УДК 338.332

ПОВЫШЕНИЕ КАЧЕСТВА И НАДЕЖНОСТИ УПРАВЛЕНИЯ СЛОЖНЫМИ СИСТЕМАМИ КРИТИЧЕСКОЙ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В ЕЭС РОССИИ

Е. Л. ЛОГИНОВ,
доктор экономических наук,
вице-президент Национального института энергетической безопасности
E-mail: evgenloginov@gmail. com

А. Е. ЛОГИНОВ,
старший аналитик ОАО «Гловерс»
E-mail: aleksloginov@gmail. com

В статье рассматриваются проблемы повышения надежности управления сложными системами критической энергетической инфраструктуры в условиях формирования конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России. При этом используется база построения информационно-технического комплекса мониторинга электронных управляющих транзакций, что имеет большое значение для развития экономики страны и повышения ее энергетической безопасности.

***Ключевые слова**: управление, электроэнергетика, безопасность, инфраструктура, информационная система.*

В последний период в электроэнергетике мира и России идет активная работа по внедрению «интеллектуальных сетей» (smart grid). В США и Западной Европе уже реализуется ряд крупных и еще больше мелких проектов по переходу электроэнергетики и ЖКХ на «интеллектуальные сети». В последний период США озвучили ряд новых проектов в сфере глобальных информационно-мониторинговых сетей: Cisco Planetary Skin – система планетарного мониторинга (*букв*. – «кожа планеты»), Central Nervous System for the Earth (*букв*. – «центральная нервная система Земли») и др.

В этих условиях Президент РФ и Правительство РФ поставили министерствам, ведомствам и энергетическим корпорациям нашей страны задачу по разработке и реализации проектов по переходу электроэнергетики России на «интеллектуальные сети». Реализуется также ряд аналогичных проектов в других секторах, включая сегментивные проекты «Электронное Правительство», grid-системы, облачные вычисления.

При этом за рубежом предпринимаются активные усилия по получению возможностей для реализации технологических преимуществ с целью осуществления [со стороны государственных (в том числе военного и специального назначения) и корпоративных структур] различных стратегий несанкционированного манипулирования электронными системами управления объектами критической энергетической инфраструктуры России.

Недостаток информации о характере попытки перехвата управления объектами критической энергетической инфраструктуры России может привести к развитию ситуации с катастрофическими последствиями. В этих условиях актуальными становятся проблемы мониторинга электронных управляющих транзакций в ЕЭС России, учета фактора неопределенности при принятии решений, оптимального

распределения ресурсов, привлекаемых для повышения качества и надежности систем управления и оценки темпов использования этих ресурсов.

Формирование в России комплекса «интеллектуальных сетей» в различных секторах электроэнергетики и других секторах закономерно ведет к созданию нового системно-структурного образования, которое можно назвать конвергентной информационной платформой в Единой энергетической системе России (ЕЭС России). Хотя различные проявления конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы уже реально наблюдаются с середины первого десятилетия XXI в., ее комплексное научное исследование еще только начинается.

Преимуществом конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России, являются качественно более широкие возможности сбора, обработки, хранения, распределения информации, то есть способность адаптироваться к динамике информационного спроса и потребления и обеспечение электроэнергетики (с ее технологической составляющей) информацией при современном уровне удовлетворения запросов потребителей.

В то же время сложившаяся информационная инфраструктура в ЕЭС России с ее традиционной, оправданной современной практикой решения инфокоммуникационных проблем в сложных условиях информационного, технического и природно-климатического характера, ориентацией на крупные объекты и сети информационного назначения требует новых подходов с учетом задач повышения надежности управления электроэнергетическими объектами.

Такие подходы в нашей стране должны значительно отличаться от практикуемых в большинстве зарубежных информационных образований, ведь информационная система ЕЭС России требует качественно иного (более высокого) уровня интегрированности и должна развиваться на основе принципов функционирования больших систем со значительно более высоким уровнем сложности системных взаимосвязей и, соответственно, решаемых задач принципиального построения и функционирования.

