УДК 004.822

СЕМИОТИЧЕСКАЯ СИСТЕМА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ В ИТ-ИНФРАСТРУКТУРЕ ВУЗА

Л.С. БОЛОТОВА[1]
А.А. КАРАСЁВ[1]
С.С. СМИРНОВ[1]
В.А. СМОЛЬЯНИНОВА[2]

[1)] ФГАУ ГНИИ Информационных технологий и телекоммуникаций «Информика», г. Москва
[2)] ФГБОУ ВПО Российский государственный университет инновационных технологий и предпринимательства, г. Москва

e-mail:
lubolotova@mail.ru
akarasev@informika.ru
smirnov@informika.ru
valerysmol@mail.r

В статье рассматривается перспективный подход в области управления инцидентами на примере ИТ-инфрастуктуры вуза. Утверждается, что управление инцидентами можно осуществлять на новом качественном уровне за счет использования логико-семиотических систем поддержки принятия решений. Предлагаются типовые концептуальные структуры, описывающие действия администраторов в процессе разрешения инцидентов. Структуры были получены при помощи специальной методики концептуального анализа предметной области. Приводится фрагмент онтологической модели, полученный в результате интерпретации этих структур.

Ключевые слова: управление инцидентами, концептуальный анализ, база знаний, поддержка принятия решений.

На современном этапе развития высшего образования трудно представить ВУЗ без развитой ИТ-инфраструктуры. При этом нагрузка на неё постоянно возрастает, соответственно, всё более усложняются процессы управления и, как следствие, растут трудозатраты на качество работы и поддержание её работоспособности. Сегодня – это сложная сервис- ориентированная структура с постоянно растущим числом компонент, включающая множество разнообразного аппаратно-программного обеспечения. Очевидно что поддержка функционирования ИТ – систем требует привлечения квалифицированных специалистов, которые очень дороги. Поэтому ВУЗы стараются сами воспитывать своих администраторов из способных студентов. Но, фактически каждые 2-3 года на должности администраторов приходится приглашать новых людей. Смена поколений администраторов является чрезвычайно болезненным моментом, поскольку преемственность при передаче знаний отсутствует, т.к. в большинстве ВУЗов все возникающие задачи решаются системными администраторами, что называется «по ситуации». Это, естественно, затрудняет процессы накопления и преемственности знаний по разрешению инцидентов, их обобщению и сокращению сроков на обучение.

В этой связи, представляется необходимым переход ВУЗов на качественно новый уровень систем автоматизированной поддержки процессов администрирования, инвариантных по отношению к конкретным ИТ – структурам. Следует заметить, что классические системы отслеживания инцидентов типа Bagzilla и другие зарубежные аналоги, используемые в качестве посредников для передачи подобного опыта, подходят мало, т.к. оперируют лишь текстовыми описаниями происходящих инцидентов, не опираясь на какую-либо модель предметной области.

Анализ показал, что при кажущемся разнообразии инцидентов, они:

1. не описываются средствами строгих математических моделей, но;
2. хорошо поддаются типизации;
3. имеют чёткую концептуальную структуру, хорошо описываемую на едином понятийном языке.

Поэтому к созданию систем управления инцидентами (СУИ) был предложен подход с позиции ситуационного управления и логико–семиотического (логико–лингвистического) моделирования [1, 2, 3] . Как известно, под семиотической моделью предметной области (МПрО) понимается знаковая (лингвистическая, или псевдофизическая) модель, в которой роль объектов (любых сущностей, событий, процессов, и т.п.) свойств, отношений между ними играют их языковые эквиваленты во внешнем мире. Наглядно семиотическая модель может быть представлена в виде семантической сети, вершины которой интерпретируются как сущности (объекты), а дуги – как отношения между ними. Тогда основной проблемой построения МПрО является: выявление совокупности имен (знаков), обозначающих сущности предметной области, определение их содержания (концептов, понятий) и объемов (денотатов), а также выявление системы отношений, харак-

терных для описания классов ситуаций и решений. Все процессы, объекты, структуры, их существенные свойства и принимаемые решения должны описываться в терминах естественного языка ситуационного пространства, установленного и оговоренного соответствующими нормативными документами. В этом смысле можно говорить о необходимости единого языка описания.

