УДК 004.822+89

Л.С. Болотова, д-р техн. наук, профессор, Национальный исследовательский университет «Высшая школа экономики», г. Москва

А.А. Карасев, Ведущий инженер Департамента информационных технологий, Национальный исследовательский университет «Высшая школа экономики» г. Москва,

В.А. Старых, канд. техн. наук, доцент, профессор кафедры, Национальный исследовательский университет «Высшая школа экономики», г. Москва

Формализация экспертных знаний для управления инцидентами информационных систем на основе онтологического подхода

Аннотация

Данная статья посвящена решению проблемы сбора и формализации экспертных знаний, представляющих инциденты, получаемых в процессе эксплуатации информационных систем и предназначенных для решения задачи повышения эффективности их управления. Рассматриваются существующие подходы и инструменты решения проблемы управления инцидентами, определяются их основные недостатки. В качестве перспективного подхода предлагается использование онтологии предметной области, обеспечивающей базис для формирования концептуальной модели предметной области управления инцидентами информационных систем; организация объектов предметной области осуществляется с использованием классификации инцидентов ИС с использованием структурного подхода и классификатора, основанного на модели OSI. В статье также изложены основные принципы разработки прототипа системы управления инцидентами предназначенной для решения поставленных задач с использованием инструментальных средств Thinkmap SDK.

Ключевые слова: информационная система, управление, процессный подход, инцидент, онтология, классификация, модель предметной области, база знаний, экспертные знания.

Ludmila S. Bolotova

National Research University Higher School of Economics,

Dr. sc., prof., professor of the Department

Andrey A. Karasev

Lead Engineer, Department of Information Technology

National Research University Higher School of Economics

Vladimir A. Starykh

National Research University Higher School of Economics,

Ph. D., dean, professor of the Department

Formalization of the expert knowledge for incident`s management of information system based on the ontological approach

Summary

This article is devoted to a solution of the problem of collecting and formalization of the expert knowledge representing incidents received during the operation of information systems and designed to address the problem of increasing the efficiency of their management. The existing approaches and tools of a solution of the problem of incident management, their main shortcomings are defined. As perspective approach use of ontology subject domain providing basis for formation of conceptual model of subject domain for incident`s management of information system is offered; the organization of objects of subject domain is carried out with use of classification of incidents for information systems with use of structural approach and the qualifier based on the OSI/ISO model. The article also outlines the basic principles of developing a prototype incident management system by using Thinkmap SDK tools.

Keywords: information system, control, process approach, the incident, ontology, classification, the domain model, knowledge base, the expert knowledge.

Введение.

Постоянный рост объемов обрабатываемой информации, количества пользователей и повышение требований к производительности и надежности приводит к неизбежному увеличению сложности информационных систем (ИС). Современная ИС является децентрализованным разнородным программно-аппаратным комплексом, требующим для успешного функционирования значительных затрат материальных, финансовых, временных и человеческих

ресурсов. Децентрализация в данном случае означает наличие нескольких территориально-распределенных центров хранения и обработки данных, не всегда связанных друг с другом. Разнородность комплекса объясняется использованием в его составе оборудования и программного обеспечения (ПО) различных производителей, а также наличием разных версий программных продуктов и инструментов, созданных или доработанных самостоятельно. Ограниченность доступных ресурсов при построении и модернизации также приводит к росту разнородности ИС. Обеспечением ее функционирования при этом занимаются специалисты с разным уровнем квалификации и опытом работы, не всегда обладающие полной информацией о принципах организации работ смежных подсистем.

В этой ситуации особое значение приобретает задача эффективного управления программно-аппаратным комплексом, заключающаяся в управлении процедурами, связанными с обслуживанием аппаратного и программного обеспечения, а также информационными, материальными и временными ресурсами. На сегодняшний день наибольшее распространение получил процессный подход, рассматривающий задачу управления как совокупность взаимосвязанных процессов[1], выполняющихся на протяжении всего жизненного цикла ИС.

