УДК 32.327.57

БЕЗОПАСНОСТЬ ЭНЕРГЕТИЧЕСКИХ СЕТЕЙ США: ПРОБЛЕМЫ БОРЬБЫ С КИБЕРНЕТИЧЕСКИМ ТЕРРОРИЗМОМ

© 2011 г. **А.В. Корнеев**[*]

Институт США и Канады РАН, Москва

Широкое распространение автоматизированных компьютерных систем управления энергетическими сетями и производственными процессами на предприятиях ТЭК в последние годы способствует возникновению опасных угроз кибернетических атак нового типа. Они могут осуществляться не только в форме несанкционированного доступа к закрытой информации, но и в виде технических возможностей для дистанционных диверсионных действий, в том числе скрытно организуемых с территорий других стран. Заметно участившиеся случаи возникновения опасных аварийных ситуаций свидетельствуют о том, что современные предприятия электроэнергетической инфраструктуры становятся всё более уязвимыми в отношении сетевых террористических внедрений и актов высокотехнологичного саботажа.

Ключевые слова: *США, энергетическая безопасность, активно-адаптивные энергетические сети, кибернетический терроризм, технологии дистанционного контроля, защитные системы и процедуры, российско-американское научно-техническое сотрудничество.*

Внедрение современных «интеллектуальных» сетей электропередач

Выступая в октябре 2010 г. в Белом доме на совещании руководства профильных государственных ведомств и энергетического бизнеса по вопросам капиталовложений в инфраструктурные проекты, президент США Б. Обама в своём программном заявлении отметил, что для выхода из кризиса стране остро необходима «умная инфраструктурная система», включающая энергетические составляющие и транспортные мощности общего назначения, которые бы полностью отвечали многосторонним и постоянно усложняющимся потребностям XXI века. При этом для восстановления лидирующих позиций в конкурентной борьбе за себестоимость и качество товарной продукции была поставлена задача в короткие сроки инвестировать в инфраструктурную модернизацию США в процентном отношении к ВВП значительно больше средств, чем в Западной Европе или Китае. По предварительным оценкам для решения этой задачи на первом этапе может потребоваться не менее 50 млрд. долл. с

[*] **КОРНЕЕВ Андрей Викторович – кандидат экономических наук, руководитель Центра проблем энергетической безопасности ИСКРАН.** E-mail: akorneev@online.ru

последующим ростом затрат в диапазоне от 134 до 194 млрд. долларов [20]. В основе перехода к интеллектуальным энергосетям (ИЭС) в США после окончательного завершения в конце 1990-х годов структурного перехода от вертикально интегрированных региональных монополий к интенсивной конкуренции независимых производителей и системных операторов лежат растущие требования рынка по формированию новой, более гибкой и оперативно управляемой полицентричной системы электропередач со встроенными динамичными и адаптивными обратными связями [25, p. 1].

Всесторонняя государственная поддержка интенсивного развития новых современных типов линий электропередач в США была обеспечена федеральным законом 2007 г. «Об энергетической независимости и безопасности» (*Energy Independence and Security Act of 2007*), в соответствии с которым предусмотрено ежегодное выделение не менее 100 млн. долл. на модернизацию и строительство электроэнергетической сетевой инфраструктуры. Ответственность за своевременный ввод в строй новых мощностей и соблюдение более строгих стандартов возложена на специальную Федеральную комиссию по модернизации электрических сетей (*Federal Grid Modernization Commission*).

Кроме того, к этой работе с самого начала был подключен Национальный институт технологических стандартов (*National Institute of Standards and Technology*) и Федеральная комиссия по энергетическому регулированию (*Federal Energy Regulatory Commission – FERC,* ФКЭР). Два года спустя уточнённый и скорректированный проект создания единой системы ИЭС в масштабах всей страны получил дальнейшую поддержку после того, как в 2009 г. был принят закон «О восстановлении и реинвестировании американской экономики» (*American Recovery and Reinvestment Act of 2009*), в соответствии с которым всего на эти цели было выделено около 11 млрд. долл. [26, p. 2].

В июле 2009 г. ФКЭР выработала окончательный вариант плана действий по внедрению и соблюдению единых новых стандартов для управляемых сетей активного типа. Учитывая интенсивный процесс внедрения новых технологий, комиссия установила общие принципы их целевого использования. Они включают преимущественную ориентацию на расширение эксплуатации возобновляемых энергетических источников, создание систем динамичных коммуникаций для непрерывного учёта изменений конечного спроса на электроэнергию, более экономичных промежуточных энергоаккумулирующих подсистем различного типа, а также энергосберегающих электрических транспортных средств личного и общественного пользования. При этом предполагается создать все необходимые технические условия для гарантированного бесперебойного снабжения транспортного сектора электроэнергией для зарядки аккумуляторных батарей в ночное время и в периоды повышенной пиковой нагрузки. С этой целью планируется обновить передающую инфраструктуру для резкого увеличения её пропускных и аккумулирующих характеристик. Полезность таких сетей определяется их более высокой эффективностью и выгодностью для производителей и потребителей электроэнергии.

В традиционных сетях электроэнергия передаётся в одном направлении – от небольшого числа крупных электростанций к потребителю. Однако по мере увеличения доли альтернативных источников электроэнергии стремительно растёт число дополнительных входных точек, через которые энергия поступа-

ет в сети. Современные линии электропередач на такой сложный режим эксплуатации изначально при проектировании рассчитаны не были. Поэтому развитие ИЭС станет чрезвычайно важным моментом с точки зрения возможности управления распределенной генерацией при подключении сотен и тысяч новых маломощных электростанций различных типов.

При наличии оптимизированных двусторонних активных управляющих коммуникаций в энергосетях, генерирующие и передаточные компании смогут сократить потери и более эффективно управлять потоками электроэнергии. Такие сети позволяют поощрять повышение энергетической эффективности генерирующих компаний и решать проблемы энергосбережения. Для реализации этих проектов государство должно поощрять инвестиции в технологии «интеллектуальной энергетики». Тем не менее, вместе с автоматизацией передающих сетей и внедрением новых коммуникационных технологий возрастает вероятность кибернетических атак на энергосети, что требует введения в действие специальных программ защитных мероприятий.

По закону «О восстановлении и реинвестировании американской экономики» было дополнительно выделено свыше 4 млрд. долл. на программу целевых субсидий и грантов для ИЭС. При этом на отдельные проекты прокладки новых и модернизацию старых линий выделялось от 500 тыс. до 20 млн. долл.; на разработку и монтаж систем непрерывного мониторинга режимов электропередач предусматривалось ассигнование до 5 млрд. долл. Условием выделения субсидий бизнесу по линии Министерства энергетики было обеспечение за счёт этих средств не более 50% общей стоимости соответствующих коммерческих проектов. Было принято также дополнительное решение о выделении 615 млн. долл. на создание полностью за счёт федеральных средств серии небольших региональных демонстрационных линий для ознакомления предпринимателей с практическими возможностями и преимуществами новых цифровых компьютеризированных систем дистанционного мониторинга и управления в реальном масштабе времени [32].

