

УДК 004.896, 004.414.2

С. В. Лебедев, М. Г. Пантелеев

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Д. В. Скориков

Научно-инженерный центр Санкт-Петербургского электротехнического университета (АО «НИЦ СПб ЭТУ»)

Построение онтологических баз знаний для информационно-аналитического сопровождения международных договоров и соглашений в военной области

Обсуждаются вопросы построения баз знаний для сопровождения международных договоров и соглашений в области ограничения и сокращения вооруженных сил и вооружений с использованием онтологического подхода. Базы знаний используются для фиксации единого представления о текущем состоянии предметной области в формальном виде. Благодаря формализации представления могут обрабатываться ЭВМ и передаваться по сети. Единое формальное представление предметной области используется для принятия обоснованных и скоординированных решений организациями, обслуживающими международные договоры и соглашения. Построение таких баз представляет собой непрерывный процесс. Для его реализации предложена и реализована архитектура единой информационной системы. Архитектура построена на основе модели ситуационной осведомленности. Архитектура апробирована на фрагменте предметной области. Представлены примеры построения онтологий. Рассматриваются программные инструменты для построения, хранения, извлечения и визуализации знаний из онтологических баз знаний.

Ограничение и сокращение вооружений, единая информационно-аналитическая система, база знаний, онтологии

Ключевым фактором поддержания международной стабильности является система действующих многосторонних и двусторонних договоров и соглашений в области ограничения и сокращения вооруженных сил и вооружений (ДСОСВС) [1]. Реализация договоров предусматривает решение соответствующими органами военного управления широкого круга задач в рамках различных видов деятельности – уведомленческой, инспекционной и др. Эффективное решение этих задач требует развитой информационной поддержки с использованием единой интегрированной информационно-аналитической системы (ЕИАС). Ядром такой ЕИАС должна быть база знаний (БЗ), содержащая данные и знания обо всех аспектах сопровождаемых договоров и соглашений, включая информацию о состоянии объектов и размещаемых на них вооружений для всех государств-участников договоров и соглашений.

Важнейшим требованием к таким БЗ является эффективная поддержка работы со знаниями,

включая оценку, анализ и прогнозирование состояния вооруженных сил и вооружений по различным договорам, странам, видам вооружений и т. п. Перспективным подходом к построению баз знаний для информационно-аналитических систем с развитой поддержкой логического вывода является использование онтологий [2]. В последние годы данный подход находит все более широкое практическое применение, в том числе в информационно-аналитических системах, разрабатываемых в интересах МО РФ.

Краткая характеристика проблемной области и постановка задачи. Деятельность органов по сопровождению ДСОСВС характеризуется вовлеченностью в нее значительного числа участников (органов и подразделений) и необходимостью координации их усилий. Так, например, планирование инспекций должно опираться на текущие знания о состоянии вооруженных сил инспектируемой страны. Поскольку деятельность

по обеспечению различных договоров в общем случае реализуется разными органами и подразделениями, актуальной является задача формирования единого представления о текущем состоянии предметной области, позволяющего принимать обоснованные и скоординированные решения всеми участниками. Другой важной особенностью является необходимость постоянного и оперативного обновления единой БЗ о вооруженных силах и вооружениях всех государств-участников, поддерживающей комплексный анализ хода выполнения договоров и соглашений.

Эти обстоятельства позволяют рассматривать задачу построения единой модели предметной области для информационно-аналитического сопровождения договоров и соглашений с позиций обеспечения *ситуационной осведомленности* (situation awareness) в рамках концепции Системы систем [3]. Особенностью систем данного класса, в отличие от систем слияния данных [4], является ориентация на участие человека.

Одной из первых и наиболее известных моделей ситуационной осведомленности является модель Эндсли [5], [6]. Обеспечение ситуационной осведомленности предполагает получение данных из внешней среды (восприятие), их осмысление и прогнозирование событий. В БЗ при этом должно формироваться единое представление о текущем состоянии предметной области, отражающее ситуационную осведомленность. Таким образом, одной из основных задач построения ЕИАС является оперативное обновление БЗ с использованием одной из моделей ситуационной осведомленности.

Процесс построения полной БЗ для рассматриваемой ЕИАС, учитывающей потребности всех специалистов по всем договорам, является весьма сложной задачей, выходящей за рамки одной статьи. Поэтому в данной статье предлагаемый подход иллюстрируется на примере задачи учета данных, содержащихся во входящих уведомлениях по Договору о стратегических наступательных вооружениях (ДСНВ). Уведомления, в частности, содержат информацию о развертывании или сворачивании стратегических вооружений, количество которых регламентируется договором. Примером может служить уведомление о загрузке БРПЛ (баллистическая ракета подводной лодки) на подводную лодку.

