УДК 004.056.5+620.9

Массель Л.В.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В SMART GRID КАК УГРОЗА КИБЕРБЕЗОПАСНОСТИ ЭНЕРГЕТИЧЕСКИХ СИСТЕМ РОССИИ

Анотація:

Розглядається проблема використання сучасних інформаційних технологій в SMART GRID як загроза кібербезпеки енергетичної системи Росії.

Анотация:

Рассматриваются проблемы спользования современных информационных технологий в SMART GRID как угроза кибербезопасности энергетических систем России

Abstract:

The problem of the use of modern information technology in SMART GRID as a threat to cyber security of the energy system of Russia is considered.

Введение

Одной из тенденций развития мировой энергетики является создание концепции и внедрение технологий Smart Grid. Основными достигнутыми результатами должны стать наблюдаемость, контролируемость, автоматизация управления электроэнергетической системы (ЭЭС), обеспечивающие её высокую надёжность и высокие экономические показатели работы. Всё большее внедрение находят глобальные распределённые системы мониторинга, защиты и управления, в основе которых лежит технология векторных измерений с высокой точностью синхронизации пространственно разнесённых устройств. Наиболее полно общую функционально-технологическую идеологию этой концепции, по-видимому, отражает сформулированное IEEE определение Smart Grid как концепции «полностью интегрированной, саморегулирующейся и самовосстанавливающейся электроэнергетической системы, имеющей сетевую топологию и включающей в себя все генерирующие источники, магистральные и распределительные сети и все виды потребителей электрической энергии, управляемые единой сетью информационно-управляющих устройств и систем в режиме реального времени».

Если первоначально работы в области создания Smart Grid в России велись преимущественно в области электроэнергетики (в России употреблялся термин «Интеллектуальные электроэнергетические системы с активно-адаптивной сетью» – ИЭС ААС [1], то сейчас говорят уже о создании интегрированных интеллектуальных энергетических систем (ИИЭС), под которыми понимаются системы, ориентированные на использование нескольких видов энергоносителей с комплексным применением информационных технологий и телекоммуникаций, в совокупности обеспечивающих возможность построения более эффективной системы энергопроизводства, энергоснабжения и энергопотребления [2]. Иначе говоря, интеллектуальная энергетическая система предусматривает интеграцию энергетических систем с новыми коммуникационными технологиями и целостной многоуровневой автоматизированной системой управления.

Очевидно, что успешная реализация этой концепции требует повышенного внимания к проблемам как современных информационных технологий (ИТ), так и к проблемам кибербезопасности, поскольку усложнение современных информационно-телекоммуникационных технологий увеличивает уязвимость создаваемых систем. В статье рассматриваются проблемы, касающиеся состояния работ в этой области и опыта их решения в других странах, в частности, в США, обосновывается необходимость специальных мероприятий, направленных на предотвращение угроз, обусловленных использованием новейших информационных технологий.

Общие проблемы развития интеллектуальных энергетических систем с точки зрения ИТ

В России работы по тематике Smart Grid сейчас ведутся преимущественно в области совершенствования технологических основ электроэнергетики. В то же время, очевидно, что необходим новый подход к решению проблемы интеллектуальной и информационной поддержки принятия решений при моделировании и управлении режимами в активно-адаптивных электрических сетях. Этот подход должен интегрировать как интеллектуальные методы, так и методы, основанные на численных расчетах. В последнем случае необходимо решать задачу реинжиниринга унаследованных программных комплексов. Кроме того, необходимо создание новой технологии работы, которая позволяла бы интеграцию, помимо программных комплексов (ПК) для решения расчетных задач, новых методов интеллектуальной поддержки принятия решений и их интеграции с традиционными ПК.

