УДК 338.332

ПРОБЛЕМЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ 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 безопасности систем управления в Единой энергетической системе (ЕЭС) России в условиях возрастания угроз потери управляемости на основе новых системотехнических факторов с учетом процессов и тенденций формирования конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы.

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

Развитие информационно-технической среды мировой экономики сопровождается нарастанием угроз функционированию сложных информационных систем управления промышленной, энергетической, научной и т. п. инфраструктурой.

Подтверждением этому являются широко известные факты утечки информации: данных из ядерной лаборатории Los Alamos (2007 г.); базы данных NASA о новых проектах (ущерб более 720 тыс. долл., 2006 г.); секретных информации и разработок Lockheed Martin (ущерб более 1 млрд долл., 2006 г.); «Формулы-1» (утечка данных из «Феррари» в МакЛарен, 2008 г.) и т. п.

В 2011 г. продолжалось совершенствование технологий кибероружия: появились новые промышленные вирусы, ломающие производство на предприятиях без просматривающейся материальной выгоды для организатора атаки. Был отмечен ряд целевых атак, относящих к типу APT (Advanced Persistent Threat), когда злоумышленники разрабатывают специфическую технику, предназначенную для взлома ресурсов определенной организации [4].

В сентябре 2011 г. была зафиксирована волна кибератак на государственные учреждения стран СНГ. Нападение осуществлялось через загрузчик Lurid, являющийся модификацией трояна Enfal, который в прошлом использовался для внедрения на сайты правительства США. Специалисты Trend Micro насчитали более 300 управляемых целевых атак. Им удалось идентифицировать 47 жертв и 1 465 взломанных ПК, большая часть из них в России.

Осенью 2011 г. появилась информация о новом высокотехнологическом вирусе Duqu, который проникает в компьютер под управлением Windows, используя критическую уязвимость с идентификатором CVE-2011-3402. Затем вирус способен внедриться в смежную SCADA-систему предприятия в целях похищения информации об ИТ-инфраструктуре и установления контроля за промышленными объектами. Фрагменты кода Duqu имеют большое сходство с червем Stuxnet, который в 2010 г. вывел из строя несколько иранских заводов по обогащению урана. По мнению ряда специалистов, Duqu – это новейшая разработка в сфере кибероружия [2].

В основе такой тенденции лежит общее расширение угроз информационной безопасности.

Так, в 2011 г. «Лаборатория Касперского», собирающая статистику по своим антивирусам, насчитала за год 946 393 693 атак через браузер. Это в 1,6 раза больше, чем в 2010 г., когда было зафиксировано 580 371 937 атак (рис. 1).

Стремительное развитие компьютерных и телекоммуникационных сетей в сфере управления энергосистемами привело к появлению специфического вида потери управляемости на основе системотехнических факторов, пока не нашедшего своего комплексного отражения как в научных исследованиях, так и в практических разработках органов государственного управления и соответствующих федеральных служб.

В последние годы за рубежом активно развиваются научно-практические разработки в области повышения качества и надежности систем управления в различных областях предметной деятельности гражданского, военного и специального назначения. Наиболее важными документами в США в этой сфере являются «Национальная стратегия кибернетической безопасности» (The National Strategy to Secure Cyberspace) и «Национальная стратегия физической защиты критической инфраструктуры» (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets), в которых постулируется подход к обеспечению взаимодействия всех американских участников программ по защите критической инфраструктуры государства.

Новый (интеллектуально-сетевой) формат угроз процессам управления сложными системами критической инфраструктуры выходит за рамки традиционных концепций обеспечения информационной и энергетической безопасности. Традиционные модели угроз здесь неэффективны, поскольку средства и способы деструктивного воздействия могут оказаться принципиально новыми: как вследствие применения принципиально новых технологий функционирования интеллектуальной информационно-сетевой инфраструктуры (среды), где будет совершена атака на управляющие системы, так и методов действий агентов информационного воздействия, которые в ряде случаев могут находиться за пределами сферы их возможного обнаружения и идентификации [5].

