КИБЕРОПАСНОСТЬ КАК ОДНА ИЗ СТРАТЕГИЧЕСКИХ УГРОЗ ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

Массель Л.В.[1], Воропай Н.И.[2], Сендеров С.М.[3], Массель А.Г.[4]

В статье рассматриваются вопросы кибербезопасности во взаимосвязи в энергетической безопасностью России. Даются определения энергетической безопасности и кибербезопасности энергетических систем. Отмечается возрастание угроз кибербезопасности с связи с распространением концепции интеллектуальных энергетических систем, в рамках которой предусматривается повышение уровня компьютеризации и интеллектуализации энергетики. Предлагается рассматривать киберугрозы как одну из важнейших современных угроз энергетической безопасности России. Анализируется современное состояние в области кибербезопасности энергетических систем. Энергетическая инфраструктура рассматривается как одна из критических инфраструктур. Формулируется предлагаемый авторами методический подход к разработке мер обеспечения кибербезопасности в энергетических системах и рассматриваются результаты его реализации.

***Ключевые слова**: кибербезопасность, энергетическая безопасность, киберугрозы, критическая инфраструктура, критически важный объект*

DOI 10.21681/2311-3456-2016-4-2-10

Введение

Энергетическая безопасность (ЭБ) является одной из важных составляющих национальной безопасности страны. Развитие концепции интеллектуальных энергетических систем (Smart Grid) в России усугубляет проблему кибербезопасности в энергетике, в связи с чем авторы предлагают рассматривать киберугрозы как один из важнейших современных видов угроз ЭБ. Киберопасность определяется как опасность, вызванная пребыванием и деятельностью в киберсреде[5], включая как прямые атаки на компьютеры, так и следствия неправильных или ошибочных действий пользователей, не уделяющих внимания специальным средствам защиты и правилам безопасной работы в компьютерных сетях.

Анализируется современное состояние в области кибербезопасности энергетических систем. Энергетическая инфраструктура рассматривается как одна из важных критических инфраструктур. Предлагается подход к ранжированию критически важных объектов (КВО) на основе анализа возможных критических ситуаций (КС) и учета рисков КС.

Обосновывается необходимость разработки методического подхода к исследованию проблем кибербезопасности энергетической инфраструктуры. Предлагаются методика анализа угроз и оценки риска, как одна из составляющих этого подхода, и экспертная система, реализующая предложенную методику. Для однозначного понимания определения основных терминов, связанных с кибербезопасностью, приводятся в подстрочных ссылках.

1. Энергетическая безопасность как составляющая национальной безопасности. Институт систем энергетики им. Л.А. Мелентьева (ИСЭМ) СО РАН является одним из лидеров в области исследований ЭБ. Энергетическая безопасность рассматривается как состояние защищенности страны, ее граждан, общества, государства, экономики от угроз надежному топливо- и энергообеспечению. Эти угрозы определяются как внешними (геополитическими, макроэкономическими, конъюнктурными) факторами, так и собственно состоянием и функционированием энергетического сектора страны [1]. ЭБ является важной составляющей национальной безопасности страны,

1 Массель Людмила Васильевна, доктор технических наук, профессор, Институт систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, massel@isem.irk.ru

2 Воропай Николай Иванович, член-корреспондент РАН, доктор технических наук, профессор, Институт систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, voropai@isem.irk.ru

3 Сендеров Сергей Михайлович, доктор технических наук, Институт систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, ssm@isem.irk.ru

4 Массель Алексей Геннадьевич, кандидат технических наук, Институт систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, amassel@isem.irk.ru

5 Кибернетическая среда – это подключенные компьютерные устройства, персонал, 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.

поскольку энергетика связана со всеми отраслями и во многом обеспечивает их функционирование. При рассмотрении угроз ЭБ выделяют тактические и стратегические угрозы [2]. Первые создают временные массовые нарушения бесперебойного энергоснабжения из-за физической или экономической недоступности топливно-энергетических ресурсов (ТЭР) приемлемого качества. Стратегические угрозы ЭБ ведут к формированию значительного и длительного дефицита энергоресурсов, который приводит к сдерживанию (торможению) экономического роста и соответственно социального прогресса или даже препятствует поддержанию нормального функционирования общества и экономики при незначительном либо нулевом экономическом росте. Следует отметить, что тактические угрозы не менее важны, чем стратегические. Если первые вызывают обычно различные ЧС с возможными серьезными перерывами в энергоснабжении, то вторые формируют нарастание проблем в перспективе, что способно привести к долговременным крупномасштабным дефицитам энергии в будущем, а это, в свою очередь, может усугубляться возможной реализацией тактических или текущих угроз энергетической безопасности.