В мае 2009 г. в Вашингтоне по инициативе Министерства торговли США было проведено инструктивное совещание руководителей всех электроэнергетических компаний страны с ведущими представителями федеральной администрации для обсуждения и согласования новых отраслевых промышленных стандартов и сетевых технологий, на котором с основным докладом выступил министр энергетики США Стивен Чу. Ранее, в сентябре 2008 г., при Национальном научном фонде для предварительной проработки технических условий модернизации электроэнергетической инфраструктуры в тесном партнёрстве с корпорациями ИБМ и «Интел» был сформирован новый крупный федеральный исследовательский и инженерный Центр перспективных систем транспортировки и управления использованием возобновляемой электроэнергии, главной задачей которого стало обеспечение одновременной бесперебойной работы старых и новых передающих сетей на переходный период их реконструкции с использованием генерации на базе возобновляемых источников [16].

Именно ИЭС стали органичной частью глобальной программы корпорации «Интел» под названием «Открытая энергетическая инициатива», целью которой является успешная интеграция разнородных возобновляемых источников энергии, в том числе посредством управляемых «умных сетей» (*smart grids*), а

также развитие энергосберегающих моделей «умных зданий» (*smart buildings*) и энергетических потребителей с повышенными возможностями контроля и регулирования. Цель проекта заключается в демонстрации возможности объединения систем накопления энергии и распределённых генерирующих мощностей, а также создание всеобщей сенсорной сети, позволяющей дистанционно контролировать и оптимизировать производство и локальное потребление. В рамках данной программы под ИЭС понимается такая система передачи и распределения электрической энергии, которая сочетает в себе элементы традиционной энергетики и новейшие комплексные инструменты мониторинга, а также информационные технологии и средства связи, обеспечивающие более высокую производительность и позволяющие коммунальным и генерирующим компаниям более эффективно осуществлять прочие бизнес-процессы, с растущим приоритетом предоставления качественных услуг (см. схему 1).

Главные цели внедрения ИЭС заключаются в росте доступности, надежности, эффективности и безопасности энергетического обслуживания потребителей. Ожидается, что к 2030 г. такие сети должны обеспечивать 20%-ное снижение пиковых нагрузок, 100%-ную устойчивость работы сетей без массовых аварийных отключений, 40%-ное улучшение системной транспортной эффективности, а также полное использование дополнительных распределённых мощностей возобновляемых источников энергии. Особое место в концепции ИЭС уделяется перспективному использованию магистральных и локальных сверхпроводящих кабельных линий, позволяющих передавать значительные мощности с минимальными потерями. Необходимые меры по обеспечению энергетической безопасности при создании ИЭС представлены на схеме 2.

В середине 2009 г. Министерство энергетики выделило около 47 млн. долл. на восемь демонстрационных проектов ИЭС для ускорения их ввода в строй. При этом большинство из них одновременно включали как обычные электростанции, так и генерирующие мощности на базе возобновляемых источников энергии – преимущественно ветровых и геотермальных. Встроенные системы динамичной адаптации этих линий к изменениям объёма конечного спроса на электроэнергию обеспечили снижение средней пиковой нагрузки не менее чем на 15%. Были практически отработаны проекты быстро адаптирующихся к переменной нагрузке конечных распределительных локальных электросетей, специально рассчитанных на устойчивую работу при подключении на входе большого количества ветровых электростанций, отличающихся значительными нерегулярными перепадами эксплуатационной мощности генерации.

По долгосрочному плану реконструкции американской энергетики президента Б. Обамы, с 2010 г. началась реализация 100 новых коммерческих проектов модернизации линий электропередач, на которые совместными усилиями государства и бизнеса было выделено в общей сложности 8,1 млрд. долл. Все эти проекты составлены с учётом возможности последующего массового подключения к единой национальной электроэнергетической системе десятков тысяч ветровых, солнечных и геотермальных электростанций с неравномерными режимами работы [13].

Основой автоматических систем дистанционного контроля и регулирования режимов работы передающих сетей в США должны стать более 2,5 млн. контрольно-измерительных приборов для оперативного контроля объёма текуще-

Схема 1

Основные участники развития концепции «умных сетей» в США [2, с. 27]

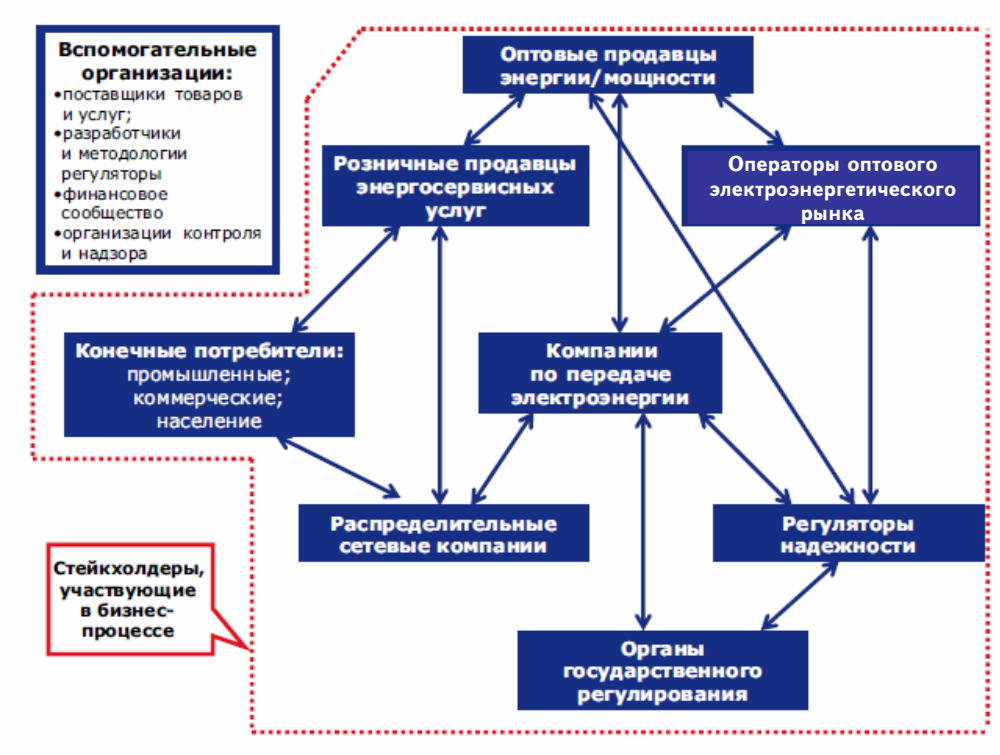

Схема 2

Направления государственного контроля для обеспечения энергетической безопасности при создании ИЭС

Составлено автором.

го энергопотребления, подключённых к программно-аппаратным комплексам дистанционного управления. Выделенные государственные субсидии и целевые гранты должны также обеспечить в ближайшие несколько лет установку таких дополнительных элементов систем автоматизированного управления, как 170 тыс. дистанционно-управляемых термостатов, 180 тыс. датчиков силы тока и напряжения, а также свыше 1 млн. автономных интегрированных системных вычислительных блоков, работающих в автоматическом режиме. Помимо монтажа контрольно-измерительных приборов предусматривается размещение 200 тыс. новых распределительных трансформаторов, 850 региональных пультов системного сетевого мониторинга, а также строительство свыше 700 новых автоматизированных силовых подстанций с дистанционным управлением. Их использование создаст реальные возможности для генерирующих компаний, промежуточных операторов передающих сетей и конечных потребителей непрерывно контролировать свою энергетическую эффективность и перейти к осознанному и последовательному энергосбережению. Кроме того, такая комплексная модернизация позволит резко снизить риск неоднократно происходивших в прошлом массовых аварийных отключений электроснабжения.