На первом этапе для создания семиотической системы поддержки управления инцидентами в ИТ-модели необходимо было решить следующие проблемы:

- выявить и исследовать типологию инцидентов в ИТ – системах ВУЗов;
- разработать методику построения концептуальной модели инцидента, допускающую интерпретацию применительно к любым конкретным инцидентам;
- разработать концептуальные модели типовых инцидентов;
- построить концептуальную модель пространства предметной области инцидентов ИТ-системы (ситуационное пространство принятия решений) конкретного Вуза;
- решить вопрос о наиболее подходящей модели представления знаний;
- решить вопрос о выборе инструментальной программной системе для реализации прототипа системы управления инцидентами;
- реализовать и протестировать прототип на способность к выполнению поставленных задач.

Общий принципом, заложенным в ИТ – системы, является сервис – ориентированная архитектура и, в частности, технологии XML Web-сервисов для интеграции информационных ресурсов. Т.е., информационные ресурсы – централизованы, а все остальные компоненты обеспечивают надлежащий доступ к ним. Поэтому, каждый компонент аппаратного и программного обеспечения ИТ – архитектуры является объектом управления. При этом должны быть обеспечены соответствующие уровни надежности, доступности и взаимодействия между компонентами. Соответственно, системное управление должно обеспечивать: мониторинг состояния всех компонент архитектуры, анализ этого состояния, планирование ресурсов; принятие решений как по компонентам, так и по системе в целом; развитие системы; поддержание всех ее компонент, а также связей между ними в актуальном состоянии.

Например, в качестве основы для типизации инцидентов в ИТ– архитектуре выделены предметные области со следующими основными функциональными составляющими:

1. система доступа в ИНТЕРНЕТ;
2. почтовая система;
3. телефонная система;
4. система кондиционирования;
5. система электропитания;
6. хранилище документов;
7. система резервного копирования;
8. сервис печати;
9. серверы;
10. ЛВС;
11. ПК.

В качестве примера на рис. 1 представлен фрагмент пространства типовых инцидентов в системе «Почта».

Рис. 1. Фрагмент пространства инцидентов в почтовой системе

За основу методики построения концептуальных семиотических моделей взята методика, разработанная авторами в работах [4, 5, 6].

В нашем случае все инциденты представляются однотипной структурой, в которой выделяются:

1. субъект, установивший наличие инцидента;
2. уровень структурной организации субъекта инцидента, т.е. уровень элемента организационно – регламентной структуры ИТ – системы, на котором возник инцидент;
3. факторы проявления инцидента или его контекст;
4. временные факторы, т.е. время фиксации инцидента;
5. действия субъекта, установившего наличие инцидента до обращения к ЛПР (администраторам);
6. способ или средство доведения информации о наличии инцидента;
7. услуга, которую хотел получить субъект, установивший инцидент (задачу, которую он хотел решить).

Перечисленные факторы служат основой для идентификации данного инцидента и начала процесса вывода его вторичных признаков для синтеза алгоритма принятия решения.

Вторичными могут быть любые признаки, необходимые для классификации и интерпретации элементов структуры решения (СР), а также некоторые сопутствующие, необходимые для определения значений внешних параметров ИТ – системы, например, экономических. К вторичным признакам относятся следующие:

- субъект (ЛПР), отвечающий за разрешение инцидента на текущий момент времени;
- тип инцидента (локальный, глобальный и на какие уровни данный инцидент может распространяться);
- параметры инцидента – внешние, внутренние:
- стоимость неразрешения (продолжения) инцидента в единицу времени.
- В результате устанавливаются:
- алгоритм разрешения инцидента, т.е. последовательность действий, необходимых для его снятия;
- ситуация – причина (ситуация – предусловие);
- ситуация – следствие (ситуация – постусловие);
- суммарная стоимость ПС;
- кто должен нести издержки.

На рис. 2 – 5 приведены концептуальные структуры основного (целевого) действия «Выработать рекомендации» и его поддействия:

1. Идентифицировать, какое событие произошло в сети,
2. Определить причину события,
3. Обработать событие.