В терминах модели ситуационной осведомленности Эндсли можно выделить следующие основные задачи:

– восприятие – получение уведомления в виде исходного (слабоструктурированного) текста и извлечение из него понятий предметной области;

– осмысление – связывание извлеченных понятий отношениями, их привязка к имеющимся знаниям, проверка согласованности новых и имеющихся знаний, обновление БЗ в соответствии с содержащейся в уведомлении информацией;

– прогнозирование возможного развития событий (в данной статье не рассматривается).

Технологии построения онтологических БЗ. Применение онтологий в задачах обеспечения ситуационной осведомленности нашло отражение в ряде работ, например [7], [8]. В настоящее время технологии онтологического инжиниринга активно развиваются и широко используются в области Семантического Веб. Семантический Веб – это область информационных технологий, в рамках которой исследователи и разработчики ставят своей целью сделать традиционный Веб доступным для машинной обработки. Основу технологий Семантического Веб составляют языки формального описания предметных областей в форме онтологий и языки выполнения запросов к таким описаниям.

Онтология представляет собой семантическую сеть, описывающую предметную область. В рамках Семантического Веб развитие получили такие языки для построения онтологий, как RDF/RDFS и OWL. Онтология на указанных языках представляет собой множество троек «субъект-предикат-объект». Основными элементами онтологического описания являются классы и свойства, составляющие терминологическую часть онтологии (TBox), и экземпляры классов, образующие множество конкретных утверждений (ABox). Язык OWL основан на дискрипционной логике, поддерживающей логический вывод для получения новых утверждений о предметной области. В качестве языка запросов к онтологиям используется SPARQL.

Кроме того, в области Семантического Веб активно развиваются инструменты для работы с онтологиями, наиболее известными из которых являются: TobBraid [9], Protégé [10] – графические редакторы онтологий; Ontodia [11] – веб-приложение для визуализации онтологий в виде графов; AllegroGraph [12], Blazegraph [13] – графовые базы данных для хранения онтологий, которые поддерживают возможность удаленных запросов на языке SPARQL.

Использование онтологий для построения БЗ имеет следующие преимущества:

- возможность формального описания предметной области, более близкого к представлениям экспертов, чем традиционные схемы баз данных;
- богатые выразительные возможности, возможность использования логического вывода, языков правил [14] и ограничений [15]. Кроме того, могут использоваться возможности графовых баз данных (например, AllegroGraph предлагает возможность использования на стороне базы языков Prolog и Lisp; Blazegraph позволяет использовать некоторые алгоритмы на графах, например поиск кратчайшего пути);
- простота расширения и изменения описания предметной области;
- онтологии поддерживают использование модельно-ориентированного подхода, позволяющего повысить эффективность проектирования и разработки программного обеспечения.

Основной недостаток подхода, опирающегося на технологии Семантического Веб, состоит в том, что предлагаемые инструменты продолжают активно развиваться и разработчики не гарантируют стабильность работы и сопровождения. Кроме того, не все разработчики открывают исходный код предлагаемых ими инструментов, некоторые инструменты остаются платными.

Рассмотренные технологии закрывают отдельные задачи, возникающие при создании информационной системы на основе БЗ: представление, хранение, извлечение и визуализация знаний. Тем не менее, остается задача интеграции этих технологий в единую предметно-ориентированную систему. Основой такой интеграции должна быть общая архитектура ЕИАС.

Архитектура онтолого-ориентированной ЕИАС. На рис. 1 представлен вариант архитектуры информационной системы, опирающейся на

технологии Семантического Веб. Пунктирными линиями обозначены элементы, относящиеся к этапу разработки.

Онтология формально описывает предметную область в терминах классов и отношений между ними. В данном случае это может быть иерархия классов стратегических вооружений или объектов их размещения. Кроме того, онтология содержит описание конкретных вооружений с уникальными собственными опознавательными знаками (СОЗ), однозначно идентифицирующими объект вооружения. В онтологии эта информация представляется экземплярами соответствующих классов вооружений. Для создания онтологий используются существующие редакторы.

В контексте решаемой задачи исходные данные представляют собой уведомления, предусмотренные тем или иным договором. Обработка уведомлений (данных) предусматривает:

- формализацию уведомлений переводом их в онтологическую форму;
- согласование уведомлений с онтологией предметной области;
- изменение онтологии предметной области в соответствии с уведомлениями.