Угрозы ЭБ систематизируются в пять основных групп: экономические, социально-политические, техногенные, природные и управленческо-правовые [2]. Среди этих угроз до последнего времени не рассматривались угрозы кибербезопасности, реализация которых может спровоцировать серьезнейшие чрезвычайные ситуации в энергетике, чреватые значительным снижением возможностей обеспечения энергоресурсами потребителей. Например, в случае успешной атаки киберпреступников на компьютеры, контролирующие работу энергосистемы, последствия могут быть катастрофическими для целого города, региона или даже страны.

Стремительное распространение компьютерной среды, развитие информационных технологий и тенденция перехода к интеллектуальной энергетике делают киберугрозы[6]. одной из важнейших тактических угроз ЭБ. В то же время, недооценивание необходимости проведения систематических превентивных мероприятий по предотвращению киберугроз и постоянного обновления средств защиты (аналогичного необходимости постоянного обновления оборудования энергетических систем), в также возможность возникновения значительного и длительного дефицита энергоресурсов в зависимости от масштаба и последствий кибератак[7], требуют рассмотрения киберугроз как стратегических угроз ЭБ [3-5].

2. Кибербезопасность энергетических систем. В России до сих пор нет однозначного понимания кибербезопасности. Часто ее считают синонимом информационной безопасности или ее составляющей, в силу чего кибербезопасности не уделяется достаточного внимания. Так, в отличие от большинства развитых стран, в России до сих пор не принята доктрина кибербезопасности, и, как следствие, отсутствуют соответствующие стандарты, как, например, в США: «Guidelines for Smart Grid Cyber Security» (Руководство по обеспечению кибернетической безопасности Smart Grid) [7]. Учитывая, что всем нам приходится жить и работать в кибернетической среде, что усугубляет, том числе, и проблему информационной безопасности, целесообразно рассматривать кибербезопасность как результат конвергенции пяти основных составляющих: безопасность приложений, информационная безопасность, сетевая безопасность, безопасность интернет-приложений, защита ключевых информационных систем объектов критических инфраструктур. Согласно стандарту ISO 27032:2012 [8], кибербезопасность базируется на этих пяти составляющих, но не является синонимом ни одного из них.

При реализации концепции интеллектуальных энергетических систем необходимо учитывать следующие потенциальные риски использования современных информационных технологий:

- Повышенная сложность информационной 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.

6 *Киберугроза* – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство (киберсреду) для достижения политических, социальных или иных целей. Киберугроза может воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. http://www.ruscrypto.ru/resource/summary/rc2016/15_masalovitch.pdf (27.07.16).

7 *Кибератака* (1), или атака из киберпространства (cyber attack) – атака, проводимая с помощью программных и аппаратных средств на компьютерные сети и компьютерные системы противника; *кибератака* (2) – это намеренные попытки изменить, нарушить или остановить функционирование компьютерных систем или сетей, а также программ или информации, которые они содержат или передают [6]. Кибератака обычно поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.

• 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***.

При рассмотрении кибербезопасности энергетических систем может быть использована следующая классификация киберугроз:

- по природе происхождения (предумышленные и непредумышленные);
- по направлению осуществления (внешние и внутренние);
- по объекту воздействия (АРМы пользователей и администраторов, средства документирования и отображения, каналы связи и т.д.);
- по способу осуществления (информационные, программно-аппаратные, физические, радиоэлектронные, организационно-правовые и т.д.);
- по жизненному циклу (разработка, ввод в эксплуатацию, эксплуатация, вывод из эксплуатации) [6].

Учитывая вышесказанное, имеет смысл рассматривать киберугрозы как дополнительную угрозу ЭБ, которая становится все более актуальной с развитием интеллектуальной энергетики [9].