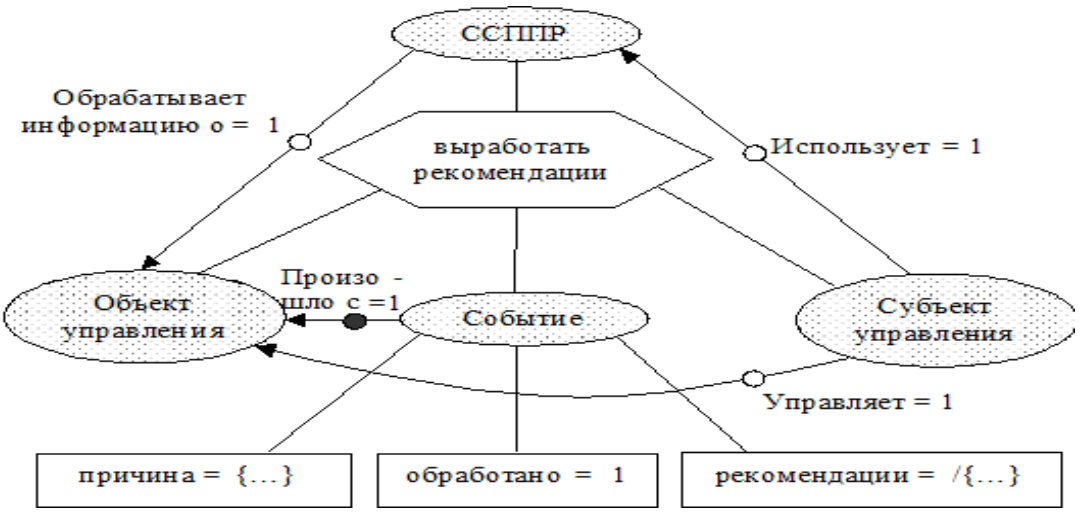

Рис. 2. Концептуальная структура действия «Выработать рекомендации»

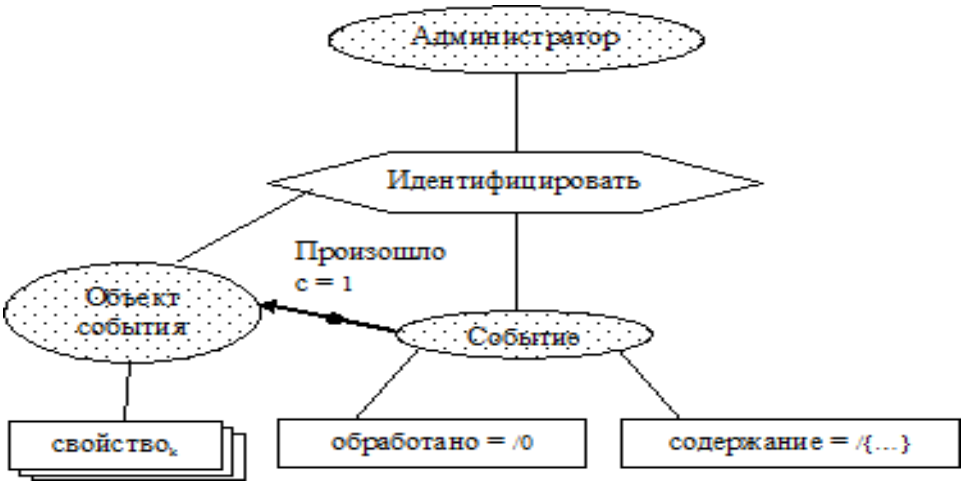

Рис. 3. Концептуальная структура действия «Идентифицировать событие»