Объектами деструктивных информационных воздействий на критическую энергетическую инфраструктуру являются:

- автоматизированные объекты управления ЕЭС России и входящие в ее состав системы управления технологическими процессами на нижнем уровне их реализации и их компоненты (серверы, в первую очередь серверы SCADA, автоматизированные рабочие места, микропроцессорные контроллеры, средства телемеханики);
- информационно-телекоммуникационные сети, поддерживающие управление технологическими и организационными процессами;
- объекты информатизации, поддерживающие процессы добычи (получения), переработки (преобразования) и транспортировки энергоресурсов (объекты, поддерживающие компрессорные системы, газоперекачку, электроснабжение и подобные им) [1].

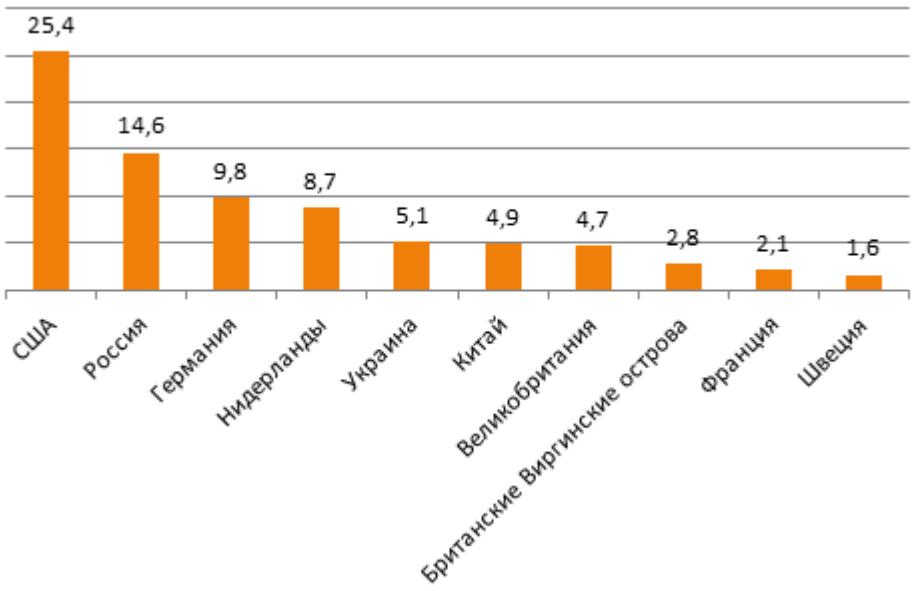

Рис. 1. Страны, на веб-ресурсах которых расположены опасные программы, % от общего числа вредоносных программ [4]

Возможность решения задач повышения безопасности систем управления в российской энергетике заключается в создании информационно-технического комплекса мониторинга электронных управляющих транзакций встроенного в системы автоматического регулирования и управления ЕЭС России для выявления электронных управляющих транзакций, опосредующих попытки перехвата управления по интеллектуальным (активно-адаптивным) сетям. Глобальной целью авто-

матизации в сфере мониторинга функционирования объектов управления энергосистемами в ЕЭС России является обеспечение комплексной информационной, методологической и программно-технологической поддержки процессов обеспечения возможности принятия решений руководством и специалистами государственных органов и энергетических компаний в рамках возложенных на них функций.

Формирование в нашей стране комплекса «интеллектуальных сетей» в различных секторах электроэнергетики закономерно ведет к созданию нового системно-структурного образования, которое можно назвать конвергентной информационной платформой в ЕЭС России. Появление конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России, привело к возникновению нового агента информационных воздействий. При этом под агентом информационных воздействий понимаются идентифицируемые и неидентифицируемые общности, виртуальные сетевые группы и отдельные индивиды, занятые информационной деятельностью или опосредующие иную (например управленческую) деятельность электронными информационными взаимодействиями.