3. Интеллектуальные энергетические системы (ИЭС) как современная концепция развития энергетики. Одной из тенденций развития мировой энергетики является создание концепции и внедрение технологий Smart Grid. Основными достигнутыми результатами должны стать наблюдаемость, контролируемость, автоматизация управления энергетической системы, 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 применительно к электроэнергетическим системам, по-видимому, отражает сформулированное IEEE[8] 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 [10], 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 [11]. Иначе говоря, интеллектуальная энергетическая система предусматривает интеграцию энергетических систем с новыми информационно-коммуникационными технологиями и целостной многоуровневой автоматизированной системой управления.

Реализация ИИЭС требует как совершенствования технологической инфраструктуры энергетики, так и развития и широкого внедрения в энергетику современных информационных технологий (ИТ), первоочередными из которых рассматриваются агентные и облачные технологии. Помимо того, что повышение уровня интеллектуальности энергетических систем (внедрение цифровых подстанций, интеллектуальных датчиков и т.п.) усугубляет проблему кибербезопасности, внедрение современных ИТ, как было сказано выше, также может быть дополнительной угрозой кибербезопасности [3-5], и, соответственно, энергетической безопасности, так как появляются новые уязвимости (их классификация дается, например, в [12]) и создаются дополнительные возможности для организации кибератак.

Киберугрозы, возникающие как результат применения современных ИТ, можно рассмотреть на примере многоагентных систем [4].

• Проблема надежности и безопасности мультиагентной системы управления (МСУ) состоит в противоречии между основными принципами организации МСУ (ее открытости к большим пото-

8 IEEE (The Institute of Electrical and Electronics Engineers, англ.) — Институт инженеров электротехники и электроники.

кам 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.

• В разработанной концепции ИЭС ААС России широко декларируется мультиагентный подход к построению системы управления энергосистемами, но, к сожалению, 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.

• Кибератаки могут быть направлены как на объекты генерации энергоресурсов, так и на объекты их транспортировки и потребления. Наиболее уязвимым звеном являются системы управления и диспетчеризации электроэнергетических систем (ЭЭС), систем газоснабжения и других энергетических систем, причем уязвимость систем управления будет возрастать по мере распространения концепции и технологий Smart Grid [9, 10]. Говоря о кибератаках, следует иметь ввиду, что, помимо умышленных действий, вред могут причинить действия неумышленные (авторы называют их киберхалатностью [5]), обусловленные, например низкой компьютерной грамотностью или пренебрежением мерами, обеспечивающими кибербезопасность, которые по причиняемому ущербу сравнимы с кибератаками. Именно последние факторы являются существенными для России, и могут иметь серьезные последствия, учитывая российский менталитет.

В ИСЭМ СО РАН ведутся исследования в области кибербезопасности, основанные на анализе данных при оценивании состояния ЭЭС [13]. Хотя кибератаки, связанные с генерированием недостоверных данных, представляются маловероятными, поскольку требуют от хакеров высокой квалификации в области энергетики, тем не менее это направление исследований заслуживает внимания, поскольку альтернативы пока отсутствуют.

4. Состояние в области кибербезопасности энергетических систем. Проблема кибербезопасности энергетических систем усугубляется тем, что более 75 % энергетического оборудования имеет иностранное происхождение (не считая 100 % компьютерного и программного обеспечения) [14, 15].

Современное состояние в автоматизированных системах управления технологическими процессами (АСУ ТП) в энергетике характеризуется следующими цифрами (по информации компании Positive Technologies):

• С 2010 года в 20 раз выросло число обнаруженных уязвимостей (рис. 1).

• Каждая пятая уязвимость устраняется дольше месяца.