Таким образом, основными информационными компонентами системы являются онтология уведомлений и онтология предметной области.

Формальное описание предметной области позволяет использовать модельно-ориентированный подход к проектированию и разработке программного обеспечения. Преимуществом данного подхода является возможность частичной автоматизации создания информационной системы, при этом предметно-зависимый программный код может быть сгенерирован по онтологии предметной области (компонент *Генератор* на рис. 1). Основы такого подхода описаны в [16].

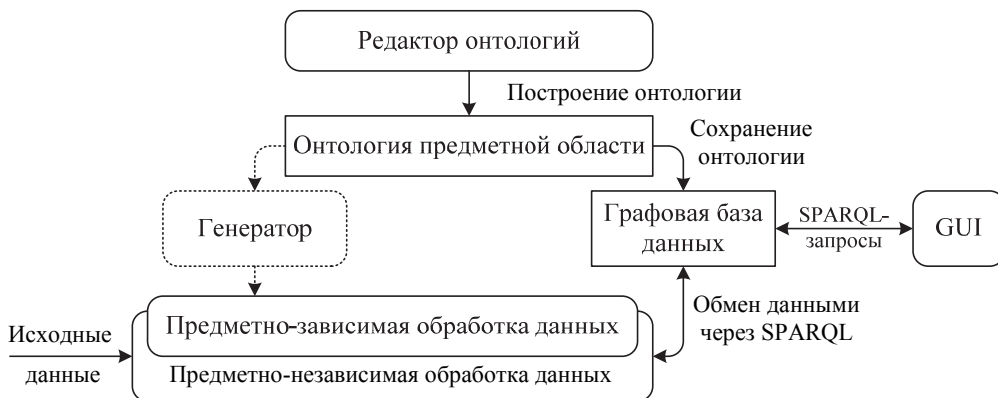


Рис. 1

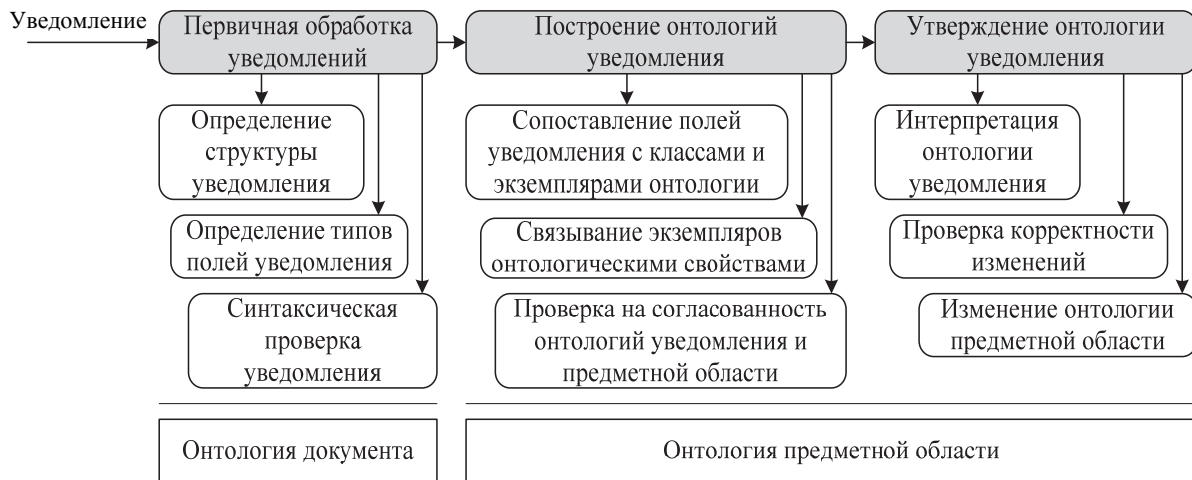


Рис. 2

Онтология, описывающая текущее состояние предметной области, сохраняется в графовой базе данных. Для работы с такими базами, как правило, используются SPARQL-запросы, позволяющие не только просматривать базу, но и изменять ее в соответствии с полученными уведомлениями.

Реализация онтолого-ориентированного учета входящих уведомлений. На основе предложенной архитектуры реализуется процесс учета входящих уведомлений, конечным результатом которого является изменение БЗ на основе полученной информации.

Процесс предусматривает ряд этапов (рис. 2). В терминах ситуационной осведомленности восприятию соответствует *первичная обработка уведомлений*, а осмыслению – *построение онтологии уведомления и утверждение онтологии уведомления*.