В качестве стартовой демонстрационной зоны был выбран город Майами, где объявлено о реализации регионального проекта по внедрению ИЭС стоимостью 200 млн. долл., цель которого – проверка концепции эталонной сети для остальных американских городов. Проект стал частью более крупной программы в масштабах всего штата Флорида, в которую планируется инвестировать около 700 млн. долл. В ходе её выполнения дистанционно управляемые датчики будут установлены более чем в 1 млн. домохозяйств и на большинстве городских предприятий. В течение последующих пяти лет планируется внедрить цифровые «интеллектуальные» счётчики дистанционного контроля с обратной связью в 4 млн. домохозяйств штата. Следующим этапом после внедрения локальных и региональных ИЭС может стать создание крупной национальной энергосистемы нового типа, которая должна объединить все существующие в стране передающие сети в единый автоматизированный и централизованно управляемый комплекс. Основу такой сети должны составить линии с повышенной пропускной способностью и напряжением тока свыше 800 киловольт.

Значительные потенциальные возможности ИЭС в условиях рыночной экономики связаны с тем, что электроэнергия как товар обладает специфическими особенностями, обусловленными её физическими свойствами, которые необходимо учитывать при организации оптовой и розничной реализации. Эти особенности включают:

– совпадение во времени процессов производства и потребления электроэнергии и равенство объёмов выработанной и потреблённой электроэнергии в каждый момент времени;

– трудности создания запасов электроэнергии в пределах энергосистем в достаточно большом объёме и невозможность заранее точно предвидеть объёмы генерации и потребления электроэнергии;

– сложность определения источника производства электроэнергии, использованную тем или иным потребителем в интегрированных передающих сетях.

На других отраслевых рынках товарной продукции кратковременный дисбаланс между производством и потреблением не приводит к потере устойчивости её обращения, поскольку может быть устранён за счёт складских запасов или товаров-заменителей. Рынок электроэнергии может нормально функционировать только при условии, что в каждый момент времени обеспечивается динамический баланс производства и потребления. При этом приходится создавать дорогостоящие резервы генерирующих мощностей, электрических сетей повышенной пропускной способности и избыточных дополнительных запасов топлива на электростанциях.

Величина повышенных резервов нормируется, а затраты на поддержание резервов включаются в стоимость электроэнергии. На практике производители и потребители периодически допускают отклонения от своих обязательств по генерации и потреблению электроэнергии. Необходимость оперативного балансирования энергосистемы в условиях переменной нагрузки требует наличия определённого числа маневренных электростанций, способных быстро и в широких пределах изменять мощность текущей генерации.

Наличие не только краткосрочных, но и сезонных колебаний сетевого баланса мощности в сочетании с тем обстоятельством, что располагаемая мощность электростанций должна превышать с гарантированным резервом величину расчётного максимума нагрузки, приводит к тому, что некоторый объём генерирующей мощности оказывается недогруженным. Непредвиденные колебания нагрузки приводят к тому, что традиционные механизмы управления режимом работы энергосистем всё чаще оказываются не в состоянии регулировать баланс нагрузки и отпуск электроэнергии потребителям в соответствии с договорами на поставку в режиме реального времени [5; 2].

В целом для развития экономики страны новая национальная энергосистема должна выполнить структурообразующую роль вполне аналогичную той, которую в прошлом сыграло строительство в США по инициативе президента Д. Эйзенхауэра системы федеральных автомобильных дорог. Ожидаемые дополнительные затраты при этом должны быть компенсированы за счёт временного повышения тарифов на электроэнергию и резкого роста энергосбережения.

Растущие угрозы безопасности энергетических сетей

В связи с общим ростом уровня террористической угрозы и увеличением числа попыток диверсионных действий в отношении различных энергетических объектов на территории России всё более актуальным становится совершенствование комплексных мер для повышения надежности их эксплуатации. За последние годы основное внимание в этой сфере уделялось разработке новой концепции безопасности предприятий генерирующей и распределительной инфраструктуры, изменению и ужесточению нормативных требований к их проектированию, строительству и эксплуатации; внедрению новых технических средств физической защиты, дистанционного мониторинга и контроля вскрытия технологической аппаратуры, маскировке охраняемых объектов, формированию и совершенствованию дополнительных ведомственных и част-

ных охранных структур; изменению законодательной базы и принятию новых правовых актов.

Например, в рамках внесённого в марте 2011 г. на рассмотрение ГД РФ президентского проекта нового федерального закона «О безопасности объектов топливно-энергетического комплекса», были более чётко определены современные принципы обеспечения безопасности энергетических предприятий, установлены дифференцированные требования к обеспечению безопасности с учётом степени угрозы совершения акта незаконного вмешательства и его возможных последствий, предусмотрены кодификация и охранная паспортизация объектов. Законопроектом регулируются порядок утверждения паспорта безопасности, вопросы обеспечения физической защиты, дополнительные права и обязанности хозяйственных субъектов ТЭК в области обеспечения безопасности.

Один из разделов законопроекта специально посвящен особенностям обеспечения безопасности объектов ТЭК, включая все виды линий электропередач и топливных трубопроводов [6, с. 2]. Активно разрабатываемая в последнее время новая российская доктрина энергетической безопасности также предусматривает необходимость постоянно совершенствовать способы защиты энергетических объектов от террористов в ходе их последовательной модернизации и перевода на инновационную модель развития. В апреле 2011 г. президент РФ Д.А. Медведев подписал дополнительный перечень поручений федеральным органам исполнительной власти, обеспечивающих усиление контроля эксплуатации и антитеррористической защищённости всех объектов топливно-энергетического комплекса [9].

Однако следует иметь в виду, что быстро набирающее темпы во всем мире интенсивное внедрение автоматизированных компьютерных систем дистанционного контроля и управления производственными процессами на предприятиях ТЭК способствует появлению дополнительных опасных угроз кибернетических атак нового типа не только в форме несанкционированного доступа к закрытой информации, но и в виде неизвестных ранее возможностей для осуществления на расстоянии разнообразных диверсионных действий, в том числе скрытно организуемых с территорий других государств.

Следует также учитывать, что в последние годы после создания первых образцов электромагнитного оружия (ЭМО) для выведения из строя электрического и электронного оборудования, а также снижения боеспособности живой силы противника, внимание авторов зарубежных военных разработок стали привлекать идеи создания комплексных систем электронно-цифровых наступательных вооружений.

При этом в странах НАТО и в Китае обычно рассматривают три основных сценария ведения возможных будущих «кибервойн». Первый и наиболее опасный представляет собой неожиданную атаку на автоматизированные информационные системы управления важнейшими государственными и коммерческими объектами: атомной промышленностью, железными дорогами, топливными трубопроводами, насосными станциями, нефте- и газохранилищами, линиями электропередач и аэропортами. Разрушения, к которым могут привести такие операции вполне сопоставимы по масштабу с последствиями реальных

бомбардировок. Второй сценарий предполагает атаку на ключевые Интернет-ресурсы, коммуникационное оборудование, веб-сайты и внутренние сети государственных органов. Взлом и блокировка этих систем неизбежно приведут к хаосу и параличу аппарата государственного управления. Третий сценарий предусматривает использование особых методов скрытного кибернетического воздействия на противника с помощью новых активно разрабатываемых программных и аппаратных средств для повышения эффективности традиционных военных действий [18].