Кратко проблемы в области ИТ характеризуются следующим:

- Необходимо развитие информационных и коммуникационных технологий, позволяющих создать качественно новые системы мониторинга и управления энергетическими системами.
- Ограниченный диапазон предложений в данном сегменте со стороны ИТ-поставщиков: решения зарубежных разработчиков довольно дороги, качественных отечественных разработок недостаточно или они просто отсутствуют.
- Использование зарубежных разработок может рассматриваться как одна из угроз кибербезопасности [3].

В энергетике используется следующая классификация [4] интеллектуальных систем. Системы называются интеллектуальными, если:

- в их составе есть аппаратные решения в виде микропроцессоров (интеллектуальный датчик, интеллектуальный исполнительный привод и т.д.);
- в них используются методы и технологии искусственного интеллекта (ИИ): экспертные системы, искусственные нейронные сети, генетические алгоритмы, аппарат нечеткой логики и т.п. [5].
- системы имеют несколько целей функционирования (или умеют генерировать эти цели), выбирая самую подходящую цель в зависимости от окружающей среды, умеют прогнозировать поведение окружающей среды и свое собственное состояние.

С точки зрения ИТ, использование датчиков для сбора информации недостаточно для повышения «интеллектуальности» системы. При использовании методов искусственного интеллекта не всегда анализируется целесообразность их применения и эффективность их использования. Наиболее привлекательным является последний класс систем,

которые называют «системами с целеполаганием», но, к сожалению, примеры промышленных образцов таких систем в нашей стране отсутствуют [6].

В разработанной концепции ИЭС ААС России широко декларируется мультиагентный подход к построению системы управления энергосистемами, но не уделяется достаточное внимание тому, что мультиагентная система управления энергосистемой будущего должна обеспечивать надежное и безопасное функционирование и управление и не становиться «слабым звеном» энергетики.

Проблема надежности и безопасности мультиагентной системы управления (МСУ) состоит в противоречии между основными принципами организации МСУ (ее открытости к большим потокам разнородных данных от разнородных источников и возможности подключения новых типов агентов) и требований по безопасности работы системы управления, в первую очередь, по отношению к намеренным кибератакам. МСУ является принципиально уязвимой с точки зрения кибербезопасности, и необходимы новые способы обеспечения ее безопасности и устойчивости по отношению к некачественным и недружественным данным. Для этого она должна быть защищена по отношению к возможным кибератакам и уметь эффективно работать в условиях поступления сверхбольших потоков данных разного качества и достоверности. В противном случае уязвимая система управления станет причиной крупных техногенных аварий. Иначе говоря, МСУ должна быть защищена по отношению к возможным кибератакам и уметь эффективно работать в условиях поступления сверхбольших потоков данных разного качества и достоверности. В противном случае уязвимая система управления станет причиной крупных техногенных аварий.

Говоря о концепции построения интегрированных систем на принципах интеллектуального управления, к основным элементам интеллектуальной управляющей инфраструктуры относят следующие [4]:

- Виртуализация и сервис-ориентированная архитектура (SOA).
- Интегрированный комплекс информационных ресурсов (GRID Computing).
- Облачные вычисления и программное обеспечение как сервис (Cloud Computing and Software as a Service)

При этом отмечается, что эффективное применение подобных интеллектуальных управляющих систем возможно только в соответствующих технологических инфраструктурах, требованиям которых реальные инфраструктуры отечественной энергетики не полностью соответствуют.

Тем не менее, как было показано на примере мультиагентных систем, использование вышеперечисленных современных информационных технологий увеличивает уязвимость создания интеллектуальных энергетических систем с точки зрения кибербезопасности. Рассмотрим далее это понятие и состояние дел в этой области.

Определение и содержание понятия «кибернетическая безопасность»

Согласно стандарту T-REC-X.1205 – ITU-T [7], ***кибернетическая безопасность*** трактуется как набор средств, стратегии, принципов обеспечения безопасности, гарантии безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологии, которые могут быть использованы для защиты кибернетической среды, ресурсов организации и пользователя. ***Кибернетическая среда*** – это подключенные компьютерные устройства, персо-

нал, инфраструктура, приложения, сервисы, телекоммуникационные системы, а также совокупность передаваемой и/или хранящейся информации.