Это требует перестройки не только присоединяемых локальных сетей, но и всех информационных сетей ЕЭС России (точнее, совокупности сложных систем критической энергетической инфраструктуры ЕЭС России) на принципах конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы. Решение задачи осложняет наличие слабых, в то же время протяженных информационно-управленческих связей, что ограничивает возможность сбора и анализа больших потоков информации. То есть в нашей стране требуется технико-организационное обеспечение качественно нового уровня интегрированности информационных систем совокупности объектов ЕЭС России, в том числе с учетом перспективных задач развития и использования конвергентной информационной платформы [4].

При развитии критической энергетической инфраструктуры нового поколения с сегментом конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России, необходимо обеспечить для них новые качества, в том числе:

- на базе конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России, создать новую информационно-технологическую основу повышения управляемости электроэнергетикой России;
- развивать интегрирующую роль активно-адаптивной сети, в том числе многофункциональной инфраструктуры объектов оперативно-диспетчерского и автоматического управления энергосистемами с гибкими управляемыми элементами активно-адаптивной сети, создающей новые возможности сбора, обработки, хранения, распределения информации;
- реализовывать системную установку в критической инфраструктуре интеллектуальных технических элементов, дающих эффект при развитии информационных систем страны в целом;
- применение новых информационно-технологических сегментов на базе концепции конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России;
- создание адаптивной нормативно-правовой базы для конвергентной информационной платформы в ЕЭС России и использования результатов мониторинга электронных управляющих транзакций;
- повышение эффективности использования данных на основе интеллектуального анализа данных и других аналитических технологий.

Схема базовых технологий и объектов интеллектуального управления энергетической деятельностью приведена на рис. 1.

Рис. 1. Базовые технологии и объекты интеллектуального управления энергетической деятельностью

В последние годы в крупных энергосистемах стран мира участились случаи крупномасштабных аварий. Какие из них носят «естественный», а какие – «намеренный» характер, часто определить затруднительно. Как пример можно привести следующие ситуации.

В июне 1998 г. в энергосистеме долины реки Теннеси на Среднем Западе США разразился энергетический кризис. Основным фактором возникновения кризиса стал феномен, получивший название «островизации» (islanding). Оказалось, что перегрузка всего нескольких компонент энергосистемы может привести к образованию своеобразных «барьеров», разделяющих энергосистему на отдельные «острова». При этом передача энергии из одного «острова» в другой становится попросту невозможной. В общей энергосистеме США и к западу, и к югу от образовавшегося «острова» электричества было в достатке. Однако передача энергии в пораженный кризисом регион была невозможна из-за перегрузки всего лишь двух элементов линии электропередачи Eau Claire Arpin на северо-западе штата Висконсин и трансформатора Kammer в юго-восточном Огайо [5].

Другой пример: 14 августа 2003 г. в США произошла авария с каскадным развитием, когда выход (дистанционное отключение неизвестными лицами) одного и более элементов энергосистемы привело к выходу из работы из-за перегрузок или повреждения других элементов, затем следующих и т. д. Всего массовыми отключениями электроэнергии были охвачены крупнейшие города в северо-восточной части США (в штатах Нью-Йорк, Огайо, Мичиган, Пенсильвания, Коннектикут, Нью Джерси) и Канады (Торонто, Оттава). Общая потеря нагрузки составила 61 800 МВт [1]. Таким образом, в результате этой аварии 50 млн потребителей не получали электроэнергию в среднем около 4 дней. Ущерб только в США составил около 10 млрд долл., а в Канаде – более 2 млрд канадских долл.

Приведем другой пример. В марте 2004 г. произошел катастрофический пожар, сопровождавшийся многочисленными мощными взрывами, на крупном нефтеперерабатывающем заводе компании British Petroleum Amoco в американском городе Техас-Сити, практически уничтоживший предприятие, вызвавший многочисленные человеческие жертвы и резкий рост биржевых цен на топливо. Одной из окончательных версий, выдвинутой ФБР в ходе расследования, стала возможность подтвержденного следственными экспериментами замаскированного дистанционного изменения параметров электроснабжения и технологических температурных режимов ректификационного оборудования по сети Интернет [7].