По мнению многих зарубежных экспертов, активные государственные НИОКР в данной области и неизбежные случаи попадания подобных новых опасных технологий в руки террористических группировок могут уже в ближайшее время стать серьезной угрозой энергетической безопасности [24]. Как следует из документов, опубликованных в прошлом году в Германии, в предложенной генеральным секретарем НАТО А.Ф. Расмуссеном новой стратегической концепции альянса, которая была одобрена в ноябре 2010 г. на саммите в Лиссабоне, для реализации обязательств его участников в рамках коллективной обороны наряду с ядерным сдерживанием предусмотрены и активные действия в международных компьютерных сетях [10].

Заметно участившиеся случаи возникновения разнообразных труднообъяснимых аварийных ситуаций во многих странах свидетельствуют о том, что современные предприятия нефтегазовой и электроэнергетической инфраструктуры становятся все более уязвимыми в отношении сетевых террористических внедрений и актов высокотехнологичного саботажа.

Крупнейшее в истории США отключение энергии 2003 г., охватившее весь северо-восток страны, усугублённое массовым распространением компьютерного вируса *Blaster* и его многочисленных модификаций, наглядно продемонстрировало, что вся американская система электроснабжения весьма уязвима в отношении аварий, терроризма и актов высокотехнологичного саботажа [19].

Так, например, одной из версий, проверявшейся ФБР в ходе засекреченного расследования катастрофического пожара и многочисленных мощных взрывов в марте 2004 г. на крупном американском нефтеперерабатывающем заводе компании «Бритиш петролиум Амоко» в г. Техас-Сити, практически уничтоживших предприятие, вызвавших человеческие жертвы и резкий рост биржевых цен на нефть, стала возможность подтверждённого следственными экспериментами замаскированного дистанционного изменения технологических режимов ректификационного оборудования по Интернету [23].

Одним из недавних и наиболее потенциально опасным из множества подобных подозрительных инцидентов стало внезапное одновременное нарушение работы сразу двух американских АЭС компании «Энтерджи корпорейшн» 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 «Вермонт янки» в штате Вермонт. Менее чем через час после инцидента неожиданно и без видимых причин взорвался и сгорел один из мощных силовых трансформаторов на территории атомной станции «Индиан пойнт», расположенной в штате Нью-Йорк, что вызвало аварийное отключение её реакторов. Во всех отмеченных случаях реги-

стрировались сбои компьютерных систем управления и несанкционированный удалённый доступ к программному обеспечению [17].

Несмотря на дорогостоящие усиленную охрану и круглосуточный мониторинг в последнее время в американских энергосистемах всё чаще стали происходить неожиданные пожары и взрывы. Ситуация усугубляется тем, что общая протяжённость действующих в США высоковольтных линий электропередач составляет свыше 253 тыс. км [22, p. 3]. Так как основная часть данных систем была построена еще в 50-е и 60-е годы прошлого века, постоянно возрастающий физический износ и устаревшее оборудование диктуют необходимость интенсивных работ по их модернизации. При этом все более широко применяются автоматизированные компьютерные системы дистанционного контроля технологических данных и управления новых поколений. Их очевидными преимуществами являются обеспечение непрерывного мониторинга состояния сетевого интерфейса и линейного оборудования, а также постоянный контроль параметров текущего использования электроэнергии на уровне конечных потребителей для стимулирования энергосбережения. Вместе с тем при этом неизбежно возникают новые возможности для опасных террористических актов и сложные системные проблемы обеспечения технологической безопасности.

К настоящему времени в США уже выявлено несколько десятков новых опасных компьютерных вирусов модульного типа, специально предназначенных для внедрения в промышленные, энергетические и финансовые сети, либо для несанкционированного доступа к конфиденциальной информации, либо для дистанционного осуществления определённых вредоносных действий. Наиболее опасным из них был признан вирус (точнее – троянский вирусный червь) *Stuxnet*, которому 17 ноября 2010 г. в Вашингтоне было посвящено специальное экстренное заседание сенатского Комитета по внутренней безопасности и правительственной деятельности.

По этому случаю в Сенат был вызван директор Национального центра кибернетической безопасности и коммуникационной интеграции (*National Cybersecurity and Communications Integration Center*) Министерства внутренней безопасности США Шон Макгурк, признавший в своём докладе исключительно серьёзный характер возникшей угрозы безопасности страны, так как под ударом оказались практически все критически важные элементы национальной инфраструктуры [28]. Как выяснилось из доклада и опроса специалистов, с начала 2010 г. в США было зарегистрировано 12 опасных вирусных инцидентов, потребовавших полной остановки заражённых систем производственного управления и выезда на места аварий федеральных групп быстрого реагирования. В ходе последующего обсуждения, ведущие американские эксперты по проблемам безопасности отметили, что так как массовое внедрение ИЭС при наличии подобных новых вредоносных программ поставит под угрозу системного заражения десятки тысяч промышленных и военных объектов по всей стране, то его целесообразно временно отложить до тех пор, пока не будут разработаны адекватные надёжные комплексные защитные меры [29].

Материалы этого заседания, а также уже опубликованные в открытой печати данные показывают, что *Stuxnet* относится к практически не имеющему

аналогов в прошлом классу программного обеспечения, разработанного на государственном уровне для диверсионных кибернетических атак и предварительного обеспечения военных наступательных операций. Эта программа использует для несанкционированного и невидимого для пользователей внедрения различные и неизвестные ранее комплексные уязвимости в защите операционных систем (так называемые *zero-day-уязвимости* с открытой датой внешней активации), похищенные или скрытно полученные у известных изготовителей подлинные сертификаты для легализации несанкционированного встраивания своих кодов в рабочие программы и дополнительные механизмы с элементами «искусственного интеллекта» для самостоятельного многоэтапного распространения вредоносных файлов.

Первоначально заражение промышленных компьютеров с операционными системами *MS Windows* происходит путем переноса вируса с инфицированных флеш-карт, с которых вредоносный код переносится в программное обеспечение *Siemens SPS Step 7* для промышленных систем управления предприятиями. В 2010 г. было зафиксировано проникновение программы *Stuxnet* в сотни тысяч производственных компьютерных систем по всему миру. По экспертным оценкам, *Stuxnet* является одним из первых образцов высокоточного вирусного оружия избирательного действия.

В июле 2010 г. американская корпорация «Майкрософт» официально подтвердила, что данный код активно и беспрепятственно заражает все компьютеры, работающие под операционной системой *Windows* в составе крупномасштабных государственных и коммерческих систем управления *SCADA* (*Supervisory Control and Data Acquisition*, т.е. систем диспетчерского управления и сбора данных), включая электростанции, сети электропередач, нефте- и газопроводы, крупные военные объекты. При этом, по мнению некоторых специалистов, без ведома производителей оказались задействованы специальные секретные недокументированные закладки операционной системы, созданные ранее в целях государственной безопасности по стандартам Агентства национальной безопасности. В конце 2010 г. *Stuxnet* был протестирован израильскими специалистами на секретном ядерном объекте «Димона» в пустыне Негев и признан эффективным средством выведения из строя скоростных газовых центрифуг и перекачивающих насосов в Иране [30].

