

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ С ПРИМЕНЕНИЕМ ОНТОЛОГИЙ

В. И. Воробьев, Т. В. Монахова

Санкт-Петербургский институт информатики и автоматизации РАН
199178, Санкт-Петербург, 14-я линия ВО, д. 39

<vvi@iias.spb.su>

УДК 681.3

В. И. Воробьев, Т. В. Монахова. Проектирование систем защиты с применением онтологий // Труды СПИИРАН. Вып. 2, т. 2. — СПб.: Наука, 2005.

Аннотация. *Рассмотрено применение онтологий в процессе проектирования системы информационной защиты предприятия. Приведены примеры возможного использования онтологий. — Библи. 4 назв.*

UDC 681.3

V. I. Vorobev, T. V. Monakhova. Designing of protection systems with ontologies application // SPIIRAS Proceedings. Issue 2, vol. 2. — SPb.: Nauka, 2005.

Abstract. *The ontologies application during designing system of information protection of the enterprise is considered. The examples of possible ontologies usage are given. — Bibl. 4 items.*

В данной статье рассмотрено использование онтологий при проектировании средств информационной защиты предприятий, а также приведены примеры использования онтологий путём указания некоторых их соответствующих элементов, поясняющие данную тему.

Проектирование системы защиты предприятия, как, впрочем, и любой крупной информационной системы, включает в себя несколько основных этапов. Первым и основным этапом является предпроектное обследование предметной области, то есть, применительно к системам защиты предприятий, самого предприятия, взаимосвязей его отделов и компонентов, а также сферы деятельности предприятия. На данном этапе возникает ряд трудностей, связанных с отсутствием единого тезауруса и словаря предметной области. В том случае, если эту проблему решить не удаётся или её решению не уделяется достаточного внимания, построение корректно работающей системы становится невозможным.

Для того, чтобы составить единое описание предметной области, применяется онтологический инжиниринг. Уточним, что же, собственно говоря, представляет собой онтология. Онтология определяет множество сущностей, описывающих и представляющих предметную область и логические выражения соотношений терминов друг с другом. Примем такое описание в соответствии с [2] как четверку вида

$$O = (E, D, R, P),$$

где E — множество сущностей (термины, классы, объекты, отношения и функции);

D — множество определений сущностей;

R — множество отношений между сущностями;

P — множество правил использования сущностей.

Онтологии применяются для описания классификаторов в базах данных и в приложениях для совместного использования информации предметной области. Онтологии используются для описания объектов с различной сложно-

стью структуры, от простой таксономии до метаданных и логических теорий, включая описание и пояснения элементов программного кода.

Онтологии позволяют определить описания для следующих видов концепций: классификация нескольких предметных областей; отношения между объектами; свойства или атрибуты, которые могут иметь объекты.

Онтологии обычно выражаются на логически основанном языке, имеющем чёткие различия между классами, свойствами и отношениями. Некоторые инструментальные средства поддерживают автоматизированное использование онтологий, и таким образом обеспечивает расширенные возможности в отношении интеллектуальных приложений типа концептуального и семантического поиска, программных агентов, поддержки решения, понимания естественного языка, управления знаниями, интеллектуальных баз данных и электронной торговли. Онтологии могут быть очень полезными для структурирования и определения значений терминов метаданных, что в настоящее время разрабатывается и стандартизируется.

Существуют различные программные средства для представления онтологий, например, VITA [2]. Одним из основных средств описания онтологий является OWL, *Ontology Web Language*. Язык OWL используется для формализации области определения классов и свойств этих классов путём определения элементов и утверждения свойств относительно них, а также причины относительно этих классов и элементов в степени, разрешенной формальной семантикой языка OWL.

OWL имеет несколько разновидностей: OWL Lite, OWL DL и OWL Full, различающиеся по своим функциональным возможностям. OWL Lite предназначена для построения классификационных иерархий и имеет сравнительно небольшие функциональные возможности. OWL DL был разработан для поддержки описательной логики, что ясно видно из названия (DL, *Description Logics*). Наконец, OWL Full имеет наиболее богатые функциональные возможности из всех перечисленных разновидностей.

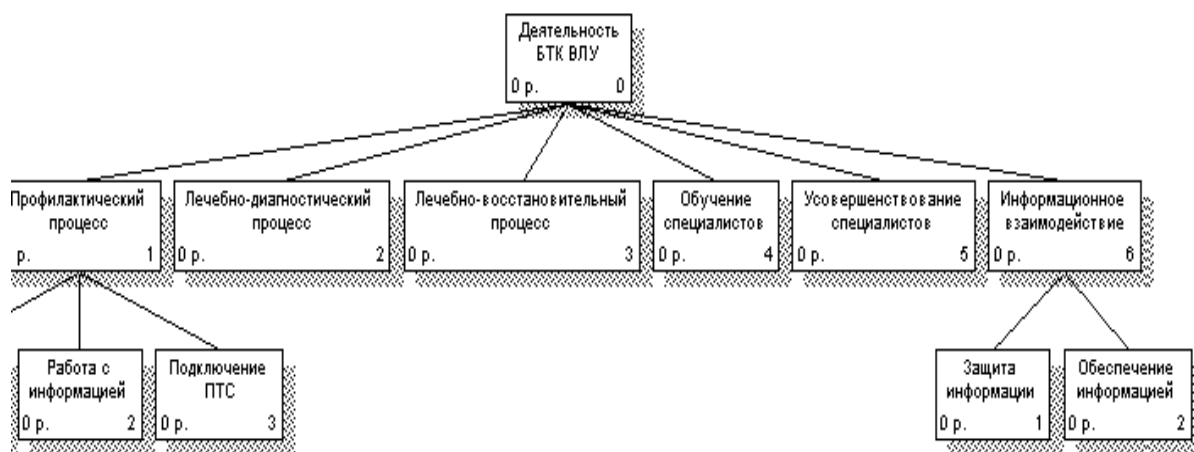


Рис. 1. Основные элементы деятельности военного лечебного учреждения.

