НОВАЯ ОНТОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ САМОВОССТАНАВЛИВАЮЩИХСЯ ЭНЕРГОСИСТЕМ SMART GRID. ЧАСТЬ I

АВТОРЫ:

С.А. ПЕТРЕНКО,
Д.Т.Н.,
ОАО «РТИ»,
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ (МФТИ)

Д.Д. СТУПИН,
К.Т.Н.,
ОАО «РТИ»,
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ (МФТИ)

Электроэнергетические сети являются ключевыми объектами национальной инфраструктуры, обеспечивающей безопасность страны. Интеллектуализация процессов энергообеспечения и использование современных информационных технологий в этих процессах, помимо естественных выгод и преимуществ, порождает целый ряд рисков, связанных с несанкционированным внешним вмешательством в нормальную работу национальной энергосистемы.

Ключевые слова: «умные» энергосистемы; Smart Grid; информационные технологии; интеллектуальные сети; онтология; информационная безопасность; кибербезопасность; информационное противоборство; негативное воздействие.

Технология интеллектуальных, или «умных» энергосистем Smart Smart Grid — это принципиально новый подход построения электроэнергетики и электросетевого комплекса

Работа выполнена при поддержке гранта РФФИ (№ 16-29-04268 офи_м), гранта Президента РФ (НШ-6831.2016.8)

ВВЕДЕНИЕ

В настоящее время в ряде развитых стран мира широкое распространение получила так называемая технология интеллектуальных, или «умных» энергосистем Smart Grid. Упомянутая технология предназначена для оптимизации процессов доставки электроэнергии потребителю с помощью современных цифровых технологий, благодаря чему обеспечивается энергосбережение, сокращаются издержки, повышаются надежность сетей и прозрачность процесса управления энергоснабжением. Для реализации таких программ преобразования современных электрических сетей в инновационные сети будущего крупнейшие компании мира создали особый альянс — Smart Energy Alliance. В него вошли такие компании, как GE Energy (General Electric), Capgemini, Cisco Systems, Siemens, HP, Intel, SAP AG, Oracle и ряд других. Типовые решения, разрабатываемые альянсом, максимально приближаются по своей структуре и функционалу к хорошо известным телекоммуникационным решениям. В этой связи обозначилась проблема защиты энергетических сетей от «информационных» воздействий, направленных на нарушения процессов управления сетями.

Актуальность разработки новой онтологии кибербезопасности самовосстанавливающихся Smart Grid объясняется необходимостью создания таких интеллектуальных систем обеспечения устойчивости «умных» энергосистем, которые будут способны эффективно противостоять современным угрозам информационной безопасности.

Сегодня наиболее значимые проекты по созданию энергосистем на основе Smart Grid выполняются в США и России, странах Евросоюза, а также в Канаде, Австралии, Китае и Корее. Например, в г. Майами (штат Флорида, США) реализуется крупный проект интеллектуальной энергосети Energy Smart Miami (www.EnergySmartMiami.com), в котором наряду с местной энергокомпанией Florida Power & Light принимают участие известные компании-производители General Electric, Cisco Systems и Silver Spring Networks. В Дании реализуется масштабный проект EDISON, объединивший компании IBM, Siemens и DONG

КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВА УСТОЙЧИВОГО РАЗВИТИЯ СИСТЕМ КЛАССА SMART GRID

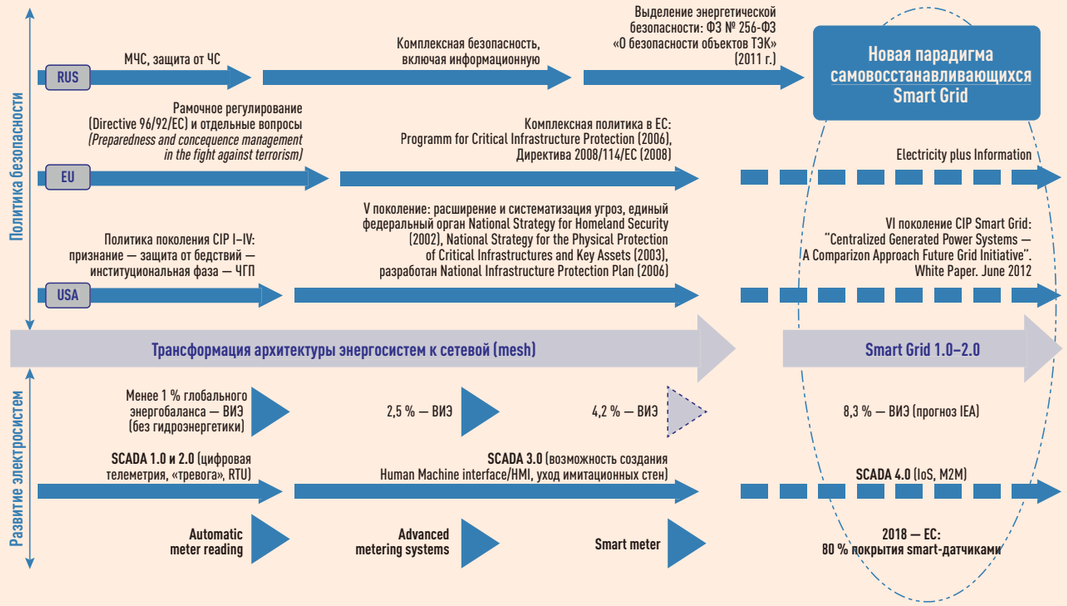


Рис. 1

ПРИМЕР ОЦЕНКИ РИСКОВ КИБЕРБЕЗОПАСНОСТИ

Уровни риска	Тип/мощность энергосистемы	Характеристики инцидента		Последствия инцидента		Потери		
		Воздействие на население	Воздействие на инфраструктуру	Воздействие на информационные ресурсы	Юридические последствия	Гуманитарные	Репутационные	Финансовые
В высшей степени критический	международные системы/ более 10 ГВт/ч	пострадало более 50 % населения страны или более 25 % населения нескольких стран	пострадала международная критическая инфраструктура	не определено	закрытие компании или внесение залога	наличие прямых и побочных жертв в результате инцидента	безвозвратная утрата доверия к компании во всем мире	менее 50 % от EBITDA
Критический	национальные системы / 1–10 ГВт/ч	пострадало от 25 до 50 % населения страны	пострадала национальная критическая инфраструктура	не определено	временное приостановление деятельности	наличие побочных жертв в результате инцидента	безвозвратная утрата доверия к компании внутри страны	менее 50 % от EBITDA
Высокий	городские системы / 0,1-1 ГВт/ч	пострадало от 10 до 25 % населения страны	пострадала значимая инфраструктура	неавторизованное раскрытие или модификация чувствительных данных	штраф до 10 % от EBITDA*	наличие прямых жертв в результате инцидента	временная утрата доверия к компании внутри страны	менее 33 % от EBITDA
Средний	местные системы / 1–100 МВт/ч	пострадало от 2 до 10 % населения страны	пострадала прочая инфраструктура	неавторизованное раскрытие или модификация персональных данных	штраф до 10 % от EBITDA	наличие пострадавших в результате инцидента	временная утрата доверия к компании внутри региона	менее 10 % от EBITDA
Низкий	домашние системы / менее 1 МВт/ч	пострадало менее 2 % населения страны	инфраструктура не пострадала	в инцидент не вовлечены персональные и другие чувствительные данные	предупреждение	незначительные аварии	кратковременная и незначительная утрата доверия к компании	менее 1 % от EBITDA

* EBITDA (Earnings before interest, taxes, depreciation and amortization) — аналитический показатель, равный объему прибыли до вычета расходов по выплате процентов, налогов и начисленной амортизации

Таблица 1

Energy. Для европейских стран в целом разработан так называемый Стратегический план энергетических технологий (Strategic Energy Technologies Plan, SET_PLAN), предусматривающий преобразование европейских электрических сетей в интеллектуальные в течение ближайших 10 лет [1–8].

Для оценки готовности современных электрических сетей к преобразованию их в интеллектуальные сети еще в 2007 г. под руководством IBM была разработана так называемая «Модель зрелости» (Maturity Model) (http://www.ibm.com/energy). Эта модель была доведена до практического использования программистами из университета Карнеги-Меллона, SEI (Software Engineering Institute). Кроме того, исследователи SEI развивают аналогичную модель (Capability Maturity Model Integration, CMMI), в основе которой лежат рекомендации и требования лучшей практики, в том числе рекомендации Национального института стандартов США NIST — EISA (Title XIII), а также соответствующих международных стандартов. Также департамент энергетики США совместно с институтом SEI разрабатывает в настоящее время модель общемировой системы управления Smart Grid (SGMM).

В России разрабатывается масштабный проект по созданию Интеллектуальной электроэнергетической системы с активно-адаптивной сетью (ИЭС ААС). Экспертными рабочими группами в рамках Архитектурного комитета при Научно-техническом Совете ПАО «ФСК ЕЭС» и Российской академии наук были разработаны основные положения и подходы к созданию эталонной архитектуры названной интеллектуальной энергосистемы. Для реализации проекта в ОЭС Востока на период до 2014–2020 гг. создан Полигон ИЭС ААС, представляющий собой комплекс программно-аппаратных средств, формирующих среду поддержки разработки решений ИЭС ААС. Полигон ИЭС ААС размещен на территории АО «НТЦ ФСК ЕЭС» и включает в себя в том числе программный моделирующий комплекс Power Factory и модели энергосистемы ОЭС Востока. В энергокластере «Эльгауголь» осуществлено пилотное внедрение мультиагентной автоматизированной системы управления напряжением и реактивной мощностью на базе Power Agents Platform [1–8].