Одним из недавних и наиболее потенциально опасных из множества подобных подозрительных инцидентов стало внезапное одновременное нарушение работы сразу двух американских АЭС компании Entergy Corporation в ноябре 2010 г. Первоначально из-за отказа дистанционно управляемых систем охлаждения, утечек радиоактивных вод и неисправности насосов первого контура была на неделю остановлена АЭС «Vermont Yankee» в штате Вермонт. Менее чем через час после первого инцидента в Вермонте неожиданно и без видимых причин взорвался и сгорел один из мощных силовых трансформаторов на территории атомной станции «Indian Point», расположенной в штате Нью-Йорк, что вызвало аварийное отключение ее реакторов. Во всех отмеченных случаях регистрировались сбои компьютерных систем управления и несанкционированный удаленный доступ к программному обеспечению [6].

В этих условиях необходимость повышения эффективности механизмов и технологий управления системами критической энергетической инфраструктуры в условиях угроз деструктивных воздействий требует новых возможностей для регулирования и мониторинга информационных взаимодействий в рамках электроэнергетики с учетом возможных угроз перехвата управления в ЕЭС России.

Скоординированное деструктивное внешнее воздействие (особенно в условиях природных кризисных факторов – низких температур, наводнений, пожаров и пр.) приводит в ряде случае к почти 100 %-ной вероятности аварийного отключения различных участков ЕЭС России, что может вызвать многократное усиление нагрузки на другие участки, приводящее к каскадному отключению или же выходу из строя систем жизнеобеспечения целых районов. В результате этого было бы на долгий срок нарушено энерго-, газо- и теплообеспечение населенных пунктов с соответствующими социальными последствиями [3].

Исходя из вышеизложенного, требуется совершенствование направлений и методов управления сложными системами критической энергетической инфраструктуры ЕЭС России в условиях внешнего электронного деструктивного воздействия, в том числе мониторинга электронных управляющих транзакций для выявления операций по перехвату

управления, определения направлений практической реализации комплексного и системного подхода к решению задачи повышения надежности управления сложными системами критической энергетической инфраструктуры.

Соответственно, под организационной архитектурой конвергентной информационной платформы в ЕЭС России следует понимать цельную систему взаимозависимых структурных, управленческих, стратификационных, коммуникационных, временных и программно-технологических компонентов, которая придает информационным взаимодействиям внутри конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России, определенный характер, форму и направленность. Именно благодаря организационной архитектуре одни информационные взаимодействия внутри конвергентной информационной платформы в ЕЭС России становятся более вероятными, чем другие.

Модель взаимосвязи функциональных управленческих сервисов, опирающихся на функционирование систем критической инфраструктуры, подверженных электронному деструктивному воздействию, приведена на рис. 2.

Агенты информационных воздействий и их группы, осуществляющие попытки перехвата управления могут функционировать в самых разных организационных формах (глобальные телекоммуникационные компании, виртуальные группы, подразделения вооруженных сил других государств и др.).

Поскольку агенты информационных воздействий и их группы, осуществляющие попытки перехвата управления имеют, как правило, разно-