Онтология, используемая в OWL, может включать описания классов, свойств и методов. Принимая такую онтологию, формальная семантика OWL определяет способы получения её логических последствий, то есть фактов, не присутствующих явным образом в онтологии, но вызванных семантикой. Это может быть основано на одном документе или множестве распределенных документов, которые были объединены, используя определенные механизмы OWL.

```

< Rdf:RDF
  Xmlns = " http: // www.w3.org/TR/2004/REC-owl-guide-200402 10/medical * "
  Xmlns:vin = " http: // www.w3.org/TR/2004/REC-owl-guide-200402 10/medical * "
  Xml:base = " http: // www.w3.org/TR/2004/REC-owl-guide-200402 10/medical * "
  Xmlns:comp = " http: // www.w3.org/TR/2004/REC-owl-guide-200402 10/comp * "
  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 * " >

```

Рис. 2. Декларация пространства имён онтологии.

```

< Owl:Ontology rdf:about = "" >
  <Rdfs:comment> пример онтологии OWL </rdfs:comment>
  < Owl:priorVersion rdf:resource = " http: // www.w3.org/TR/2003/PR-owl-guide-2003121
                                                                    5/medical " / >
  < Owl:imports rdf:resource = "http: // www.w3.org/TR/2004/REC-owl-guide-200402 10/comp " / >
  <Rdfs:label> Онтология Медицинского Учреждения </rdfs:label>

```

Рис. 3. Заголовок онтологии.

```

<owl:Class rdf:ID="Medical"/>
<owl:Class rdf:ID="Computer"/>

```

Рис. 4. Пример объявления классов.

Для того, чтобы пояснить, как и для чего могут использоваться онтологии, попробуем разобрать процесс построения онтологии медицинского учреждения [1]. Основные элементы деятельности этого объекта показаны на рис.1.

Модель рассматриваемой предметной области можно представить в виде:

$$M_{\Pi} = \langle F, T, U, I, R \rangle,$$

где $F = \{f_a \mid a = \overline{1, A}\}$ — множество функций системы; $T = \{t_j \mid j = \overline{1, J}\}$ — множество задач обработки информации; $U = \{u_k \mid k = \overline{1, K}\}$ — множество пользователей; $I = I^{\text{ex}} \cup I^{\text{bix}}$ — множество данных предметной области; $I^{\text{ex}} = \{i_x^{\text{ex}} \mid x \in X^{\text{ex}}\}$ — множество данных, необходимых для обеспечения информационных потребностей системы; $I^{\text{bix}} = \{i_x^{\text{bix}} \mid x \in X^{\text{bix}}\}$ — множество данных, являющихся результатом взаимодействия пользователей и функций системы; $R = \{r_l \mid l = \overline{1, L}\}$ — множество отношений между компонентами F, T, U, I .

На основе указанной модели осуществляем переход к описанию семантики онтологии: $O = \langle F, V, S, H \rangle,$

где F — множество функций, выполняемых системой; V — множество определений указанных функций; S — множество отношений между функциями; H — множество правил использования функций системы, что позволяет разделить её на составляющие элементы. Первым из таких элементов является пространство имён. Типичная онтология OWL начинается с декларации пространства имён, подобной приведённой на рис.2.

Такие декларации определяют пространства имён, используемые в документе, а также задают пространство имён, используемое по умолчанию.

Следующим стандартным элементом онтологии OWL является её заголовок, сформированный после тега `owl:Ontology`. Этот тег используется для решения таких задач, как комментарии, управление версиями и включение в документ другой онтологии. Заголовок может выглядеть так, как на рис.3.

Также онтология поддерживает определение пользователем классов, соответствующих рассматриваемой предметной области. Каждый объект в среде OWL рассматривается как член класса `owl:Thing`. OWL также поддерживает пустой класс, `owl:Nothing`. Создадим два основных класса: `Medical` и `Computer` (см. рис. 4).

Кроме того, онтология имеет ряд других элементов, но в связи с ограниченным объёмом данной работы мы не будем подробно их рассматривать. Упомянем лишь, что помимо классов онтология поддерживает объекты, различные виды свойств и типов данных.

Литература

- [1] Воробьёв В. И., Монахова Т. В. Функциональное моделирование системы информационной защиты // Труды СПИИРАН. Вып. 2, т. 2. СПб.: Наука, 2005. (Публикация содержится в настоящем томе Выпуска 2 Трудов СПИИРАН).
- [2] Жигалов В. А., Загорюлько Ю. А., Нариньяни А. С., Россеева О. И. Предел однородности поиска в Интернете//Системная информатика. Сб. науч. тр. Новосибирск: Наука, 2002. Вып.8.: Теория и методология программирования. 251с.
- [3] Гаврилова Т. <www.big.spb.ru>.
- [4] <www.w3c.org>.