УДК 338.332

ОРГАНИЗАЦИОННЫЕ ПОДХОДЫ К ПОВЫШЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ 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 модернизации информационной инфраструктуры российских энергетических компаний для обеспечения коллаборативных основ обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы отрасли. Делается вывод, что необходимо превращение энергетических компаний в институт коллективной информационной безопасности критической инфраструктуры России.

***Ключевые слова**: энергетические компании, информационная система, информационная безопасность, критическая инфраструктура.*

В мировой энергетике все более активно реализуются стратегические тренды интеллектуализации процессов и процедур управления критической инфраструктурой. Возникающие новые возможности информационной оптимизации управления одновременно порождают новые проблемы на всех уровнях управления, связанные с расширением спектра угроз и рисков нормальному функционированию систем критической инфраструктуры вследствие расширения возможностей дистанционного доступа к сетям и узлам информационных систем управления.

Наиболее значимой чрезвычайной ситуацией в этой сфере в мировой энергетике в последний период была кибератака на информационные системы национальной нефтяной компании Саудовской Аравии «Saudi Aramco» 15 августа 2012 г. В результате нападения было инфицировано 30 тыс. рабочих станций. Причиной заражения стал вирус Shamoon «из внешних источников».

В связи с такими тенденциями многие развитые и новые индустриальные страны реализуют активные комплексные стратегии защиты и нападения в информационных (кибернетических, электронных, виртуальных и т. п.) пространствах различного назначения.

Так, например, в 2012 г. Управление перспективных научно-исследовательских разработок Пентагона DARPA и ВВС США объявили два тендера, целью которых является приобретение наступательного кибероружия (специального программного обеспечения, предназначенного для проведения хакерских атак). Из первого тендера следует, что командование ВВС приступило к подготовке комплексной программы под названием CWOC (Cyberspace Warfare Operations Capabilities, Возможности ведения военных операций в киберпространстве). В условиях одного из тендеров DARPA и ВВС США выразили готовность потратить порядка 10 млн долл. на приобретение программ, которые позволят «уничтожать, ослаблять, нарушать, вводить в заблуждение, иска-

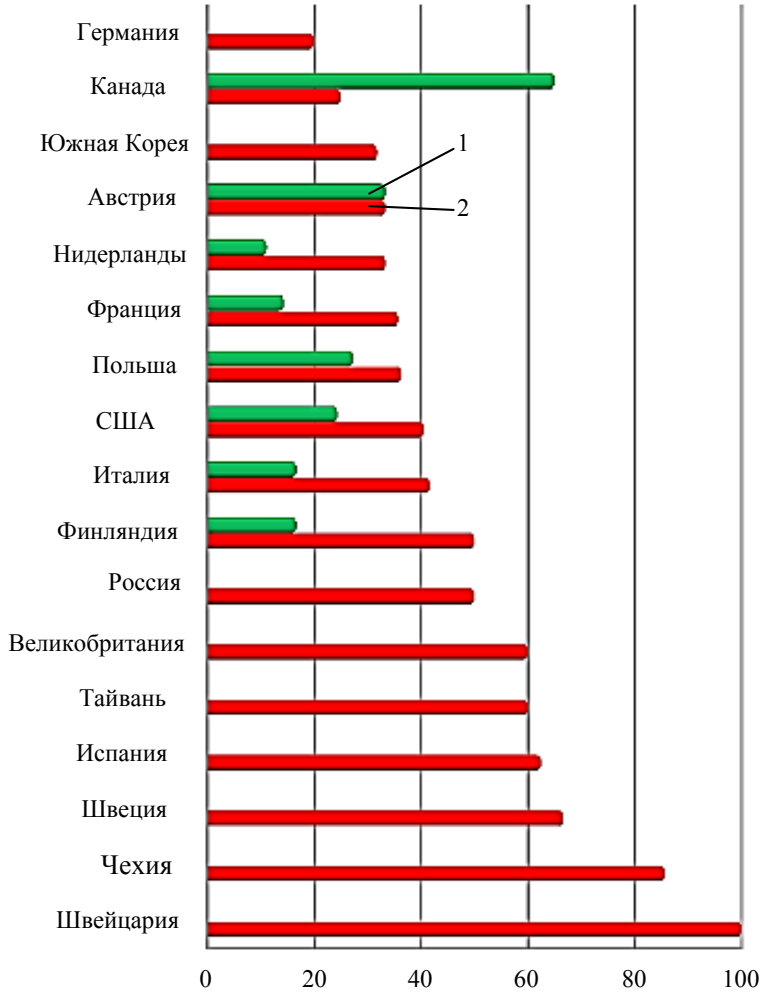

Рис. 1. Доля уязвимых компонентов АСУ ТП в разных странах [1], %:
1 – доля безопасных АСУ ТП; *2* – доля уязвимых АСУ ТП