На этапе первичной обработки формируется объектное представление уведомления в виде программной структуры документа – дерева полей документа. Листьями такого дерева являются атомарные структуры, не подлежащие дальнейшему разбору, например СОЗ. При определении типов полей в общем случае требуется анализ структуры документа. На данном этапе синтаксическая проверка документа проводится без обращения к знаниям предметной области.

Для построения на основе программной структуры онтологического представления уведомления элементам программной структуры сопоставляются онтологические классы и экземпляры. Например, полю, содержащему строку с названием базы размещения подводных лодок, сопоставляется экземпляр, описывающий данную базу. Экземпляр является элементом БЗ и позволяет получить дополнительную информацию,

например состав находящихся на базе вооружений. Таким образом БЗ обеспечивает *обогащение* принятой информации априорными знаниями.

На следующем шаге онтологические классы и экземпляры, представляющие фрагменты уведомления, связываются онтологическими отношениями (свойствами) на основе содержащейся в уведомлении информации.

Рассмотрим пример. Пусть полученное уведомление ДСНВ содержит название базы подводных лодок и название подводной лодки. Каждому элементу по его названию сопоставляется экземпляр онтологии, представляющий конкретную базу или подводную лодку. На основе содержащейся в уведомлении дополнительной информации устанавливается, что указанная лодка находится на указанной базе. Вследствие этого соответствующие экземпляры связываются отношением «находится на».

Поле этого проверяются следующие условия согласованности онтологии уведомления и онтологии предметной области БЗ:

1. Указанные в уведомлении объекты представлены в онтологии предметной области и описываются свойствами с теми же значениями.

2. В онтологии предметной области экземпляры связаны так же, как объекты в уведомлении, например, подводная лодка действительно находится на указанной базе.

Для каждого уведомления строится две онтологии:

- онтология, описывающая фрагмент текущего состояния предметной области;

- онтология, описывающая состояние предметной области после внесения изменений, указанных в уведомлении.

Проверка согласованности может быть реализована как поиск подграфа, описанного онтологией уведомления, в онтологии предметной области.

На этапе утверждения онтологии уведомления для нее подбирается интерпретация, проверяется корректность изменений и модифицируется онтология предметной области.

Уведомление содержит формальное описание некоторого изменения в состоянии вооружений. Извлечение воспринимаемой пользователем семантики изменения выполняется с помощью интерпретации. Пример интерпретации: «в уведомлении сообщается о перемещении объекта вооружения». Каждая интерпретация также представлена онтологическим классом, экземпляр которого позволяет зафиксировать историю изменения предметной области.

Поиск подходящей интерпретации может быть реализован с использованием системы продукционных правил. При этом каждое правило должно подбирать для онтологий фрагменты исходного и конечного состояний предметной области действие (интерпретацию), которое бы привело к такому переходу.

На данном этапе может быть проверена корректность вносимых изменений. Например, корректность загрузки данного типа ракет в данный тип подводной лодки. Соответствующие ограничения могут быть зафиксированы на уровне онтологии благодаря поддержке логики.

Таким образом, онтологии позволяют проверить корректность уведомления, ее согласован-

ность с имеющимися знаниями и зафиксировать интерпретацию.

Кроме того, в самой онтологии предметной области могут быть зафиксированы ограничения, предписываемые соответствующим договором. Для этого может быть использован язык ограничения форм (SHACL, Shapes Constraint Language) [15]. Ограничения записываются на языке SPARQL, транслируются в OWL и связываются с классами онтологии, относительно которых необходимо проверять ограничения. Проверка ограничений вызывается для каждого экземпляра, по результатам проверки строится список экземпляров, относительно которых выявлены нарушения. Например, можно зафиксировать ограничение, по которому на определенном типе носителей не может быть размещено стратегическое вооружение.

Апробация подхода. Для апробации описанного подхода предложенная архитектура (см. рис. 1) была реализована на языке Java. В качестве редактора онтологий использовался TopBraid, графовой базы данных – Blazegraph.

На рис. 3 представлен фрагмент онтологии предметной области, отражающий текущие представления (визуализация выполнена с использованием Ontodia). На рисунке прямоугольники с буквой «С» обозначают классы. Остальные прямоугольники – экземпляры классов. Данный фрагмент описывает состояние предметной области, при котором подводная лодка «Род Айленд» типа «Огайо» с двумя пусковыми установками размещена на базе подводных лодок. На этой базе хранятся 4 БРПЛ типа «Трайдент II».

