Сведения об авторах

Терновсков Владимир Борисович, Финансовый университет при Правительстве РФ, ул. Кибальчича, 1, 8(929)9285292, vternik@mail.ru

Данилина Марина Викторовна, Финансовый университет при Правительстве РФ, ул. Кибальчича, 1, 8(910)4307831, marinadanilina@ya.ru

Литвинов Алексей Николаевич, доцент ФГБОУ ВО Финансовый университет при Правительстве РФ, lan2703@rambler.ru

Иванова Светлана Петровна, доцент ФГБОУ ВО Московский государственный психолого - педагогический университет, 76sivanova@msil.ru

Дибиров Мурат Шамильевич, Финансовый университет при Правительстве РФ, ул. Кибальчича, 1,89886309832, dibirov.murat@mail.ru

Урусов Тимур Тимборович, Финансовый университет при Правительстве РФ, ул. Кибальчича, 1,89299098885, t.urusov15@mail.ru

УДК 65 DOI: 10.36535/0869-4176-2020-05-10

ФОРМИРОВАНИЕ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ СЕТИ КАТАСТРОФОУСТОЙЧИВЫХ ДАТА-ЦЕНТРОВ: КОНЦЕНТРАЦИЯ ЗАЩИЩЕННЫХ СИСТЕМ УПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ, АДАПТИРОВАННЫХ ДЛЯ РАБОТЫ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ И В ОСОБЫЙ ПЕРИОД[1]

Кандидат эконом. наук *Е.П. Грабчак*
Департамент оперативного контроля и управления в электроэнергетике Минэнерго России

Кандидат физ.-мат. наук *В.В. Григорьев*
МГИМО (У) МИД России

Доктор эконом. наук *Е.Л. Логинов*
Международного научно-исследовательского института проблем управления (МНИИПУ)

[1] Статья подготовлена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 19-010-00956 А «Стратегия внедрения элементов цифровой экономики России для оптимизации взаимодействия агрегированных групп экономических агентов на основе развития логистики цифровых активов и интеллектуальной мобильности»).

А.К. Деркач
Национальный исследовательский Московский государственный строительный университет

Рассматриваются проблемы поддержания устойчивости энергоснабжения в условиях чрезвычайных ситуаций и в особый период. Пандемия COVID-19 актуализировала потребность в формировании системного механизма управления энергетикой, устойчивого как к биологическому коронавирусу, так и к коронавирусам информационным. Сформулированы направления развития информационных инструментов анализа, прогнозирования и управления энергетикой с учетом результатов противодействия коронавирусной пандемии. Предложено формирование сети межкорпоративных катастрофоустойчивых дата-центров, объединенных в сетецентрическую систему повышенной устойчивости управления энергетикой.

Ключевые слова: энергетика, чрезвычайные ситуации, COVID-19, надежность, безопасность, информационная система, дата-центр, управление.

FORMATION OF A GEOGRAPHICALLY DISTRIBUTED NETWORK OF DISASTER-TOLERANT DATA CENTERS: THE CONCENTRATION OF SECURE CONTROL SYSTEMS IN THE ENERGY SECTOR, ADAPTED TO WORK IN EMERGENCY SITUATIONS AND DURING A SPECIAL PERIOD

Ph.D. (Econ.) *E.P. Grabchak*
Department for Operational Control and Management in the Electric Power Industry of the Ministry of Energy of Russia

Ph.D. (Phys.-Mat.) *V.V. Grigoriev*
MGIMO (University) of the Ministry of Foreign Affairs of Russia

Dr. (Econ.) *E.L. Loginov*
Institute for Advanced Systems (IRIAS)

A.K. Derkach
National Research Moscow State University of Civil Engineering

The article is devoted to the problems of maintaining the stability of energy supply in emergency situations and in a special period. The COVID-19 pandemic has actualized the need for the formation of a systemic energy management mechanism that is resistant to both biological coronavirus and information coronaviruses. The directions of development of information tools for analysis, forecasting and energy management are formulated taking into account the results of counteracting the coronavirus pandemic. The formation of a network of inter-corporate disaster-resistant data centers, combined into a network-centric system of increased sustainability of energy management, is proposed.

Keywords: energy, emergency situations, COVID-19, reliability, security, information system, data center, management.

Введение

Развитие российского отраслевого технологического комплекса в энергетике происходит в условиях количественных и качественных изменений в технологиях и оборудовании, а так же в структуре генерирующих мощностей и сетей транспортировки элек-

троэнергии. При этом, наблюдаются разноуровневые эффекты влияния факторов естественного и инициированного характера, которые создают новые риски и угрозы устойчивости и безопасности энергоснабжения потребителей.

Ряд исследований в этой сфере в отношении энергосистемы страны не проводились более 40 лет. Например, моделирование поведения энергосистемы в условиях электромагнитных воздействий вследствие высотного ядерного взрыва последний раз было осуществлено в 70 годах прошлого века. В последние годы появились качественно новые технологии использования электромагнитного воздействия в военных, террористических и иных аналогичных целях [1]. Резкое увеличение количества интеллектуальных элементов управляющих устройств приводит к росту уязвимости систем управления в энергетике как от техногенного электромагнитного воздействия, так и от природных электромагнитных воздействий (солнечные бури и пр.) [2].

