystem with the possibility of secure collection, storage, processing and exchange of data, necessary for managing power facilities of various sectoral subsystems of the Russian fuel and energy complex, as well as for regional and municipal authorities. Application of digital topology makes it possible, during local interactions, to search for and implement solutions for moving towards local, network and polycentric resource-operational optima in order to minimize costs (price burden on the consumer) of separate companies and the entire industry with the aim of maintaining reliability and sustainability of energy supply, including security costs of the critical information infrastructure systems.

Keywords
Energy industry, management, net-centric system, data centers, information system, digital topology, security, sustainability, emergencies.

Александр Агеев, Олег Бочкарев, Евгений Грабчак, Евгений Логинов

➢➢ Энергетика, как и оборонный комплекс, является одной из ключевых отраслей, на которых базируются процессы жизнеобеспечения страны и вытекающая отсюда устойчивость конструкции государства.

менная крупная компания мирового уровня оперирует данными объемом около 13,56 Пбайт. При этом речь идет не об операторах больших данных, а о компаниях, использующих данные. Средний объем оперируемых данных демонстрирует гипертрофированный рост, увеличившись в 831 раз с 2016 г. [5].

Происходит усложнение технических решений и схем работы с информацией. Однако ранее сформированные средства и компоненты систем информационной безопасности оказываются не в состоянии покрыть новые инфраструктуры с тем же уровнем защиты [5].

За последние шесть лет количество кибератак на информационные ресурсы Министерства обороны РФ увеличилось на 57%. Такие данные в июне 2019 г. привел глава Департамента информации и массовых коммуникаций Минобороны России генерал-майор И.Е. Конашенков в ходе круглого стола в рамках форума «Армия-2019». Он отметил, что «за шесть лет число попыток выведения из строя объектов критической информационной инфраструктуры выросло на 57%». Ведомство постоянно сталкивается «с различными попытками внешнего информационно-технического воздействия» на его системы и интернет-ресурсы. С 2013 г. Минобороны России выявило и нейтрализовало более 25 тыс. вторжений на информационные ресурсы Вооруженных сил [6].

15 июня 2019 г. *The New York Times* (NYT) опубликовала статью об увеличении количества американских кибератак на российские электрические сети, в которой эксперты ссылались на неназванные источники из числа бывших правительственных чиновников США, предоставивших соответствующие сведения в рамках интервью. В статье также сказано, что электросети России подвергались массированным кибератакам со стороны США на протяжении весны 2019 г. Целью атак было внедрение в систему вредоносного кода, способного саботировать работу электросетей. Как уточняют источники NYT, разведывательные действия в энергосистеме России ведутся с 2012 г. Но теперь, по мнению авторов этой статьи, действия становятся более агрессивными: размещение вредоносного программного обеспечения в компьютерных сетях в случае конфликта между двумя странами станет основой для полномасштабной атаки в киберпространстве [7].

Статья NYT вызвала негативную реакцию президента США Дональда Трампа. В своем официальном микроблоге в *Twitter* он назвал публикацию скандального материала актом государственной измены, а его авторов — «подлинными трусами и настоящими врагами людей».

В этих условиях российским государством принимаются меры к обеспечению безопасности информационных систем критической инфраструктуры [8]. Правительством России с учетом курса на развитие цифровой экономики принят ряд федеральных программ, направленных на повышение безопасности информационных систем. Отраслевые программы реализуются федеральными и региональными министерствами и ведомствами, а также на уровне крупных и средних компаний, в том числе в ТЭК России [9].

Проблемы, актуализирующие потребность в новых организационно-технологических решениях в сфере информационной безопасности в энергетике

В рамках стратегического тренда цифровизации можно выделить целый ряд проблем, актуализирующих потребность в новых организационно-технологических решениях, упреждающих качественный переход количества отдельных проблем в общую системную уязвимость систем управления в энергетике нашей страны в условиях сложнопрогнозируемых чрезвычайных ситуаций [10].

Прежде всего это накопленное за последние два десятилетия существенное отставание большинства российских предприятий, в том числе энергетических компаний, от предприятий наиболее развитых стран мира с точки зрения уровня цифрового развития и информационной безопасности [11]. В последние годы этот разрыв сокращается, однако и цифровое развитие зарубежных конкурентов, включая средства информационных атак и деструктивного воздействия на информационные системы, не стоит на месте [12].

Кроме того, возрастание числа интеллектуальных элементов в сетях управления в энергетике также увеличивает их уязвимость к природным и техногенным воздействиям (например, электромагнитного характера). Весьма вероятна угроза случайного или инициированного массового скольжения активно-адаптивных сегментов суперсистемы вследствие однонаправленного совпадения оптимизирующих векторов регулирования со стороны *smart grid* или аналогичных подсистем [13].

Системы управления в энергетике (в том числе SCADA, АСУ ТП, микропроцессорные устройства технологической защиты и автоматики и т.п.) более чем на 80% построены на иностранной программно-аппаратной базе. (Некоторым исключением является Росатом, в работе которого имеется гражданская и оборонная составляющая. Эта госкорпорация в значительной степени использует российские технологии и комплектующие в важнейших узлах оборудования, хотя и здесь работы еще очень много.)

Импортозамещение в информационной сфере энергетики находится в начале пути: во-первых, остро не хватает средств на финансирование импортозамещающих проектов у самих пользователей информационных систем управления технологическими и бизнес-процессами; во-вторых, утрачены целые сегменты отечественных отраслей, которые надо восстанавливать (например, гражданское приборостроение), что опять-таки требует денег, времени и очень больших организационных усилий [14].

