Разработка онтологии для семантического управления доступом

Ломов П. А., Шишаев М. Г.
Учреждение РАН Институт информатики и математического
моделирования технологических процессов КНЦ РАН
Мурм. обл., г.Апатиты, ул.Ферсмана, 24а., Россия
{lomov,shishaev@iimm.kolasc.net.ru}

Аннотация

В данной статье рассматривается разработка онтологии семантического управления доступом. Рассмотрены ее основные концепты и отношения, а также принципы ее дальнейшего расширения для применения в конкретных системах управления доступом.

Ключевые слова: онтология, управление доступом, информационная безопасность.

I. ВВЕДЕНИЕ

На сегодняшний день проблема обеспечения информационной безопасности является довольно актуальной вследствие широкого применения информационных технологий для хранения и обработки информации различных учреждений и организаций. Одним из важных аспектов обеспечения информационной безопасности является управление доступом к информационным ресурсам, то есть предоставление или отказ субъекту в возможности воздействовать на объект доступа. При этом категории объекта и субъекта, а также вид воздействия четко регламентируются с помощью некоторого набора правил.

Разумеется, осуществлять управление доступом можно на различных уровнях реализации информационной системы: аппаратном, программном, телекоммуникационном. Однако вследствие того, что информационная система работает с информационными элементами, описывающими сущности реального мира, то изначально правила доступа формулируются на языке предметной области. Впоследствии они выражаются на языке низкоуровневых компонентов системы в виде, например, правил фильтрации брандмауэром трафика или прав доступа к объектам файловой системы. Но такое представление может быть выполнено не всегда. В этом случае возможность регламентирования правил доступа к информационным ресурсам в терминах предметной области может быть предусмотрено в том программном продукте, с которым пользователь работает непосредственно, например, какой-либо системе электронного документооборота. Однако здесь возникает вопрос об обеспечении необходимой гибкости формулировки правил доступа таким способом. Это связанно с тем, что различные изменения в процессах обработки данных могут потребовать учета новых аспектов в процедуре доступа к информации, которые не учтены во встроенной в программный продукт системе формулировки правил. Подобные ситуации требуют обращения к производителю программного продукта для изменения программного кода, и, как следствие, дополнительных финансовых и временных затрат.

Также важной проблемой является управление доступом к информационным ресурсам, подвергшимся процедуре интеграции. При этом часто владельцы требуют сохранения контроля доступа к своим информационным ресурсам, и в тоже время необходимым является предоставление санкционированного доступа к данным посредством единого интерфейса системы интеграции. Соблюдение этих условий требует наличия некоторого

общего языка для описания правил доступа, что не представляется возможным ввиду использования программных продуктов от различных производителей, которые, часто, не являются интероперабельными по отношению друг к другу.

Решением данных проблем могло бы стать использование единой онтологической модели, определяющей как понятийную систему управления доступом к информационным ресурсам, так и ее формальную семантику. В этом случае комбинация такой модели с онтологической моделью предметной области позволила бы определять правила доступа в терминах предметной области с учетом их (терминов) семантики, а также принимать решение о предоставлении или отказе в доступе на основе результатов логического вывода на ней. Разработке и применению такой онтологической модели управления доступом с учетом семантики предметной области и посвящена данная работа.

II. Разработка и применение онтологии для семантического управления доступом

A. Основные направления использования формальных онтологических моделей в сфере информационной безопасности и контроля доступа

На сегодняшний день применение онтологических моделей, дескриптивных логик и логического вывода в различных аспектах информационной безопасности развивается довольно активно. В основном можно выделить следующие направления исследований в данной сфере:

- формализация подмножеств языка XACML[1] и использования логического вывода для проверки сформулированных администратором политик безопасности на предмет покрытия ими всех возможных ситуаций доступа [2, 3];

- использование логического вывода в существующих моделях контроля доступа [4, 5], таких как RBAC (Role Based Access Control) и ABAC (Attributes Based Access Control);

- создание онтологий, определяющих понятийную систему предметной области информационной безопасности General Privacy Ontology [6], Security Ontology [7], NRL Security Ontology [8].

Для данной работы наибольший интерес представляют работы последнего направления, так как онтологические модели, описанные в них, могут служить источниками необходимых понятий, которые в сочетании с понятиями предметной области позволяет создать предметно-ориентированную онтологию для решения задачи семантического управления доступом.