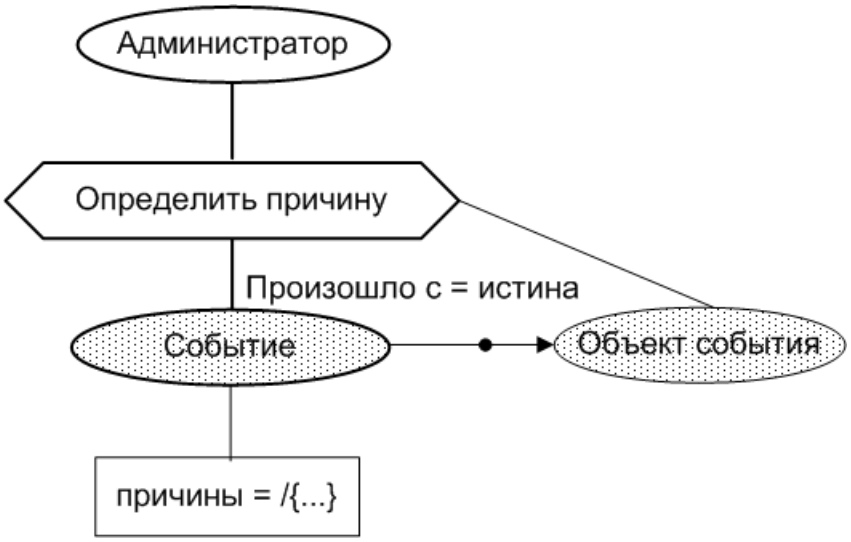

Рис. 4. Концептуальная структура действия «Определить причину события»

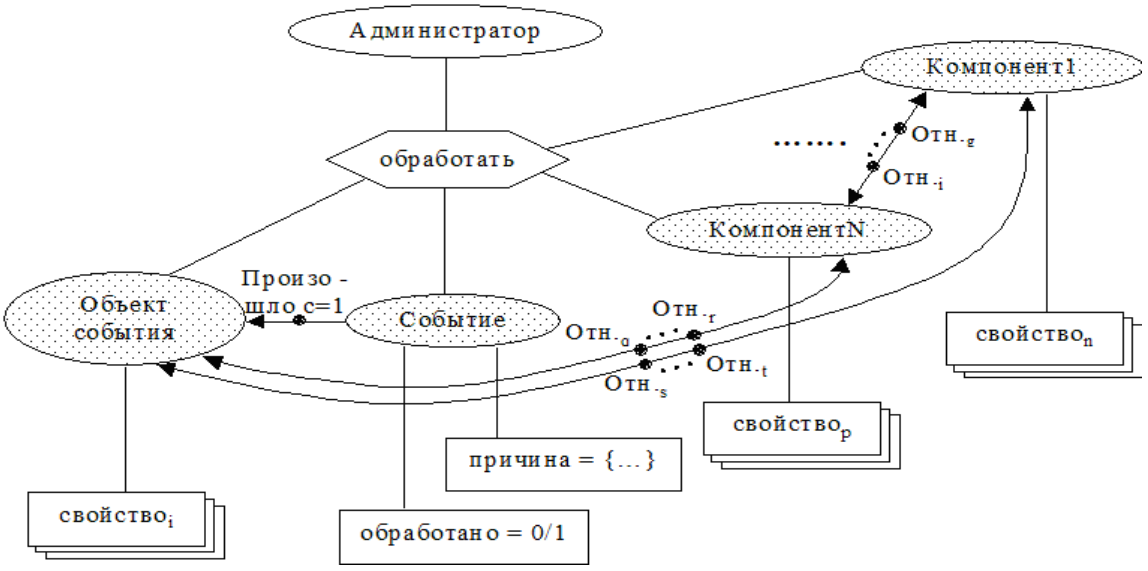

Рис. 5. Концептуальная структура действия «Обработать событие»

Действие "Обработать" Событие является абстрактным, т.к. в случае каждого конкретного события распадается на ряд определенных действий, связанных с обработкой именно этого события. Эти действия являются его поддействиями и включают в свою структуру еще один набор объектов из состава ИТ – сети, являющихся компонентами данных действий. Это означает, что значения свойств и отношений этих объектов будут изменяться в процессе обработки события, а часть их войдет в описание результирующей ситуации, соответствующей нормальной работе сети.

На основании имеющихся концептуальных моделей в итоге строится понятийно – объектная модель формального представления знаний о предметной области, дающая необходимый и достаточный язык для описания любых состояний этой системы.