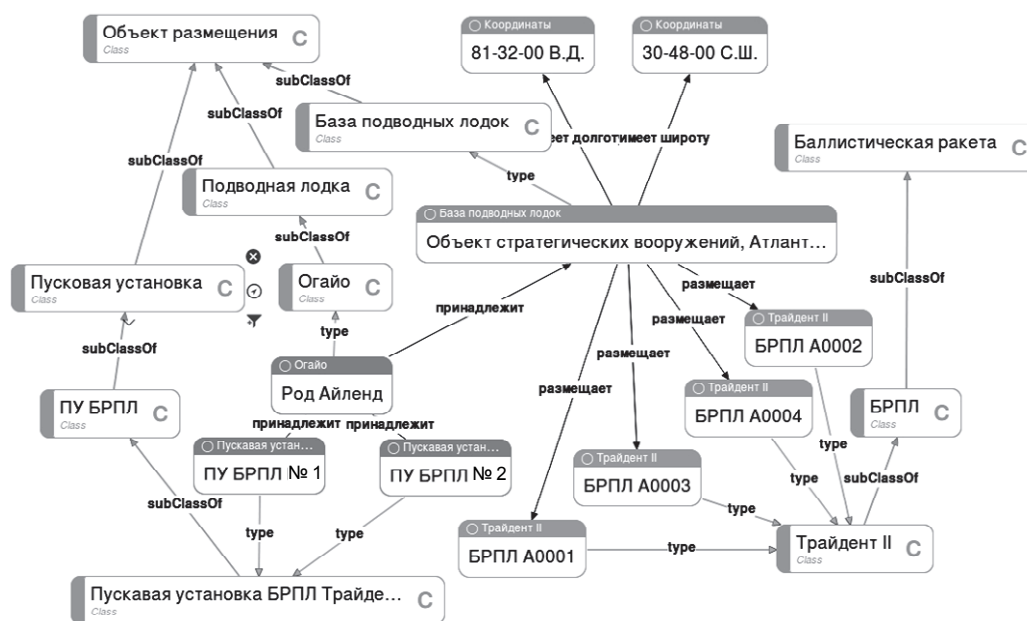


Рис. 3

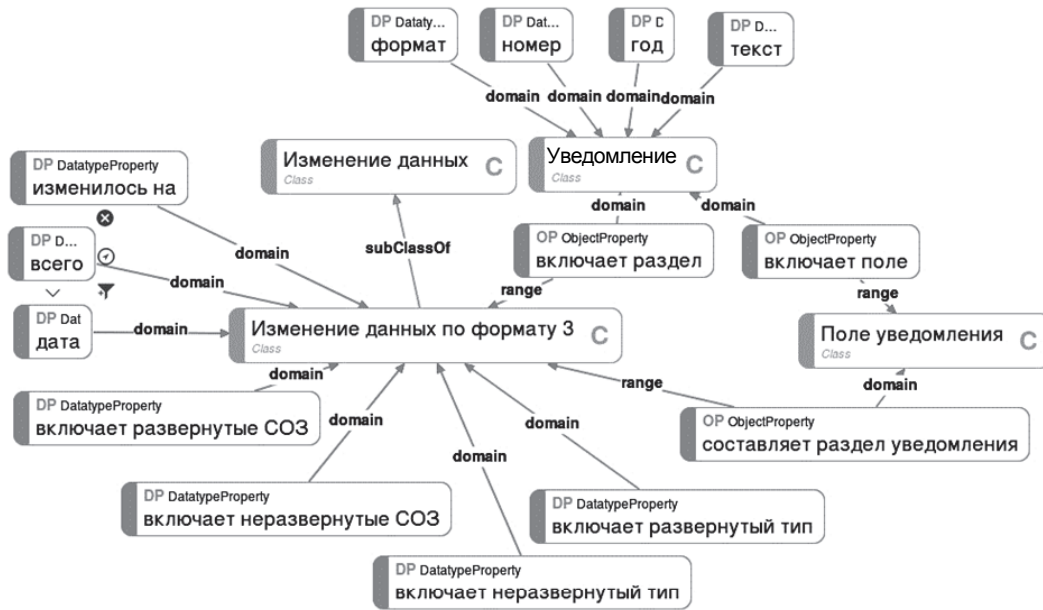


Рис. 4

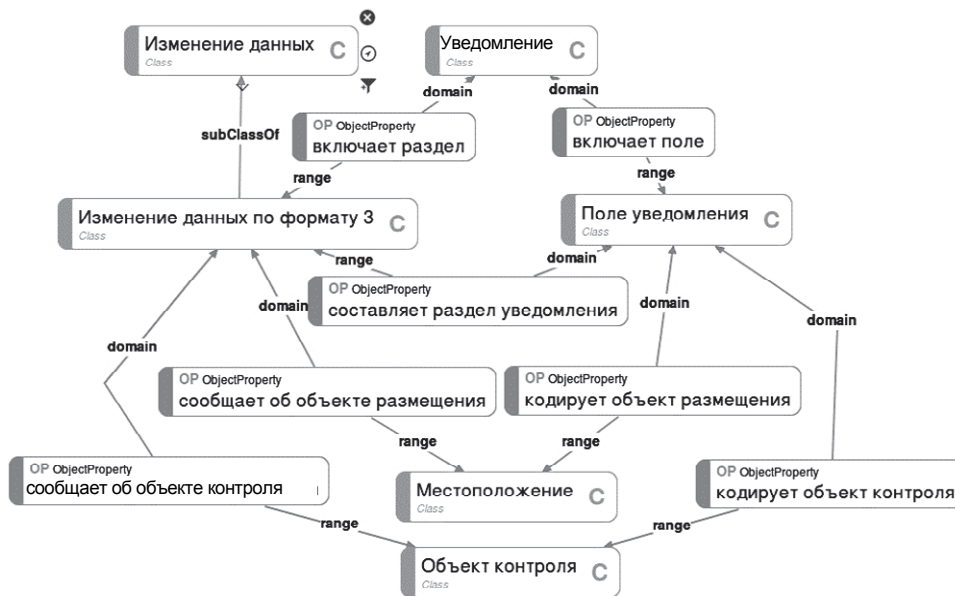


Рис. 5

В соответствии с описанным процессом (см. рис. 2) на первом этапе структурируется текст уведомления, проверяется его семантическая корректность. Для этого использованы текстовые анализаторы, построенные с помощью библиотеки ANTLR [17].

Далее на основе метаонтологии (рис. 4) строится онтология конкретного документа уведомления. Прямоугольники с буквами «DP» обозначают примитивные свойства, с буквами «OP» – объектные свойства, или отношения. Каждое уведомление разбивается на отдельные разделы и поля.

После того как онтология уведомления построена, ее отдельные элементы связываются с экземплярами онтологии предметной области. Для этого используются дополнительные отношения (рис. 5). Установление такой связи позволяет убедиться в существовании объектов, о которых говорится в уведомлении.

Далее с помощью продукционного правила строится онтология исходного и конечного состояний предметной области, подбирается интерпретация для указанного перехода. В качестве системы реализации продукционных правил выбрана система Drools [18]. На рис. 6 представлена общая структура правила.