Существенно, что в названных проектах ключевым является придание перспективным энергосистемам Smart Grid и развитие следующих двух новых способностей [9–14]:

1. Сопротивление негативным воздействиям: наличие специальных методов обеспечения устойчивости и живучести, снижающих физическую и информационную уязвимость всех составляющих энергосистемы и способствующих как предотвращению, так и быстрому восстановлению ее после аварий в соответствии с требованиями энергетической безопасности.
2. Самовосстановление при аварийных ситуациях: энергосистема и ее элементы должны быть способны постоянно поддерживать работоспособное техническое состояние путем идентификации, анализа и перехода от управления по факту возникновения ситуации к превентивному (предупреждающему) ее появлению. Самовосстанавливающаяся энергосистема должна позволять максимально возможно минимизировать сбои (возмущения) с помощью интеллектуальной системы управления, в том числе важнейшей ее составляющей — подсистемы обеспечения кибербезопасности.

Другими словами, интеллектуальная энергосистема на основе Smart Grid должна быть проактивной по отношению к изменяющимся условиям функционирования и отслеживать надвигающиеся технические проблемы еще до того, как они смогут катастрофически повлиять на ее безопасность и устойчивость функционирования в целом (табл. 1, 2). Поэтому в состав проектируемых интеллектуальных подсистем кибербезопасности должны входить соответствующие компоненты сдерживания, предупреждения, обнаружения, нейтрализации и самовосстановления.

ИЗВЕСТНЫЕ МЕТОДИКИ ОЦЕНИВАНИЯ РИСКОВ

Название методики	Тип оценки	Процент упоминаний в проанализированной литературе	Страна разработки
OCTAVE	Качественная	22 %	США
CRAMM		16 %	Великобритания
CORAS		12 %	Греция, Германия, Норвегия
FRAP		10 %	Канада
COBRA		5 %	Великобритания
NIST		16 %	США
ISRAM	Количественная	7 %	Турция
CORA		5 %	США
Risk Watch		5 %	США
IS		2 %	Южная Корея

Таблица 2

Проведенный анализ известных способов создания перспективных энергосистем Smart Grid свидетельствует о целесообразности использования следующих методов и технологий для обеспечения требуемой устойчивости:

- многоагентных (мультиагентных) технологий для координации систем управления с использованием системы мониторинга переходных режимов (СМПР) и устройств FACTS, самовосстановления районных ЭЭС;
- технологий искусственного интеллекта, в том числе нейронных сетей для решения задач идентификации и управления, экспертных систем для обучения и проведения тренировок, раннего обнаружения и локализации чрезвычайных предаварийных режимов;
- адаптивного векторного управления гибкими системами переменного тока для первичного и вторичного автоматического управления напряжением и реактивной мощностью, оптимизации режимов по мощности;
- адаптивного автоматического управления для возобновляемых источников энергии, в том числе ветровых, приливных, солнечных и в перспективе космических солнечных электростанций;
- интеллектуальной кибербезопасности (см. табл. 1, 2), способных обеспечить требуемую устойчивость перспективных энергосистем Smart Grid в условиях информационного противоборства и др.

СОВРЕМЕННЫЕ ТРАКТОВКИ ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ

Ранее вопросы онтологического моделирования рассматривались

зарубежными учеными Т. Грубером (T. Gruber), Н. Гуарино (N. Guarino) и др., а в нашей стране — Г.С. Поспеловым, Д.А. Поспеловым, Э.В. Поповым, В.Ф. Хорошевским, Т.А. Гавриловой, Ю.А. Загорулько, А.С. Нариньяни, А.С. Клещевым, И.Л. Артемьевой, И.В. Котенко, А.Г. Ломако, Д.Н. Бирюковым, Л.С. Массель, Т.Н. Ворожцовой и многими другими. В настоящее время известны модели представления знаний в виде систем фреймов, семантических сетей и систем продукций. Системы фреймов и семантические сети позволяют описать структуру объектов предметной области и связи между ними. Системы продукций (правил) используются для представления знаний предметной области в виде утверждений «если, то». На основе упомянутых моделей разработаны различные языки представления знаний, которые являются входными языками для некоторых универсальных оболочек и экспертных систем [4–8].