B. Использование онтологии Descriptions & Situations для определения политик управления доступом

Однако помимо понятий информационной безопасности онтология должна определять некоторую точку зрения на сам процесс доступа и правила его выполнения. Это позволит задать принципы формулировки правил доступа, и тем самым облегчить их дальнейшее определение. Для решения данной задачи была использована онтология *Descriptions and Situations* (далее DnS) [9]. Она направлена на реификацию (овеществление) нематериальных социальных объектов, процессов и явлений. Под реификацией в данном случае понимается представление некоторого факта в виде именованного концепта онтологии. Основу *DnS* составляют определения ситуации *(Situation)*, описания *(Description)* и пространства явлений *(State of affairs)*. Пространство явлений представляется набором утверждений, каждое из которых удовлетворяет некоторой логической теории *O*. Описание представляет логическую теорию *T*, подразумеваемую коллективом, программным агентом или сообществом. Ситуация, в свою очередь, составляется из сущностей, используемых в утверждениях, описывающих пространство

явлений, и представляет некоторую модель (интерпретацию) *M* для теории *T*, в соответствии с аксиомами *O*. Например, пространством явлений может служить набор измерений температуры, описанием – ежемесячное изменение температуры, а ситуацией – уменьшение средней температуры в октябре.

Логическая теория *O* в данном определении также называется базисной онтологией *(Ground ontology)*. В случае DnS, ее авторы используют онтологию *Descriptive Ontology for Linguistic and Cognitive Engineering* [10] (далее DOLCE) в качестве базисной. Определение или описание ситуации *(Description)* задается в DnS набором используемых ею (*d-uses*) составляющих *(Concept)*. Они отличаются друг от друга в зависимости от того, какой концепт из базисной онтологии отображается ими в описании ситуации, что выражается различных видах отношения классификации *(classifies)*. Например, в случае использования DOLCE в качестве базисной онтологии, направление *(Course)* «упорядочивает» *(sequences)* постоянные *(Perdurant)* сущности, тогда как функциональная роль *(Role)* «играется» *(played by)* длящимися *(Endurant)*; параметр *(Parameter)* оценивается *(valued by)* областью значений *(Region)*. Сама ситуация *(Situation)* определяется, как состоящее *(setting for)* из сущностей, описываемых в базисной онтологии, и удовлетворяющее *(satisfies)* некоторому описанию.

Следует заметить, что в качестве базисной онтологии может выступать и онтология предметной области, построенная с использований основных классов DOLCE. В этом случае некоторую политику доступа можно рассматривать как совокупность правил оперирования объектами, представленными в онтологии предметной области. Причем данные правила не составляют суть самих объектов или процессов с их участием, а являются лишь ментальными представлениями «корректных» действий субъекта по отношению к объекту доступа, определяемых некоторыми агентивными сущностями. Отсюда можно сделать вывод о том, что согласно онтологии DnS политику доступа можно представить как описание некоторой ситуации доступа. Сама ситуация доступа формируется из понятий онтологии предметной области.

C. Разработка онтологической модели для семантического управления доступом к информационным ресурсам

Для создания онтологической модели семантического управления доступа к ресурсам необходимо дополнить онтологию DnS элементами, представляющими различные понятия и отношения из сферы информационной безопасности и управления доступом. Для этого целесообразно повторно использовать некоторую онтологию, описывающую данную предметную область. Выбор такой онтологии следует производить с учетом следующих требований:

- ориентация онтологии на представление основных элементов ситуации доступа к ресурсу – процесс доступа, объект и субъект доступа;

- желательно наличие в онтологии понятий, выделяющих персональную информацию, а также различные аспекты работы с нею. Данное требование обусловлено тем, что, как правило, персональная информация присутствует в информационных ресурсах организаций и требует соблюдения особых правил обращения;

- возможность рассмотрения понятий и отношений онтологии в контексте онтологии DnS.

Среди рассмотренных онтологий *General Privacy Ontology*, *Security Ontology*, *NRL Security Ontology* наиболее полно данным требованиям удовлетворяет *General Privacy Ontology* (далее GPO). Она содержит понятия, представляющие различные аспекты управления доступом к информации, в том числе и персональной. Данные понятия можно использовать как составляющие описаний (в смысле DnS) ситуаций доступа.

Другие онтологии использовать в данном случае затруднительно, так как они рассматривают информационную безопасность с иных позиций. Так *NRL Security Ontology* включает несколько модулей-онтологий *(Credentials Ontology, Security Assurance Ontology, Service Security Ontology и др.)*, которые содержат понятия, представляющие в основном средства, сущности, протоколы и алгоритмы, применяемые на уровне средств передачи в информационной системе. Онтология Security Ontology, в свою очередь, направлена на представление угроз *(Threat)*, уязвимостей *(Vulnerability)* и определения на их основе требуемого уровня безопасности *(Security attribute)*.