В январе 2011 г. постоянный представитель России при НАТО Д.О. Рогозин выступил с официальным предупреждением, что *Stuxnet* может привести к катастрофе, сравнимой по масштабам с Чернобыльской трагедией 1986 г. и потребовал независимого международного расследования вирусной атаки на Бушерский ядерный реактор в Иране, особо подчеркнув, что данный инцидент мог вызвать непредсказуемые последствия из-за пульсирующей раскрутки турбин и отключений электроснабжения [12]. К апрелю 2011 г. неактивизированный, но вполне работоспособный *Stuxnet* был обнаружен уже в более чем половине компьютерных систем немецких энергетических компаний, а также трубопроводных операторов коммунального и промышленного распределения природного газа и воды. Аналогичная степень данного вирусного заражения была подтверждена во Франции, Индии и других странах [1].

В конце апреля 2011 г. иранские власти заявили об обнаружении распространения еще более совершенного аналогичного полиморфного компьютерного вируса модульного типа, получившего условное обозначение *Stars*, мишенью которого должны были стать государственные исследовательские лаборатории и учреждения. Этот новый вирус маскировался под видом стандартных компьютерных файлов, которые используют правительственные организации и мог быть нацелен против новой секретной иранской программы по разработке экспериментального реактора для управляемого термоядерного синтеза [21].

Характерной особенностью этих новых вирусов являются относительно крупные размеры скрытно исполняемых кодов, способность выполнять свыше 40 тыс. специализированных команд, меняя их последовательность в зависимости от ситуации, а также сложная система внутреннего шифрования компонентов, не позволяющая сразу определить их структуру и конкретное целевое назначение. При этом особое внимание создатели вирусов уделили тому, чтобы обеспечить скрытность работы, маскировку всех этапов внедрения и распространения, а также тому, чтобы конечная целевая миссия вирусов была запущена на гарантированное выполнение только в случае чёткого подтверждения проникновения именно в ту конкретную управляющую систему, на которую они были изначально нацелены.

После длительной и сложной декомпозиции вируса выяснилось, что *Stuxnet* применяет для внедрения не одну, а сразу четыре прежде неизвестных специалистам по информационной безопасности *zero-day*-уязвимости, включая «уязвимость спулера печати», и две *EoP*-уязвимости, резко повышающие привилегии исполняемого кода. На его вооружении оказались также способность использовать уязвимость особого типа в защите от подсоединения к ПК посторонних *USB*-устройств, пригодную для заражения любых системных блоков, независимо от версии операционной системы. После попадания в корпоративную сеть *Stuxnet* самостоятельно повышал свои системные привилегии для того, чтобы получить беспрепятственный доступ на уровне администратора ко всем другим подключенным ПК, целенаправленно разыскивая системы, в которых работали промышленные программы управления *WinCC* и *PCS 7 SCADA*, как показано на схеме 3. Захватив эти системы вирус применял украденный или скрытно полученный его разработчиками внутренний пароль корпорации «Сименс» для полного перехвата управления программным обеспечением производственного контроля. В качестве следующего шага вирус самостоятельно перепрограммировал блок *PLC* (*Programmable Logic Controller* – программируемый логический контроллер) для того, чтобы диктовать всем управляемым системой *SCADA* механизмам новые команды и инструкции. Следует особо подчеркнуть, что вредоносный код атакующего вируса для каждой заражённой операционной системы выглядел полностью легитимными, так как впервые в известной практике несанкционированного доступа был снабжен двумя подлинными цифровыми сертификатами компаний «Риалтек семикондактор» и «Джей-микрон технолоджи», беспрепятственно проходившими все проверки защитных подсистем поражаемых компьютеров.

Для минимизации риска обнаружения вируса в каждом периферийном *USB*-устройстве, с которого поступал *Stuxnet*, работал программный само-

уничтожаемый счётчик, не позволявший инфицировать более трёх компьютеров первичной контактной зоны для ограничения масштабов распространения вируса только ближайшим объектом атаки. Функционирование червя *Stuxnet* рассчитано на полностью автономную работу программы и не требует ни подключений к Интернету для дополнительных инструкций, ни дополнительного управления со стороны человека. Тем не менее, также возможен запуск его диверсионных действий и по обнаружению косвенной ручной команды или специального триггерного события в заражённой системе. Отдельные внутренние элементы данного вредоносного программного обеспечения написаны на множестве различных алгоритмических языков. Это *C*, *C++* и другие объектно-ориентированные языки высокого уровня, а также специальные коды *STL* (*Standard Template Library*) низкого уровня типа ассемблера, преимущественно используемые в системах управления промышленными процессами. Вирус дополнительно оснащён впервые используемым на практике «руткитом» контроля *PLC*, скрывающим вредоносный *STL*-код (*rootkit* – специальный модуль программного ядра OS Win 32, который взломщик устанавливает на взломанной компьютерной системе сразу после получения прав суперпользователя; он включает в себя разнообразные инструменты для «заметания следов» после вторжения в систему – снифферы, сканеры, кейлоггеры, специальные троянские подпрограммы). Особенностью универсального «руткита» вируса *Stuxnet* является возможность дополнительно замещать и основные неядерные утилиты операционной системы *UNIX*. Это позволяет ему надёжно закрепиться в любом взломанном компьютере и сделать полностью невидимыми для пользователей следы своей вредоносной деятельности путём сокрытия файлов и процессов, а также замаскировать сам факт присутствия данного «руткита» в системе. *Stuxnet* также способен неоднократно внешне модифицировать сам себя без потери функциональности, что затрудняет его выявление стандартными антивирусными программами.

Так как промышленные компьютерные системы *SCADA* отличаются очень высоким уровнем специализации, разработчики *Stuxnet* обязательно должны были иметь в своём распоряжении для тестирования именно то реально применяемое аппаратное обеспечение, против которого нацеливалось их кибернетическое оружие, то для этого надо в деталях знать все нюансы работы техники на объекте, который был избран целью атаки. По данным специалистов по безопасности компьютерных промышленных систем корпорации «Сименс», вирус *Stuxnet* был несомненно нацелен против программного обеспечения именно этой компании, доминирующей в настоящее время на рынке *SCADA*-систем.

В процессе своего распространения *Stuxnet* занят непрерывными поисками специфических установочных параметров целевой системы, работающей под управлением *PLC*. Следует иметь в виду, что промышленные *SCADA*-системы весьма специфичны для каждого конкретного предприятия. Обычно они состоят из множества небольших узлов и датчиков с дистанционным управлением, измеряющих температуру, давление, объёмы и скорость потоков жидкостей и газов. Системные рабочие узлы, получающие такие данные, управляют моторами, вентилями и прочими механизированными приводами, необходимыми для поддержания нормативных условий промышленных процессов в рамках

Схема 3

Внедрение вируса Win32/Stuxnet в закрытые сегменты управления промышленными и инфраструктурными объектами

Составлено по данным: Broad W.J., Markoff J., Sanger D.E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. 15.01.2011.

безопасности и в пределах эффективности. Поэтому оба типа компонентов управляющих систем – аппаратные модули и программное обеспечение, всегда являются специфическим набором, индивидуально изготовляемым под заказ для каждого конкретного производства. Вирусный червь *Stuxnet* начинает действовать на уничтожение объекта только в том случае, когда им идентифицирована заложенная в него при запуске надлежащая конфигурация достигнутой цели. Для предварительного изучения цели вирус должен иметь поддержку инсайдера или группы инсайдеров внутри атакуемого предприятия.

