НОВАЯ ОНТОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ САМОВОССТАНАВЛИВАЮЩИХСЯ ЭНЕРГОСИСТЕМ SMART GRID. ЧАСТЬ II

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)

В настоящее время 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.

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

Технология интеллектуальных, или «умных» энергосистем 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)

В настоящее время в развитых странах мира активно разрабатывается технология интеллектуальных, или «умных», энергосистем — Smart Grid. Эта технология предназначена для оптимизации процессов доставки электроэнергии потребителю с помощью современных цифровых технологий. Считается, что эта технология существенно повысит качество энергосбережение, будет способствовать сокращению издержек и повышению надежности сетей и прозрачности процесса управления электроэнергетической индустрии. Однако такой подход порождает новые специфические проблемы, в частности — проблему защиты всей электроэнергетической системы от посторонних «информационных» воздействий, направленных на нарушения процессов управления сетями, иными словами — проблема кибербезлпасности «умных», энергосистем.

В данной статье обсуждаются концептуальные основы обеспечения самовосстановления перспективных энергосистем в условиях роста угроз информационной безопасности. В первой части статьи (см. № 2 (37)) мы рассмотрели собственно проблему кибербезопасности и современные трактовки онтологии кибербезопасности. Во второй части статьи мы продолжаем обсуждать поднятые вопросы.

ПРЕДЛАГАЕМАЯ ОНТОЛОГИЯ КИБЕРБЕЗОПАСНОСТИ

(продолжение, начало см. в № 2 (37))

Кроме указанных в первой части статьи, использовались также следующие документы;

- Стандарты ISO/IEC 27000 в части общих принципов обеспечения безопасности цифровых систем управления. В том числе ISO/IEC 27032:2012 «Руководящие указания по кибербезопасности» и ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»; стандарты группы IEC TC57: IEC 61850, IEC60870, IEC 62351 в части безопасности коммуникационных протоколов; стандарт INL Cyber Security Procurement Language 2008;
- Рекомендации: NIST-800-82 г. 2 «Guide to Industrial Control Systems (ICS Security) — Руководство по обеспечению безопасности Систем управления технологическими объектами» 05.2015 г., Control Systems Security Program/ National Cyber Security Division (Каталог мер обеспечения безопасности систем управления. Рекомендации для разработчиков стандарта), IEC 62443 и ISA 62443 (документы Международной электротехнической комиссии (IEC) и 99 Комитета по разработке стандартов безопасности АСУ ТП Международного общества автоматизации (ISA), стандарты безопасности NERC CIP (Critical Infrastructure Protection) — Комплекс требований по безопасности критически важных объектов Североамериканского совета по надежности электрических сетей (NERC), Departament of Homeland Security: Cyber Security Procurement Language for ICS, Разработки US-CERT (руководства, модели угроз и нарушителей, регламенты реагирования на киберинциденты, базы уязвимостей и пр.

Разработка обсуждаемой онтологии кибербезопасности «умных энергосистем» была выполнена по шагам:

1. определение контекста онтологии кибербезопасности;
2. сбор данных — определение источников терминов и отбор терминов для онтологии кибербезопасности;
3. анализ данных — определение основных терминов и терминов элементов, отношений, вербальное описание терминов;
4. разработка онтологии кибербезопасности — создание схематического и аналитического описания упомянутой онтологии;
5. валидация онтологии кибербезопасности — проверка полноты и корректности онтологии, соответствие исходным требованиям.

Онтология кибербезопасности представлена графическими схемами на языке схем IDEF5 Schematic Language (524 схемы) и соответствующими аналитическими описаниями на текстовом языке IDEF5 Elaboration Language. Упомянутые аналитические описания онтологии кибербезопасности выполнены по шагам согласно ранее разработанной методике:

1. ввод обозначений основных и вспомогательных терминов кибербезопасности;
2. пояснение терминов-элементов с помощью несвязанных типов;
3. назначение каждому термину-элементу уникального идентификатора;
4. определение входных и выходных связей для каждого термина;
5. фиксация соединений элементов;
6. проверка корректности описаний.
7. при необходимости корректировка и уточнение описаний.