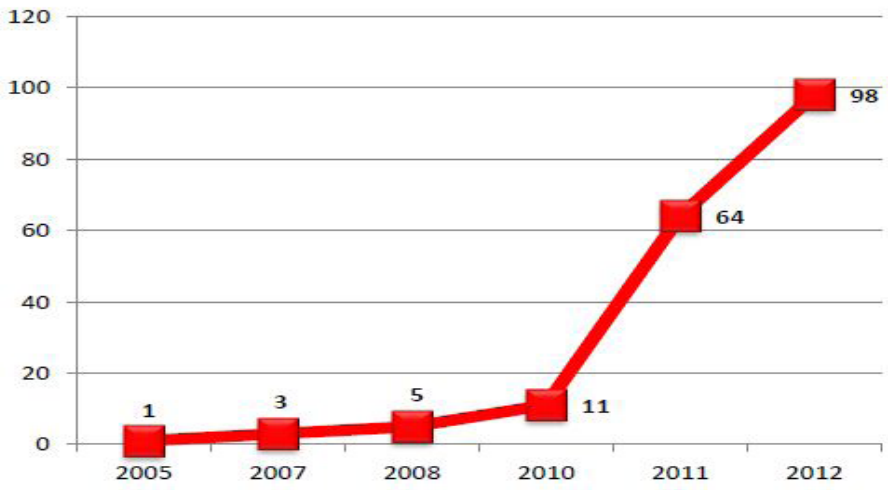

***Рис. 1**. Динамика роста уязвимостей в АСУ ТП*

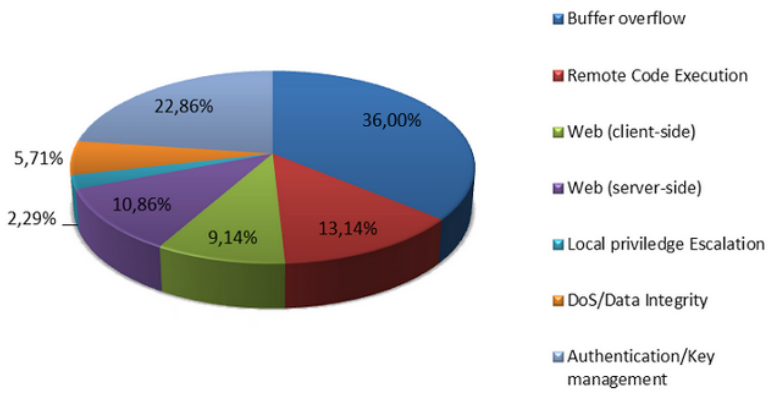

***Рис. 2**. Основные виды уязвимостей*

• 50% уязвимостей позволяют хакеру запустить выполнение кода.

• Для 35% уязвимостей есть эксплойты (специальные программы для кибератак, использующие эти уязвимости).

• Более 40% интернет-доступных систем могут взломать хакеры-любители.

• Треть доступных из интернета систем находятся в США.

• Четверть уязвимостей связана с отсутствием необходимых обновлений безопасности.

• Уязвимы 54% интернет-доступных систем в Европе и 39% в Северной Америке.

• Уязвимы 50% опубликованных в глобальной сети систем из России.

Динамика роста уязвимостей показана на (рисунке 1), основные виды уязвимостей приведены на (рисунке 2).

На (рис. 3) показано, что основными производителями SCADA (системы контроля и сбора данных в электроэнергетике) являются иностранные компании, что также является одной из угроз кибербезопасности.

Что касается доли устраненных уязвимостей, следует отметить, что большинство недостатков безопасности (81%) были оперативно ликвидированы производителями — еще до того, как сведения о них становились широко известными, или в течение 30 дней после нескоординированного разглашения информации. Однако примерно каждая пятая уязвимость «закрывалась» с серьезной задержкой, а в некоторых случаях так и не была устранена.

Наглядное представление о том, насколько серьезно относятся к проблемам информационной безопасности различные производители АСУ ТП,