В работах А.С. Клещева и И.Л. Артемьевой [5] сформулированы основные методологические принципы определения онтологии предметной области:

1. На содержательном уровне под онтологией понимается совокупность соглашений (определения терминов предметной области, их толкование, утверждения, которые ограничивают возможный смысл этих терминов, а также толкование этих утверждений). В отличие от эмпирических знаний эти соглашения не могут быть опровергнуты эмпирическими наблюдениями.
2. Онтология, концептуализация, знания и действительность должны моделироваться единой математической конструкцией.
3. Между свойствами предметных областей и элементами этой математической конструкции должно быть установлено явное соответствие.
4. Модель онтологии каждой предметной области должна содержать как формальные элементы, так и их содержательное толкование в терминах, понятных специалистам этой предметной области.
5. Онтология и ее модель должны быть обозримы даже для сложных предметных областей, обладающих большим числом понятий.

В работах И.В. Котенко [6] рассмотрены онтология и возможные мультиагентные интеллектуальные

ТИПОВЫЕ СРЕДСТВА КИБЕРЗАЩИТЫ SMART GRID

Рис. 2

НОРМАТИВНЫЕ ТРЕБОВАНИЯ

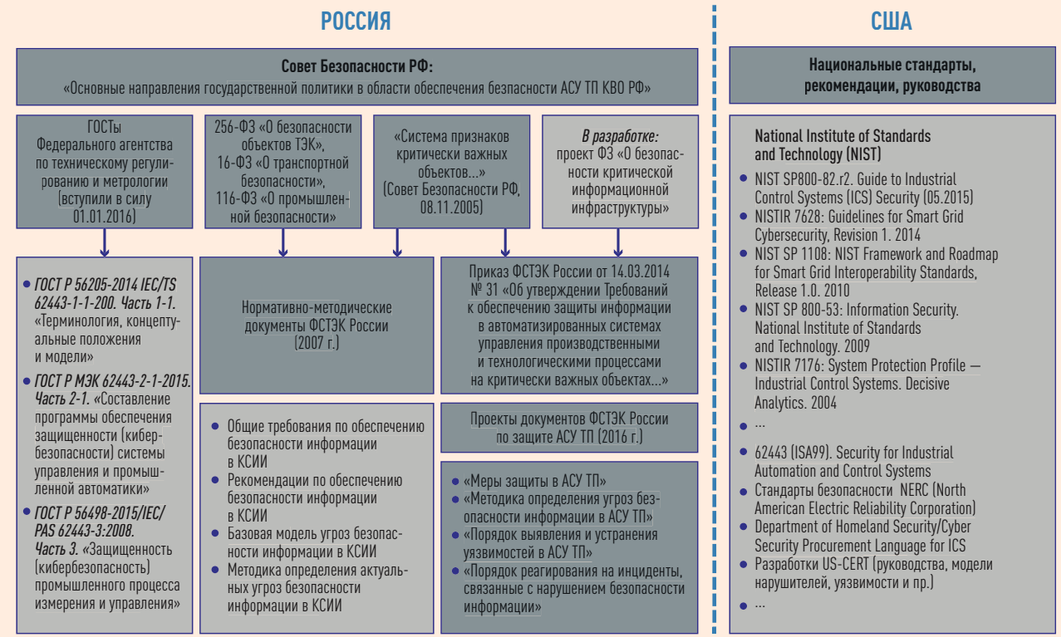


Рис. 3

механизмы управления кибербезопасностью в компьютерных системах и сетях, которые позволяют осуществлять:

1. сбор информации о состоянии информационной системы и ее анализ за счет механизмов обработки и слияния информации из различных источников;
2. проактивное предупреждение кибератак и препятствование их выполнению;
3. обнаружение аномальной активности и явных кибератак, а также нелегитимных действий и отклонений работы пользователей от политики безопасности, предсказание намерений и возможных действий нарушителей;
4. активное реагирование на попытки реализации действий нарушителей путем автоматической реконфигурации компонентов защиты для отражения действий нарушителей в реальном масштабе времени;
5. дезинформацию злоумышленника, сокрытие и камуфляж важных ресурсов и процессов, «заманивание» злоумышленника на ложные (обманные) компоненты с целью раскрытия и уточнения его целей, рефлексивное управление поведением злоумышленника;
6. мониторинг функционирования сети и контроль корректности текущей политики безопасности и конфигурации сети;
7. поддержку принятия решений по управлению политикой безопасности, в том числе по адаптации к последующим вторжениям и усилению критических механизмов защиты.

В работах Д.Н. Бирюкова и А.Г. Ломако [2] обоснованы онтология и системный облик интеллектуальных систем кибербезопасности со свойством антиципации, в частности, новый класс систем предотвращения компьютерных атак, представляющих собой самообучающиеся интеллектуальные системы самоорганизующихся гироматов. Показано, что применение предлагаемых интеллектуальных систем на практике позволяет более успешно решать задачи, связанные с предотвращением рисков реализации киберугроз.