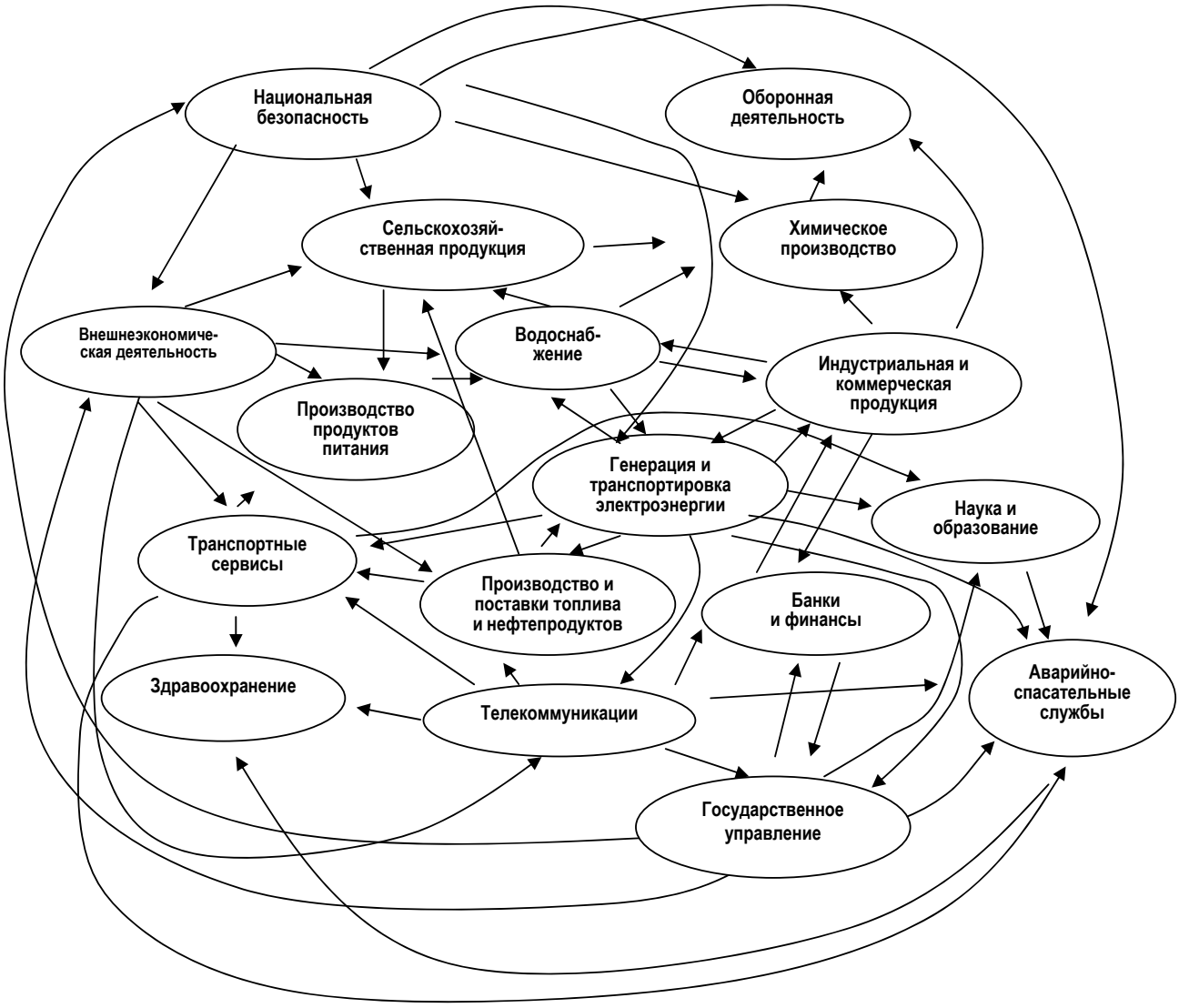


Рис. 2. Модель взаимосвязи функциональных управленческих сервисов, опирающихся на функционирование систем критической инфраструктуры, подверженных электронному деструктивному воздействию

образные интересы, коммьюнити, имеющие разветвленную структуру, они зачастую используют одновременно несколько организационных форм. Определение этих «индикативных зон опасных состояний» во всех сферах функционирования «интеллектуальных сетей» в аспекте оперативно-диспетчерского и автоматического управления энергосистемами и выбор достаточно эффективных мер противодействия попыткам перехвата управления составляют важную часть государственного регулирования в этой сфере развития ЕЭС России.