Наращивание числа потребителей электроэнергии и генерирующих объектов также усложняет поддержание устойчивости энергоснабжения в обычных условиях.

Еще более проблематично поддержание устойчивости энергоснабжения в условиях чрезвычайных ситуаций и в особый период.

Пандемия COVID-19 актуализировала потребность в формировании системного механизма управления энергетикой, устойчивого как к биологическому коронавирусу, так и к коронавирусам информационным.

Требуется формирование информационно-вычислительных инструментов мониторинга, сбора информации, анализа, моделирования и прогнозирования процессов энергоснабжения потребителей, включая критические воздействия природного, технического и специального характера в условиях чрезвычайных ситуаций и в особый период [3].

Развитие информационных инструментов анализа, прогнозирования и управления энергетикой с учетом результатов противодействия коронавирусной пандемии

Предварительные итоги противодействия коронавирусной пандемии позволяют сформулировать следующие предложения развития информационных инструментов анализа, прогнозирования и управления энергетикой:

- Разработка сценариев последствий возможных управляющих воздействий со стороны органов государственной власти на институциональную и конъюнктурную среду, электроэнергетические, теплоэнергетические, нефтегазовые и угольные компании, финансово-банковские структуры с целью поддержания устойчивости электроэнергетики России в условиях мировой пандемии и постпандемийного периода. Выработка мер по повышению эффективности управляющих воздействий со стороны органов государственной власти с целью поддержания устойчивости электроэнергетики России в условиях мировой пандемии и постпандемийного периода.

- Диагностика энергетической безопасности РФ в условиях мировой пандемии и постпандемийного периода в мире и в России. Выяснение влияния рисков внешних угроз энергетической безопасности страны вследствие пандемии коронавируса, введения карантина в мире и в России, в частности, на функционирование электроэнергетики в условиях нарушения кооперационных, экономических и социальных связей, а также на эффективность работы и развития отдельных секторов электроэнергетики (генерация электроэнергии и тепла, магистральная транспортировка, распределение электроэнергии, энергосбытовая деятельность, обеспечение топливно-энергетическими ресурсами объектов электро- и теплогенерации), в т.ч. выполнение инвестиционных программ.

- Построение карты рисков технического и экономического развития электроэнергетики России в условиях пандемии в мире в увязке с другими секторами ТЭК России и с

учетом наибольшего влияния их как в отдельности, так и в совокупности на устойчивость энергетической суперсистемы. Построение сценарного «дерева рисков».

- Выявление сфер электроэнергетики в отраслевом, территориальном и корпоративном аспектах, нуждающихся в первоочередной государственной поддержке в условиях пандемийного и постпандемийного этапа развития с определением сценарных макроэкономических и производственно-технологических эффектов от оказания различных мер господдержки.

- Систематизация опыта подержания работы энергетических систем в условиях пандемии с детализацией по основным технологическим профилям и техническим подсистемам. Определение необходимых мер для снижения негативного воздействия пандемий на работу отраслевого технологического комплекса в энергетике [применительно с возможным пандемиям с более тяжелыми последствиями в отношении заболеваемости и смертности, чем от COVID-19] с учетом его технологических, организационных и экономических взаимосвязей.

- разработка предложений по совершенствованию нормативно-правовой базы для создания возможностей для федеральных органов исполнительной власти по управлению энергетическими компаниями в условиях пандемий или иных аналогичных ситуаций в случае неэффективности управления ими со стороны органов корпоративного управления и собственниками. Детализация полномочий федеральных и региональных органов исполнительной власти в условиях невозможности или неэффективности работы органов корпоративного управления и собственников энергетических компаний.

- Формирование типового набора мер по противодействию пандемии на уровне головной компании корпоративной группы федерального уровня, региональной энергетической компании и их взаимодействие с ДЗО[2] и филиалами, в том числе, находящимися в территориально удаленных регионах России и на объектах за рубежом (в рамках ЕАЭС, в постсоветских государствах не входящих в ЕАЭС).

Формирование сети межкорпоративных катастрофоустойчивых дата-центров, объединенных в сетецентрическую систему повышенной устойчивости управления энергетикой

Нагромождение различных технических решений в сфере телекоммуникаций, информационной безопасности и т.п. «на земле» (в регионах) приводит к неоправданному дублированию, неэффективному расходованию средств, и, в конечном результате, к недостаточной защищенности систем управления и оборудования как отдельных энергокомпаний, так и большинства сегментов энергосистемы [4].

В этих условиях целесообразно создание в каждом 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 цели цифровизации и информационной безопасности (компании: генерация электроэнергии, ее распределение и сбыт, сервисные услуги, поставка топливно-энергетических ресурсов, генерация и распределение тепла и т.п.) сформировать дата-центр с качественно более высокими 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 (напри-

[2] ДЗО – дочерние и зависимые общества

мер, федеральных округов, или кластеров активных энергетических комплексов, или мегарегионов, или иных агломераций территориального или функционального уровней). Также создается возможность обеспечения максимальной надежности, в т.ч. защищенности, магистральных каналов связи, выгодности условий SLA (Service Level Agreement), пропускной способности 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 сохраняющей 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.