В работах Т.Н. Ворожцовой и Л.В. Массель [4, 7] рассмотрена

СХЕМА ФОРМИРОВАНИЯ ИММУНИТЕТА

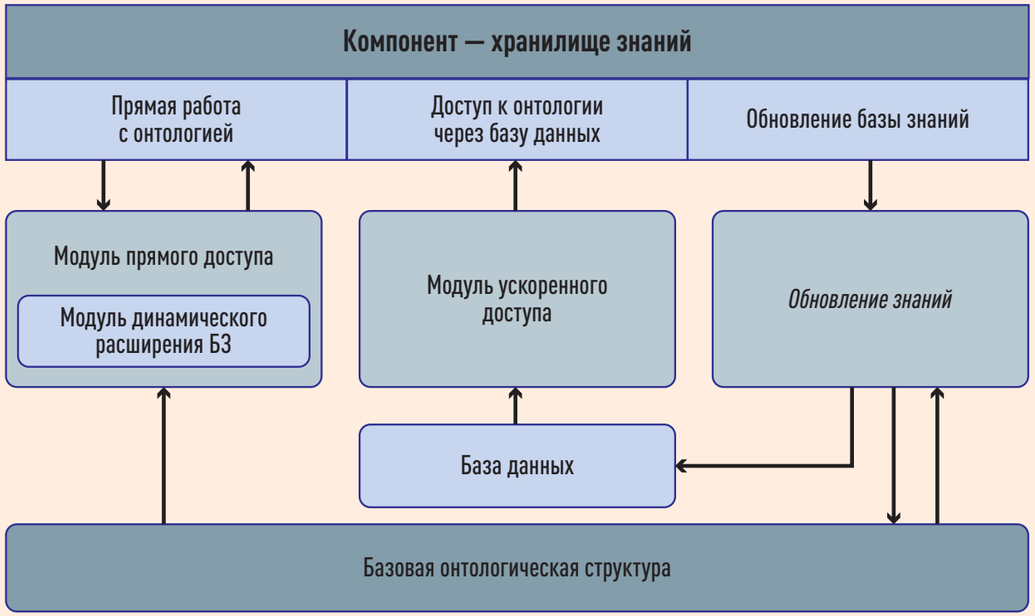


Рис. 4

онтология кибербезопасности Smart Grid, которая была разработана в Институте систем энергетики им. Л.А. Мелентьева Сибирского отделения РАН (ИСЭМ СО РАН) в рамках грантов:

- РФФИ № 13-07000140 «Методология создания и интеграции интеллектуальных, агентных и облачных вычислений в Smart Grid (умных энергетических системах)»;
- Программа Президиума РАН (229) «Методы и инструментальные средства поддержки принятия решений в исследованиях и обеспечении энергетической безопасности на основе интеллектуальных вычислений».

Для разработки упомянутой онтологии кибербезопасности был использован тезаурус следующих нормативных документов:

- ГОСТ Р 53114-2008 «Обеспечение информационной безопасности в организации»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- стандарт ISO/IEC 27032:2012 «Руководящие указания по кибербезопасности»;
- стандарт ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

По мнению разработчика [4], предложенная онтология кибербезопасности отражает только один из начальных этапов рассмотрения проблемы кибербезопасности, так как не затрагивает такие сферы, как информационная безопасность, безопасность приложений, сетей, информационных систем и др. В связи с этим принято решение продолжить исследования для дальнейшей детализации рассмотренных понятий в их привязке к особенностям конкретных информационных систем и систем управления энергетическими объектами.

Работа И.Н. Пащенко, В.И. Васильева и М.Б. Гузаирова [8] основана на более общей онтологии энергосистем Smart Grid — Gridpedia. К существующим классам и свойствам Gridpedia были добавлены классы и свойства онтологии кибербезопасности Т.Н. Ворожцовой [4]. При этом для лучшей наглядности основные классы и свойства упомянутой исход-