До сих пор не внедрены в полном объеме стандартизированные основные технические решения по обеспечению информационной и иной безопасности систем управления энергетическими объектами, хотя эта работа ведется.

В этой сфере компании применяют разные решения. Более или менее системно, хотя и на очень упрощенном уровне, эта работа поставлена в крупных и средних энергетических компаниях. В мелких компаниях, особенно муниципальных, если не брать областные центры, эта работа вообще в зачаточном состоянии и по финансовым, и по кадровым причинам, и по приоритетности для вышестоящего руководства.

Нагромождение различных технических решений в сфере телекоммуникаций, информационной безопасности и иных «на земле» (в регионах) приводит к неоправданному дублированию, неэффективному расходованию средств и в конечном итоге к недостаточной защищенности систем управления и оборудования как отдельных энергокомпаний, так и большинства сегментов энергосистемы, в особенности в дотационных депрессивных регионах нашей страны [15]. Исключением является Системный оператор Единой энергетической системы (АО «СО ЕЭС»), защищенность которого обусловлена тем, что в постсоветский период здесь сумели сохранить и развить советские подходы к решению этих проблем.

С учетом перспектив увеличения телекоммуникационного и телеметрического оборота цифровых данных и потребностей в вычислительных сервисах выходом для энергетики в современных сложных экономических условиях может быть формирование сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть межкорпоративных дата-центров по обработке и хранению сверхбольших массивов данных для энергетических компаний и региональных и муниципальных властей. На этой основе будет обеспечено сокра-

щение числа маломощных корпоративных дата-центров в каждой отдельной энергокомпании, их укрупнение на коллективных финансовых началах, стандартизация технических решений по защите оборота и хранения информации для поддержания устойчивости управления энергетикой России как квазиинтегрированным технологическим комплексом в условиях естественных и искусственных угроз.

Повышение эффективности управления на основе цифровой топологии в рамках единой цифровой модели отраслевой энергетической суперсистемы

Общим результатом использования территориально распределенной сети межкорпоративных дата-центров с учетом резкого возрастания объема обрабатываемых данных является возможность повышения эффективности управления на основе цифровой топологии в рамках единой цифровой модели отраслевой энергетической суперсистемы.

Оптимизация достигается через упрощение и ускорение планирования, настройки, управления, улучшение параметров работы элементов энергетической суперсистемы на основе внедрения цифровых «двойников» технологических процессов, физических систем, объектов и изделий. Каждый из этих объектов представляет собой цифровой информационный комплекс систем обработки данных и систем автоматики в управлении производственными и организационно-экономическими процессами [16].

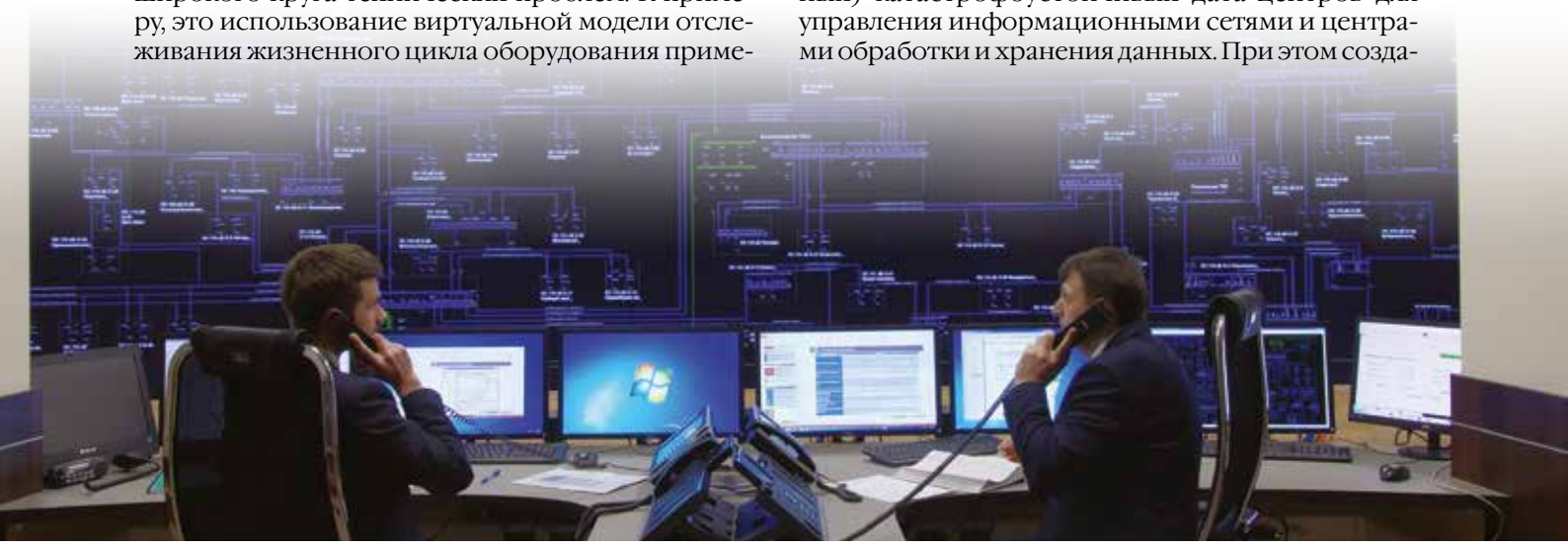
Реализация цифровой топологии в рамках единой цифровой модели отраслевой энергетической суперсистемы на основе сети межкорпоративных (областных) дата-центров для управления информационными сетями и центрами обработки и хранения данных может быть применена к решению широкого круга технических проблем. К примеру, это использование виртуальной модели отслеживания жизненного цикла оборудования применительно к объектам энергетической суперсистемы, структурированной как комплекс небольших оцифрованных энергетических кластеров (например, в форме активных энергетических комплексов) [17].