Таким образом, выбрав онтологию GPO, необходимо рассмотреть ее основные понятия и представить их в качестве компонентов ситуаций и описаний онтологии DnS. Детально приводить анализ онтологии GPO не представляется возможным в виду ограниченного объема статьи.

Рассмотрим фрагмент полученной в результате представления понятий GPO в контексте DnS онтологии семантического управления доступом (рис. 1).

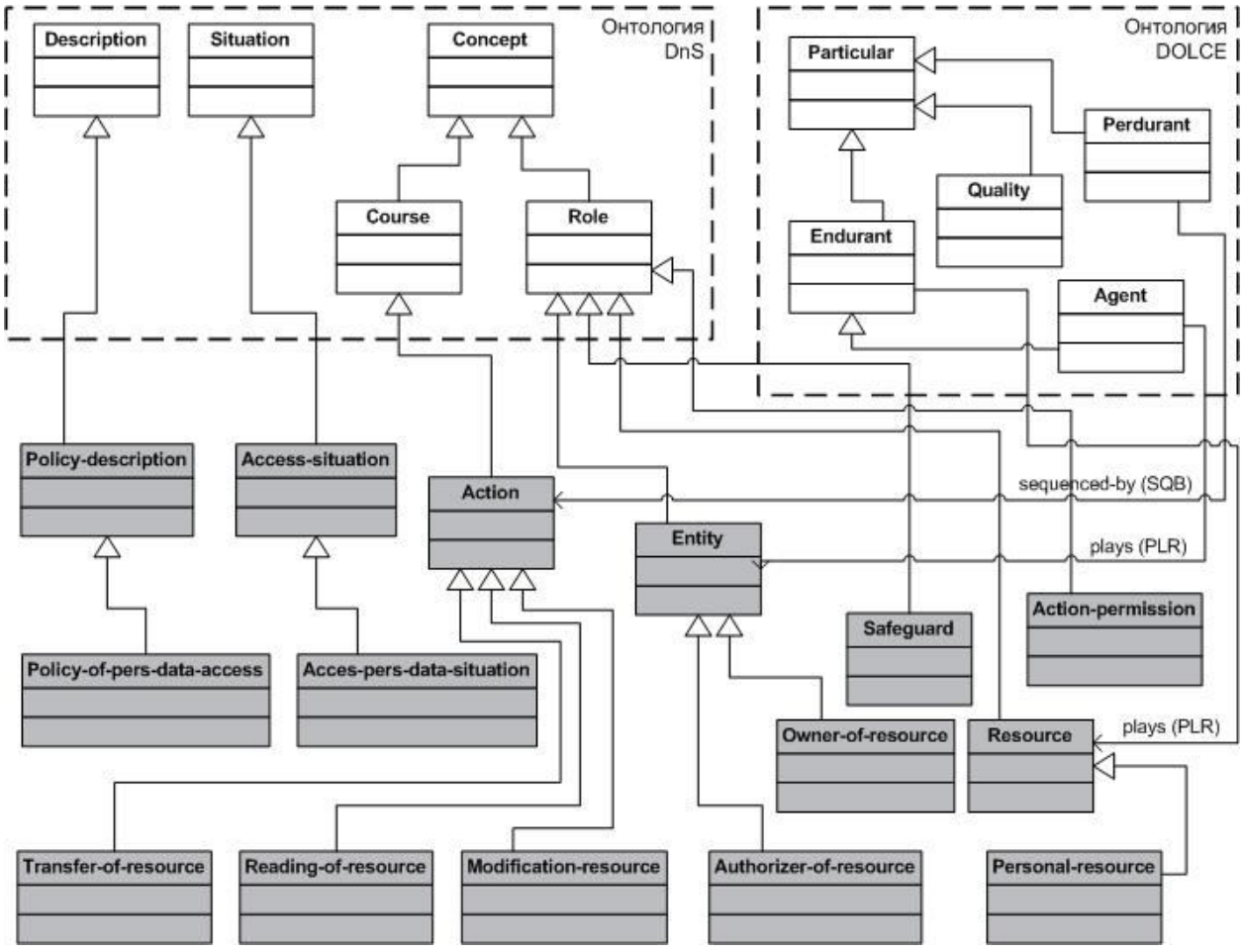

Рисунок 1. Основные концепты и отношения онтологии семантического управления доступом (выделены серым цветом).