Кибернетическая безопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в кибернетической среде.

В настоящее время кибербезопасность все чаще рассматривается, как стратегическая проблема государственной важности, затрагивающая все слои общества. Государственная политика кибербезопасности (national cyber security strategy – NCSS) служит средством усиления безопасности и надежности информационных систем государства.

Первые стратегии кибербезопасности начали появляться в начале предыдущего десятилетия. Одной из первых стран, которая стала воспринимать кибербезопасность, как вопрос государственной важности были Соединенные Штаты Америки. В 2003 году в США была опубликована Национальная стратегия безопасности в киберпространстве (National Strategy to Secure Cyberspace). В 2005–2011 гг. еще двенадцать стран - членов Евросоюза опубликовали свои государственные стратегии кибербезопасности.

В России стратегия кибербезопасности в явном виде не сформулирована, но разработаны «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ» [8].

Настоящие «Основные направления» разработаны в целях реализации основных положений Стратегии национальной безопасности РФ до 2020 года, в соответствии с которой одним из путей предотвращения угроз информационной безопасности РФ является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в РФ.

Критически важный объект инфраструктуры РФ - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта РФ либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок. Энергетика, безусловно, является одной из критически важных инфраструктур.

Рабочей группой CIGRE (CIGRE Working Group the B5.38, August 2010) были сформулированы требования к обеспечению кибербезопасности в энергетике (The Impact of Implementing Cyber Security Requirements using IEC 61850), основные из которых приведены ниже:

- ***управление доступом*** (AC — Access Control) - для защиты от несанкционированного доступа к устройству или информации;
- ***управление использованием*** (UC — Use Control) – для защиты от несанкционированного оперирования или использования информации;
- ***целостность данных*** (DI — Data Integrity) - для защиты от несанкционированного изменения;
- ***конфиденциальность данных*** (DC — Data Confidentiality) – для защиты от несанкционированного доступа;

- ***ограничение потока данных*** (RDF — Restrict Data Flow) - для защиты от публикации информации на несанкционированных источниках;
- ***своевременный ответ на событие*** (TRE — Timely Response to Event), мониторинг и протоколирование связанных с безопасностью событий и принятие своевременных мер по ликвидации последствий в ответственных задачах и в критических ситуациях по безопасности;
- ***доступность сетевого ресурса*** (NRA — Network Resource Availability) – для защиты от атак «отказ в обслуживании».

Среди основных задач обеспечения кибернетической безопасности в Smart Grid выделяют целостность, доступность и конфиденциальность, причем главной задачей является обеспечение доступности, при одновременном обеспечении целостности и конфиденциальности. Это означает, что субъекты, имеющие право на доступ к информации, должны иметь возможность реализовать свое право беспрепятственно, но в то же время система должна быть безопасной и обеспечивать защиту от кибернетических угроз.

Кибернетическая безопасность может быть нарушена при следующих обстоятельствах:

- Незащищенность информационного ресурса на носителе (отсутствие качественной криптографической защиты)
- Незащищенность каналов передачи информации
- Незащищенность носителя информации или устройств передачи информации (например, несоответствующий контроль доступа в помещение)

Кибернетическая безопасность рассматривает обеспечение безопасности информационных ресурсов, средств передачи информации, средств хранения и определяет требования к обеспечению как информационной, так и физической безопасности.

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования или уничтожения, а так же защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Основные требования к обеспечению информационной безопасности:

- Применение надежных алгоритмов шифрования;
- Предельно безопасная аутентификация сотрудников и клиентов энергетической компании;
- Предельное уменьшение возможности реализации угроз информационной безопасности.
- Основные требования к обеспечению физической безопасности:
- Порядок доступа и способы охраны помещения и его периметра (включая видеофиксацию и сигнализацию);
- Способы охраны каналов передачи данных (кабели и т.д.)
- Порядок действий для проведения профилактических мероприятий;
- Порядок действий по факту происшествия;
- Обучение сотрудников.