Для оптимизации цепочки информационного обмена данными, их вычислительной обработки и фиксирования с использованием виртуальной модели отслеживания жизненного цикла оборудования в систему следует включить компоненты, формирующие инвариантное ядро интеллектуального генератора и транслятора данных, интегрируемого из отдельных квазиавтономных элементов в сети (полицентрической системе) оцифрованных энергетических кластеров.

Использование межкорпоративных дата-центров по обработке и хранению сверхбольших массивов данных позволит реализовать при локальных взаимодействиях поиск и реализацию решений по продвижению к локальным и сете- и полицентрическим ресурсно-операционным оптимумам работы технических и организационных систем. В том числе предлагается контроль и анализ эффективности использования каждого рубля по цепочке технологических операций в процессе эксплуатации и ремонта как элемента оптимума более высокого организационного уровня в режиме, близком к реальному времени.

Ключевые характеристики создания сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть межкорпоративных дата-центров

Ускоренное внедрение цифровой топологии в рамках единой цифровой модели отраслевой энергетической суперсистемы может быть реализовано именно на основе использования в энергетике России сети межкорпоративных (областных) катастрофоустойчивых дата-центров для управления информационными сетями и центрами обработки и хранения данных. При этом созда-



➢➢ Мировая практика четко выявила ключевую зависимость внутриполитической и социальной стабильности от надежности и устойчивости энергоснабжения.

ется возможность для обеспечения согласованности действий цифровых «двойников» энергетических объектов и процессов, селективности коммуникаций, а также восстановления в случае аварии функциональности агентов и реализации обратной связи.

Сейчас каждая энергетическая компания на уровне областного центра (административного центра субъекта Российской Федерации) формирует свой корпоративный дата-центр. В зависимости от ее финансовых возможностей, компетенции специалистов самой компании и ее головной компании, уровня цифровизации в отрасли и в корпоративной группе, развитости информационно-телекоммуникационной инфраструктуры в регионе эти программно-аппаратные комплексы кардинально отличаются по всем возможным параметрам. Борьба специалистов самой компании за «освоение» как можно большего объема финансовых средств и конкуренция близких к руководству компании структур, обеспечивающих формирование и реализацию проектов цифровизации, привела к анархическому нагромождению различных стратегий, подходов, концепций, конкретных технологических решений, как правило, меняющихся со сменой очередного руководства. Новое руководство в большинстве случаев отказывается от старого проекта (и услуг компании, его реализующей) и запускает новый проект. Случайный характер преемственности реализующихся технических решений в цепочке цифровых трансформаций компании обеспечивает все что угодно, кроме эффективности корпоративного дата-центра, в том числе защищенности оборота и хранения информации.

В этих условиях целесообразно создание в областном центре на коллективных финансовых началах единого межкорпоративного катастрофоустойчивого дата-центра. Создание такого центра позволит на основе концентрации совокупных финансовых средств энергетических компаний, которые они тратят на цифровизацию и информационную безопасность (компании: генерация электроэнергии, ее распределение и сбыт, сервисные услуги, поставка топливно-энергетических ресурсов, генерация и распределение тепла и т.п.), сформировать дата-центр с более высокими качественными характеристиками как самих услуг, так и защищенности передачи и хранения информации.

При наличии сети таких дата-центров, объединенных в сетецентрическую систему повышенной устойчивости управления энергетикой, может быть обеспечена синхронная репликация данных между дата-центрами в рамках группы соседних регионов (например, федеральных округов, кластеров активных энергетических комплексов, мегарегионов, а также иных агломераций территориального или функционального уровня). Кроме того, появляется возможность обеспечить максимальную надежность, в том числе защищенность, магистральных каналов связи, предложить выгодные условия SLA (*Service Level Agreement*), повысить пропускную способность каналов до точек обмена трафиком (региональных и международных), а также число прямых пиринговых стыков сети дата-центра с провайдерами и т.п.

Синхронная репликация данных между дата-центрами позволяет сформировать информационную инфраструктуру, адаптированную к сложнопрогнозируемым чрезвычайным ситуациям, обеспечивающую живучесть систем управления и сохраняющую накопленную информацию, даже если значительная часть информационных систем управления технологическими и бизнес-процессами в группе регионов будет физически уничтожена в ходе природной или техногенной катастрофы.

Иначе говоря, на базе единого межкорпоративного катастрофоустойчивого дата-центра в каждом субъекте Российской Федерации создаются более широкие возможности оказания информационно-коммуникационных и вычислительных услуг, повышения их количества и качества, в том числе специализированных услуг, которые каждая компания в отдельности не могла себе позволить в принципе. Одновременно обеспечивается максимально возможная защищенность информационного обмена и хранения информации с постепенным доведением безопасности до параметров, свойственных военным или специальным объектам. Применяются отработанные в оборонной и тому подобных сферах (Росатом, Роскосмос и др.) технические решения на полностью отечественной программной и компонентной базе.

Ядром системы должна стать цифровая платформа, одновременно формирующая драйвер сетевого взаимодействия других маршрутизаторов как элементов регулирующего комплекса, включающего мониторинговый детектор, фильтр данных и модуль оптимизации. Такая система должна объединить информационные, телеметрические и вычислительные сервисы для развития информационных систем управления технологически-

ми и бизнес-процессами при управлении оцифрованными кластерами энергетических объектов.