То есть, на базе единого межкорпоративного катастрофоустойчивого дата-центра в каждом субъекте Российской Федерации формируются более высокие возможности как по количеству, так и по качеству информационно-коммуникационных и вычислительных услуг, в т.ч. специализированных, которые каждая компания в отдельности себе не могла 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 т.п. сферах (Росатом, Роскосмос и пр.) 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 технологическими и бизнес-процессами при управлении оцифрованными кластерами энергетических объектов.

Укрупненные блоки сетецентрической системы повышенной устойчивости управления энергетикой

Укрупненные блоки сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть катастрофоустойчивых межкорпоративных дата-центров:

- 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 со структурами региональных и муниципальных властей и пр.;
- поэтапная полная цифровизация всех энергетических компаний и органов власти и управления с информационно-телекоммуникационным оборудованием, позволяющих обеспечить 100% 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 к распространению информации;

- создание таких центров и инфраструктуры в энергетике сегодняшних и будущих стран – членов ЕАЭС (Армении, Белоруссии, Казахстане, Киргизии и пр.), изучение возможности создания таких центров в других странах, граничащих и осуществляющих энергообмен с Россией (Таджикистан, Монголия и пр.);

- строительство в России предприятий по производству компьютерного и иного оборудования, позволяющих через 3-4 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 т.ч. защиту передачи и хранения информации от любых естественных и инициированных угроз), а также организовать качественное наращивание информационных сервисов на уровне наиболее развитых стран мира;

- 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[3] 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.

Заключение

Формирование сети межкорпоративных катастрофоустойчивых дата-центров, объединенных в сетецентрическую систему повышенной устойчивости управления энергетикой, должно как на сетецентрическое ядро опираться на полноценный «Национальный центр управления энергетикой» Минэнерго России, аналогичный «Национальному центру управления в кризисных ситуациях» МЧС России. Предлагается интегрировать такой центр с функционалами информационных систем управления других министерств и ведомств федерального и регионального уровней, ситуационно-аналитическими центрами и центрами управления сетями госкорпораций и энергетических компаний.

В последующем целесообразно расширение функционала центра на республики ЕАЭС и другие государства, в т.ч. подключение к системе, участия в бизнес-процессах и формирование подсистем сетецентрической системы повышенной устойчивости управления энергетикой в федеральных органах исполнительной власти (ФОИВ), в госкорпорациях и энергокомпаниях, в субъектах Российской Федерации.

Необходим запуск нового научно-технического цикла формирования конвергентной инфраструктуры интегрирующей энергетические и информационные технологии в рамках бесшовной цифровой среды как основы функционирования систем жизнеобеспечения в России и других государствах в обычных условиях, в условиях чрезвычайных ситуаций и в особый период. Требуется также формирование инфраструктурных основ

[3] TIA 942 - Telecommunications Industry Association - Telecommunications Infrastructure Standard for Data Centers

внедрения существенных элементов планового государственно-частного управления в рыночную среду энергетики, адаптированных к любым угрозам и рискам: от пандемии, до военных действий или масштабных природных катастроф.

Литература

1. 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. С.10-14.

2. Грабчак Е.П., Логинов Е.Л., Логинова В.Е. Управляемая кластеризация и самовосстановление работы информационных систем в электро- и теплоэнергетике в условиях каскадных аварийных ситуаций // Проблемы безопасности и чрезвычайных ситуаций. - 2020. № 1. С. 133-138.

3. 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 ситуации и критического недостатка информации // Проблемы безопасности и чрезвычайных ситуаций. - 2019. № 4. С. 104-110.

4. 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 (51). С. 24-28.

Сведения об авторах

***Грабчак Евгений Петрович*,** директор Департамента оперативного контроля и управления в электроэнергетике Минэнерго России, 107996, ГСП-6, г. Москва, ул. Щепкина, дом 42, 8(495) 631-90-43, E-mail: Grabchak.eugene@gmail.com

***Григорьев Владимир Викторович*,** доцент кафедры математики, эконометрики и информационных технологий факультета международных экономических отношений, МГИМО (У) МИД России, 119454, Москва, пр. Вернадского, 76, 8(985)997-07-44, E-mail: grigorievvv@mail.ru

Логинов Евгений Леонидович, профессор РАН, дважды лауреат премии Правительства РФ в области науки и техники, начальник службы Ситуационно-аналитического центра Минэнерго России, 107996, ГСП-6, г. Москва, ул. Щепкина, дом 42, 8(903) 100-78-24, E-mail: evgenloginov@gmail.com

Деркач Андрей Константинович, бакалавр Национального исследовательского Московского государственного строительного университета, 129337, г. Москва, Ярославское шоссе, д. 26, 8(903) 100-78-24, E-mail: derkachak@mail.ru