жать и захватывать» компьютерные системы потенциального противника. Среди прочего американские военные намерены «выводить из строя, в том числе при помощи DDoS-атак, заражать и взламывать операционные системы, серверы и иные сетевые устройства противника», а также «устанавливать временный контроль над киберпространством». Второй тендер DARPA предполагает приобретение программы «Plan X» за 110 млн долл. Речь идет о масштабном исследовании кибервозможностей потенциальных противников, а также о создании интерактивной карты Digital battlefield map, которая будет отображать объекты военной инфраструктуры противника, степень их защищенности и т. п. [8].

В 2010–2015 гг. американское правительство планирует инвестировать примерно 7,2 млрд долл. во внедрение технологий для защиты национальной инфраструктуры. Данные инвестиции предполагается делать в рамках программы «Эйнштейн», которую реализует ряд федеральных ведомств США под эгидой Министерства национальной безопасности США. «Эйнштейн» – это недавно рассекреченная программа, связанная с обеспечением комплексной компьютерной безопасности, которая представляет собой набор мер, включая создание специализированных информационных систем («Эйнштейн-2», «Эйнштейн-3»), предназначенных для идентификации, анализа, защиты и активного реагирования на кибератаки.

Такая озабоченность американского руководства не случайна. Эксперты компании Positive Technologies провели исследование безопасности мировых и российских систем АСУ ТП (ICS/SCADA). Сегодня трудно найти область, где бы не использовались такие системы: это нефте- и газопроводы, атомные и гидроэлектростанции, сети распределения электроэнергии и водоснабжения. Было выявлено, что США и Европа лидируют по числу доступных из Интернета систем АСУ ТП[1], при этом 54 % доступных извне SCADA[2] систем в Старом Свете и 39 % в США – уязвимы и могут быть взломаны. На третьей позиции – Азия (32 %). В России уязвима ровно половина интернет-доступных систем АСУ ТП (рис. 1).

Корпорация Symantec опубликовала результаты исследования степени защищенности объектов критической инфраструктуры в России. Данные исследования показывают:

- 20 % объектов критической инфраструктуры РФ не реагируют должным образом на инциденты информационной безопасности;
- 26 % объектов критической инфраструктуры не применяют достаточных мер для контроля за доступом к инфраструктуре на основании учетных данных;

[1] АСУ ТП – автоматизированная система управления технологическим процессом – комплекс технических и программных средств, предназначенный для автоматизации управления технологическим оборудованием на промышленных предприятиях. URL: http://ru. wikipedia. org.

[2] SCADA (аббр. от англ. supervisory control and data acquisition, диспетчерское управление и сбор данных) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. URL: http://ru. wikipedia. org.

- 30% объектов критической инфраструктуры не имеют плана аварийного восстановления информационных систем либо он находится в низкой степени готовности;
- 30% объектов критической инфраструктуры не применяют достаточных мер для обеспечения безопасности веб-сайтов;
- 33% объектов критической инфраструктуры не осуществляют должным образом мониторинга информационной безопасности;
- 34% объектов критической инфраструктуры не применяют достаточных мер для защиты сети;
- исполнительное руководство 35% объектов критической инфраструктуры не осознает важности угроз информационной безопасности в достаточной мере;
- 37% объектов критической инфраструктуры не применяют достаточных мер для обеспечения безопасности электронных сообщений;
- на 39% объектов критической инфраструктуры не проводятся на достаточном уровне тренинги по безопасности;
- 45% объектов критической инфраструктуры не проводят на достаточном уровне аудита безопасности;
- более половины (51%) объектов критической инфраструктуры не применяют либо применяют недостаточные меры для защиты конечных точек (рабочих компьютеров пользователей, серверов, терминалов и т. п.), т. е. более половины предприятий не защищены [2].

Такая ситуация не могла не вызвать озабоченности российского руководства.