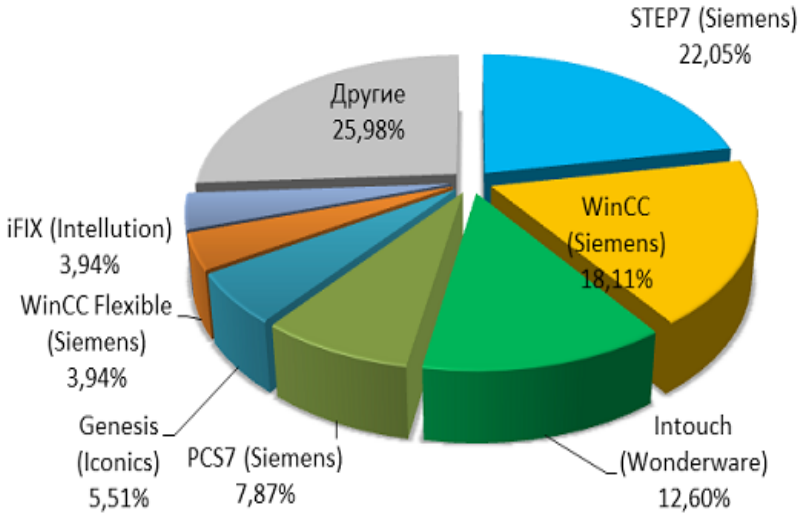

***Рис. 3**. Основные производители SCADA*
(по информации компании Positive Technologies)

дает доля «закрытых» уязвимостей. Например, Siemens устранила и выпустила обновления для 98% уязвимостей, тогда как Schneider Electric ликвидировала только чуть больше половины (56%) обнаруженных уязвимостей.

Самые распространенные недостатки безопасности (выявлены в 36% случаев) связаны с ошибками конфигурации. Сюда относятся и некорректная парольная политика (например, использование стандартных инженерных паролей), доступ к критической информации, ошибочное разграничение полномочий. Четверть уязвимостей связана с отсутствием необходимых обновлений безопасности.

Таким образом, приведенные факты подтверждают неблагополучное состояние в области кибербезопасности в энергетической инфраструктуре России [14, 15].

5. Энергетическая инфраструктура как одна из важных критических инфраструктур. Помимо рассмотрения киберугроз как стратегических угроз ЭБ, одним из путей решения проблемы кибербезопасности является рассмотрение энергетической инфраструктуры как одной из важных критических инфраструктур.

Исследования критических инфраструктур являются достаточно молодым направлением, но становятся приоритетными во многих странах мира, и в первую очередь в США [16]. Актуальность этих исследований усугубляется угрозами кибернетической безопасности. К критическим инфраструктурам относят энергетику, транспорт, службы по чрезвычайным ситуациям, банковский и финансовый, телекоммуникационный сектора экономики и другие жизненно важные ресурсы. В исследованиях критических инфраструктур большое внимание уделяется выявлению ключевых объектов (или их совокупности), воздействие на которые может оказать наиболее негативный эффект на отрасль экономики, ключевой ресурс или всю инфраструктуру, а также в оценке последствий подобного воздействия и разработке механизмов снижения таких рисков. Под энергетической инфраструктурой, которую относят к критически важным инфраструктурам, понимают совокупность энергетических объектов и систем энергетики, включая энергетические транспортные магистрали.

Критически важными объектами называют ключевые объекты (или их совокупности) соответствующих инфраструктур, воздействие на которые может оказать наиболее негативный эффект на отрасль экономики, ключевой ресурс или всю инфраструктуру. В исследованиях критических инфраструктур особое внимание уделяется выявлению критически важных объектов, а также оценке последствий воздействия на них и разработке механизмов снижения рисков таких воздействий.

В России существует «Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам (КВО) для национальной безопасности Российской Федерации» [17]. В ИСЭМ СО РАН в соответствии с этой методикой выполнена работа по выявлению критически важных объектов газотранспортной сети России [18]. Критически важным предлагается считать каждый объект, при нарушении работы которого суммарная относительная недопоставка газа потребителям составит 5% и более от суммарной потребности в газе. На основании проведенных расчетов в газотранспортной системе России выявлено около 20 потенциально опасных для функционирования системы пересечений газопроводов.

Следуя данной методике, большинство энергетических объектов можно отнести к критическим, но в ней не предусматривается ранжирование объектов по степени значимости для экономики страны в целом. Авторы предлагают выполнять такое ранжирование на основе анализа возможных критических ситуаций (КС) и учета рисков КС. Риск-ориентированный подход сейчас получает распространение в области кибербезопасности. Например, в [19] он предлагается как новая парадигма сертификации средств защиты информации.