Упомянутые нововведения затрагивают главным образом информационную надстройку ЕЭС России: сферу управления и информационную инфраструктуру. Изменения в процессах оборота энергоресурсов – вторичны и пока не столь радикальны. Наблюдается постоянный рост количества объектов, участвующих в схемно-режимных процессах, которые опираются на сетевые формы взаимодействия друг с другом. При этом совместная деятельность объектов управления энергосистемами в рамках конвергентной информационной платформы в ЕЭС России основана на использовании новых информационных технологий, в перспективе – это активно-адаптивные сети. Поэтому энергетика в большей степени, чем ранее, может регулироваться на основе прямых информационных взаимодействий между всеми составляющими конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России.

Итак, с учетом изложенных обстоятельств допустимо, на взгляд авторов, говорить о существовании конвергентной информационной платформы в ЕЭС России как устойчивой специфической совокупности агентов информационных воздействий и их взаимосвязей, участвующих в сетевых коммуникационных процессах, и возникающих между ними организационно-технических отношений. Иными словами, конвергентную информационную платформу в ЕЭС России образуют участники информационно-управленческих процессов (реализующихся через сетевую инфраструктуру) и отношения, возникающие между ними, причем специфика этих отношений в значительной степени определяется рассмотренными особенностями конвергентной информационной платформы, объединяющей телематические, вычислительные и информационные сервисы в ЕЭС России и одновременно являющейся своего рода единым телекоммуникационным пространством осуществления электронных управляющих транзакций.

Осмысление сущности конвергентной информационной платформы в ЕЭС России позволяет заключить, что необходимо рассматривать ее как некий феномен, в определенной степени оказывающий непосредственное влияние на структуру современных «интеллектуальных сетей» в аспекте управления энергосистемами. В качестве такового она обладает рядом специфических свойств, анализ которых позволит глубже понять методологические проблемы, возникающие при использовании интеллектуальных сетей в электроэнергетике как сложных систем критической энергетической инфраструктуры, выработать основные подходы к их решению.

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

Однако интенсивно развивающиеся в России информационно-сетевая и энергосетевая инфраструктуры, а также методы и алгоритмы мониторинга состояния энергосистем в настоящее время пока не объединяют сквозным управлением комплексным образом все разноуровневые, территориально разнесенные электроэнергетические объекты и сети, входящие в ЕЭС России. При этом интенсивно развиваются новые технические решения в этой сфере, что открывает новые возможности управления, но и создает новые угрозы.

На рис. 2 приведены возможности и тенденции развития технологий нанесения ущерба интеллектуальным сетям.