Укрупненные блоки сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть катастрофоустойчивых межкорпоративных дата-центров, предполагают:
• формирование в каждом субъекте Российской Федерации межкорпоративного облачного дата-центра для оказания информационных услуг и вычислительных сервисов с подключением высокоскоростных телекоммуникационных сетей от энергетических компаний и органов власти и управления;
• формирование в таких межкорпоративных облачных дата-центрах универсального набора информационных услуг и вычислительных сервисов, позволяющих обслуживать компании в сфере генерации и транспортировки электроэнергии и тепла, производства, хранения и распределения других видов топливно-энергетических ресурсов, оказания коммунальных услуг, сбыта топливно-энергетических ресурсов и сбора платежей, обмена информацией с региональными и муниципальными властями и пр.;

>> Современная крупная компания мирового уровня оперирует данными объемом около 13,56 Пбайт.

• поэтапную полную цифровизацию всех энергетических компаний и органов власти и управления с использованием информационно-телекоммуникационного оборудования, позволяющего обеспечить 100-процентный электронный документооборот (обычного и защищенного характера) как в рамках субъекта Российской Федерации, так и с выходом на федеральный центр и другие регионы России, с упорядоченным доступом к открытой и ограниченной для распространения информации;
• создание таких центров и инфраструктуры в энергетике актуальных и потенциальных государств — членов ЕАЭС, изучение возможности создания таких центров в других странах, граничащих с Россией и осуществляющих энергообмен с нашей страной (Таджикистан, Монголия и др.);
• строительство в России предприятий по производству компьютерного и иного оборудования, что позволит через три-четыре года перестать ввозить компьютерные и телекоммуникационные комплектующие из стран за пределами ЕАЭС;
• формирование инфраструктуры электронной торговли (через электронные торговые площадки), позволяющей качественно перестроить в государственных и коммерческих интересах управление энергоснабжением, маркетинг, энергосбытовой, фискальный и управленческий учет, планирование и прогнозирование энергетического и социально-экономического развития;
• формирование информационно-вычислительных мощностей, позволяющих защитить информационно-телекоммуникационные сети и системы энергетических компаний и органов власти и управления от информационных атак (в том числе защитить передачу и хранение информации от любых естественных и инициированных угроз), а также организовать качественное наращивание информационных сервисов на уровне наиболее развитых стран мира [18];
• формирование в регионах качественно новых сервисов, обеспечивающих мониторинг и прозрачность информационно-коммуникационной электронной среды и т.п.

Катастрофоустойчивость дата-центра должна соответствовать *Tier 3* стандарта TIA-942 (*Telecommunications Industry Association — Telecommunications Infrastructure Standard for Data Centers*) с постепенным переходом к *Tier 4*. (Уровень *Tier 3*: все инженерные системы многократно зарезервированы — имеется множество каналов электропитания и охлаждения, однако постоянно активным является только один из них. Такая схема резервирования называется 2N, все основные системы продублированы.) Предполагается, что *Tier 4* пригоден для работы в военных условиях.

Продвижение к локальным и сете- и полицентрическим ресурсно-операционным оптимумам работы технических и организационных систем в энергетике

В результате формирования сети межкорпоративных (областных) катастрофоустойчивых дата-центров создается возможность системного технологического выигрыша за счет сочетания советских подходов и решений к формированию и развитию ЕЭС СССР и ЕЭС России и новых решений сете- и полицентрического характера с квазиинтеграцией на различных уровнях управления и в рамках территориальных систем и кластеров генерирующих мощностей и энергопотребителей.

Информационно-коммуникационные и вычислительные мощности таких межкорпоративных дата-центров на уровне областного центра позволяют внедрить в энергетике сквозные — в рамках крупных корпоративных групп с большим количеством ДЗО — полноценные ERP-системы на всей территории страны с выходом на квазиинтегрированное информационное поле в рамках каждой отрасли с максимальной детализацией составляющих.

В результате осуществляется поддержание цифрового мониторинга процессов старения, износа, выбытия, ремонта и замены функциональ-

ных узлов энергетических объектов, в том числе для обеспечения согласованности действий в отношении эксплуатации и ремонта объектов и их функциональных узлов, а также обеспечение селективности коммуникаций и реализация обратной связи [19].

Важная задача, решаемая при этом с целью повышения надежности и безопасности энерго- и теплоснабжения в рамках имеющейся тарифно-ценовой нагрузки на потребителя, — оптимизация затрат на поддержание надежности и устойчивости энергоснабжения, включая затраты на безопасность систем критической информационной инфраструктуры, через контроль и анализ эффективности использования каждого рубля по цепочке технологических операций в процессе эксплуатации и ремонта.

Цифровизация позволяет перейти к анализу максимально детализированного (применительно к отдельной детали или комплексу оборудования) состава закупаемых энергокомпаниями запчастей и комплектующих с позиций обеспечения приоритетов импортозамещения, сравнения технических характеристик, выявления отличий в ценовых показателях и иных параметрах закупочных операций и реальных процессов замены оборудования максимально широкого перечня, в том числе в ретроспективе [20].