В качестве модели представления знаний для реализации СУИ, на наш взгляд, наиболее эффективна форма онтологии, обеспечивающая требуемую полноту описания, открытость к расширению и модификации, логический вывод вторичных признаков, возможности использования её в различных качествах:

1. Системы поддержки принятия решений;
2. Системы моделирования сценариев типа «если – то»;
3. Информационно – поисковой системы;
4. Системы обучения – тренажёра.

Для реализации СУИ принята открыто поставляемая Среда Protégé 4.1, как наиболее соответствующая передовым стандартам представления знаний, а в качестве тестовой системы рассматривалась ИТ – инфраструктура РГУИТП (подсистема «ЭЛЕКТРОННАЯ ПОЧТА»). Сущности концептуальных моделей инцидентов (объекты, субъекты, компоненты) представлены как экземпляры и внесены в подкласс «Entity», где в свою очередь рассортированы по подклассам, выбранным в соответствии с типами сущностей. Экземпляры действий помещены в подкласс «Action».

Древовидная структура класса «Entity» представлена на рис. 6. Часть визуального представления иерархии классов, построенного средствами Protégé, представлена на рис. 7. Пример описания конкретного экземпляра аппаратуры через аксиоматические отношения – на рис. 8

В онтологию были внесены описания 20 инцидентов.

Готовая онтология предметной области в формате OWL, содержит:

1. 72 класса и подкласса;
2. 94 экземпляра;
3. 41 объектное отношение;
4. 45 свойств или отношений типа;
5. 110 отношений метаданных (комментариев).

В среде Protégé возможна также проверка онтологии на запросы с помощью специальной вкладки DL Query. Запросы производятся на языке OWL, но для их задания необходимо иметь общее представление о структуре онтологии.

Построенная онтология способна отвечать, например, на следующие запросы:

1. Какие действия может выполнить действующее лицо?
2. Какие ошибки произошли с заданным устройством?
3. Какой пользователь рассылает спам?
4. Какие компоненты у заданного действия?
5. Какие инциденты происходили с объектом?
6. Какие действия были выполнены для их устранения?
7. и другие.

Результаты тестирования эксперты приняли, как вполне удовлетворительные.

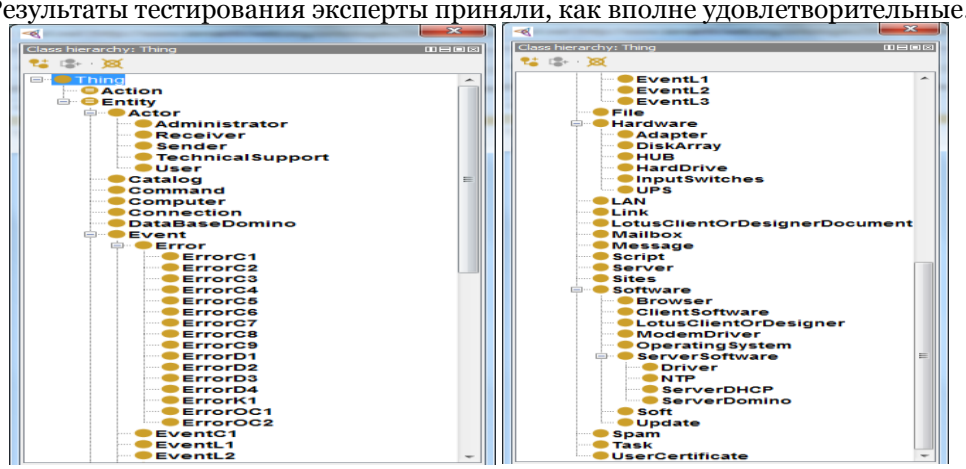

Рис. 6. Фрагмент древовидной структуры класса «Entity»