Во втором методологическом подходе, для представления онтологии кибербезопасности в контексте семантической паутины (web 3.0)

использованы методические рекомендации консорциума W3C (The World Wide Web Consortium) [22–24]. По времени реализация второго подхода заняла 4 года (2006–2010 гг.). Для описания иерархии возможных онтологий кибербезопасности Smart Grid с памятью используется язык OWL, предоставляющий возможность детального описания классов онтологии, индивидов, относящихся к данным классам, а также существующих связей между ними. Данный язык расширяет возможности языка RDF, предоставляющего возможность оперировать базовыми структурами «субъект — предикат — объект», а также языка RDFS, задающего базовые структуры и отношения между классами и индивидами. При этом для обеспечения возможности описания сложных связей между индивидами онтологии кибербезопасности Smart Grid используется вариант языка OWL DL (см. табл. 4).

Это позволило использовать перечислимые типы для описания фиксированных словарных структур базы знаний предметной области, определять множественные связи для задания связей «многие ко многим», применять логические (булевы) комбинации классов для определения связей сложной структуры онтологии кибербезопасности Smart Grid с памятью. Было показано, что язык OWL позволяет задать различные представления упомянутой онтологии кибербезопасности.

Было принято решение об использовании представления OWL в синтаксисе языка XML, как наиболее распространенного и удобного для автоматической обработки и анализа текстов онтологий кибербезопасности соответствующими программными средствами. В листинге 1 приведен пример описания онтологии кибербезопасности с использованием указанного синтаксиса:

Для интеграции отдельных частей онтологии кибербезопасности использовано включение онтологий друг в друга на уровне языка (конструкция *owl:imports*). Это позволило описать базовые концепты, связи и индивиды, относящиеся к названной предметной области.

ПРИМЕР ПРЕДСТАВЛЕНИЯ ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ

```
<?xml version="1.0"?>

<!DOCTYPE rdf:RDF [
  <!ENTITY dl-safe "http://owldl.com/ontologies/dl-safe.owl#">
  <!ENTITY swrl  "http://www.w3.org/2003/11/swrl#" >
  <!ENTITY owl "http://www.w3.org/2002/07/owl#" >
  <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#" >
  <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#" >
  <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#" >
  <!ENTITY ruleml  "http://www.w3.org/2003/11/ruleml#" >
  <!ENTITY escience "http://escience.sec.ru/escience.owl#" >
]>

<rdf:RDF
  xml:base="http://escience.sec.ru/escience.owl#"
  xmlns="http://escience.sec.ru/escience.owl#"
  xmlns:owl="http://www.w3.org/2002/07/owl#"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
  xmlns:swrl="http://www.w3.org/2003/11/swrl#"
  xmlns:ruleml="http://www.w3.org/2003/11/ruleml#">

  <!-- Область знаний -->
  <owl:Class rdf:ID="FieldOfKnowledge"/>

  <!-- Метод решения -->
  <owl:Class rdf:ID="Method"/>

  <!-- Задача -->
  <owl:Class rdf:ID="Problem"/>

  <!-- Набор данных (входных или выходных) -->
  <owl:Class rdf:ID="DataSet"/>
```

Листинг 1

СООТВЕТСТВИЕ МЕЖДУ ПРИМИТИВАМИ OWL И UML

OWL-тэг	Название элемента в UML
<owl: Class rdf:ID= "...">	Класс
<wl: Thing rdf: ID= "...">	Экземпляр
<owl: ObjectProperty rdf: I D= "... ">	Отношение
<owl:DatatypeProperty rdf:ID="...">	Атрибут