Разработанные технологии позволят получать достоверные оценки эффективности мониторинга и анализа соответствия процессов старения, износа, выбытия, ремонта и замены функциональных узлов реализуемым режимам эксплуатации систем энерго- и теплоснабжения и обеспечат возможность обоснованного выбора корректирующих команд в отношении очередности замены функциональных узлов для минимизации рисков нарастания аварийности вследствие износа. Фактически создается возможность прогнозирования, планирования, операционного сопровождения жизненного цикла каждой закупаемой и заменяемой детали во временной динамике от технических проектов, планов и факта закупки до замены, утилизации и списания сквозным образом по всему комплексу технической, бухгалтерско-экономической и иной управленческой документации. Цифровизация позволит использовать для этого автоматизированные сервисы с наращиванием объемов анализируемых данных и выявлением ранее недоступных характеристик как технологических операций и процессов, так и действий производственного и управленческого персонала.

Важным эффектом является возможность консолидированного управления активами для государственных ведомств и корпоративных групп, для всех компаний в сфере ТЭК и ЖКХ.

➤➤ За последние шесть лет количество кибератак на информационные ресурсы Министерства обороны РФ увеличилось на 57%.

Создается возможность мониторинга движения финансовых средств в привязке к материальным объектам (ресурсно-финансовых трансакций) в рамках интегрированных ERP-систем с формированием квазиинтегрированного информационного поля по отраслевому, корпоративному или территориальному критериям с максимальной детализацией составляющих. Это позволяет наладить поитерационный мониторинг финансовых цепочек с контролем движения денег от инвестора (или тарифно-ценового источника средств) до завершения инвестиционного проекта, выхода на плановые производственные показатели и последующей уплаты налогов с реализуемой продукции или услуг. Иначе говоря, появляется возможность обеспечить «закольцовку» мониторинга и анализа полного финансово-инвестиционного цикла с оценкой эффективности инвестиций как начального вектора для формирования плановой налоговой базы, выступающей в качестве основы благополучия бюджетов всех уровней.

Интеграция ERP-систем на базе межкорпоративных дата-центров на уровне областного центра с включением в него сервисных компаний и субподрядчиков позволяет обеспечить прозрачность операций в рамках кооперации, субподряда или аутсорсинга с доступностью анализа добавленной стоимости, налоговой базы и доходов сотрудников.

Упорядочение структуры оборудования, программного обеспечения и технических реше-

ний, реализованных в рамках межкорпоративных дата-центров на уровне областного центра, позволяет проконтролировать учет требований и внедрение стандартизированных отраслевых технологических решений с учетом требований безопасности в инвестпрограммах энергетических компаний и проектах субъектов Российской Федерации и крупных муниципальных образований.

Новый по количеству и качеству данных массив технологической информации позволяет сформировать основы оптимизации режимов энергоснабжения в рамках регионов, энергетических кластеров как единого вычислительного пространства для оптимизации и подержания устойчивости энергоснабжения как в обычных условиях, так и в условиях сложнопрогнозируемых чрезвычайных ситуаций.

При этом создается база для качественного расширения возможностей управления энергосетями низкого и средних уровней для сетевых компаний.

Для Минэнерго России как регулятора создаются возможности формирования единой информационной основы для управления комплексом генерации и энергосетей на межкорпоративном уровне независимо от организационно-правовой формы юридических лиц, формы собственности, структуры собственников и величины корпоративно оперируемых активов и ресурсов.

Интеграционный информационно-управленческий контур энергетики, ОПК России и госуправления в рамках консолидированного (пакетного) отраслевого заказа

Цифровой мониторинг и анализ процессов старения, износа, выбытия, ремонта и замены функциональных узлов в увязке с режимами эксплуатации, построенных на основе конфигурирования синхронизирующихся цифровых «портретов» (двойников) генерирующего и сетевого энергетического оборудования позволяет детализировать плановые показатели оборудования и комплектующих, которые требуется заменить, в натуральных, финансовых, корпоративных, объектных и территориальных показателях [21].

Плановые показатели оборудования и комплектующих, которые требуется заменить, позволяют энергокомпаниям сформировать консолидированный (пакетный) отраслевой заказ, направляемый промышленным предприятиям [22]. Оператором отраслевого заказа, своего рода системным интегратором, осуществляющим сбор информации, формирование (структурированных по заказчикам и производителям) пакетов плановых

➢➢ Формирование сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть межкорпоративных дата-центров по обработке и хранению сверхбольших массивов данных, необходимо не только для упорядочения процессов цифровизации управления в энергетике.

заказов оборудования и технологий с необходимым уровнем локализации в рамках критериев импортозамещения и показателей инновационности, должен быть федеральный орган исполнительной власти (например, Минэнерго России или Военно-промышленная комиссия). Оператором отраслевого заказа со стороны промышленных предприятий может быть головная компания крупной промышленной корпоративной группы, например Ростех.

Элементы такого управления реализованы при формировании крупных военных заказов, например в США [23].

Особенно важно формирование консолидированного отраслевого заказа для целей обеспечения информационной и иной безопасности при реализации проектов цифровизации в энергетике.

Именно формирование территориально распределенной сети межкорпоративных катастрофоустойчивых дата-центров позволяет сформировать отраслевой заказ для предприятий оборонно-промышленного комплекса (ОПК) по производству оборудования и комплектующих для систем управления в энергетике, соответствующих самым жестким критериям и стандартам защищенности.

Отраслевой заказ энергетики по конкретным видам оборудования и комплектующих можно на 80–85% рассчитать на 5–10 лет вперед, что может служить основой для планов предприятий ОПК, нацеленных на модернизацию производства, расширение производственных мощностей и внедрение новых технологий [24].

Кроме того, формирование территориально распределенной сети межкорпоративных катастрофоустойчивых дата-центров и отработка для них стандартизированных технологических решений (аппаратной и программной базы) позволяет осуществить распространение этих технологических и организационных решений на промышленность, транспорт, сельское хозяйство и другие отрасли. Это позволит увеличить объем заказов на оборудование для ОПК России.