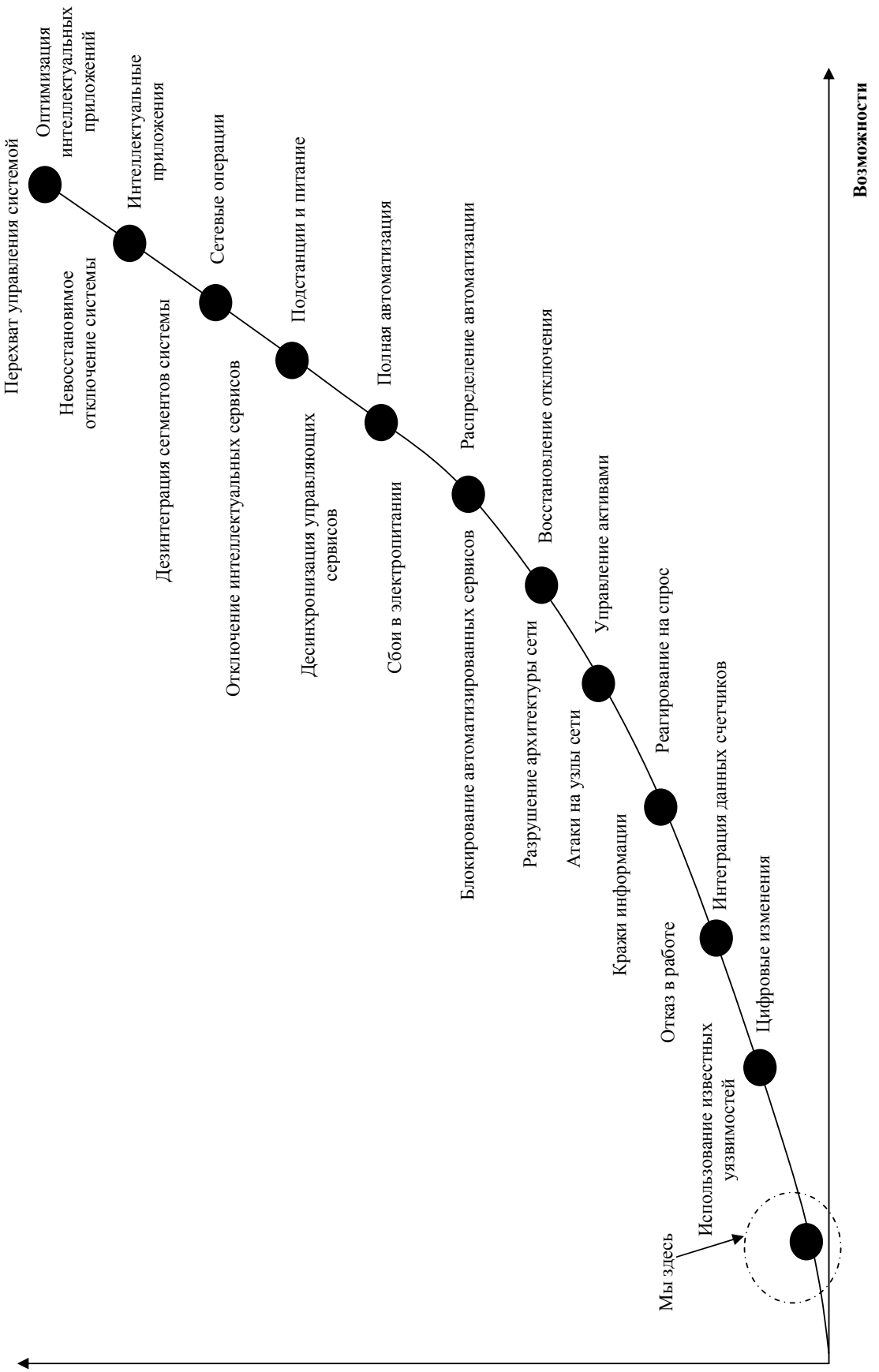

Рис. 2. Возможности и тенденции развития технологий нанесения ущерба интеллектуальным сетям

Применительно к конвергентной информационной платформе в ЕЭС России требуется разработка отечественного программного комплекса, позволяющего интегрировать данные, циркулирующие на различных уровнях в существующих системах (ОАО «СО ЕЭС», ОАО «ФСК России», ОАО «Холдинг МРСК» и пр.), и предоставляющего общие программные сервисы для сетецентрического взаимодействия «центр – периферия» с целью оперативного предоставления текущей информации в режиме реального времени [7].

На рис. 3 приведена объемная матрица характеристик нападений на объекты и системы управления критической инфраструктуры.

Обобщенная модель взаимосвязей при осуществлении информационных атак на линиях информационно-сетевой и энергосетевой инфраструктур приведена на рис. 4.

При этом, как видно из предлагаемой модели, в случае обоснованного сценария и эффективно реализованных диверсионных мер [для злоумышленников] возможно достижение системного управленческого коллапса значительных сегментов национального хозяйства.