Таблица 4

ПРИМЕР ПРЕДСТАВЛЕНИЯ ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ (ПРОДОЛЖЕНИЕ)

```
<!-- Генерализация метода -->
<owl:ObjectProperty rdf:ID="generalizedBy">
  <rdf:type rdf:resource="&owl;TransitiveProperty"/>
  <rdfs:domain rdf:resource="#Method"/>
  <rdfs:range rdf:resource="#Method"/>
</owl:ObjectProperty>

<!-- Параметризация метода -->
<owl:ObjectProperty rdf:ID="hasParameter">
  <rdfs:domain>
    <owl:Class>
      <owl:unionOf rdf:parseType="Collection">
        <owl:Class rdf:about="#Method"/>
        <owl:Class rdf:about="#Problem"/>
      </owl:unionOf>
    </owl:Class>
  </rdfs:domain>
  <rdfs:range rdf:resource="#DataSet"/>
</owl:ObjectProperty>

<!-- Входной параметр -->
<owl:ObjectProperty rdf:ID="hasInput">
  <rdfs:subPropertyOf rdf:resource="#hasParameter"/>
</owl:ObjectProperty>

<!-- Выходной параметр -->
<owl:ObjectProperty rdf:ID="hasOutput">
  <rdfs:subPropertyOf rdf:resource="#hasParameter"/>
</owl:ObjectProperty>

</rdf:RDF>
```

Листинг 1

Для динамического расширения и модификации базы знаний используется описание правил построения связей на языке SWRL, интегрируемом в состав онтологий, сформированных на языке OWL. Правила используются для описания динамических отношений между индивидами онтологий, возникающих при наличии определенных условий. Так, например, подобные отношения могут описывать применимость метода для решения поставленной задачи обеспечения требуемой устойчивости Smart Grid в условиях информационного противоборства в зависимости от характеристик входных данных. Использование построения динамических отношений совместно с включением онтологии делает возможным реализацию частичного логического вывода уже на уровне интерпретации онтологической структуры. Для этого набор активных фактов, формируемый в процессе взаимодействия с пользователем, оформляется в виде отдельной онтологии, использующей включение базовой онтологической структуры. Интерпретация полученной структуры позволяет осуществить анализ базовой онтологической структуры с учетом введенных фактов.

Для выполнения запросов к онтологической структуре используется язык SPARQL, позволяющий с использованием существующих средств интерпретации онтологической структуры произвести анализ онтологии кибербезопасности Smart Grid с памятью (включая построение динамических отношений на основании правил). Пример запроса приведен в листинге 2.

ПРИМЕР СТРУКТУРЫ ОНТОЛОГИИ

Приведем возможную структуру онтологии кибербезопасности для описания совокупности знаний, используемых при организации самовосстановления «умных энергосистем» Smart Grid в условиях роста угроз информационной безопасности. Упомянутая структура была апробирована в 2012–2017 гг. в рамках совместных исследований по проблематике кибербезопасности, проводимых в АО «РТИ», МФТИ, а также Академии имени А.Ф. Можайского.

В составе онтологии выделим два основных слоя: описание концептов (классов) и индивидов, реализующих концепты. При этом индивиды могут быть связаны отношениями, определенными на уровне концептов. Кроме того, допустимы отношения между отдельными концептами (например, отношение генерализации). В простейшем случае множество отношений может быть ограничено двумерными отношениями. Еще одним элементом онтологии являются атрибуты (характеристики) индивидов, детализирующие их описание. Кроме того, одним из возможных расширений является ассоциация характеристик не только с индивидами (как реализациями классов), но и со связями между ними (как реализации классов допустимых связей).

Формально слой классов онтологии определяется как граф $O = \langle C, R \rangle$, где C — множество классов, R — множество абстрактных отношений, свя-

ПРИМЕР ЗАПРОСА К ОНТОЛОГИЧЕСКОЙ СТРУКТУРЕ

```
PREFIX nano: <http://escience.ru/sec.owl#>
PREFIX escience: <http://escience.ru/escience.owl#>
PREFIX rdf: <http://www.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www. org/2000/01/rdf-schema#>

SELECT ?E ?L ?C WHERE {
  ?E rdf:type escience:DataSet .
  ?E rdfs:label ?L .
  OPTIONAL {?E rdfs:comment ?C} .
  nano:Hf escience:hasInput ?E .
  ?E escience:isValue ?V .
  ?V rdf:type escience:SelectedValue
}
```