В январе 2013 г. Президент РФ В. В. Путин издал Указ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Задача по созданию соответствующей структуры возложена на ФСБ России. Основной целью информационной системы является установление причин инцидентов, касающихся работы информационных ресурсов РФ, в том числе информационных систем и информационно-телекоммуникационных сетей, находящихся на территории РФ и в дипломатических представительствах и консульских учреждениях России за рубежом [6].

Ранее, в середине 2012 г., Совет Безопасности РФ опубликовал «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». В документе указано, что Основные направления были разработаны в целях реализации основных положений Стратегии национальной безопасности Российской Федерации до 2020 г., которая предполагает и совершенствование ИТ-инфраструктуры критически важных объектов в целях защиты их от угроз.

К критически важным относят объекты, нарушение или прекращение функционирования которых может привести к потере управления инфраструктурой, ее разрушению и негативному изменению экономики страны или региона, где объект располагается. Целью разработки политики является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования ИТ-систем, а также минимизация негативных последствий такого вмешательства.

Среди задач госрегулирования в документе выделяется создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую инфраструктуру, создание и поддержание в постоянной готовности сил и средств ликвидации последствий компьютерных инцидентов в ней, создание хранилища эталонного программного обеспечения, использующегося в ИТ-системах критической инфраструктуры, создание условий, стимулирующих развитие в России производства телеком-оборудования, устойчивого к компьютерным атакам [7].

Аналогичные процессы по принятию первоочередных мер для защиты именно критической инфраструктуры интенсивно развиваются и за рубежом. Так, наиболее важными документами в США в этой сфере являются «Национальная стратегия кибернетической безопасности» (The National Strategy to Secure Cyberspace) и «Национальная стратегия физической информационной безопасности 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.

Министерство энергетики США (Department of Energy) в середине 2012 г. предложило энергетическим компаниям страны создать специальный

совет по киберзащите энергетической отрасли. В качестве нормативного акта подготовлен документ Electricity Subsector Cybersecurity Capability Maturity Model, Version 1.0, который был разработан в тесном сотрудничестве с представителями энергетического рынка США [10]. Среди прочего Министерство энергетики США предлагает наладить каналы обмена информацией о различных угрозах и инцидентах информационной безопасности, способных нанести существенный ущерб энергосистемам страны.

В таких условиях (эскалации внешних и внутренних информационных угроз) переход ЕЭС России к интеллектуальной энергетике требует тщательной проработки с целью обеспечения информационной безопасности. Информационная инфраструктура ЕЭС России требует серьезной трансформации. Ее главная цель состоит в превращении энергетических компаний в институт коллективной информационной безопасности критической инфраструктуры России (при сохранении базовых функций каждой отдельной компании) для многопрофильной организации информационной безопасности. Отличительной чертой качественно нового этапа модернизации информационной инфраструктуры российской энергетики является необходимость адаптировать ЕЭС России к новым, трансграничным угрозам, связанным с интеграцией энергосистем, а следовательно, и информационных систем разных стран. При интеграции энергосистем (а также энергорынков, энерго-сетевой и информационно-сетевой инфраструктур) происходит непрерывное расширение информационного функционала энергетической отрасли России.

В рамках такого подхода к модернизации информационной инфраструктуры энергетических компаний для обеспечения коллаборативных основ обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы отрасли в качестве трех ключевых задач ЕЭС России необходимо выделить следующие:

- обеспечение коллективной информационной безопасности критической инфраструктуры России;
- оптимизация корпоративной, отраслевой и территориальной информационной инфраструктуры энергетических компаний;
- построение кооперационной модели информационной безопасности на основе сотрудничества с организациями других отраслей в данной сфере деятельности и энергетическими компаниями – партнерами зарубежных стран (прежде всего участниками Таможенного союза).

По мере своего развития с учетом продолжения рыночных реформ ЕЭС России должна превратиться в «гибридный» многосторонний поликорпоративный альянс, решающий задачи как в сфере информационной безопасности критической инфраструктуры России, так и энергетической безопасности, являющийся своего рода интегратором общих отраслевых усилий и имеющий явно выраженные оборонный, специальный, правоохранительный и пр. компоненты национальной безопасности.