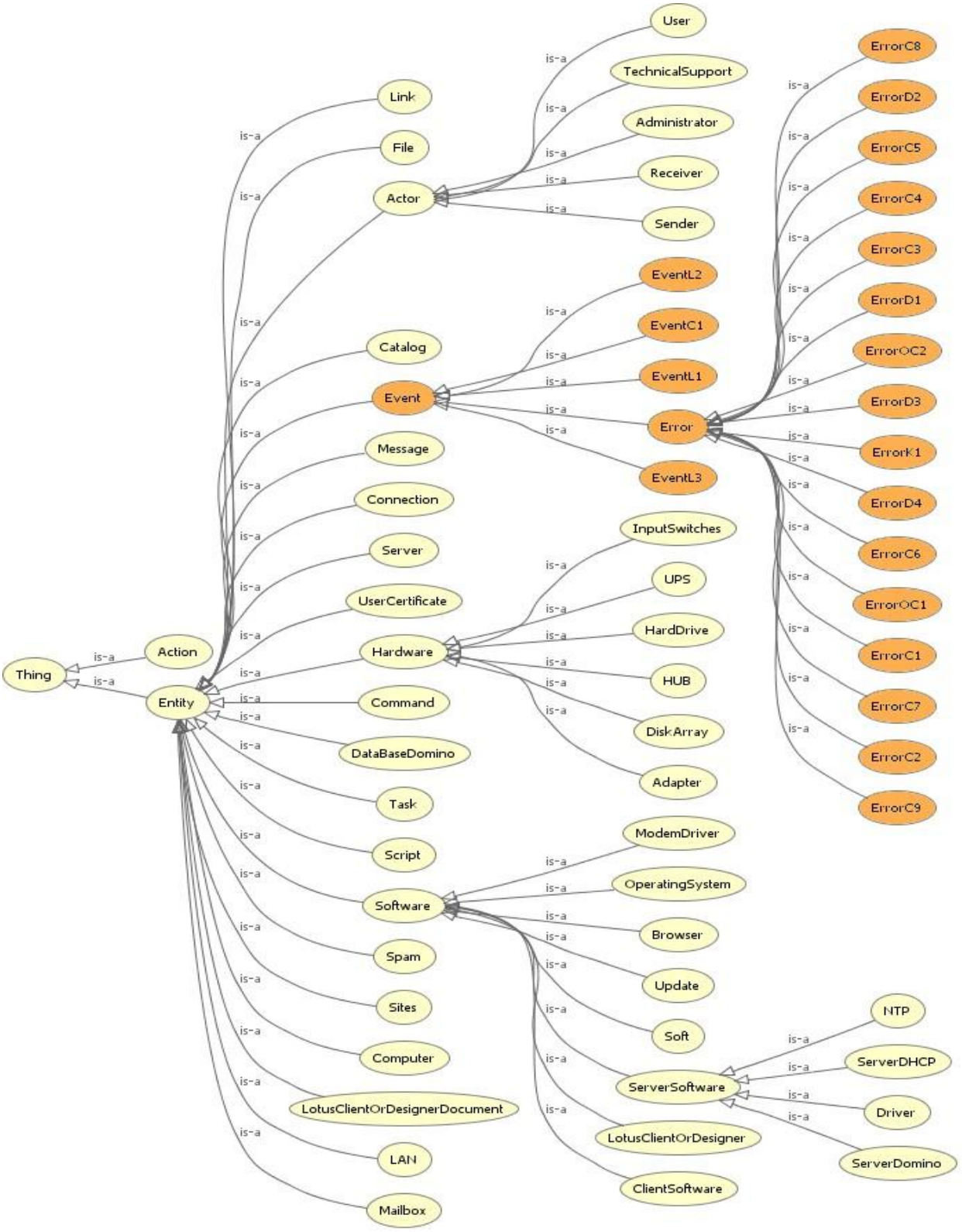

Рис. 7. Фрагмент иерархии классов онтологии для управления инцидентами

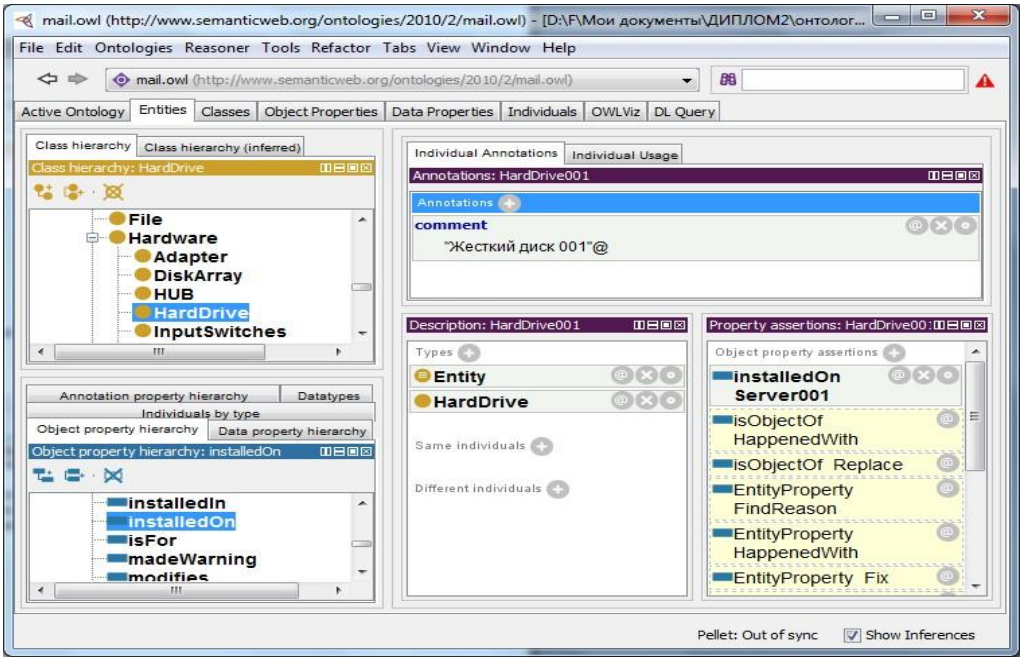

Рис. 8. Пример описания класса «HardDrive» в среде Protege

Заключение.

В статье рассмотрен прототип СУИ в ИТ-инфраструктуре вуза, который, как показало те- стирование, может стать единым прототипом для ВУЗов. Предложенные методические средства и подходы позволяют перейти к созданию унифицированной системы такого типа.

Литература

1. Поспелов Д.А. Ситуационное управление: Теория и практика.- М.:Наука 1986.
2. Поспелов Д.А. Логико-лингвистические модели в системах управления. – М.:Энергия, 1981
3. Болотова Л.С. Системы искусственного интеллекта: модели и технологии основанные на знаниях /
учебник. ФГБОУ ВПО РГУИТП; ФГАУ ГНИИ ИТТ «Информика». – М: Финансы и статистика, 2012, – 664с
4. Л.С. Болотова, В.А. Смольянинова, С.С. Смирнов Концептуальное проектирование модели пред-
метной области при помощи программных систем разработки баз знаний для систем поддержки принятия
решений, «Радиотехника», Наукоемкие технологии, №8, 2009, т.10
5. В.А. Смольянинова Понятийно-объектная модель как способ представления знаний в программ-
ных системах поддержки концептуального проектирования, «Радиотехника», Наукоемкие технологии, №9,
2009, т.10