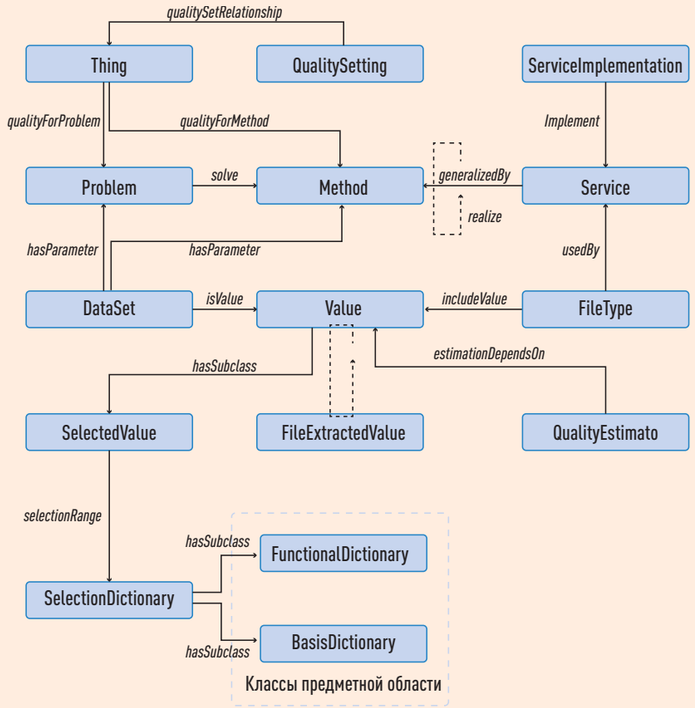
ной онтологии кибербезопасности были перегруппированы в соответствии с требованиями к созданию перспективных энергосистем Smart Grid.

Однако в условиях информационного противоборства требуется более совершенная онтология кибербезопасности Smart Grid, позволяющая упреждать приведение энергосистем к состояниям, чреватым катастрофическими последствиями.

Такая постановка задачи потребовала существенного пересмотра известной концепции обеспечения информационной безопасности Smart Grid. Дело в том, что современные энергосистемы, представляющие собой сложные распределенные гетерогенные системы, не обладают требуемой устойчивостью для целевого функционирования в условиях текущего и предполагаемого информационного противоборства из-за высокой сложности построения и потенциальной опасности недекларированного функционирования оборудования и общесистемного программного обеспечения, в том числе гипервизоров. Все еще недостаточно эффективны применяемые средства выявления и комплексной нейтрализации информационно-технических воздействий, сочетающих возможности совместного комбинированного применения технологий получения несанкционированного доступа, аппаратно-программных закладок и вредоносного программного обеспечения.

Более того, ни традиционные средства защиты информации на различных уровнях (Level 4 — ERP; Level 3 — MES; Level 2 — SCADA; Level 1 — ПЛК/РЗА; Level 0 — полевые устройства, включающие в свой состав традиционные средства: защиты от несанкционированного доступа, межсетевого экранирования, фильтрации трафика (Modbus, OPC, МЭК 104), обнаружения и предупреждения кибератак (IDS/IPS), антивирусной защиты, криптографической защиты информации, анализа защищенности, контроля целостности и управления кибербезопасностью в целом на основе SCIRT/CERT/SOC), ни известные средства обеспечения устойчивости энергосистем, использующие возможности резервирования, эталонирования и реконфигурации, уже не пригодны для обеспечения требуемой работоспособности перспективных энергосистем Smart Grid в условиях информационного противоборства (рис. 2 на с. 66).

СТРУКТУРА КЛАССОВ ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ



Problem — задача, решаемая в рамках предметной области.
Method — метод, обеспечивающий решение поставленной задачи.
Service — вычислительный сервис, реализующий данный метод.
ServiceImplementation — экземпляр сервиса, доступный в составе программного комплекса.
DataSet — набор входных или выходных данных для заданного метода или решаемой задачи.
Value — величины предметной области, используемые в качестве входных и выходных данных для решения задач. Выделяется два специфических класса величин, различающихся способом их задания:

- FileExtractedValue — извлекаемые из файлов величины (способ извлечения описан в виде класса (в исходном коде компонента), реализующего унифицированный интерфейс IfileValueExtractor).
- SelectedValue — величины, выбираемые из списка доступных (список доступных значений задается в составе онтологии индивидами, относящимися к подклассам класса SelectionDictionary).

FileType — файл, содержащий доступные для извлечения значения.

Рис. 5

СООТВЕТСТВИЕ МЕЖДУ ГРАФИЧЕСКИМИ ПРИМИТИВАМИ IDEF5 И UML

IDEF5		UML	
Название элемента	**Изображение**	**Название элемента**	**Изображение**
Тип (класс)	Метка типа	Класс	Имя класса
Индивид	Метка индивида	Экземпляр	Имя экземпляра
Двуместные отношения первого порядка part-of		Агрегатная ассоциация	
Двуместные отношения первого порядка subkind-of		Отношения обощения, is-a	
Переход между состояниями		Переход между состояниями	Событие
Процесс	Метка процесса	Состояние действия	Действие
Маркер мгновенного перехода		Нетриггерные переходы	

Таблица 3

Для разработки новой онтологии кибербезопасности был проведен анализ вероятных сценариев проведения целенаправленного информационного воздействия на перспективные энергосистемы Smart Grid. Рассмотрена типовая структура упомянутых энергосистем и дана характеристика их уязвимостей. Выявлены особенности реализации угроз безопасности и возможные риски нарушения работоспособности типовой энергосистемы, определена специфика осуществления информационно-технических воздействий на критически важные элементы перспективных энергосистем [9–14].