Вместе с тем отраслевые особенности функционирования именно единой энергетической системы страны как своего рода уникального единого распределенного технологического объекта (суперсистемы) определяют потребность абсолютного приоритета «коллективной безопасности» в сфере обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы отрасли и других отраслей и сфер деятельности в экономике России. При этом принцип коллективной информационной безопасности критической инфраструктуры России, корпоративно дезинтегрированной в ходе рыночных реформ, теперь (несмотря на корпоративное обособление) должен жестко форматироваться совместными обязательствами в сфере информационной безопасности для отражения информационной агрессии со стороны любых источников информационных атак и иных угроз. Увеличение перечня коллективных задач энергетических компаний (вне зависимости от формы собственности и состава собственников) в этой сфере и их увязывание с уточненными приоритетами, определенными Президентом России и Советом безопасности РФ, в сфере информационной безопасности являются императивом, который необходимо учитывать при дальнейшей структурно-корпоративной трансформации отрасли.

Ранее существовавшие и новые трансграничные угрозы информационной безопасности отрасли рассматриваются авторами как области для применения «коалиционной солидарности» и требуют увязки напрямую с инвестиционными программами с использованием мер государственного регулирования со стороны министерств и ведомств [5]. Вместе с тем важно то, что все эти информационные угрозы необходимо учитывать в процессе планирования деятельности и развития энергетических компаний.

В результате проводимой модернизации ЕЭС России должна достичь координационной эффективности во всех сферах взаимодействия с энергетическими компаниями сопредельных стран (информационной, технологической и др.), обеспечив информационную безопасность движения энергетических ресурсов по жизненно важным национальным и трансграничным коммуникациям. Более того, информационная безопасность энергетических компаний должна стать универсальным предметом повсеместного информационного и энергетического партнерства, способным оказывать целевое воздействие на отраслевую, национальную и международную среду энергетической безопасности. При этом с учетом ключевого значения ЕЭС России в евро-азиатской трансграничной энергетической инфраструктуре, объединяющей энергосистемы и энергорынки разных стран, российская информационная инфраструктура электроэнергетики должна стать узловым центром стратегической информационной безопасности энергоснабжения европейских и азиатских энергопотребителей, партнерство должно означать стратегическое воздействие на нее.

Концепция взаимодействия крупных российских энергетических компаний (ГК «Росатом», ОАО «Интер РАО ЕЭС», ОАО «ФСК ЕЭС» и пр.) как узловых центров информационной системы безопасности отрасли базируется на новом подходе с опорой на развитие кооперационных программ энергетических компаний. В настоящее время заметный рост активности по линии партнерств происходит в рамках общего укрепления информационной составляющей модернизации ЕЭС России. Можно также говорить о новой (в рамках Таможенного союза) легитимизации информационной компетенции энергетических компаний, которая до сих пор понималась достаточно узко – в рамках поддержания «корпоративной стабильности» – для наращивания возможностей по урегулированию кризисов информационной безопасности в перспективе создания квазиинтегрированной ЕЭС Таможенного союза.

Надо сказать, что в основу развития кооперационных программ энергетических компаний изначально был положен весьма прагматичный подход. Повышенное внимание к отраслевой политике именно сейчас мотивируется банальной нехваткой ресурсов для антикризисного регулирования и модернизационного стимулирования в отраслевом масштабе.

В свою очередь, привлекательность императивов информационной безопасности российской электроэнергетики для партнеров и инвесторов должна быть обусловлена не столько задачами обеспечения территориальной информационной безопасности критической инфраструктуры России, сколько ее новой ролью как организационного каркаса, обеспечивающего коллективную информационную безопасность энергетической деятельности на постсоветском пространстве и далее – при обороте энергоресурсов в энергосистемах Европы и Азии.

Данный подход определяет необходимость для российских энергетических компаний игнорирования границ между внутренней и внешней информационной безопасностью их энергетической деятельности, с учетом тенденций, формируемых международным законодательством.

В практической политике коллаборативный подход к обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы отрасли также предполагает горизонтальную кооперацию между различными энергетическим компаниями по принципу взаимодополняемости и частичного дублирования функций обеспечения информационной безопасности, что находит свое воплощение в развитии отраслевых отношений энергетических компаний на институциональном уровне.

Такой подход направлен на получение максимальной отдачи от действующих программ сотрудничества, а также от углубленной информационной кооперации на индивидуальной основе. Вместе с тем возможно появление новых структурных компонентов отраслевых отношений российских энергетических компаний, их структур за рубежом, зарубежных контрагентов (потребителей энергетических ресурсов) в сфере обеспечения информационной безопасности.

Необходимо также повышение эффективности механизмов государственного управления и контроля за счет интеграции в единый комплекс оргструктур и информационных систем различных государственных ведомств и компаний, что наиболее эффективно может быть формализовано как сетецентрическая информационная решетка деятельности государственных органов России (рис. 2).