6. Необходимость разработки методического подхода к обеспечению кибербезопасности. Очевидно, что одной из первоочередных проблем обеспечения кибербезопасности критически важных объектов энергетики и энергетических систем в целом является разработка как российских стандартов (с учетом зарубежного опыта и специфики России), так и методик обеспечения кибербезопасности, которые должны статью частью стандартов, законодательно утвержденных на государственном уровне [3, 4].

Авторы считают, что такие 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; специ-

алисты, 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 приведенный перечень методик 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

Первым шагом на пути обеспечения кибербезопасности КВО энергетической инфраструктуры может стать предложенная авторами методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов [20]. В настоящее время под руководством авторов реализован научный прототип экспертной системы, реализующей эту методику [21].

Заключение

В статье рассматривается состояние в области кибербезопасности энергетических систем России. Обращается внимание на то, что проблема кибербезопасности в энергетике усугубляется в связи с распространением концепции интеллектуальных энергетических систем. Предлагается рассматривать угрозы кибербезопасности, как один из видов стратегических угроз ЭБ. Формулируется методический подход к разработке мер обеспечения кибербезопасности, рассматриваются результаты его реализации. Обращается внимание на необходимость принятия мер по обеспечению кибербезопасности энергетических систем на государственном уровне (включая разработку доктрины кибербезопасности и соответствующих стандартов).

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э.Баумана, г. Москва, v.tsirlov@bmstu.ru*

Литература

1. Воропай Н.И., Сендеров С.М., Пяткова Н.И., Славин Г.Б. Энергетическая безопасность России. Новосибирск: Наука, 1998. 302 с.
2. Рабчук В.И., Сендеров С.М., Славин Г.Б. Энергетическая безопасность России: проблемы и пути решения / Отв. ред. Н.И. Воропай. Новосибирск: Издательство Сибирского отделения РАН, 2011. 197 с.
3. Массель Л.В. Использование современных информационных технологий в Smart Grid как угроза кибербезопасности энергетических систем России // Труды Международной конференции «Кибербезопасность-2013». , Киев, Институт специальной связи и защиты информации НТУ Украины «КПИ». 2013. №1 (3). С. 56-65.
4. Массель Л.В. Проблемы создания Smart Grid в России с позиций информационных технологий и кибербезопасности // Методические вопросы исследования надежности больших систем энергетики Международный научный семинар им. Ю.Н. Руденко. Утверждено к печати Институтом систем энергетики им. Л.А. Мелентьева СО РАН; Редакционная коллегия: ответственный редактор Н.И. Воропай, Н.И. Илькевич, Г.Ф. Ковалев, Л.В. Массель, С.М. Сендеров. 2014. С. 171-181.
5. Массель А.Г. Кибератаки как угроза энергетической безопасности России // Труды Международной конференции «Кибербезопасность-2013». Украина, Киев, Институт специальной связи и защиты информации НТУ Украины «КПИ». 2013. №1 (3). С. 49-56.
6. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Екатеринбург: Изд-во Уральского федерального университета, 2008. 212 с.
7. http://www.slideshare.net/CiscoRu/nerc-cip.
8. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cyber security.
9. Кобец Б.Б., Волкова И.О. Инновационное развитие электроэнергетики на базе концепции Smart Grid. М.: ИАЦ Энергия, 2010. 207 с.
10. Бердников Р.Н., Бушуев В.В., Васильев С.Н., Веселов Ф.В., Воропай Н.И., Волкова И.О. и др. Концепция интеллектуальной электроэнергетической системы России с активно-адаптивной сетью / Под ред. академиков Фортова В.Е. и Макарова А.А. М.: ОАО «НТЦ ФСК ЕЭС», 2012. 235 с.
11. Воропай Н.И., Стенников В.А. Интегрированные интеллектуальные энергетические системы // Известия Российской академии наук. Энергетика. 2014. № 1. С. 64-73.