* * *

Формирование сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть межкорпоративных дата-центров по обработке и хранению сверхбольших массивов данных, необходимо не только для упорядочения процессов цифровизации управления в энергетике.

Это новый прорывной проект, позволяющий в рамках более эффективного использования имеющихся у энергокомпаний финансовых средств, ежегодно тратящихся на информационные задачи, резко нарастить параметры цифровизации в энергетике с одновременным повышением защищенности от любых возможных угроз информационным системам управления технологическими и бизнес-процессами на принципах импортозамещения с учетом критериев инновационности.

Создание сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть межкорпоративных дата-центров, позволяет внести элементы стабильного планового управления в хаотические процессы функционирования рыночной экономики, подверженной не только экономическим кризисам, но и воздействию сложнопрогнозируемых глобальных чрезвычайных ситуаций. Одной из таких чрезвычайных ситуаций стала коронавирусная пандемия, а могут быть природные катастрофы или военные действия. ЭС

ПЭС 21040 / 11.05.2021

Источники

1. Агеев А.И., Авдеев С.В., Новоточинов А.А., Рыжов В.А., Фадеева Т.И. IBM как зеркало мировой эволюции IT и пришествие второй информационной революции. Скрытые интеллектуальные пружины, возможные технологические и гуманитарные тормоза, ожидаемые последствия // Экономические стратегии. 2016. № 4. С. 84–107.

2. Грабчак Е.П. Применение интеллектуальных технологий в электроэнергетике: Материалы VII Международного форума «Россия в XXI веке: Глобальные вызовы и перспективы развития» (Москва, 21–22 декабря 2018 г.). М.: ИПР РАН, 2018. С. 137–141.

3. Юсупова Н.И., Шахмаметова Г.Р., Еникеева К.Р. Интеллектуальные технологии обработки информации для антикризисного управления в организационно-технических системах // Проблемы сбора, подготовки и транспорта нефти и нефтепродуктов. 2013. № 1. С. 113–124.

4. Абросимов Н.В., Агеев А.И., Бочкарев О.И. и др. Безопасность России. Правовые, социально-экономические и научно-технические аспекты // Сводный том «Фундаментальные и прикладные проблемы комплексной безопасности». М.: Знание, 2017. 992 с.

5. Щербаков Б. Безопасность — понятие многопрофильное [Электронный ресурс] // ИКС-медиа. 2020. 15 мая. URL: http://www.iksmedia.ru/articles/5662566-Bezopasnost-ponyatie-mnogoprofilnoe.html.

6. Число атак на ресурсы Минобороны РФ за 6 лет возросло почти на 60% [Электронный ресурс] // SecurityLab.ru. 2019. 27 июня. URL: https://www.securitylab.ru/news/499655.php.

7. Sanger D., Perlroth N. U.S. Escalates Online Attacks on Russia's Power Grid [Электронный ресурс] // The New York Times. 15 June. 2019. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

8. Агеев А.И., Логинов Е.Л., Райков А.Н. Информационные системы управления в чрезвычайных ситуациях // Экономические стратегии. 2019. № 2. С. 20–29.

9. Новак А. Энергетика: взгляд в будущее // Энергетическая политика. 2019. № 2. С. 6–11.

10. Агеев А.И., Грабчак Е.П., Логинов Е.Л. Smart-коллапс в цифровой энергетике будущего: угрозы глобального обрушения информационных систем управления в условиях возможной самоорганизованной информационной блокады // Энергетик. 2020. № 6.

11. Агеев А.И., Бондарик В.Н., Иванова О.Д., Кудрявцев А.В., Лощинин А.А. Технократическая концепция проектов цифровой экономики: синергия интеграции систем и данных // Микроэкономика. 2018. № 5. С. 14–21.

12. Грабчак Е.П., Григорьев В.В., Логинов Е.Л., Райков А.Н., Шкута А.А. Управление экономикой России в условиях с предельно большой компонентой неопределенности развития чрезвычайных ситуаций и критического недостатка информации // Проблемы безопасности и чрезвычайных ситуаций. 2019. № 4. С. 104–110.

13. Грабчак Е.П., Логинов Е.Л. Цифровые технологии автоматизированного документооборота в рамках электро- и теплоэнергетических систем с элементами SMART GRID // Проблемы сертификации, управления качеством и документационного обеспечения управления: Сб. материалов Всерос. науч.-практ. конф. Красноярск: СибГУ им. М.Ф. Решетнева, 2020. С. 39–43.

14. Агеев А.И., Смирнова В.А. Адаптивность высокотехнологичного комплекса к цифровым вызовам // Экономические стратегии. 2018. № 1. С. 164–166.

15. Грабчак Е.П., Логинов Е.Л. Анализ и прогнозирование критических ситуаций в электро- и теплоэнергетике России на основе внедрения инновационных информационных сервисов // Инновационная деятельность. 2019. № 4. С. 24–28.

16. Грабчак Е.П. Цифровая трансформация электроэнергетики. М.: Кнорус, 2018. 340 с.

17. Грабчак Е.П. Цифровизация в электроэнергетике: к чему должна прийти отрасль? // Энергетическая политика. 2019. № 1. С. 16–21.

References

1. Ageev A.I., Avdeev S.V., Novotochinov A.A., Ryzhov V.A., Fadeeva T.I. IBM kak zerkalo mirovoi evolyutsii IT i prishestvie vtoroi informatsionnoi revolyutsii. Skrytye intellektual'nye pruzhiny, vozmozhnye tekhnologicheskie i gumanitarnye tormoza, ozhidaemye posledstviya [IBM as a Mirror of the Global IT Evolution and Advent of the Second Information Revolution. Hidden Intellectual Springs, Possible Technological and Humanitarian Brakes, Expected Implications]. *Ekonomicheskie strategii*, 2016, no 4, pp. 84–107.