С учетом изложенного можно сделать вывод, что в нашей стране необходимо сочетание мониторинга электронных управляющих транзакций на

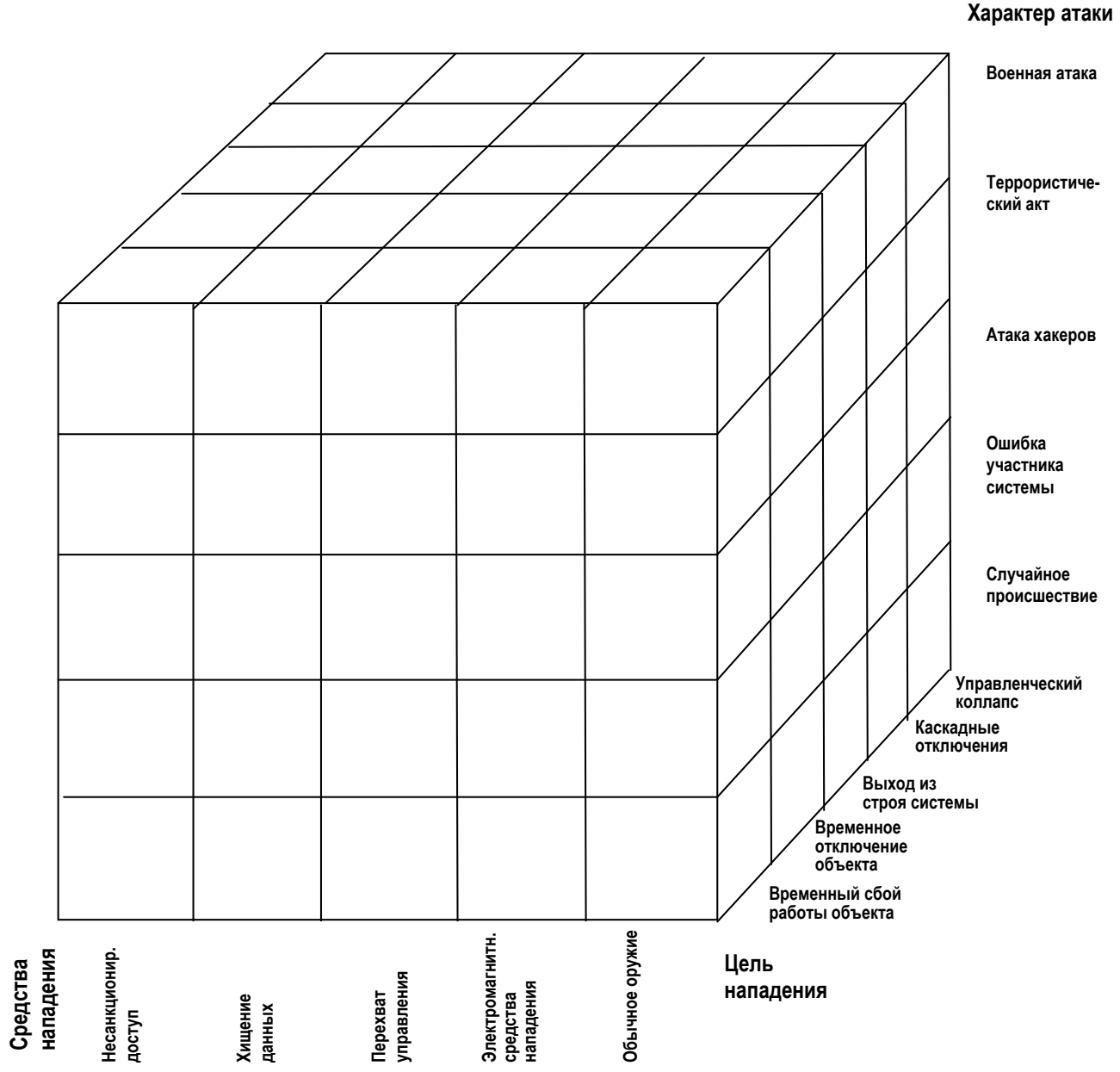

Рис. 3. Объемная матрица характеристик нападений на объекты и системы управления критической инфраструктуры