Проведен критический анализ существующих методов и средств по обнаружению и нейтрализации информационно-технических воздействий, в том числе целевых или таргетированных атак, APT. Дана оценка пригодности традиционным средствам защиты информации энергосистем для предупреждения, обнаружения и нейтрализации информационно-технических воздействий. Показаны недостатки организации применяемых средств обеспечения и контроля политики кибербезопасности на основе IEC 62351-8.

Выявлено несовершенство традиционных средств контроля и восстановления работоспособности энергосистем Smart Grid. Исследованы пути обеспечения устойчивости функционирования энергосистем при враждебных массовых информационно-технических воздействиях. Проведен критический анализ подходов и методов обеспечения устойчивости процессов функционирования энергосистем при их дестабилизации. Выработана идеология поддержания работоспособности энергосистем Smart Grid на основе иммунитета. Формализованы цель и задачи обеспечения устойчивости упомянутых перспективных энергосистем в условиях информационного противоборства [10, 14].

В результате была предложена онтология кибербезопасности самовосстанавливающихся Smart Grid, которая позволяет описать организацию самовосстановления перспективных энергосистем в условиях информационного противоборства на основе

иммунитета на возмущения по аналогии с иммунной системой защиты живого организма.

Актуальность такой новой онтологии кибербезопасности Smart Grid подтверждается требованиями (рис. 3 на с. 67) следующих нормативных документов:

- Доктрина информационной безопасности России, 2016 г.;
- ФЗ «О безопасности критической информационной инфраструктуры»;
- «Основные направления государственной политики в области обеспечения безопасности АСУ ТП КВО РФ», Совет Безопасности РФ;
- Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- Проекты документов ФСТЭК по защите АСУ ТП 2017 г.:

1. Меры защиты в АСУ ТП;
2. Методика определения угроз безопасности информации в АСУ ТП;
3. Порядок выявления и устранения уязвимостей в АСУ ТП;
4. Порядок реагирования на инциденты, связанные с нарушением безопасности информации);

- ГОСТы Федерального агентства по техническому регулированию и метрологии «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы» (вступили в силу 01.01.2016 г.):

1. ГОСТ Р 56205-2014 IEC/TS 62443-1-1-200. Часть 1-1. «Терминология, концептуальные положения и модели»;
2. ГОСТ Р МЭК 62443-2-1-2015. Часть 2-1. «Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики»;
3. ГОСТ Р 56498-2015/IEC/PAS 62443-3: 2008. Часть 3. «Защищенность (кибербезопасность) промышленного процесса измерения и управления».

ПРЕДЛАГАЕМАЯ ОНТОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ

В настоящей статье под онтологией кибербезопасности самовосстанавливающихся энергосистем Smart Grid (далее — онтология кибербезопасности) понимается база повторно используемых знаний специального вида, или «спецификация концептуализации» такой трудно формализуемой предметной области, как обеспечение устойчивости функционирования перспективных энергосистем в условиях информационного противоборства. Это означает, что в этой предметной области необходимо, во-первых, выделить основные понятия (концепты), и, во-вторых, определить связи между ними (концептуализация). При этом онтология кибербезопасности может быть представлена как в графическом, так и в аналитическом виде (например, формальной грамматикой и языком программирования или некоторой математической моделью).

В нашей работе разработка обсуждаемой онтологии основывалась на двух различных методологических подходах. В первом для графического представления онтологии используется язык схем IDEF5 Schematic Language, а для аналитического описания — текстовый язык IDEF5 Elaboration Language (табл. 3 — сравнение IDEF5 и Unified Modeling Language). При этом автоматизация процесса моделирования онтологии кибербезопасности осуществлялась с помощью демонстрационного прототипа средства SBONT компании Knowledge Based Systems, Inc. Реализация этого методологического подхода заняла 5 лет (2000–2005 гг.). В настоящее время онтология кибербезопасности содержит описание более 800 терминов из области информационной безопасности (подготовлено два тома объемом 1284 страницы с текстом и графическими схемами). Вся база терминов постоянно поддерживается в актуальном виде.