2. Grabchak E.P. *Primenenie intellektual'nykh tekhnologii v elektroenergetike: Materialy VII Mezhdunarodnogo foruma "Rossiya v XXI veke: Global'nye vyzovy i perspektivy razvitiya". Moskva, 21–22 dekabrya 2018 g.* [Application of Intelligent Technologies in the Electric Power Industry: Proceedings of the VII International Forum "Russia in the XXI Century: Global Challenges and Development Prospects", Moscow, December 21-22, 2018]. Moscow, IPR RAN, 2018, pp. 137–141.

3. Yusupova N.I., Shakhmametova G.R., Enikeeva K.R. Intellektual'nye tekhnologii obrabotki informatsii dlya antikrizisnogo upravleniya v organizatsionno-tekhnicheskikh sistemakh [Intelligent Information Processing Technologies for Crisis Management in Organizational and Technical Systems]. *Problemy sbora, podgotovki i transporta nefti i nefteproduktov*, 2013, no 1, pp. 113–124.

4. Abrosimov N.V., Ageev A.I., Bochkarev O.I., et al. *Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty* [Security of Russia. Legal, Socio-economic and Scientific and Technical Aspects]. Svodnyi tom "Fundamental'nye i prikladnye problemy kompleksnoi bezopasnosti". Moscow, Znanie, 2017, 992 p.

5. Shcherbakov B. *Bezopasnost' — ponyatie mnogoprofil'noe* [Security is a Multidisciplinary Concept]. IKS-media, 2020, May, 15, available at: http://www.iksmedia.ru/articles/5662566-Bezopasnost-ponyatie-mnogoprofilnoe.html.

6. *Chislo atak na resursy Minoborony RF za 6 let vozroslo pochti na 60%* [Number of Attacks on the Resources of the RF Defence Ministry in 6 Years has Increased by Almost 60%]. SecurityLab.ru, 2019, June, 27, available at: https://www.securitylab.ru/news/499655.php.

7. Sanger D., Perlroth N. *U.S. Escalates Online Attacks on Russia's Power Grid*. The New York Times, 2019, June, 15, available at: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

8. Ageev A.I., Loginov E.L., Raikov A.N. Informatsionnye sistemy upravleniya v chrezvychainykh situatsiyakh [Emergencies Information Management Systems]. *Ekonomicheskie strategii*, 2019, no 2, pp. 20–29.

9. Novak A. Energetika: vzglyad v budushchee [Energy Industry: Looking to the Future]. *Energeticheskaya politika*, 2019, no 2, pp. 6–11

10. Ageev A.I., Grabchak E.P., Loginov E.L. Smart-kollaps v tsifrovoi energetike budushchego: ugrozy global'nogo obrusheniya informatsionnykh sistem upravleniya v usloviyakh vozmozhnoi samoorganizovannoi informatsionnoi blokady [Smart Collapse in the Digital Energy Sector of the Future: Threats of the Global Collapse of Information Management Systems in the Context of a Possible Self-organized Information Blockade]. *Energetik*, 2020, no 6.

11. Ageev A.I., Bondarik V.N., Ivanova O.D., Kudryavtsev A.V., Loshchinin A.A. Tekhnokraticheskaya kontseptsiya proektov tsifrovoi ekonomiki: sinergiya integratsii sistem i dannykh [Technocratic Concept of Digital Economy Projects: Synergy of Systems and Data Integration]. *Mikroekonomika*, 2018, no 5, pp. 14–21.

12. Grabchak E.P., Grigor'ev V.V., Loginov E.L., Raikov A.N., Shkuta A.A. Upravlenie ekonomikoi Rossii v usloviyakh s predel'no bol'shoi komponentoi neopredelennosti razvitiya chrezvychainykh situatsii i kriticheskogo nedostatka informatsii [Russian Economy Management in Conditions with Extremely Large Component of Uncertainty in Emergency Situations Development and Critical Lack of Information]. *Problemy bezopasnosti i chrezvychainykh situatsii*, 2019, no 4, pp. 104–110.

18. Агеев А.И., Кузьмин О.В., Перминова Е.А. Информационная безопасность автоматизированных систем управления производственными и технологическими процессами управления объектов критической информационной инфраструктуры Российской Федерации: Учеб. пособие. М.: МНИИПУ, ИНЭС, 2021.

19. Грабчак Е.П., Логинов Е.Л. Цифровая энергетика: повышение надежности управления электро- и теплоэнергетическими системами на основе внедрения цифровых технологий. М.: МНИИПУ, ИНЭС, 2020. 222 с.

20. Агеев А.И., Логинов Е.Л., Райков А.Н. Интеллектуальные технологии организации финансового мониторинга и контроля при реализации госзакупок // Экономические стратегии. 2016. № 1. С. 16–27.

21. Грабчак Е.П., Логинов Е.Л. Актуализация элементов централизованного государственного управления в рыночной среде ТЭК России в условиях многофакторной нестабильности с расширенной компонентой неопределенности // Искусственные общества. 2020. № 2. С. 52–57.

22. Агеев А.И., Бочкарев О.И., Грабчак Е.П., Логинов Е.Л. Пакетный отраслевой заказ как эффективный инструмент управления импортозамещением, созданием новых технологий и модернизацией энергетики [Электронный ресурс] // Экономические стратеги. 2020. № 3. С. 6–17. URL: https://doi.org/10.33917/es-3.169.2020.6-17.