12. Зубарев И.В., Жидков И.В., Кадушкин И.В., Медовщикова С.А. Уязвимости информационных систем // Информационные и математические технологии в науке и управлении. 2016. №3. С. 174-184.
13. Колосок И.Н., Гурина Л.А. Снижение показателя уязвимости системы SCADA к кибератакам методами обнаружения ошибочных измерений при оценивании состояния ЭЭС // Информационные и математические технологии в науке и управлении. 2016. №1 (27). С. 103-112.
14. Massel A., Massel L. The current state of cyber security in Russia's energy systems and the proposed activities for situation improving // Proceedings of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. Saint Petersburg, 2015. P. 183-189.
15. Massel L., Massel A. Cyber security of Russia's energy infrastructure as a component of national security // Proceedings of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. Saint Petersburg, 2015. P. 66-72.
16. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах // Зарубежное военное обозрение. 2012. №1. С. 19-30. URL: http://pentagonus.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnykh_stranakh_2012/19-1-0-2082 (дата обращения 7.09.2015).
17. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации. URL: http://lawru.info/dok/2012/10/17/n164727.htm (дата обращения 26.07.2016).
18. Еделев А.В., Сендеров С.М., Сидоров И.А. Применение распределенных вычислений для выявления критически важных объектов газотранспортной сети России // Информационные и математические технологии в науке и управлении. 2016. №1 (27). С. 55-62.
19. Марков А.С., Рауткин Ю.В. Сертификация средств защиты информации по требованиям безопасности информации. Новая парадигма // Информационные и математические технологии в науке и управлении. 2016. №1 (27). С. 94-102.
20. Массель А.Г. Методика анализа угроз и оценки риска нарушения информационно-технологической безопасности энергетических комплексов // Информационные и математические технологии в науке и управлении / Ответственный редактор Л.В. Массель. 2015. С. 186-195.
21. Гаськова Д.А., Массель А.Г. Разработка экспертной системы для анализа угроз кибербезопасности в энергетических системах // Информационные и математические технологии в науке и управлении. 2016. №1 (27). С. 113-122.

CYBER DANGER AS ONE OF THE STRATEGIC THREATS TO RUSSIA'S ENERGY SECURITY

Massel L.[9], Voropay N.[10], Senderov S.[11], Massel A.[12]

The article deals with cybersecurity in relation to the energy security of Russia. The definitions of energy security and cyber security of energy systems are given. It's marked increasing of cyber threats in connection with proliferation of Smart Grid concept, which provides raising level of computerization and intellectualization of energy systems. It is proposed to consider cyber threats as one of the most important contemporary threats to Russia's energy security. The current state of cybersecurity energy systems is analyzed. Energy infrastructure is considered as one of the critical infrastructures. Proposed by the authors a methodological approach to the development of cybersecurity measures in energy systems is formulated and the results of its implementation is regarded.

***Keywords**: cybersecurity, energy security, cyber threats, critical infrastructure, critical facilities*

Reference

1. Voropay N.I., Senderov S.M., Pyatkova N.I., Slavin G.B. Energeticheskaya bezopasnost' Rossii. Novosibirsk: Nauka, 1998. 302 P.
2. Rabchuk V.I., Senderov S.M., Slavin G.B. Energeticheskaya bezopasnost' Rossii: problemy i puti resheniya / Otv. red. N.I. Voropay. Novosibirsk: Izdatel'stvo Sibirskogo otdeleniya RAN, 2011. 197 P.
3. Massel' L.V. Ispol'zovanie sovremennykh informatsionnykh tekhnologiy v Smart Grid kak ugroza kiberbezopasnosti energeticheskikh sistem Rossii // Trudy Mezhdunarodnoy konferentsii «Kiberbezopasnost'-2013». Ukraina, Kiev, Institut spetsial'noy svyazi i zashchity informatsii NTU Ukrainy «KPI». 2013. No1 (3), pp. 56-65.

9 Liudmila Massel, Dr.Sc., Professor, Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, massel@isem.irk.ru

10 Nikolay Voropay, Corresponding Member, Dr.Sc., Professor, Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, voropai@isem.irk.ru