Листинг 2

зывающих классы. Аналогично слой индивидов онтологии определяется как граф $\widetilde{O} = \langle \widetilde{C}, \widetilde{R} \rangle$, где $\widetilde{C}$ — множество индивидов, а $\widetilde{R}$ — множество отношений между индивидами. При этом для каждого элемента слоя индивидов определены:

а) отношение генерализации $gn^{(C)} : \widetilde{C} \to C$, $gn^{(R)} : \widetilde{R} \to R$, определяющее связь индивидов и связей между ними с соответствующими классами и связями классов;

б) «сторожевые» условия (guard condition), определяющие применимость элементов в данных условиях $gc^{(C)}(F) : \widetilde{C} \to \{0,1\}$, $gc^{(R)}(F) : \widetilde{R} \to \{0,1\}$, где F — множество активных фактов, определенных для текущей задачи;

в) функция критериальной оценки $k^{(C)}(F) : \{\widetilde{c} \in \widetilde{C} \mid gc^{(C)}(\widetilde{c}) = 1\} \to \Psi^{(C)}$, $k^{(R)}(F) : \{\widetilde{r} \in \widetilde{R} \mid gc^{(R)}(\widetilde{r}) = 1\} \to \Psi^{(R)}$, где $\Psi^{(C)}$ и $\Psi^{(R)}$ — соответственно пространство критериев оценки индивидов и отношений между ними.

Блок логического вывода позволяет определить способ решения поставленной задачи как кортеж $S=\{s_1, s_2 \ldots s_N\}$ фиксированной структуры, i-м элементом которого являются множества вида $s_i = \{\widetilde{c} \in \widetilde{C} \mid gn^{(C)}(\widetilde{c}) = c_i\}$, где последовательность классов $c_i \in C$ и требований к множествам s_i определяет общую структуру решения. Для оценки построенного решения по системе критериев применяется анализ графа $\widetilde{O}' = \langle \widetilde{C}', \widetilde{R}' \rangle : \widetilde{C}' = \bigcup_i s_i \cup \widetilde{C}_S$, где $\widetilde{C}_S$ — присоединенная система классов $\widetilde{C}_S = \left\{ \widetilde{c}_S \mid \widetilde{c}_S \notin \bigcup_i s_i, \exists \widetilde{c}_1 \in \bigcup_i s_i : rch(\widetilde{c}_S, \widetilde{c}_1) \right\}$, $rch(\widetilde{c}_S, \widetilde{c}_1)$ — отношение достижимости на графе $\widetilde{O}'$. Оценка $\widetilde{O}'$ осуществляется в пространстве критериев Ψ, определяемом пересечением множеств критериев, описывающих пространства $\Psi^{(C)}$ и $\Psi^{(R)}$.

Возможная схема формирования иммунитета на возмущения представлена на рис. 4 и 5 (см. часть I в № 2 (37)).

Структура базы данных накопленных иммунитетов задана моделью ADO.NET Entity Framework. Для организации доступа к базе данных построена библиотека, обеспечивающая доступ к экземплярам сущностей, хранящимся в базе данных, посредством ADO.NET Entity Framework. Этот подход обеспечил возможность обращения к базе данных как к набору взаимосвязанных коллекций, хранящих экземпляры классов, эквивалентных сущностям базы данных. Предложена реализация прямого доступа к онтологической структуре с использованием API программного средства Pellet (вариант RunLib). Реализуемый данным модулем интерфейс включает в себя следующие базовые методы работы с онтологической структурой:

На рис. 6 представлена общая схема взаимодействия реализации RunLib с интерпретатором онтологии.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы были выдвинуты и обоснованы концептуальные основы обеспечения самовосстановления перспективных энергосистем в условиях роста угроз информационной безопасности и разработана новая, более совершенная, онтология кибербезопасности самовосстанавливающихся энергосистем Smart Grid.

Сформированы базовые понятия, составляющие самовосстановление умных энергосистем. Определены содержания элементарного, сложного и возмущенного процессов функционирования энергосистемы.