Основные угрозы физической безопасности:

1. *Противоправная деятельность* преступных групп, конкурирующих экономических структур, а также отдельных лиц, в отношении собственности и сотрудников пред-

приятия, которые могут привести к материальным и финансовым потерям предприятия и нанесения ущерба здоровью его персонала.

2. *Преднамеренные* (в корыстных целях, по принуждению, со злым умыслом) *действия сотрудников предприятия*, допущенных к материальным, финансовым и информационным ресурсам.

3. *Непреднамеренные* (ошибочные, случайные, необдуманные, без корыстных целей) *нарушения* установленных требований учета, хранения, оборота и продажи товарно-материальных ценностей, финансовых ресурсов, служебных документов и информации, приводящие к утере ресурсов и хищениям.

4. *Преднамеренные отказы и сбои в работе:*

а) инженерно-технических систем (электро- и водоснабжения, вентиляции, отопления, и др.), приводящие к производственным потерям;

б) средств охраны (систем СКУД, охранно-пожарной сигнализации (ОПС), видеонаблюдения и связи), приводящие к несанкционированному проникновению посторонних лиц на территорию предприятия и хищению материальных, финансовых и информационных ресурсов.

5. *Чрезвычайные ситуации:* пожары, аварии, разрушения, техногенные катастрофы и природные катаклизмы.

Основные задачи физической безопасности (охраны) любого объекта:

- Контроль пропускного режима;
- Мониторинг систем видеонаблюдения;
- Предотвращение несанкционированного доступа
- Меры предотвращения последствий чрезвычайного происшествия (пожар, землетрясение)
- Меры предосторожности, направленные на уменьшение воздействия на обеспечение безопасности во время чрезвычайного происшествия.

Среди основных составляющих обеспечения кибернетической безопасности выделяют:

1. Средства (ресурсы): люди, технические средства (программные и аппаратные); регламент и другие документы (техника безопасности); страхование.

2. Процессы: подготовка (обучение), получение соответствующего практического опыта; конкретные действия по факту происшествия; проведение профилактических мер для предотвращения угроз безопасности; прогнозирование и предотвращение угроз на основе полученного опыта.

Существующие подходы к обеспечению кибербезопасности в Smart Grid за рубежом

15 февраля 2011 в University of Maryland, Baltimore County (UMBC) прошла конференция: «Кибернетическая безопасность в Smart Grid», организатором которой выступил Факультет Вычислительной техники и Электроэнергетики. В рамках конференции был представлен отчет Национального института по стандартизации и технологиям **NISTIR 7628**, носящий название «Инструкции по обеспечению кибернетической безопасности в интеллектуальных сетях» (разработан в 2010 г.). В 2011 году был разработан подход к безопасности, основанный на NISTIR 7628, под названием «OpenWay Security», данный

подход был разработан двумя крупными компаниями: ITron и Cisco, при поддержке NETL и NISTIR.

Полностью документ называется: «Guidelines for Smart Grid Cyber Security» (перевод: руководство по обеспечению кибернетической безопасности Smart Grid) и он состоит из введения и трех томов:

- Том 1: «Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements» (Стратегии, архитектуры и требования высокого уровня к обеспечению кибернетической безопасности Smart Grid)
- Том 2: «Privacy and the Smart Grid» (Конфиденциальность в Smart Grid)
- Том 3: «Supportive Analyses and References» (Анализ результатов и литература).

В этом документе представляет интерес рассмотрение риска как продукта взаимодействия угроз, уязвимостей и их последствий. Отмечается, что кибернетическая безопасность должна быть направлена не только на преднамеренные действия злоумышленников, но и на случайные ошибки, в этом смысле определяя человеческий фактор.