11 Sergey Senderov, Dr.Sc., Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, ssm@isem.irk.ru

12 Aleksei Massel, Ph.D., Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, Irkutsk, amassel@isem.irk.ru

4. Massel' L.V. Problemy sozdaniya Smart Grid v Rossii s pozitsiy informatsionnykh tekhnologiy i kiberbezopasnosti, Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki Mezhdunarodnyy nauchnyy seminar im. Yu.N. Rudenko. Utverzhdeno k pechati Institutom sistem energetiki im. L.A. Melent'yeva SO RAN; Redaktsionnaya kollegiya: otvetstvennyy redaktor N.I. Voropay, N.I. Il'kevich, G.F. Kovalev, L.V. Massel', S.M. Senderov. 2014, pp. 171-181.
5. Massel' A.G. Kiberataki kak ugroza energeticheskoy bezopasnosti Rossii, Trudy Mezhdunarodnoy konferentsii «Kiberbezopasnost'-2013». Ukraina, Kiev, Institut spetsial'noy svyazi i zashchity informatsii NTU Ukrainy «KPI». 2013. №1 (3), pp. 49-56.
6. Gaydamakin N.A. Teoreticheskie osnovy komp'yuternoy bezopasnosti. Ekaterinburg: Izd-vo Ural'skogo federal'nogo universiteta, 2008. 212 P.
7. http://www.slideshare.net/CiscoRu/nerc-cip.
8. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cyber security.
9. Kobets B.B., Volkova I.O. Innovatsionnoe razvitie elektroenergetiki na baze kontseptsii Smart Grid. M.: IATs Energiya, 2010. 207 P.
10. Berdnikov R.N., Bushuev V.V., Vasil'yev S.N., Veselov F.V., Voropay N.I., Volkova I.O. i dr. Kontseptsiya intellektual'noy elektroenergeticheskoy sistemy Rossii s aktivno-adaptivnoy set'yu / Pod red. akademikov Fortova V.E. i Makarova A.A. M.: OAO «NTTs FSK EES», 2012. 235 P.
11. Voropay N.I., Stennikov V.A. Integrirovannye intellektual'nye energeticheskie sistemy // Izvestiya Rossiyskoy akademii nauk. Energetika. 2014. No 1, pp. 64-73.
12. Zubarev I.V., Zhidkov I.V., Kadushkin I.V., Medovshchikova S.A. Uyazvimosti informatsionnykh system, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2016. No3, pp. 174-184.
13. Kolosok I.N., Gurina L.A. Snizhenie pokazatelya uyazvimosti sistemy SCADA k kiberatakam metodami obnaruzheniya oshibochnykh izmereniy pri otsenivanii sostoyaniya EES, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2016. No1 (27), pp. 103-112.
14. Massel A., Massel L. The current state of cyber security in Russia's energy systems and the proposed activities for situation improving, Proceedings of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. Saint Petersburg, 2015, pp. 183-189.
15. Massel L., Massel A. Cyber security of Russia's energy infrastructure as a component of national security, Proceedings of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. Saint Petersburg, 2015, pp. 66-72.
16. Kondrat'yev A. Sovremennye tendentsii v issledovanii kriticheskoy infrastruktury v zarubezhnykh stranakh, Zarubezhnoe voennoe obozrenie. 2012. No1, pp. 19-30. URL: http://pentagonus.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnykh_stranakh_2012/19-1-0-2082.
17. Metodika otneseniya ob"ektov gosudarstvennoy i negosudarstvennoy sobstvennosti k kriticheski vazhnym ob"ektam dlya natsional'noy bezopasnosti Rossiyskoy Federatsii. URL: http://lawru.info/dok/2012/10/17/n164727.htm.
18. Edelev A.V., Senderov S.M., Sidorov I.A. Primenenie raspredelennykh vychisleniy dlya vyyavleniya kriticheski vazhnykh ob"ektov gazotransportnoy seti Rossii, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2016. No1 (27), pp. 55-62.
19. Markov A.S., Rautkin Yu.V. Sertifikatsiya sredstv zashchity informatsii po trebovaniyam bezopasnosti informatsii. Novaya paradigm, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2016. No1 (27), pp. 94-102.
20. Massel' A.G. Metodika analiza ugroz i otsenki riska narusheniya informatsionno-tekhnologicheskoy bezopasnosti energeticheskikh kompleksov, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii / Otvetstvennyy redaktor L.V. Massel'. 2015, pp. 186-195.
21. Gas'kova D.A., Massel' A.G. Razrabotka ekspertnoy sistemy dlya analiza ugroz kiberbezopasnosti v energeticheskikh sistemakh, Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2016. No1 (27), pp. 113-122.