Среди специфических запрограммированных шагов, которые способен делать *Stuxnet* при обнаружении цели, оказались блокирующие и замедляющие изменения во фрагментах программного кода корпорации «Сименс», известного как оперативный «Блок 35». Этот важный и уникальный компонент программ «Сименс» занимается мониторингом критических производственных

операций, требующих срочной реакции автоматического управления в пределах не более 100 миллисекунд. Целенаправленно вмешиваясь в работу «Блока 35», *Stuxnet* может гарантированно вызвать аварийный сбой в работе, ведущий к саморазрушению любого опасного промышленного процесса с катастрофическими последствиями [14].

Хотя точное назначение всех выполняемых вредоносной вирусной программой операций до сих пор остается невыясненным, они могут включать перевод скорости вращения турбины на максимально возможные обороты, отключение системы смазки, или любые другие жизненно важные для нормальной работы функции. Конкретная природа повреждений, вызываемых червём, перехваченным сразу после первичного заражения, остаётся неизвестной операторам атакуемой системы до момента его срабатывания, так как по внутреннему коду программы *SPS* без технологической схемы конечной цели атаки нельзя понять, за что именно отвечают задаваемые параметры. Как только исходный код *PLC* перестаёт выполняться, происходит крупная необратимая авария.

Данные особенности работы *Stuxnet* хорошо иллюстрируют его действия по выводу из строя высокоскоростных турбин и центрифуг. Вирус при этом перехватывает управляющие коды частотных преобразователей, изменяя поведение контролируемых ими устройств. *Stuxnet* в течении очень короткого интервала времени посылает команды, предписывающие создание скачка выходной частоты преобразователя, сначала до 1410 Гц, затем падения до 2 Гц и подъём до 1064 Гц. В результате оборудование периодически выходит за пределы допустимого режима работы, накапливая внутренние усталостные повреждения конструкционных материалов без срабатывания датчиков аварийной защиты и уведомления обслуживающего персонала. Аналогичные кумулятивные эффекты, как известно, привели к катастрофическому выходу из строя второй турбины Саяно-Шушенской ГЭС в августе 2009 года.

Таким образом, в отличие от большинства ранее известных вирусов, по своей сути *Stuxnet* представляет собой не инструмент промышленного шпионажа или похищения финансовой информации, а программное обеспечение целенаправленной кибернетической атаки, нацеленной на диверсионное уничтожение вполне определённого промышленного процесса за пределами компьютерных сетей в физическом мире. Оно характеризуется относительной дешевизной и простотой применения, а также хорошей совместимостью со старыми диверсионными средствами. Сам выявленный в 2010 г. *Stuxnet* уже не опасен, однако в будущем по описанной схеме могут создаваться новые, гораздо более сложные и эффективные инструменты вредоносного кибернетического воздействия.

Американский опыт борьбы с кибернетическим терроризмом

Несомненно, что перспективные ИЭС, базирующиеся на сложном компьютерном и коммуникационном оборудовании, будут отличаться повышенной уязвимостью ко всем видам локального и дистанционного несанкционированного доступа и злонамеренного переключения на внешнее управление. Поэтому начиная с данного момента обязательным условием бесперебойной работы

предприятий ТЭК становится системная организация их защиты не только от обычных средств террористических нападений, но и от быстро развивающегося «компьютерного оружия», которое отличает относительная дешевизна и простота применения, скрытность использования, избирательность зон поражения национальных систем жизнеобеспечения и прямая нацеленность на дезорганизацию техногенной среды обитания развитых государств.

Именно в этой связи в США активно осуществляются целенаправленные государственные меры по совершенствованию и ужесточению стандартов и процедур обеспечения производственной безопасности всех энергетических предприятий. Основные приоритеты таких мероприятий связываются с разработкой и использованием более надёжного и безопасного технологического оборудования, с постоянной охраной производственных территорий и элементов их транспортной инфраструктуры, непрерывной профессиональной переподготовкой персонала, регулярными тренировками и учениями специализированных корпоративных, муниципальных и федеральных служб безопасности по проведению спасательных и контртеррористических операций в чрезвычайных ситуациях. Наибольший практический интерес для перспективных российских разработок в данной области представляет американский опыт предварительной оценки коммерческих и военных рисков аварийных ситуаций, создания систем непрерывного планирования и совершенствования мер по предотвращению террористических действий, а также обеспечения промышленной информационной безопасности ТЭК.

Высокая насыщенность современных американских энергетических предприятий компьютерными информационными и управляющими системами, без которых они уже не могут нормально функционировать, создаёт постоянно растущую угрозу возникновения новых специфических аварийных ситуаций и дополнительные возможности для диверсий. Обеспечение информационной безопасности энергетических предприятий преследует три основные цели: а) конфиденциальность – защита закрытой производственной информации от любых видов несанкционированного доступа; б) целостность – охрана программного обеспечения и данных от несанкционированных модификаций; в) доступность – гарантированная выдача только санкционированной информации и основных услуг по работе с ней для каждого идентифицированного пользователя в нужное для него время.

Ежегодный ущерб американских коммерческих предприятий от хищений и разнообразных мошенничеств, совершаемых с помощью информационных технологий только через Интернет, достигает 5–7 млрд. долл.; ещё не менее 3 млрд. теряются из-за взломов и повреждений локальных сетей. Неоднократно проводимые Пентагоном и ФБР в последние годы комплексные учения по имитации скрытого проникновения в информационные системы военного назначения, обычно более защищённые, чем гражданские, показали, что в среднем в 88% случаев такие атаки увенчались успехом и лишь 4–5% попыток дистанционного несанкционированного доступа были своевременно обнаружены и пресечены.

В июне 2009 г. ответственность за регулярное проведений подобных контрольных мероприятий была возложена на новое Кибернетическое командова-

ние (*U.S. Cyber Command* – *USCYBERCOM*) – подразделение вооружённых сил США, ответственное за безопасность военных информационных сетей [27].

Специалисты по информационной безопасности Американского нефтяного института и федерального Центра защиты национальной инфраструктуры выделяют семь основных типов возможных локальных и дистанционных атак на производственные компьютерные системы. К ним относятся: 1) нарушение целостности имеющейся структуры данных при осуществлении скрытого несанкционированного доступа к файловой системе компьютеров; 2) организация отказа в предоставлении информационных ресурсов корпоративным пользователям в результате намеренного вывода из строя, как аппаратных, так и программных компонентов или же отключения многопользовательского режима; 3) остановка поступлений внешних данных путём блокирования каналов рассылки электронной почты или изменения функциональных свойств компьютеров в результате вирусного заражения; 4) промышленный или военный шпионаж, осуществляемый в ходе взлома корпоративных или правительственных сетей и скрытой установки особых программ для перехвата данных в компьютерных сетях, почтовых серверах и на рабочих местах операторов производственных предприятий; 5) проведение атак в отношении промышленных компьютеров с использованием специализированных программных вирусов, саморазмножающихся «троянских червей» и специальных контрольных кодов, для получения прав дистанционного управления операционными системами и технологическими процессами, хищения паролей и модификации записей программных средств контроля текущего состояния вычислительных систем для маскировки доступа террористов к закрытой информации; 6) скрытое использование взломанных компьютерных систем различных предприятий для частных коммерческих операций хакеров, проведения распределённых массовых сетевых атак, непосредственного осуществления террористических актов или в ходе операций по отвлечению внимания сетевых администраторов от защиты определённой части компьютерных сетей, которые планируется вывести из строя; 7) преднамеренные ложные утечки информации и массовое распространение фальсифицированных данных об аварийных ситуациях и новых видах уязвимости компьютерных операционных систем для отвлечения внимания служб безопасности от направления «главного удара» [4, с. 114–116].