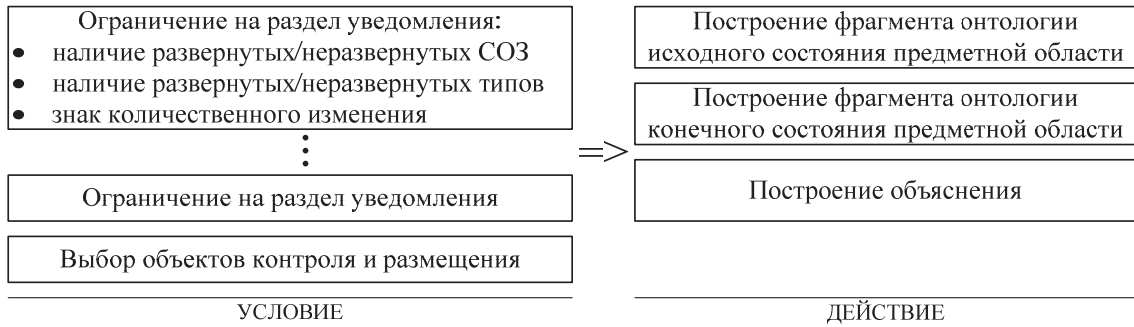


Рис. 6

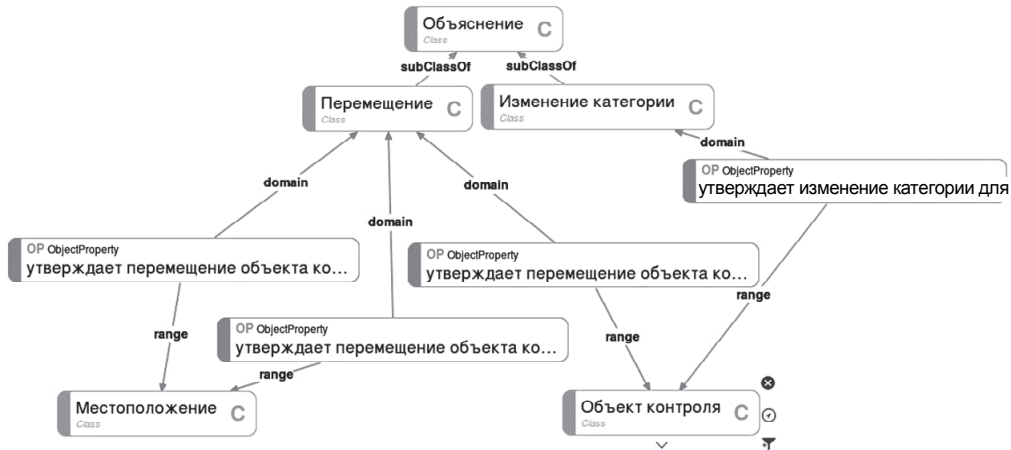


Рис. 7



Рис. 8

Онтология исходного состояния предметной области используется для проверки согласованности уведомления с текущим состоянием предметной области. Онтология конечного состояния позволяет проверить корректность действий, описываемых в онтологии, относительно имеющихся знаний.

На рис. 7 представлен фрагмент онтологии интерпретации уведомления. В соответствии с этим фрагментом экземпляр класса «Перемещение» может быть через соответствующие отношения связан с местоположением, с которого перемещается объект контроля, местоположением,

на которое перемещается объект контроля, и с самим перемещаемым объектом контроля.

На рис. 8 представлен фрагмент интерпретации рассматриваемого уведомления. В частности, в интерпретации утверждается перемещение БРПЛ с собственным опознавательным знаком «A0001» с базы подводных лодок в пусковую установку БРПЛ № 1, а также изменение категории для указанного объекта контроля.

На рис. 9 представлен фрагмент онтологии предметной области после применения изменений, описанных в уведомлении: БРПЛ с собственными

опознавательными знаками «А0001» и «А0002» перемещены с базы подводных лодок в пусковые установки подводной лодки «Род Айленд».

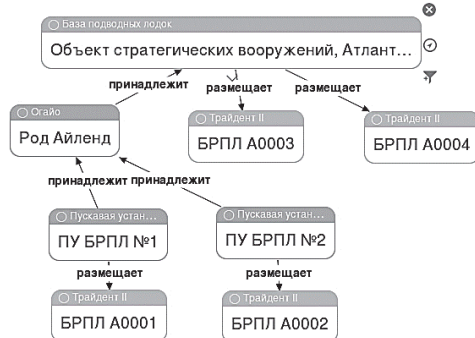


Рис. 9

Предложенный подход к построению БЗ позволяет поддерживать единое представление о текущем состоянии выбранной предметной области. Такое представление строится на основе постоянно поступающих данных и может быть ис-

пользовано экспертами для принятия обоснованных и скоординированных решений.

Использование онтологий позволяет работать со знаниями в виде, наиболее приближенном к представлениям экспертов. Так, применение языка SPARQL вместо SQL позволяет работать с понятиями и отношениями предметной области, а при использовании SQL работа идет с таблицами, являющимися единицами хранения информации, а не описания предметной области. Доступные инструментальные средства с развитым графическим интерфейсом позволяют значительно упростить создание и визуализацию таких онтологий.

Перспективы развития предложенного подхода связаны с внедрением средств автоматизации проектирования и разработки информационных систем. Общая идея автоматизации заключается в том, чтобы использовать онтологию предметной области для расширения и настройки предметно-независимого программного каркаса ЕИАС.