Ранее, в постсоветское время, такая задача не ставилась в связи с тяжелым финансовым положением предприятий электроэнергетики. Однако теперь, в условиях интенсивного развития, такая задача стала крайне актуальной. В связи с этим необходима модернизация управления энергосистемами, в том числе: 1) на уровне оперативно-диспетчерского управления (ОАО «СО ЕЭС»); 2) на уровне магистральных энергосетей (ОАО «ФСК ЕЭС»); 3) на уровне распределительных электросетей (ОАО «Холдинг МРСК»). Причем требуется усиление сквозного информационного обмена на основе интеграции информационных систем.

Необходимы мониторинг динамических свойств энергосистем, в том числе выявление управляющих транзакций, опасных для устойчивости энергосистем, а также оценка демпферных свойств энергосистем в режиме реального времени, формирование динамических моделей ЕЭС/ОЭС для обеспечения точности прогнозных расчетов динамической устойчивости и динамического поведения ЕЭС России при различных колебаниях (например аварийных возмущениях в ней).

Однако интенсивно развивающаяся в России информационно-сетевая и энерго-сетевая инфраструктура, а также методы и алгоритмы мониторинга состояния энергосистем в настоящее время пока не объединяют сквозным, комплексным образом все разноуровневые, территориально разнесенные электроэнергетические объекты и сети, входящие в ЕЭС России. При этом интенсивно развиваются новые технические решения в этой сфере [2].

Развитие RFID, позволяющее связать через глобальные сети информационных агентов и технические объекты (с радиометками) с уточненной пространственно-временной идентификацией на основе технологии ГЛОНАСС, становится одной из самых перспективных тенденций в развитии информационно-коммуникационных технологий, важным сегментом архитектуры конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России (рис. 3).