6. В.А. Смольянинова Анализ концептуальных структур действий как основа разработки баз знаний,
Труды ИСА РАН, Динамика неоднородных систем / Под редакцией Ю.С. Попкова. Т. 39 (1). –М.: Книжный
дом «ЛИБРОКОМ», 2008. – 253 с.

SEMIOTICS MANAGMENT SYSTEM OF INCINDENTS FOR UNIVERSITY`S IT-INFRASTRUCTURE

L.S. BOLOTOVA[1]
A.A. KARASEV[1]
S.S. SMIRNOV[1]
V.A. SMOLYANINOVA[2]

[1)] State Institute of Information Technologies and Telecommuni- cations "Informika", Moscow

[2)] Russian State University for Innovation Technologies and Business, Moscow

e-mail: lubolotova@mail.ru akarasev@informika.ru smirnov@informika.ru valerysmol@mail.ru

This article is devoted to perspective approach in the field of man- agement of incidents for example of the university's IT-infrastructure. Affirms that management of incidents can be carried out at new qualitative level at the expense of use of logical-semiotics decision support systems. The standard conceptual structures describing actions of system administrators in the course of permission of incidents are offered. Structures were received by means of a special technique of the conceptual analysis of subject domain. The fragment of ontological model received as a result of interpretation of these structures is given.

Keywords: management of incidents, conceptual analysis, knowledge base, decision-making support.