Концепт «Policy-description» представляет собой описание общей политики доступа состоящее *(d-uses)* из компонентов: некоторого воздействия *(Action)*, субъекта *(Entity)* и объекта воздействия *(Resourse)* (используется манчестерский синтаксис[11]):

Class: Policy-description

EquivalentTo:

d-uses some Action

and (modal-target-of some Entity)

and (modal-target-of some Resource)

SubClassOf:

description

Компоненты, в свою очередь, задают условия участия сущностей, представленных в онтологии предметной области, в процессе воздействия на ресурс. Например, для того чтобы играть роль субъекта воздействия *(Entity)* экземпляр, представляющий некоторую сущность, должен входить в класс «Агент» *(Agent)*, представляющий множество активных объектов:

Class: Entity

EquivalentTo:

role and (played-by some agent)

SubClassOf:

modal-target some Action

DisjointWith:

Resourse

Концепт «Access-situation», в свою очередь, определяет множество ситуаций, составляющие которых классифицируются компонентами «Policy-description»:

Class: Access-situation

EquivalentTo:

setting-for some (participant some (plays some Entity)

and (participant some (plays some Resource))

and (sequenced-by some Action))

SubClassOf:

situation,

satisfies only Policy-description

Нетрудно заметить, что в это множество попадают все ситуации, предполагающие некоторое воздействие на информационный ресурс.

Далее путем конкретизации обобщенного описания и ситуации доступа и их компонентов можно определять более строгие политики доступа, которым будут удовлетворять лишь некоторые описания и ситуации. Например, описание ситуации доступа к персональным данным *(Policy-of-personal-data-access)* требует того, чтобы в качестве субъекта доступа выступал хозяин ресурса *(Owner-of-resourse)* или поверенный *(Authorizer-of-resourse)*.

Также в ситуацию могут входить дополнительные компоненты «Средство защиты» *(Safeguard)* и «Разрешение» *(Action-permission)*. Их использование позволяет ставить дополнительные условия воздействия на ресурс. Например, средством защиты может быть какой-либо алгоритм шифрования или некоторый физический контейнер, предохраняющий информационный ресурс при его передачи по каналам связи или транспортировке. Использование понятия «Разрешения» *(Action-permission)* дает возможность регламентировать доступ по наличию некоторого документа или иной сущности, играющей данную роль, и участвующей в ситуации доступа.

Таким образом, для задания совокупности правил доступа в рамках конкретной системы управления доступом необходимо задать описание политики и удовлетворяющую ей ситуацию доступа, как подклассы концептов «Policy-description» и «Access-situation». Далее приведены принципы последующего определения политик и ситуаций доступа:

- описания, уточняющие обобщенное описание политики доступа *(Policy-description)* задается набором своих компонентов – подклассов концептов «Субъекта воздействия» *(Entity),* «Объект воздействия» *(Resource)*, «Воздействие» *(Action)* и других, а также связей между ними;

- определения ситуации доступа, удовлетворяющей некоторому описанию политики, должно включать требования ролей, формирующих это описание политики, а также связей между объектами, имеющими значение в данной ситуации. Например, ситуация обращения пользователя к ресурсу требует, чтобы документ и пользователь играли роли ресурса и обращающегося и были связанны с процессом чтения документа;

- определения ролей, уточняющих роль субъекта *(Entity)* и объекта воздействия *(Resource)* должны включать условия участия в ситуации каких-либо объектов, представленных в онтологии предметной области. Например, такие определения могут требовать наличия каких-либо атрибутов (стажа работы, уровня доступа и т.д.) или других ролей (руководитель, директор и т.д.), а также связей с другими объектами (наличие документов, разрешений и т.д.);

C. Пример использования

Для иллюстрации описываемого метода семантического управления доступом с помощью онтологии рассмотрим простой пример. Зададим некоторую политику доступа в виде концепта «Policy-read-resourse», разрешающую просмотр информационного ресурса гражданам, имеющим удостоверение личности:

Class: Policy-read-resource

EquivalentTo:

d-uses some Reading-of-resource

and (modal-target-of some Ident-entity)

and (modal-target-of some Resource)

SubClassOf:

Policy-description

Определим также удовлетворяющую политике ситуацию доступа «Situation-read-resource»:

Class: Situation-read-resource

EquivalentTo:

setting-for some (participant some (plays some Ident-entity)

and participant some (plays some Resource)

and sequenced-by some Reading-of-resource))