Можно выделить следующие задачи в контексте развития энергетических компаний в рамках отраслевой политики обеспечения информационной безопасности: достижение большей эффективности

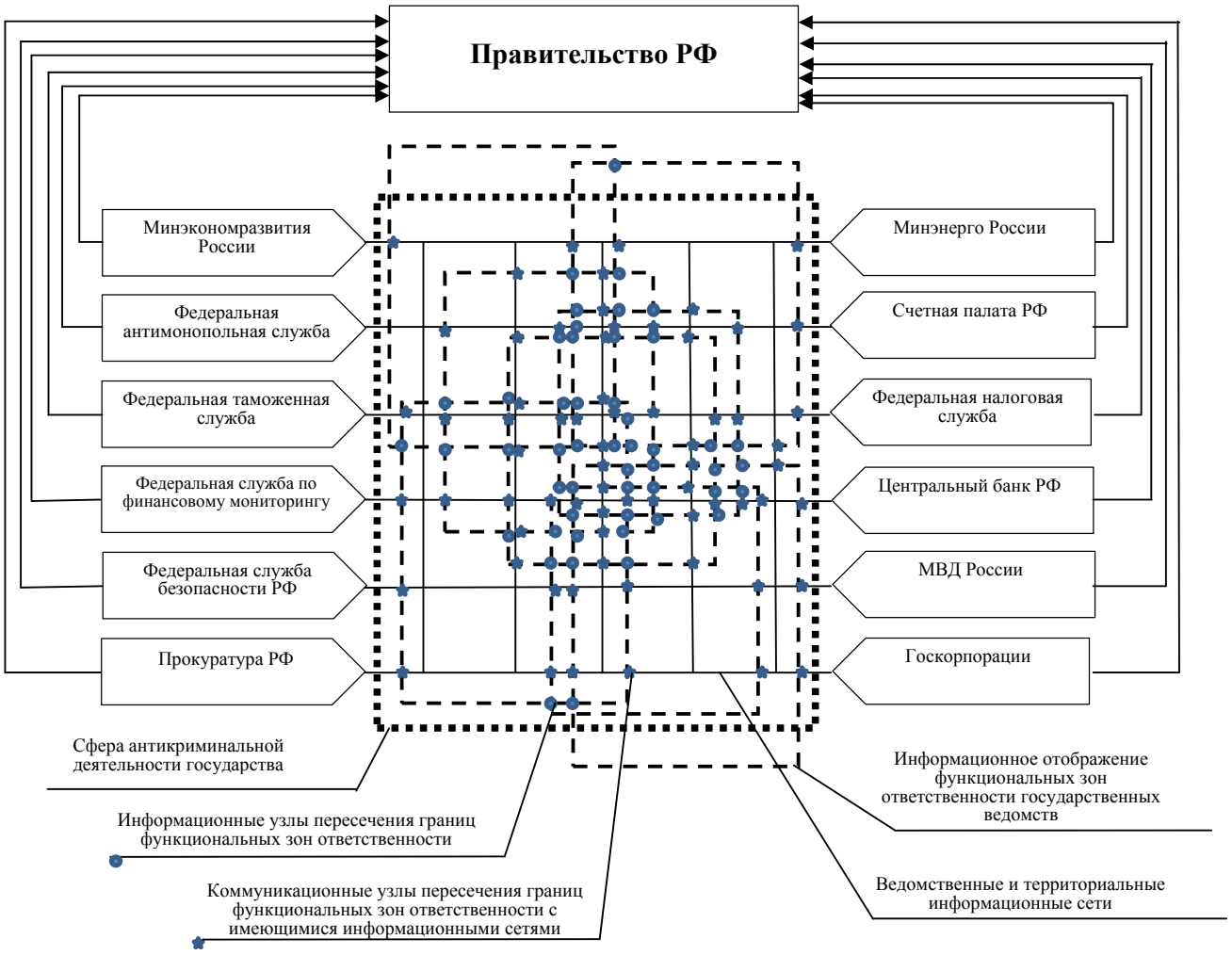

Рис. 2. Обобщенная схема сетецентрической информационной решетки деятельности государственных органов в экономике России [4]

стратегий обеспечения информационной безопасности энергетических компаний; расширение перечня задач, решаемых в рамках отраслевых программ обеспечения информационной безопасности; целевое воздействие непосредственно на внутреннюю политику отдельных энергетических компаний, в частности в области информационных аспектов модернизации ЕЭС России.