Примеры потенциальных рисков:

- Повышенная сложность сети повышает количество уязвимостей для потенциальных атак и непреднамеренных ошибок
- Сети, взаимосвязанные с другими сетями, которые также могут занимать несколько «умных» доменов сети, увеличивают вероятность каскадных аварий
- Большое количество взаимосвязей программных компонентов увеличивает уязвимость программного кода, что упрощает злоумышленникам внедрение в программный код вредоносного кода и уязвимостей
- По мере увеличения узлов сети увеличивается и число точек входа в систему для злоумышленников
- Использование новейших технологий – это новые риски.

Ниже дается краткий перечень стандартов CIP (critical infrastructure protection). Цель этих стандартов заключается в том, чтобы гарантировать, что автоматизированные системы и коммуникационные сети, необходимые для надежной поставки электроэнергии в стране, разумно защищены от атак из различных, заслуживающих доверия источников угроз, а также поддерживать жизнеспособность и эффективность такой защиты.

CIP включает в себя 11 стандартов, каждый стандарт определяет требования к объекту защиты. Уже перечисление названий этих стандартов дает представление о широте охвата различных областей, в которых могут возникнуть киберугрозы, например: CIP-001 - «Отчеты по подозрительной активности» ; CIP-002 – «Критически важные it-ресурсы»;

CIP-003 – «Кибернетическая безопасность - управление в области кибернетической безопасности»; CIP-004 – «Персонал и его обучение»; CIP-005 – «Защита электронного периметра»; CIP-006 – «Физическая безопасность»; CIP-007 – «Управление защитой систем»; CIP-008 – «Управление инцидентами» и др.

Необходимость разработки методического подхода к определению состава угроз кибербезопасности в ИИЭС, обусловленных использованием современных информационных технологий

Очевидно, что для анализа уязвимостей энергетических систем, вызываемых использованием современных информационных технологий, необходима разработка соответствующего методического подхода. Естественно, он должен быть составляющей более

широкого, комплексного рассмотрения проблемы кибербезопасности ИИЭС. Методический подход должен включать ряд методик, например, методику анализа угроз и оценки риска нарушения кибербезопасности энергетических объектов, обусловленных использованием современных информационных технологий. Методики должны быть разного уровня детальности, начиная от методики аудита состояния кибербезопасности энергетических объектов, до конкретных инструкций персоналу, основанных на разработке мер по предотвращению киберугроз, их реализации в виде кибератак и/или ликвидации последствий кибервторжений (успешных кибератак).

Методики должны, в частности, определять:

1. Порядок анализа угроз и оценки риска, в том числе критичность поддерживаемых информационно-телекоммуникационными технологиями целевых функций ИИЭС и стоимость защиты ИТ-ресурсов и ИТ-систем.

2. Уровень детализации анализа угроз в зависимости от ориентации на категорию лиц, принимающих решения: высшее руководство; специалисты, ответственные за безопасное функционирование ИТ-систем; руководство функциональных подразделений энергетических систем.

3. Состав и порядок сбора данных для анализа угроз и оценки риска (данные об угрожающих факторах, угрожающих событиях и слабых местах (уязвимости) анализируемых систем).

4. Порядок тестирования и состав тестов для определения слабых мест (уязвимостей) анализируемых систем, вплоть до организации искусственных кибератак с целью определения надежности и выявления слабых мест действующих систем защиты.

5. Состав рекомендуемых мероприятий по повышению надежности функционирования анализируемых систем; перечень возможных кибератак и действий, необходимых для их отражения; регламент мероприятий по ликвидации последствий кибервторжений (в случае удачных кибератак).

Очевидно, что этот перечень не является исчерпывающим, но работа в этом направлении необходима, в первую очередь для того, чтобы специалисты-энергетики отчетливо представляли масштабы киберугроз и последствия для энергетических систем в случае их реализации

Заключение

Из вышесказанного можно сделать следующие выводы:

- Наряду с развитием технологической инфраструктуры энергетики для создания Smart Grid необходимо развитие и усовершенствование современных информационных технологий.
- Использование новейших ИТ создает новые уязвимости с точки зрения кибербезопасности.
- Основные составляющие кибербезопасности – информационная безопасность и физическая безопасность.
- Кибербезопасность все чаще рассматривается, как стратегическая проблема государственной важности, затрагивающая все слои общества; в ряде стран разработаны государственные стратегии кибербезопасности.