23. Федорович В.А., Муравник В.Б., Бочкарев О.И. США: военная экономика (организация и управление). М.: Международные отношения, 2013. 616 с.

24. Бочкарев О.И., Тюлин А.Е., Асанова Е.А. Жизненный цикл деятельности организаций ОПК: от фискальной экономики к мотивационной [Электронный ресурс] // Экономические стратегии. 2019. № 7. С. 6–25. URL: https://doi.org/10.33917/es-7.165.2019.6-25.

13. Grabchak E.P., Loginov E.L. *Tsifrovye tekhnologii avtomatizirovannogo dokumentooborota v ramkakh elektro- i teploenergeticheskikh sistem s elementami SMART GRID: Problemy sertifikatsii, upravleniya kachestvom i dokumentatsionnogo obespecheniya upravleniya: Sb. materialov Vseros. nauch.-prakt. konf.* [Digital Technologies of Automated Document Circulation in the Framework of Electric and Heat Power Systems with SMART GRID Elements: Problems of Certification, Quality Management and Documentation Support of Management: Materials of the All-Russian Scientific and Practical Conference]. Krasnoyarsk, SibGU im. M.F. Reshetneva, 2020, pp. 39–43.

14. Ageev A.I., Smirnova V.A. Adaptivnost' vysokotekhnologichnogo kompleksa k tsifrovym vyzovam [Adaptability of the High-Tech Complex to Digital Challenges]. *Ekonomicheskie strategii*, 2018, no 1, pp. 164–166.

15. Grabchak E.P., Loginov E.L. Analiz i prognozirovanie kriticheskikh situatsii v elektro- i teploenergetike Rossii na osnove vnedreniya innovatsionnykh informatsionnykh servisov [Analysis and Forecasting of Critical Situations in the Electric and Heat Power Industry of Russia Based on Introduction of Innovative Information Services]. *Innovatsionnaya deyatel'nost'*, 2019, no 4, pp. 24–28.

16. Grabchak E.P. *Tsifrovaya transformatsiya elektroenergetiki* [Digital Transformation of the Electricity Industry]. Moscow, Knorus, 2018, 340 p.

17. Grabchak E.P. Tsifrovizatsiya v elektroenergetike: k chemu dolzhna priiti otrasl'? [Digitalization in the Electricity Industry: What Should the Industry Come To?]. *Energeticheskaya politika*, 2019, no 1, pp. 16–21.

18. Ageev A.I., Kuz'min O.V., Perminova E.A. Informatsionnaya bezopasnost' avtomatizirovannykh sistem upravleniya proizvodstvennymi i tekhnologicheskimi protsessami upravleniya ob"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii: Ucheb. Posobie [Information Security of Automated Control Systems for Production and Technological Processes of Management of Critical Information Infrastructure Facilities of the Russian Federation: Textbook]. Moscow, MNIIPU, INES, 2021.

19. Grabchak E.P., Loginov E.L. *Tsifrovaya energetika: povyshenie nadezhnosti upravleniya elektro- i teploenergeticheskimi sistemami na osnove vnedreniya tsifrovykh tekhnologii* [Digital Power Industry: Improving Reliability of Electrical and Heat Power Systems Management Through Introducing Digital Technologies]. Moscow, MNIIPU, INES, 2020, 222 p.

20. Ageev A.I., Loginov E.L., Raikov A.N. Intellektual'nye tekhnologii organizatsii finansovogo monitoringa i kontrolya pri realizatsii goszakupok [Intelligent Technologies for Organizing Financial Monitoring and Control of the Public Procurement Implementation]. *Ekonomicheskie strategii*, 2016, no 1, pp. 16–27.

21. Grabchak E.P., Loginov E.L. Aktualizatsiya elementov tsentralizovannogo gosudarstvennogo upravleniya v rynochnoi srede TEK Rossii v usloviyakh mnogofaktornoi nestabil'nosti s rasshirennoi komponentoi neopredelennosti [Updating the Elements of Centralized Public Administration in the Market Environment of the Russian Fuel and Energy Complex in Conditions of Multifactor Instability with an Extended Uncertainty Component]. *Iskusstvennye obshchestva*, 2020, no 2, pp. 52–57.

22. Ageev A.I., Bochkarev O.I., Grabchak E.P., Loginov E.L. Paketnyi otraslevoi zakaz kak effektivnyi instrument upravleniya importozameshcheniem, sozdaniem novykh tekhnologii i modernizatsiei energetiki [Package Sectoral Order as an Effective Tool for Managing Import Substitution, Development of New Technologies and Energy Modernization]. *Ekonomicheskie strategi*, 2020, no 3, pp. 6–17, available at: https://doi.org/10.33917/es-3.169.2020.6-17.

23. Fedorovich V.A., Muravnik V.B., Bochkarev O.I. *SShA: voennaya ekonomika (organizatsiya i upravlenie)* [USA: War Economy (Organization and Management)]. Moscow, Mezhdunarodnye otnosheniya, 2013, 616 p.

24. Bochkarev O.I., Tyulin A.E., Asanova E.A. Zhiznennyi tsikl deyatel'nosti organizatsii OPK: ot fiskal'noi ekonomiki k motivatsionnoi [Life Cycle of the Military-Industrial Complex Organizations: the Shift from Fiscal to Motivational Economy]. *Ekonomicheskie strategii*, 2019, no 7, pp. 6–25, available at: https://doi.org/10.33917/es-7.165.2019.6-25.