Согласно данным портала информационной безопасности известной международной специализированной компании «Контент секьюрити», сравнительные уровни опасности «человеческого фактора» внутренних и внешних угроз распределяются следующим образом: разглашение данных из-за излишней болтливости персонала – 32%; несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок – 24%; отсутствие надлежащего внутреннего режима и жестких условий обеспечения информационной безопасности – 14%; традиционный неконтролируемый обмен производственным опытом – 12%; бесконтрольное использование информационных систем – 10%; возникновение среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой по сплочению производственного коллектива – 8%. Таким образом, наибо-

лее уязвимым элементом производственных систем является недостаточно мотивированный и плохо подготовленный к критическим ситуациям персонал.

Основным способом обеспечения необходимого уровня информационной безопасности в энергетическом секторе США является формирование на каждом предприятии постоянно действующей группы реагирования на нарушения безопасности работы компьютерных систем. Главными задачами таких групп являются непрерывный мониторинг всех имеющихся компьютеров на рабочих местах, внутренних локальных сетей и их соединений с Интернетом, устранение имеющихся и вновь возникающих уязвимостей программного обеспечения путём регулярного обновления его компонентов, ликвидация вирусных заражений, восстановление вредоносно модифицированных программ, аудит информационных угроз и атак взломщиков, совершенствование политики внутренней информационной безопасности, обучение персонала необходимым действиям с доведением их до автоматизма в случаях возникновения аварийных ситуаций в корпоративных компьютерных системах.

Из-за сложности большинства подобных ситуаций практически невозможно решать все возникающие задачи одновременно. Поэтому действующими федеральными нормативными документами были установлены пять последовательных приоритетов, которые должны соблюдаться этими группами в ходе ликвидации любых компьютерных инцидентов.

Эти приоритеты включают следующие требования: 1) обеспечивать сохранение жизни людей и их физическую безопасность, так как совокупная прямая и косвенная ценность «человеческого капитала», включая обязательные страховые выплаты чаще всего превышает стоимость производственного оборудования; 2) оберегать закрытые информационные ресурсы, непосредственно связанные с национальной безопасностью и коммерческими интересами энергетических компаний; 3) обеспечивать сохранность прочих управленческих, статистических и аналитических данных, потеря которых ведёт к значительным убыткам; 4) заблаговременно предотвращать необратимые повреждения программных и аппаратных ресурсов компьютерных систем, вызывающие большие затраты рабочего времени и финансовых средств; 5) защищать отдельные компьютеры на рабочих местах путём их быстрого отключения от локальных сетей и питания в момент возникновения аварийной ситуации, а не пытаться ценой их потери продолжать сохранять работоспособность распределённых вычислительных сетей.

Одной из главных задач сотрудников таких групп является постоянный контроль, связанный с соблюдением десяти обязательных правил компьютерной безопасности на рабочих местах, установленных Центром защиты национальной инфраструктуры для всех предприятий государственного и коммерческого секторов: 1) постоянное использование изменяемых в неодинаковые промежутки времени и не повторяемых надёжных паролей машинной генерации; 2) обязательная идентификация и мониторинг доступа всех пользователей к компьютерам; 3) ежесуточное резервное копирование данных на защищённые удалённые носители; 4) регулярное обновление программных средств антивирусной защиты; 5) применение защитных сетевых экранов; 6) регулярное обновление программного обеспечения для закрытия вновь обнаруживае-

мых уязвимостей; 7) быстрое физическое отключение компьютеров от сетей при авариях и длительных перерывах в работе; 8) полная фильтрация и строгий контроль вложений электронной почты; 9) применение съёмных жёстких дисков магнитной памяти со встроенной криптографией, обеспечивающих раздельное защищённое хранение информации; 10) создание многоконтурных зон физической защиты оборудования и автоматизированных постоянно действующих систем контроля вскрытия аппаратуры [15].

В состав групп реагирования на нарушения безопасности работы компьютерных систем обычно входят: ведущий координатор группы, администратор защитных сетевых экранов, главный системный администратор предприятия, менеджер по выявлению внешних и внутренних компьютерных атак и случаев несанкционированного доступа к системным ресурсам, администратор систем антивирусной защиты, администратор контроля электронной почты, вебмастер внутренних и внешних корпоративных сайтов. Важное условие своевременного предотвращения угроз информационной безопасности и ликвидации коррупционных утечек данных заключается в том, чтобы не допускать совместного выполнения указанных функций одними и теми же сотрудниками.

Каждый из администраторов при этом должен нести персональную ответственность только за свой участок работы и никогда не иметь доступа к закрытой информации других членов группы. Применяются также составные пароли, изменяемые части которых хранятся у разных сотрудников и срабатывают только при коллективном одновременном или разнесённом по времени вводе в строго определённой последовательности. Эффективным методом профилактической защиты может быть создание фрагментов ложных компьютерных сетей для выявления инсайдерской агентурной активности, внутренней коррупции и избирательного вирусного заражения. На практике такая группа всегда действует в тесном контакте с директором информационной службы предприятия, службой внутренней безопасности, внутренними и внешними экспертами по информационной безопасности, менеджерами функциональных информационных систем, юридическими консультантами и специалистами по связям с общественностью. Доклад по каждому выявленному инциденту направляется руководству предприятия и служит основанием для привлечения к расследованию местных и федеральных правоохранительных органов.

Принятая в США унифицированная система мер государственного управления для обеспечения энергетической безопасности обеспечивает постоянное циклическое обновление и адаптацию используемых защитных мер к новым видам угроз с учетом внутреннего и международного опыта.

* * *

Рассмотренные данные об активизации работ по внедрению новейших технологий ИЭС в США свидетельствуют о высокой приоритетности этого направления в рамках программы модернизации национальной энергетической инфраструктуры. Это связано с тем, что большинство используемых при этом технических решений многократно проверено на практике и гарантировано обеспечивает существенное снижение трансмиссионных потерь, повышенную стабильность и управляемость работы сетей, а также беспрепятственное под-

ключение новых генерирующих мощностей на базе первичных возобновляемых источников энергии со специфическими характеристиками.

Внедрение прогрессивного зарубежного опыта развития новых типов «интеллектуальных» электроэнергетических сетей в России открывает дополнительные возможности повышения энергетической эффективности и надёжного энергоснабжения нашей страны. Вместе с тем уязвимость ИЭС в отношении новых видов кибернетических угроз требует особых мер по их защите от любых видов несанкционированного доступа и целенаправленного нападения, способных повлечь за собой исключительно тяжёлые и опасные последствия системного характера.