- В России начинают уделять все большее внимание безопасности критических инфраструктур, одной из которых является энергетика; развитие Smart Grid усугубляет проблему кибербезопасности в энергетике.
- К сожалению, в России проблема кибербезопасности в Smart Grid практически еще не сформулирована, в отличие, например, от США, где проработаны практические подходы к ее решению.
- Наряду с разработкой общей стратегии кибербезопасности страны необходима разработка методического подхода к анализу угроз и оценке риска нарушения кибербезопасности энергетических систем и объектов, обусловленных все более широким использованием в ИИЭС современных информационных технологий.

Тем не менее, в России ведется работа в области кибербезопасности. При этом отмечается, что достигнут технологический потолок в развитии большинства типов средств защиты информации (СЗИ), дальнейший рост эффективности СЗИ невозможен без централизации управления информационной безопасностью (ИБ) [9].

Выделен класс продуктов SIEM (Security Information and Event Management), которые способны решить задачу централизации управления ИБ как для оперативной обработки событий, так и для их комплексного анализа и оценки соответствия. Для эффективного использования SIEM-систем необходима их сопрягаемость со всеми элементами автоматизированной системы и корректная настройка правил корреляции и оповещения.

Представляется обоснованным предложение авторов [9] о необходимости создания ситуационных центров для реализации сложных и распределенных проектов по обработке событий и другой информации в области безопасности, программной основой которых могут стать SIEM-системы и другие подсистемы класса управления ИБ.

Благодарности

Работа выполняется при частичной финансовой поддержке гранта РФФИ №13-07-00140, гранта Программы Президиума РАН №229, грантов интеграционных проектов СО РАН №145, СО РАН и НАН Беларуси №18. Автор выражает благодарность этим организациям.

Литература:

1. Кобец Б.Б. Инновационное развитие электроэнергетики на базе концепции Smart Grid / Кобец Б.Б., Волкова И.О. – М.: ИАЦ Энергия, 2010. – 208 с.

2. Воропай Н.И. Интеллектуальные электроэнергетические системы: концепция, состояние, перспективы / Н.И. Воропай // Автоматизация и IT в энергетике. – 2011. – № 3. – С. 11–16.

3. Массель Л.В. Проблема построения интеллектуальных и программных компонентов Smart Grid и подход к ее решению на основе агентной технологии / Л.В. Массель // Материалы XL Международной конференции «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». – Гурзуф, 2012. – С.22–25.

4. Егоров А.А. Интеллектуальная энергетика: мифы и реальность / А.А. Егоров // Автоматизация и IT в энергетике. – 2011. – № 3. – С. 17–22.

5. Рассел С. Искусственный интеллект: современный подход, 2-е издание / С. Рассел, П. Норвиг ; [пер. с англ.]. – М.: Издательский дом «Вильямс», 2006. – 1408 с.

6. Массель Л.В. Интеллектуализация поддержки принятия решений при моделировании и управлении режимами в Smart Grid / Л.В. Массель // Интеллектуализация обработки информации: Труды 9-й Международной конференции. – Черногория, Будва, 2012. – С. 692–695.

7. Марков А.С. Корпоративные информационные системы управления событиями информационной безопасности / А.С. Марков, Ю.В. Рауткин, А.А. Фадин // Труды XVIII Байкальской Всероссийской конференции. – Иркутск, 2013. – С. 412–416.

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

9. Лукацкий А. Обзор стандартов NERC CIP для отрасли энергетики. Безопасность инфраструктурыэнергоснабжения [Электронный ресурс] / Алексей Лукацкий. – Режим доступа: http://www.slideshare.net/CiscoRu/nerc-cip.