SubClassOf:

Access-situation,

and satisfies only Policy-read-resource

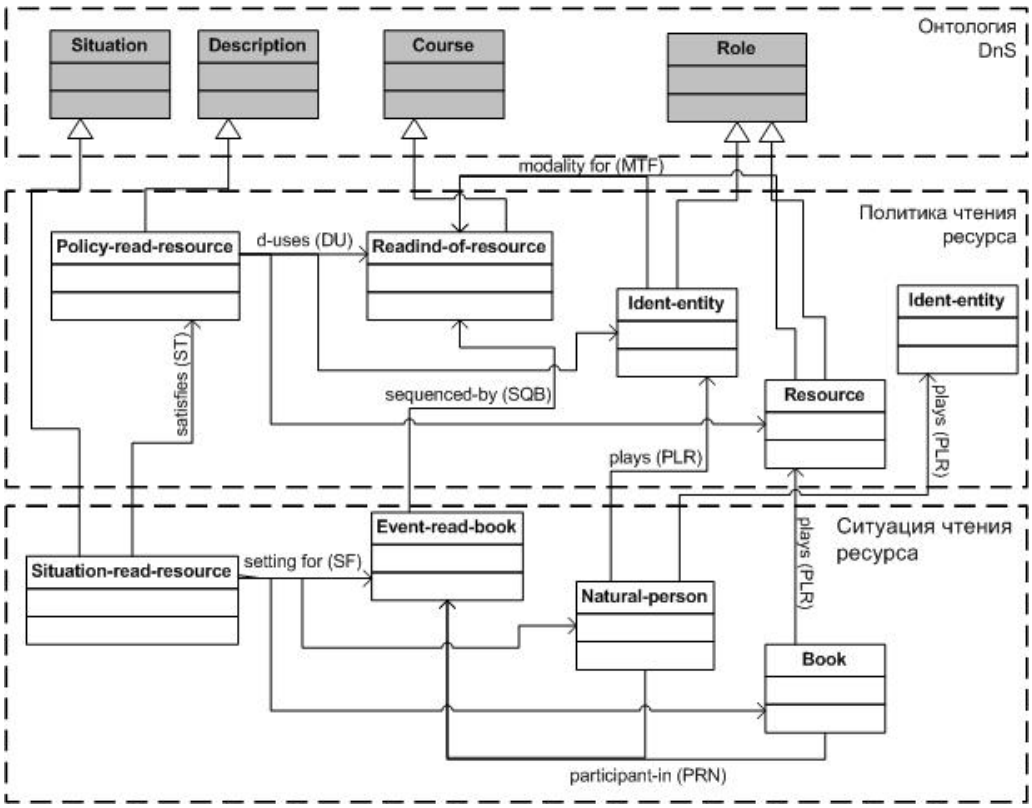

Рисунок 2. Политика и ситуация доступа к ресурсу.

На рисунке 2 представлена схема отношений концептов определенной ситуации и описания. Рассмотрим формальное определение идентифицированной обращающейся сущности *(Ident-entity)* в онтологии:

Class: Ident-entity

EquivalentTo:

played-by some (natural-person and (plays some Ident-person))

SubClassOf:

modal-target some Action

DisjointWith:

Resourse

В представленном определении концепты «Natural-person», обозначающие физическое лицо и являющиеся ролью «Ident-person», которая играется физическим лицом, имеющим удостоверение личности, заимствованы из онтологии предметной области. Таким образом, из данного определения видно, что роль идентифицированной обращающейся сущности может выполняться физическим лицом *(Natural-person)*, играющем роль идентифицированной персоны *(Ident-person)*.

Само принятие решения о предоставлении доступа к ресурсу заключается в проведении логического вывода над онтологией. Он производиться после добавления в нее экземпляров описания, удовлетворяющей ей ситуации, и отношений с составляющими их экземплярами-компонентами. Если в результате вывода установлен факт принадлежности экземпляра-описания к классу-политике «Policy-read-recourse», то это значит, что все экземпляры-компоненты ситуации удовлетворяют заданным в определении «Situation-read-resource» условиям и доступ может быть разрешен. В противном случае – данная ситуация доступа не удовлетворяет заданной политике и доступ не разрешается.

Разумеется, можно далее расширять набор требуемых ролей у обращающейся сущности, и тем самым определять дополнительные условия участия физического лица в данном действии над ресурсом. Подобным образом можно также поступать в отношении ролей объекта и воздействия на него, определяя их подклассы, задающие дополнительные требования.