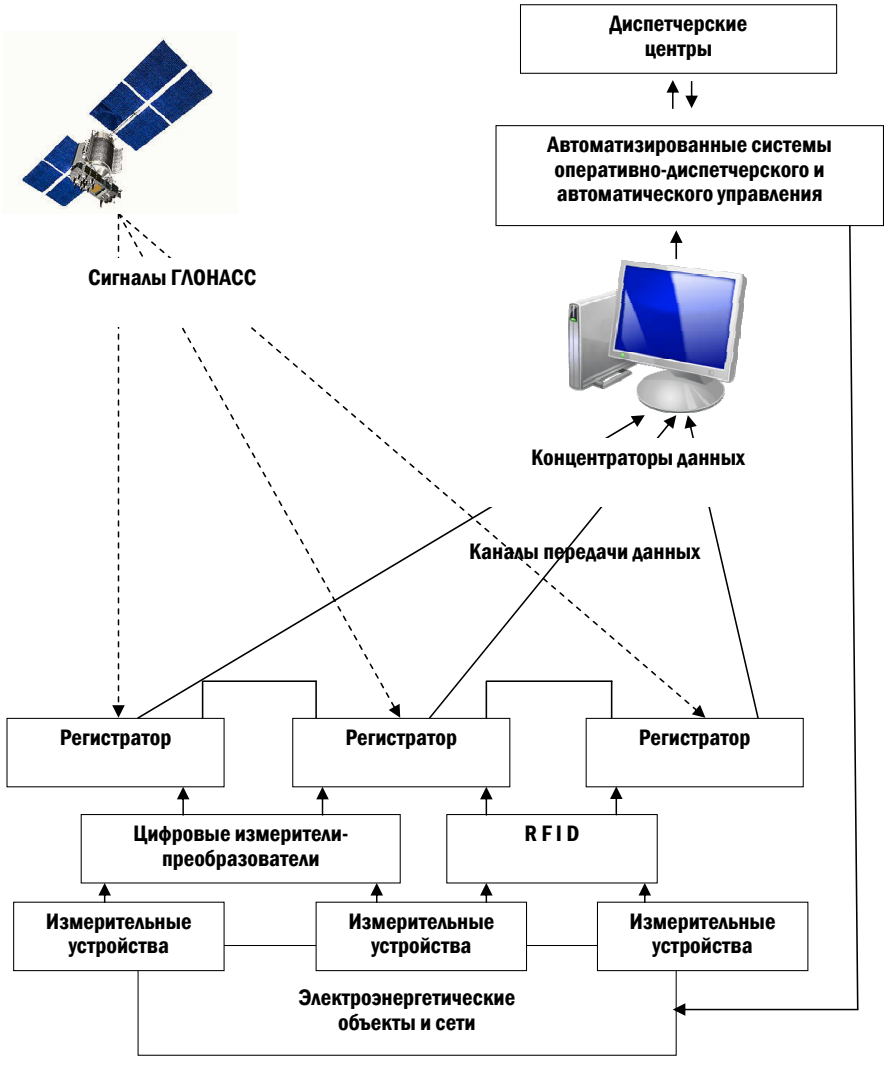
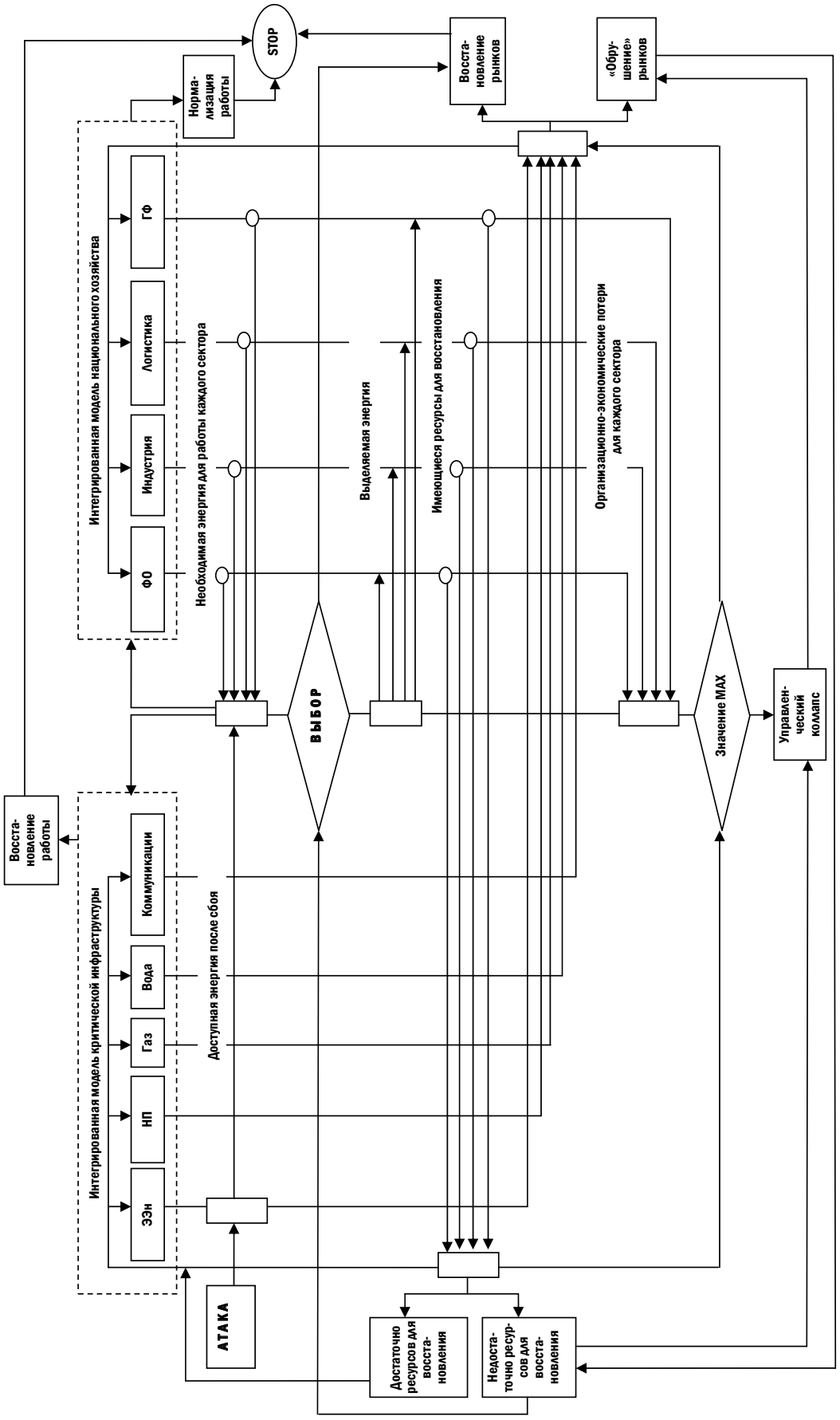