Выявлены характерные особенности единичных, групповых и массовых возмущений. Предложена модель самовосстановления перспективных энергосистем с привлечением формального аппарата теории динамических систем Р.Е. Калмана. Введена и раскрыта идеология функционирования энергосистем Smart Grid с памятью для привития иммунитета к возмущениям. Рассмотрено общее представление иммунной системы, обеспечивающей устойчивость функ-

СХЕМА ВЗАИМОДЕЙСТВИЯ РЕАЛИЗАЦИЙ

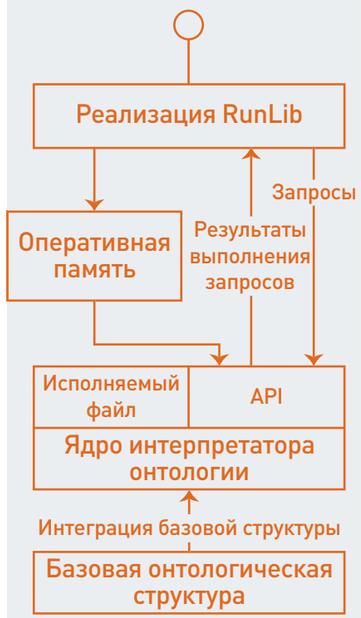

Рис. 6

ОРГАНИЗАЦИЯ САМОВОССТАНОВЛЕНИЯ SMART GRID

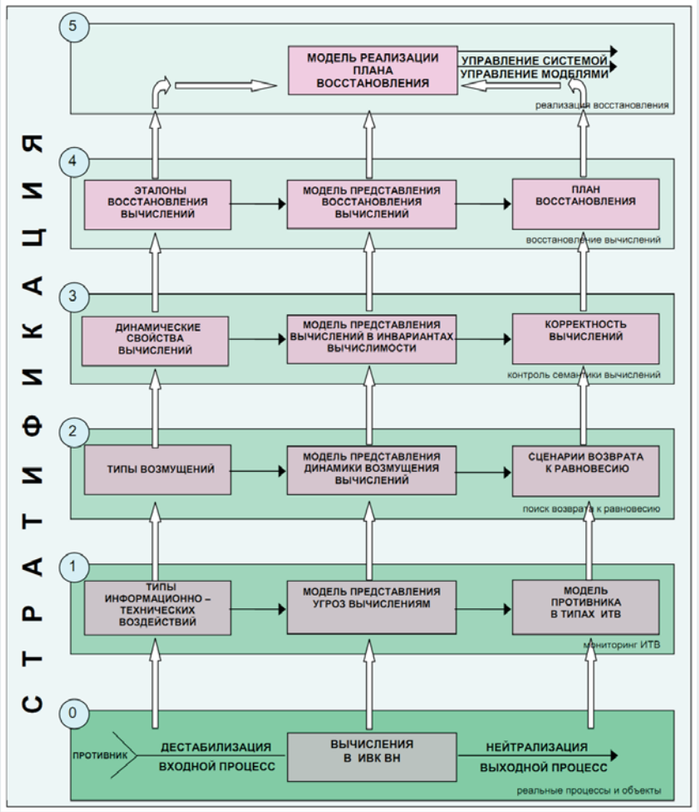

Рис. 7

реклама

КАБЕЛЬНЫЕ МУФТЫ

Произведено в России

Кабельные термоусаживаемые муфты до 10 кВ

Надежное решение для соединения и подключения подземных линий электропередачи

Концевые муфты наружной и внутренней установки

Соединительные муфты

- Для кабеля с бумажной маслопропитанной изоляцией
- Для кабеля с пластмассовой изоляцией с броней и без брони
- Широкий диапазон сечений от 16 до 240 мм²
- Комплектация болтовыми наконечниками и соединителями
- Комплект заземления брони под пайку или с пружинами постоянного давления

www.iek.ru

НАРОДНАЯ МАРКА

ИЗ ФЕДЕРАЛЬНОГО ЗАКОНА № 187-ФЗ «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РФ»

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

[...]

2. безопасность критической информационной инфраструктуры — состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;
3. значимый объект критической информационной инфраструктуры — объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

ционирования энергосистем Smart Grid в условиях роста угроз информационной безопасности [9–17].