III. Заключение

Данная работа посвящена проблеме разработке онтологической модели семантического управления. К основным результатам можно отнести:

- проведение анализа существующих онтологий, описывающих понятийную систему информационной безопасности и выявление основных понятий, используемых для описания правил доступа к информационным ресурсам;

- представление обобщенных понятий управления доступом в контексте онтологии DnS в виде наборов аксиом для обеспечения возможности проведения логического вывода при принятии решения о разрешении или запрете доступа;

- формулировка принципов дальнейшего расширения описаний и ситуаций доступа для определения более сложных правил доступа в контексте конкретной системы управления доступом.

К положительным свойствам семантического управления доступом на основе представленной модели являются:

- возможность определять права доступа к информационным ресурсам требуемой сложности в терминах предметной области. При этом отсутствует необходимость привлечения дополнительных специалистов для их трансляции в правила какого-либо низкоуровневого компонента системы информационной безопасности;

- использование формальной онтологической модели делает возможным проведение логического вывода в процессе выработки решения о предоставлении или отказе в доступе. Это позволяет определять основную часть механизма данного процесса непосредственно в самой онтологической модели, тогда как обычно она определяется различными способами в приложениях, играющих роль менеджеров доступа;

- повторное использование проработанных онтологических моделей DOLCE и DnS, разработанных авторитетными специалистами в области онтологического моделирования. Это обуславливает правильность полученной онтологии с точки зрения подхода к построению определений ее понятий.

Необходимо отметить, что применение сложных онтологических моделей и машин логического вывода в управлении доступом может требовать больших вычислительных и временных ресурсов. Поэтому их следует использовать лишь в тех ситуациях, где решении о доступе невозможно принять ввиду наличия условий, определяемых предметной областью. Правильным решением будет их комбинирование с традиционными средствами защиты информации. Это позволит в итоге построить гибкую предметно-ориентированную систему информационной безопасности.

БЛАГОДАРНОСТИ

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 08-07-00301-а «Разработка информационной технологии и распределенной информационно-аналитической среды поддержки инновационной деятельности»).

ЛИТЕРАТУРА

[1] OASIS eXtensible Access Control Markup Language Technical Committee, «eXtensible Access Control Markup Language (XACML). – Режим доступа: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[2] Fisler K., Krishnamurthi S., Meyerovich L.A., Tschantz M.C., Verification and change – impact analysis of access – control policies. In ICSE'05: Proceedings of the 27th international conferenceon Software engineering, pages 196 – 205, 2005.

[3] Kolovski V., Hendler J., Parsia B., "Analyzing web access control policies" in WWW '07: Proceedings of the 16th international conference on World Wide Web, (New York, NY, USA), pp. 677–686, ACM, 2007.

[4] Knechtel M., Hladik J., Dau F. "RBAC Authorization Decision with DL Reasoning" In ICWI '08: Proceedings of the IADIS International Conference WWW/Internet, pages 169–176, 2008.

[5] Torsten P., Wolfgang D., Nora K. "Supporting Attribute-based Access Control with Ontologies,", First International Conference on Availability, Reliability and Security (ARES'06), 2006 - pp.465-472.

[6] Hecker A., Dillon T., Elizabeth C. «Privacy Ontology Support for E-Commerce», Internet Computing, Issue No. 2 - March/April, 2008 – pp. 54 – 61.

[7] Fenz S., Ekelhart A. Formalizing information security knowledge ASIACCS '09: Proceedings of the 2009 ACM symposium on Information, computer and communications security, ACM, 2009 - 183-194.

[8] Kim A, Luo J. Myong K, "Security Ontology for Annotating Resources", Naval Research Lab, NRL Memorandum Report, NRL/MR/5540-05-641: Washington, D.C., 2005 - pp. 51

[9] Gangemi A., Mika P., «Undeistanding the Semantic Web through Descriptions and Situations» Lecture Notes in Computer Science Vol. 2888/2003: On the Move to Meaningful Internet Systems 2003: CooplS DOAandODBASE. pp. 689-706. 2003

[10] Masolo C., Borgo S., Gangemi A, Guarino N., Oltramari A., Schneider L. DOLCE: a Descriptive Ontology for Linguistic and Cognitive Engineering // DOLCE documentation – Режим доступа: http://www.loa-cnr.it/DOLCE.html.

[11] OWL 2 - Web Ontology Language Manchester Syntax, 2009. – Режим доступа: http://www.w3.org/TR/owl2-manchester-syntax