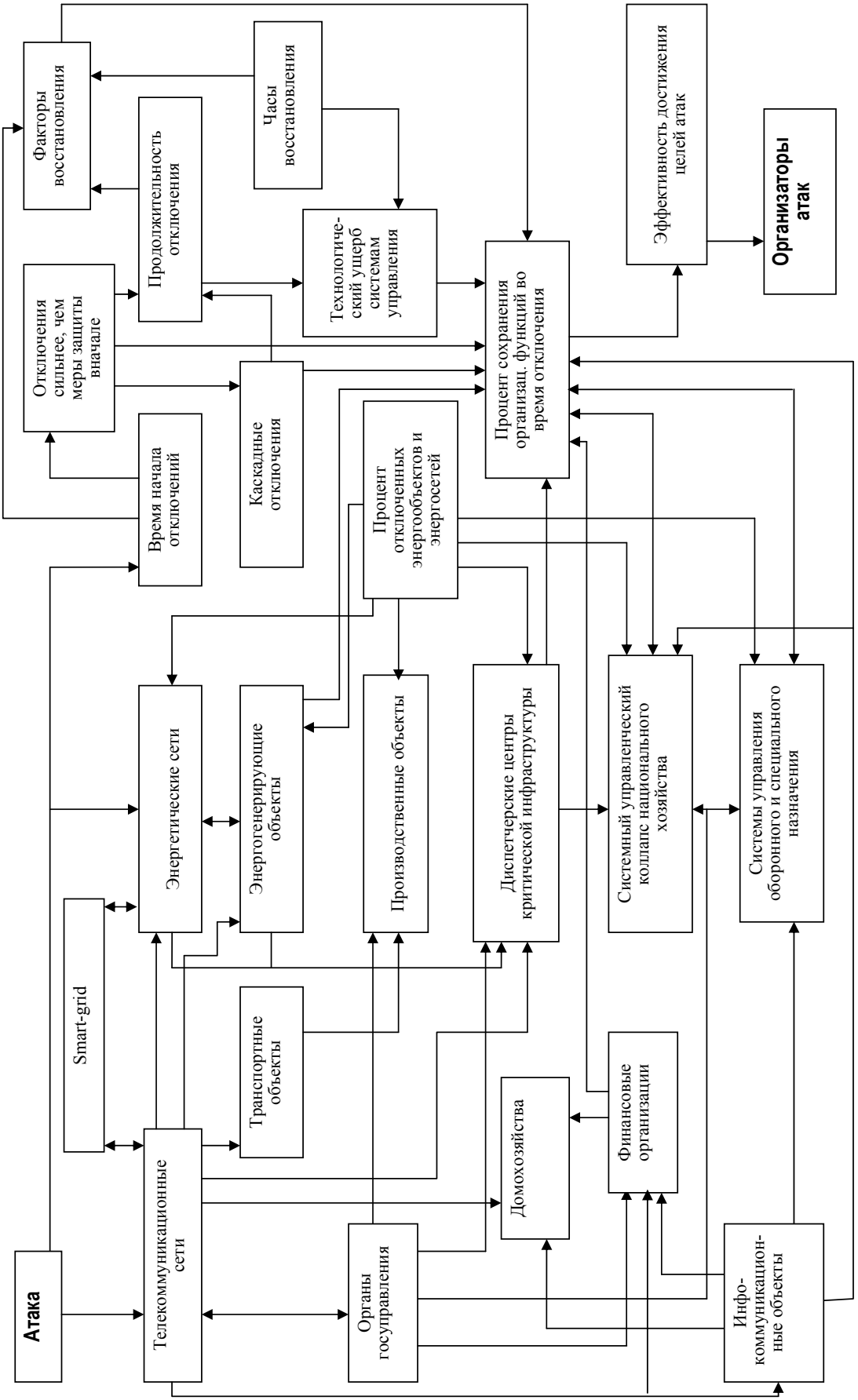

Рис. 4. Модель взаимосвязей при осуществлении информационных атак на линиях информационно-сетевой и энергосетевой инфраструктур