Предложена стратификация самовосстановления перспективных энергосистем в условиях массовых и групповых информационно-технических воздействиях противника (см. рис. 7). Рассмотрены организация мониторинга фактов дестабилизации и определение типа и характера их возмущения. Проведен анализ динамики возмущений и выработаны решения по возврату к равновесию. Выработан абстрактный план самовосстановления. Предложена реализация иммунной системы, обеспечивающей восстановление энергосистемы после возмущений. В соответствии с выдвинутой концепцией на основе теории идентификации и контроля сложных технических систем представлена обобщенная постановка задачи разработки соответствующей интеллектуальной подсистемы обеспечения кибербезопасности Smart Grid [3, 9–17].

Осуществлен выбор научно-методического аппарата, пригодного для решения задач организации самовосстановления Smart Grid. Обосновано применение теории многоуровневых иерархических систем для проектирования упомянутой интеллектуальной подсистемы кибербезопасности. Предложено использование теории формальных языков и грамматик для порождения и распознавания возможных типов структур массовых возмущений. Обоснованы возможности применения теории катастроф для анализа динамики поведения возмущенных процессов функционирования энергосистем по аналогии с моделированием возмущений в живой природе. Предложено формирование иммунитета к деструктивным возмущениям с привлечением результатов теории контроля и восстановления процессов функционирования энергосистем Smart Grid [3, 9].

В результате, это позволяет разработать системный облик перспективной интеллектуальной подсистемы обеспечения кибербезопасности «умных энергосистем» Smart Grid в типах моделей тех теорий, которые позволяют синтезировать искомую структуру самовосстановления, конструировать и исполнять соответствующий план самовосстановления в условиях роста угроз информационной безопасности.

ЛИТЕРАТУРА

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.
15. Петренко С.А. Способы обеспечения устойчивости функционирования киберсистем в условиях деструктивных воздействий // Труды ИСА РАН, 2010. Т. 52. Управление рисками и безопасностью. С. 106–151.
16. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность (Информационные технологии для инженеров). М.: ДМК-Пресс, 2005.
17. Ступин Д.Д., Петренко С.А. Концепция создания когнитивной системы раннего предупреждения о компьютерном нападении. В сб.: Суперкомпьютерные технологии (СКТ-2016) // Материалы 4-й Всероссийской научно-технической конференции. В 2-х т. 2016. С. 103–107.
18. Поспелов Д.А. Мышление и автоматы. М.: Советское радио, 1972.
19. Jaquith A. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison Wesley, 2007.
20. Gruber T. Toward Principles for the Design of Ontologies Used for Knowledge Sharing // International Journal Human-Computer Studies — Elsevier, 1995.
21. Guarino N. Formal Ontology and Information Systems. In Proceeding of International Conference on Formal Ontology in Information Systems (FOIS'98), N. Guarino (ed.), Trento, Italy, June 6–8, 1998. Amsterdam, IOS Press, pp. 3–15.
22. Microsoft — Smart Energy Reference Architecture V2.0, March 2013.
23. Smart Grid Reference Architecture, SCE□Cisco□IBM SGRA Team July 14, 2011.
24. W3C, "Rdf vocabulary description language 1.0: Rdf schema," 2004.
25. W3C (2004) OWL Web Ontology Language Overview. http://www.w3.org/TR/owl-features.
26. Denker G., Kagal L., Finnin T. Security in the Semantic Web using OWL // Information Security Technical Report. 2005. No. 10(1). Pp. 51–58.

INNOPROM
KOREA
Partner Country 2018
9–12 июля 2018,
Екатеринбург
МЕЖДУНАРОДНАЯ ПРОМЫШЛЕННАЯ ВЫСТАВКА **ИННОПРОМ – 2018**
ТЕМА:
ЦИФРОВОЕ ПРОИЗВОДСТВО
600 индустриальных компаний-экспонентов
50 000 посетителей
95 стран мира
160 мероприятий деловой программы
Организатор МИНПРОМТОРГ РОССИИ
Оператор business event ГРУППА КОМПАНИЙ FORMIKA
Реклама 12+