Рис. 3. Архитектура конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России



Примечание: ЭЭн – электроэнергия; НП – нефтепродукты; ФО – финансовые организации; ГФ – государственные функции.

Рис. 4. Модель функционирования критической инфраструктуры после атаки на системы управления ЕЭС России

В настоящий период участники информационных процессов, действующие в рамках конвергентной информационной платформы в ЕЭС России, взаимосвязаны через общие информационные и вычислительные сервисы. Развитие конвергентной информационной платформы в ЕЭС России (интеграция систем измерения, систем передачи данных и средств для их обработки) формирует информационную базу для внедрения в практику управления новых математических и электротехнических методов, ранее не применявшихся в силу низкого качества исходных данных.

Модель функционирования критической инфраструктуры после атаки на системы управления ЕЭС России приведена на рис. 4.

Эффективность функционирования энергосистем связана с состоянием информационных систем в распределенной структуре объектов Единой энергетической системы России. Нерешенные проблемы управления критической инфраструктурой, отсутствие обоснованной стратегии обновления и развития информационных систем в существенной мере определили необходимость внедрения новых информационных технологий.

Для решения первоочередных задач управления необходима интеграция данных по различным сферам перехода к новому формату управления на принципах интеллектуальной энергетики. Наличие указанной информации позволяет использовать оптимизационные методы и разрабатывать модели, на основе которых определяются меры воздействия, необходимые для конкретной ситуации.

Анализ опыта установления прозрачности электронных управляющих транзакций в зарубежных странах дает основание считать, что предложенная концепция построения информационно-технического комплекса мониторинга электронных управляющих транзакций для выявления попыток перехвата управления по интеллектуальным (активно-адаптивным) сетям соответствует ключевым направлениям совершенствования аналогичных информационных систем передовых стран мира. Необходимо принципиально изменить информационные технологии поддержки рабочих процессов административного мониторинга объектов оперативно-диспетчерского и автоматического управления энергосистемами в рамках конвергентной информационной платформы в ЕЭС России. От позадачного подхода следует перейти к комплексной технологии предоставления информационного сервиса поддержки рабочих процессов мониторинга электронных управляющих транзакций.

Список литературы

1. *Душин В. К.* Теоретические основы информационных процессов и систем. М.: Дашков и К., 2003.

2. *Иванов С. Н., Иванов Т. В., Логинов Е. Л., Наумов Э. Б.* Интеллектуальная электроэнергетика. М.: Изд-во «Спутник+», 2012.

3. *Логинов Е. Л.* Проблемы противодействия информационному терроризму // Национальные интересы: приоритеты и безопасность. 2008. № 4. С. 72–76.

4. *Логинов Е. Л.* Проблемы разработки и практической реализации автоматизированной информационной системы мониторинга электронных транзакций в глобальных телекоммуникационных сетях // Приборы и Системы: управление, контроль, диагностика. 2006. № 1. С. 32–34.

5. *Рахманов М.* Аварии энергосистем парализуют мир. URL: http://www. CNews. ru.

6. *Karp Z.* Federal Smart Grid Initiatives a Big Boost for IT // Matter Network, 2009.

7. Oil Hits New High After Refinery Blast // Reuters, 2004.