Исходные данные для построения описываемой онтологии кибербезопасности были взяты из следующих российских нормативных документов и рекомендаций лучших международных организаций, а именно:

- Тезаурус нормативных документов «Доктрина информационной безопасности России» 2016 г., «Основные направления государственной политики в области обеспечения безопасности АСУ ТП КВО РФ» и «Система признаков критически важных объектов» Совета Безопасности РФ;
- Тезаурус ФЗ РФ № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», ФЗ РФ № 16-ФЗ от 09.02.2007 «О транспортной безопасности», ФЗ РФ № 256-ФЗ от 21.07.2011 «О безопасности объектов топливно-энергетического комплекса», ФЗ РФ № 116-ФЗ от 21.07.1997 «О промышленной безопасности опасных производственных объектов», ФЗ РФ № 170-ФЗ от 21.11.1995 «Об использовании атомной энергии», проект ФЗ «О безопасности критической информационной инфраструктуры»;
- Документы ФСТЭК Российской Федерации: Приказ № 31

от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- Документы 2007 г. («Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», «Положение о реестре ключевых систем информационной инфраструктуры»);
- Проекты документов 2016 г. (Меры защиты в АСУ ТП, Методика определения угроз безопасности информации в АСУ ТП, Порядок выявления и устранения уязвимостей в АСУ ТП, Порядок реагирования на инциденты, связанные с нарушением безопасности информации);
- ГОСТ Р 53114-2008 «Обеспечение информационной безопасности в организации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Федерального агентства по техническому регулированию и метрологии «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы» (вступил в силу 01.01.2016 г.):
- ГОСТ Р 56205-2014 IEC/TS 62443-1-1-200. Часть 1-1. «Терминология, концептуальные положения и модели»;
- ГОСТ Р МЭК 62443-2-1-2015. Часть 2-1. «Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики»;
- ГОСТ Р 56498-2015/IEC/PAS 62443-3: 2008. Часть 3. «Защищенность (кибербезопасность) промышленного процесса измерения и управления»;
- ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

Заметим, что последний ГОСТ, помимо всего прочего, определяет состав сведений об уязвимостях, которые разработчики средств контроля защищенности должны включать в базу данных своих решений. При этом данный документ учитывает уже имеющуюся практику и инструменты описания уязвимостей, такие как классификатор типов уязвимостей Common Weakness Enumeration (CWE), язык формального описания Open Vulnerability and Assessment Language (OVAL), методику оценки степени опасности уязвимости Common Vulnerability Scoring System (CVSS), ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем».

ЛИТЕРАТУРА

1. Концепция развития интеллектуальной электроэнергетической системы России с активно-адаптивной сетью. ОАО «ФСК ЕЭС» ОАО «НТЦ электроэнергетики». М., 2011.
2. Отчет о выполнении проекта реализации технологической платформы «Интеллектуальная энергетическая система России» (ТП ИЭС) в 2014 г. и план действий ТП ИЭС на 2015 г. М., 2015.
3. Бирюков Д.Н., Ломако А.Г., Ростовцев Ю.Г. Облик антиципирующих систем предотвращения рисков реализации киберугроз // Труды СПИИРАН. 2015. Вып. 39. С. 5–25.
4. Ворожцова Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности // Онтология проектирования. 2014. № 4 (14). С. 69–77.
5. Клещев А.С., Артемьева И.Л. Математические модели онтологий предметных областей. Ч. 2. Компоненты модели // НТИ. Сер. 2. 2001. № 3. С. 19–29.
6. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью / Труды ИСА РАН, 2009. Т. 41. Управление рисками и безопасностью. С. 74–103.
7. Массель Л.В. Проблемы создания Smart Grid в России с позиций информационных технологий и кибербезопасности / Труды Всероссийского семинара с международным участием «Методические вопросы исследования надежности больших систем энергетики»: Вып. 64. Надежность систем энергетики: достижения, проблемы, перспективы. Иркутск: ИСЭМ СО РАН, 2014. С. 171–181.
8. Пащенко И.Н., Васильев В.И., Гузаиров М.Б. Защита информации в сетях Smart Grid на основе интеллектуальных технологий: проектирование базы правил // Известия ЮФУ. Технические науки. 2015. С. 28–37.
9. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / Под общей ред. С.Ф. Боева. Университет Иннополис. СПб.: Издательский дом «Афина», 2017.
10. Петренко С.А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия / Труды ИСА РАН, 2009. Т. 41. Управление рисками и безопасностью. С. 104–146.
11. Петренко С.А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий / Труды ИСА РАН, 2009. Т. 41. Управление рисками и безопасностью. С. 175–193.
12. Петренко С.А. Методы обнаружения вторжений и аномалий функционирования киберсистем / Труды ИСА РАН, 2009. Т. 41. Управление рисками и безопасностью. С. 194–202.
13. Петренко С.А. Модель киберугроз по аналитике инноваций DARPA / Труды СПИИРАН. 2015. Вып. 39. С. 26–41.
14. Петренко С.А. Проблема устойчивости функционирования киберсистем в условиях деструктивных воздействий / Труды ИСА РАН, 2010. Т. 52. Управление рисками и безопасностью. С. 68–105.