основе базовой системообразующей инфраструктуры, реализующей функции регистрации, передачи, сбора и обработки информации в центрах управления энергетических компаний с посегментным технологически системно согласованным внедрением элементов smart grid в рамках парадигмы Единой энергетической системы России. Это позволит избежать тех многочисленных организационно-технологических ошибок и неэффективных решений, которые были допущены в развитых и новых индустриальных странах мира при реализации непродуманной политики бессистемного внедрения распределенной генерации, превращения части потребителей в энергопоставщиков с их участием в управлении режимами энергосетей общего пользования на основе smart grid [6].

Интересным примером создания элементов такого мониторинга является проект по созданию прототипа комплексной системы защиты от терроризма на основе решения SAP Business Objects Event Insight, на базе которой будет строиться прототип системы защиты от террористов в ОАО «РусГидро». Этот программный комплекс относится к категории продуктов бизнес-аналитики, в основе которого лежит механизм обработки сложных событий (Complex Event Processing, CEP). Он позволяет обрабатывать огромные объемы данных о различных событиях в режиме реального времени и выявлять закономерности. Как платформа для разработки приложений CEP обеспечивает высокоуровневые средства, позволяющие задавать порядок обработки и анализа событий. Как механизм для реализации архитектуры, управляемой событиями (EDA), CEP формирует своего рода «интеллект», впитывающий, агрегирующий, коррелирующий и анализирующий события, производящий новые события высокого уровня, которые могут инициировать ответную реакцию, а также генерирующий высокоуровневую информацию о текущем состоянии бизнеса.

При разработке алгоритмов работы прототипа имеется возможность использовать различные методики построения систем комплексной безопасности, как, например, общеизвестную методологию CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability). Она позволяет оценить критичность объекта для работы всей системы, возможность доступа к объекту, время и усилия, требуемые для восстановления его работы, возможность его повреждения или уничтожения, масштабы возможных негативных последствии от незаконного вмешательства, вероятность того, что объект будет расценен как цель [3].

Таким образом, в связи с формированием в нашей стране комплекса «интеллектуальных сетей» в различных секторах электроэнергетики, ведущих к созданию нового системно-структурного образования, которое можно назвать конвергентной информационной платформой в ЕЭС России, существенно возрастают технические возможности осуществления операций по попыткам перехвата управления (гражданского, военного, специального, террористического и т. п. характера) по интеллектуальным (активно-адаптивным) сетям. Такая ситуация требует новых методов и алгоритмов снижения рисков надежности управления объектами критической энергетической инфраструктуры нашей страны, что пока не решено ни в теоретическом, ни в практическом плане.

Список литературы

1. *Васенин В. А.* Критическая энергетическая инфраструктура: кибертеррористическая угроза и средства противодействия // Информационные технологии. 2009. № 9. С. 34–35.

2. Крупнейшие инциденты 2011. URL: http://www. cnews. ru/reviews/free/2011/articles/articles10. shtml.

3. *Лаврентьева Н.* SAP защитит «Русгидро» от террористов. URL: http://corp. cnews. ru/news/top/index. shtml?2012/04/25/487094.

4. *Лебедев П.* Мировой рынок ИБ: эволюция угроз. URL: http://www. cnews. ru/reviews/free/2011/articles/articles7.shtml.

5. *Логинов Е. Л.* Новые информационные технологии для контрольной деятельности в сфере государственного и корпоративного управления // Информационное общество. 2011. № 6. С. 32–39.

6. *Логинов Е. Л.* Развитие «интеллектуальных сетей в электроэнергетике отраслей, регионов, городов России // Управление мегаполисом. 2011. № 5. С. 92–100.

7. *Логинов Е. Л., Мищенко В. А.* Методы анализа электронных транзакций в глобальных информационных сетях // Инженерная физика. 2006. № 4. С. 72–78.