Поэтому в методологическом плане такие угрозы целесообразно рассматривать как возможность использования новой разновидности информационного оружия. При этом следует учитывать, что информационное оружие подразделяется на оборонительное и наступательное. Имеющиеся оборонительные системы в первую очередь предназначены для защиты собственной информационной инфраструктуры и личного состава. К ним относятся защитные информационно-программные средства, нацеленные на профилактику, своевременное выявление фактов атак и на их отражение. Для успешной борьбы с кибернетическим терроризмом необходимы также и комплексы наступательного оружия, которое используется для уничтожения вражеских систем получения, хранения и обработки информации для принятие решений, кибернетических средств нападения противника, а также для перехватов его управляющих сигналов и подачи ложных данных в коммуникационные системы террористов.

Для реализации такого наиболее результативного подхода необходимы новые независимые государственные и частные охранные структуры, осуществляющие постоянный мониторинг возможного внедрения нового вредоносного ПО во все промышленные системы, аудит установленных защитных систем, а также независимый контроль качества обучения и переподготовки персонала. Актуальность этого направления была дополнительно подчеркнута недавним решением Правительственной комиссии по высоким технологиям и инновациям РФ, которая в апреле 2011 г. возложила координацию соответствующих работ в нашей стране в рамках технологической платформы «Интеллектуальная энергетическая система России» на Российское энергетическое агентство (РЭА РФ) [7, с. 11].

Важное значение в данной сфере имеет и многостороннее международное сотрудничество, которое желательно развивать на базе взаимного укрепления коллективной технологической безопасности, организации многосторонней региональной охраны международных и внутренних топливных трубопроводов, привлечения экспертов из разных стран для прогнозирования и профилактики перспективных угроз.

Показательным примером такого подхода является недавнее российско-американское межправительственное «Соглашение о сотрудничестве в области мирного использования атомной энергии» (так называемое «Соглашение 123»), вступившее в силу в начале 2011 г. Этот документ формирует необходимые правовые рамки для выстраивания полномасштабного и эффек-

тивного сотрудничества России и США в гражданской ядерной энергетике, а также создает условия для реализации взаимовыгодных совместных проектов и проведения перспективных научно-технологических исследований, включая обеспечение кибернетической безопасности производственных систем [3]. Указанные целевые приоритетные позиции также предусмотрены в рамках недавно ратифицированных аналогичных соглашений нашей страны с Японией и Турцией.

Не менее важным представляется и реализация новых российских инициатив на встрече стран «большой восьмёрки» 2011 г. в Довиле по активному распространению и принятию во всех странах мира унифицированных повышенных стандартов технологической и информационной безопасности в энергетической сфере с помощью различных специализированных международных организаций, профессиональных ассоциаций и объединений.

Список литературы

1. *Вачедин Д.* Немецкие энергетические системы заражены компьютерным вирусом Stuxnet // Deutsche Welle. 16.04.2011.

2. *Кобец В.Б., Волкова И.О.* Инновационное развитие электроэнергетики на базе концепции Smart Grid. М.: ИАЦ Энергия, 2010. С. 27.

3. *Корнеев А.В.* «Соглашение 123» формирует правовые рамки для сотрудничества России и США в сфере мирного атома // Пресс-центр атомной энергетики. 14.01.2011 (http://www.minatom.ru/comments).

4. *Корнеев А.В.* Если для нефтянки прозвучит сигнал «мэйдэй»: американские новации в борьбе с угрозой террористических актов в нефтяной отрасли // Нефть России. 2004. № 6. С. 114–116.

5. *Максимов Б.К., Молодюк В.В.* Теоретические и практические основы рынка электроэнергии. М.: Издательский дом МЭИ, 2008. 292 с., ил.

6. *Медведев Д.А.* Вступительное слово на заседании Совета Безопасности РФ «О состоянии и мерах по обеспечению энергетической безопасности России». Москва: Президент России, официальный сайт. 13.12.2010.

7. Протокол заседания Правительственной комиссии по высоким технологиям и инновациям РФ от 1 апреля 2011 г. № 2 // Наука и технологии России. 1.04.2001 (http://strf.ru).

8. *Тарасов В.Н.* Механизмы Саяно-Шушенской аварии: факты и гипотезы // Тайга.инфо. 9.03.2011 (http://tayga.info).

9. Утверждён перечень поручений о мерах антитеррористической безопасности объектов ТЭК. Москва: Президент России, официальный сайт. 11.04.2011.

10. *Blechschmidt P.* Nato rüstet sich für Computer-Kriege // Süddeutsche Zeitung. 1.10.2010.

11. *Broad W.J., Markoff J., Sanger D.E.* Israeli Test on Worm Called Crucial in Iran Nuclear Delay // The New York Times. 15.01.2011.

12. *Brunnstrom D.* Russia Says Stuxnet Could Have Caused New Chernobyl // Reuters (Brussels). 26.01.2011.

13. *Carey J.* Obama's Smart-Grid Game Plan // Bloomberg Businessweek. 27.10.2009.

14. *Falliere N., Murchu L.O., Chien E.* W32.Stuxnet Dossier. Washington: Symantec Corporation, February 2011. 69 p.

15. Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents, DOE No. 205.4. U.S. Department of Energy. Washington. March 2002. 8 p.

16. *Karp Z.* Federal Smart Grid Initiatives a Big Boost for IT // Matter Network. 19.05.2009.

17. *Malik N.S.* Entergy Ends Effort to Sell Vermont Nuclear Plant // The Wall Street Journal. 30.03.2011.

18. *Markoff J., Sanger D.E., Shanker T.* In Digital Combat, U.S. Finds No Easy Deterrent // The New York Times. 25.01.2010.

19. *Minkel J.R.* The 2003 Northeast Blackout – Five Years Later // Scientific American. 13.08.2008.

20. *Montgomery L.* Obama Calls for $50 Billion Infrastructure Initiative // The Washington Post. 11.10.2010.

21. *Mostafavi R.* Iran Says It Has Detected Second Cyber Attack // Reuters (Tehran). 25.04.2011.

22. National Transmission Grid Study. U.S. Department of Energy. Washington. May 2002. Tab. 1.1. P. 3.

23. Oil Hits New High after Refinery Blast // Reuters. 13.05.2004.

24. *Pérez A.* La ciberguerra pasa al ataque // Público.es. 27.06.2010.

25. Remarks by the President on Rebuilding America's Infrastructure. The White House. Office of the Press Secretary. Washington. 11.10.2010. P. 1.

26. Remarks by the President on Recovery Act Funding for Smart Grid Technology. The White House. Office of the Press Secretary. Washington. 27.10.2009. P. 2.

27. *Shanker T.* New Military Command for Cyberspace // The New York Times. 23.06.2009.

28. Statement for the Record of Sean P. McGurk, Acting Director, National Cybersecurity and Communications Integration Center. Office of Cybersecurity and Communications National Protection and Programs Directorate Department of Homeland Security. The United States Senate. Homeland Security and Governmental Affairs Committee. Washington. 17.11.2010. 13 p.

29. Statement of Ranking Member Senator Susan M. Collins «Securing Critical Infrastructure in the Age of Stuxnet» before the U.S. Senate Committee on Homeland Security and Governmental Affairs. The United States Senate Homeland Security and Governmental Affairs Committee. Washington. 17.11.2010. 3 p.

30. Stuxnet Specifically Targeted Iranian Nuclear Program // The Jerusalem Post. 20.11.2010.

31. Texas City Put on Edge by BP Explosion // Texas City Sun. 30.03.2004.

32. What's in the Stimulus Bill – A Breakdown // The Wall Street Journal. 17.02.2009.