Этот «пакет» мер базируется на концепции «Интеллектуальной энергетической системы России», идея которой направлена на качественное совершенствование информационного потенциала энергетических компаний и органов госуправления в условиях ограниченных финансовых ресурсов на цели модернизации.

В целом решения находятся в русле последовательной реализации технологической платформы «Интеллектуальная энергетическая система России», в соответствии с которыми в арсенале ЕЭС России должны появиться качественно новые как информационные, так и энергетические возможности [3]. Необходимо формирование модели обеспечения информационной безопасности Таможенного союза при доминирующей роли России с упором на повышение в нем роли информационной инфраструктуры российской электроэнергетики при решении многих задач такого лидерства.

Интеграция различных технологий в области информационной безопасности стала ключевым трендом последних лет. Интересен подход, реализуемый американской компанией McAfee: при полном и комплексном взгляде на информационную безопасность все модули управления должны быть сконцентрированы в едином центре (McAfee ePolicy Orchestrator), необходимо поддерживать масштабы компаний от нескольких пользователей до несколь-

ких сотен тысяч и даже миллионов: как известно, самая крупная управляемая инфраструктура безопасности McAfee насчитывает 5 млн рабочих мест. Это решение носит название McAfee Security Connected и призвано совместить все имеющиеся средства безопасности в едином корпоративном периметре безопасности, уменьшить операционную нагрузку на штат служб информационных технологий и информационной безопасности, и в первую очередь снизить уровень риска безопасности до приемлемого. При этом подходе управление безопасностью на наладоннике или на продуктивном сервере базы данных процессинговой системы производится из единого центра, и разница между типами управляемых систем выражается только в специфике политик безопасности, которые офицер безопасности разрабатывает для тех или иных устройств, просто переключаясь между вкладками одного стандартизованного интерфейса. Например, последние разработки компании (решения для защиты баз данных в системе сбора и корреляции событий) были интегрированы в общую линейку продуктов с централизованным управлением через единую консоль управления McAfee ePolicy Orchestrator (ePO) [9].

В связи с расширением функциональной сферы ЕЭС России, охватывающей в настоящее время целый ряд как энергетических, так и информационных вызовов, можно говорить об использовании информационной инфраструктуры российской энергетики как инструмента противодействия различным системным угрозам России, в том числе в свете повышения информационной значимости российской электроэнергетики, для чего необходимо придать ей роль эффективного проводника интересов обеспечения информационной безопасности в максимально широкой сфере деятельности.

Список литературы

1. Безопасность промышленных систем в цифрах v. 2.1* / Positive Technologies. [Электронный ресурс]. URL: http://www. ptsecurity. ru/download/SCADA_analytics_russian. pdf.

2. Более половины российских объектов критической инфраструктуры не обеспечивают должных мер информационной безопасности / Symantec. [Электронный ресурс]. URL: http://www.symantec. com/ru/ru/about/news/release/article.jsp?prid=20110126_01.

3. *Логинов Е.Л., Логинов А.Е.* Проблемы повышения безопасности систем управления в ЕЭС России // Национальные интересы: приоритеты и безопасность. 2012. № 45. С. 31–37.

4. *Логинов Е.Л., Матвеев А.Г.* Повышение эффективности управленческой деятельности государственных органов в экономике России на основе сетецентрической информационной решетки антитеневой деятельности // Экономические науки. 2010. № 9. С. 32–38.

5. *Логинов Е.Л., Пинчук В.Н.* Императивы глобального управления: фазовый переход от «информатизации «хаоса» к «синергии конвергентного управленческого пространства» // Национальные интересы: приоритеты и безопасность. 2011. № 39. С. 25–31.

6. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента РФ от 15.01.2013 № 31с.

7. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» / Совет безопасности Российской Федерации. [Электронный ресурс]. URL: http://www.scrf. gov. ru/documents/6/113.html.

8. США объявили тендеры на закупку наступательного кибероружия. [Электронный ресурс]. URL: http://www. securitylab. ru/news/429357.php.

9. *Чернышев М.* Безопасная мобильность: научная фантастика или достижимая реальность? // CIO: руководитель информационной службы. 2012. № 12.

10. Electricity Subsector Cybersecurity Capability Maturity Model, Version 1.0. URL: http://energy. gov/sites/prod/files/Electricity Subsector Cyber security Capabilities Maturity Model (ES-C2M2). May 2012. pdf.