СПИСОК ЛИТЕРАТУРЫ

1. Антонов А. И. Контроль над вооружениями: история, состояние, перспективы. М.: Российская политическая энциклопедия (РОССПЭН), ПИР-Центр, 2012. 245 с.
2. R. Ferrario W. Kuhn. Formal Ontology in Information Systems // Proc. of the 9th Intern. Conf. (FOIS 2016). Amsterdam: IOS Press, 2016. 392 p.
3. Van de Laar P., Tretmans J., Borth M. Situation Awareness with Systems of Systems. New York: Springer-Verlag, 2013. 272 p.
4. Steinberg A. N., Bowman C. L. Revisions to the JDL Data Fusion Model // Handbook of Multisensor Data Fusion: Theory and Practice. Boca Raton: CRC Press, 2009. P. 44–67.
5. Salmon P. M., Stanton N. A., Jenkins D. P. Distributed situation awareness – Theory measurement and application to teamwork. Farnham: CRC Press, 2009. 266 p.
6. Endsley M. R. Toward a theory of situation awareness in dynamic systems // The J. of the Human Factors and Ergonomics Society. 1995. № 37 (1). P. 32–64.
7. Norbert B., Werner R. A Survey of Upper Ontologies for Situation Awareness // Proc. of the Intern. Conf. on Knowledge Sharing and Collaborative Engineering KSCE'06, 2006. Calgary: ACTA Press. 2006. P. 1–9.
8. Kokar M. M., Matheus C. J., Baclawski K. Ontology-based situation awareness // Information Fusion. Elsevier. 2009. № 10 (1). P. 83–98.
9. TopBraid IDE. URL: <https://www.topquadrant.com/tools/modeling-topbraid-composer-standard-edition/> (дата обращения 24.01.2019).
10. Protégé ontology editor. URL: <https://protege.stanford.edu/> (дата обращения 24.01.2019).
11. Ontodia – a platform to build web applications for exploration and visualization of graph data. URL: <http://ontodia.org/> (дата обращения 24.01.2019).
12. Semantic database engine. URL: <https://franz.com/agraph/allegrograph/> (дата обращения 24.01.2019).
13. Blazegraph database. URL: <https://github.com/blazegraph/database/> (дата обращения 24.01.2019).
14. A Semantic Web rule language (SWRL). URL: <https://www.w3.org/Submission/SWRL/> (дата обращения 24.01.2019).
15. Shapes constraint language (SHACL). URL: <https://www.w3.org/TR/shacl/> (дата обращения 24.01.2019).
16. Lebedev S., Panteleyev M. Ontology-Driven Situation Assessment System Design and Development in IoT Domains // IJERTCS. IGI Global. 2017. 8 (1). P. 1–17.
17. ANother Tool for Language Recognition (ANTLR). URL: <http://www.antlr.org/> (дата обращения 24.01.2019).
18. Drools – Business Rules Management System. URL: <https://www.drools.org/> (дата обращения 24.01.2019).

S. V. Lebedev, M. G. Panteleyev
Saint Petersburg Electrotechnical University «LETI»

D. V. Skorikov
Research and Engineering Center of Saint Petersburg
Electro-Technical University JSC (REC ETU SEC JSC)

CONSTRUCTION OF KNOWLEDGE BASES FOR ANALYTICAL WORK MAINTENANCE IN THE REALM OF INTERNATIONAL WEAPON REDUCTION TREATIES

A problem of developing the ontology-based approach for knowledge base maintenance in the realm of international weapon reduction treaties is discussed. Knowledge bases are used to support shared situation awareness that enables rational and coordinated decision making. Such knowledge bases are formalized with the help of ontology languages. Thanks to formalization such knowledge can be processed with machines and transmitted through a network. Knowledge bases are built continuously based on the incoming information. To support this process an ontology-based architecture is suggested. The architecture is evaluated on a Strategic Arms Reduction Treaty domain fragment. Examples of ontologies construction are shown. The usage of ontology-oriented instruments for building, storage, extraction and visualization of knowledge is demonstrated.

Weapon reduction treaties, unified information and analytical system, knowledge base, ontology

УДК 304.444

В. Гарате Гонзалес
Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Применение передовой методологии безопасности в беспроводных сетях

Предложена методология по улучшению безопасности беспроводных сетей, сформированная на основе методологии непрерывного совершенствования и практического опыта в данной отрасли с целью обеспечения высокого уровня безопасности при проектировании и развертывании беспроводных сетей. Рассматриваются способы защиты от распределенных беспроводных компьютерных атак и подчеркивается важность наличия политики беспроводной безопасности организации, а также компетентность персонала. Методология способствует формированию процессного подхода к созданию, внедрению, эксплуатации, мониторингу, проверке, поддержанию и совершенствованию политики безопасности беспроводных сетей организаций. Методология обеспечивает надежную модель для реализации принципов безопасности, регулирующих оценку рисков, разработку и реализацию мер безопасности, управление безопасностью и переоценку. Информационная безопасность играет важную роль в выравнивании бизнеса компании со своей стратегией информационной технологии, и в этом контексте информационная безопасность имеет первостепенное значение, поскольку она помогает компаниям внедрять экономически эффективные меры безопасности.

Беспроводные сети, проектирование, моделирование, методология, шифрование, беспроводная инфраструктура

В настоящее время беспроводные сети (WLAN) в стандарте 802.11, который был опубликован в 1997 г. Институтом инженеров по электротехнике и электронике (IEEE), по-прежнему являются одной из технологий, широко использу-

емых в любом сценарии, когда необходим обмен информацией (дома, на работе, в общественных и частных организациях, образовательных центрах) и можно воспользоваться предоставляемыми преимуществами (мобильность, масштабируе-