Типовые решения эффективного управления.

Стандартом де-факто процессного подхода к управлению ИС стала библиотека инфраструктуры информационных технологий ITIL (IT Infrastructure Library), первая версия которой была разработана по заказу правительства Великобритании в конце 1980-х гг. Текущая версия библиотеки ITIL v3 2011 Edition [1] объединяет все процессы и функции управления ИС в пять групп: стратегия, проектирование, преобразование, эксплуатация и постоянное улучшение услуг. Особую роль в управлении ИС играют процессы, относящиеся к группе эксплуатации услуг (Service Operation), в первую очередь – процессы управления инцидентами[2] и проблемами[3].

---

[1] Процесс в данном случае определяется как логически организованная последовательность работ или видов деятельности, направленная на достижение поставленной цели

[2] Библиотека ITIL определяет термин «инцидент» [2] как любое событие, не являющееся частью штатного функционирования ИС, и могущее привести к ухудшению параметров функционирования ИС, отдельной ее подсистемы или службы

[3] Проблемой [2] называется причина возникновения одного или нескольких инцидентов, не зарегистрированная к моменту их возникновения

Алгоритмы выполнения этих процессов, а также программные инструменты, предназначенные для их автоматизации, используются в первую очередь службой технической поддержки, Service Desk в терминологии ITIL. К ее основным функциям относятся регистрация, сбор необходимой информации, классификация и категоризация, разрешение и документирование информации о способах и методах разрешения возникающих инцидентов. В ходе работы служба технической поддержки (СТП) использует как нормативные данные, так и специальные знания об особенностях функционирования конкретной системы, накопленные в процессе эксплуатации и являющиеся для нее уникальными [3].

Нормативные данные могут быть представлены в виде справочников, спецификаций, инструкций по установке, настройке и эксплуатации серверного и сетевого оборудования, руководств администраторов и пользователей программных продуктов. К их преимуществам относится легкость хранения и передачи между сотрудниками организации; к недостаткам – описание функционирования отдельно взятого объекта, не учитывающее влияние других компонентов существующей инфраструктуры. С этой точки зрения специальные знания, позволяющие учитывать аспекты взаимодействия аппаратных и программных компонентов различных производителей в составе действующей ИС, не всегда отраженные в соответствующей документации разработчика, обладают большей ценностью.

Таким образом, эффективность функционирования ИС (определяемая, в том числе, количеством возникающих инцидентов и временем, затрачиваемым на их обнаружение и разрешение) зависит от возможности накопления (фиксации) и повторного использования информации, полученной в ходе обработки ранее возникавших инцидентов, для сокращения времени разрешения схожих и однотипных инцидентов в дальнейшем. В то же время отсутствие такой информации приводит к возникновению целого ряда факторов, негативно воздействующих на функционирование ИС и возможность управлять ею, в том числе:

- необходимость повторного многократного поиска способа разрешения однотипных инцидентов вместо использования стандартной, ранее задокументированной последовательности действий;

- невозможность заранее устранить причину инцидента на основании имеющейся информации – управляющее воздействие оказывается после возникновения инцидента, т.е. нарушения штатного режима функционирования ИС;
- недостаток управляющей информации, приводящий к принятию решений на основе предположений, а не ранее зафиксированных фактов;
- потеря значительного объема незафиксированных уникальных знаний в случае увольнения сотрудников СТП.

Инструментом, используемым в соответствии с рекомендациями библиотеки ITIL для хранения данных о зарегистрированных в системе инцидентах, причинах их возникновения и способах разрешения, являются базы данных инцидентов и проблем. Данные об инцидентах могут поступать из различных источников: от пользователей предоставляемых услуг, сотрудников организации, в автоматическом режиме от установленных систем мониторинга и управления. Обнаруженный любым из перечисленных способов инцидент регистрируется сотрудниками СТП в базе данных инцидентов.

Запись об инциденте содержит набор типовых полей: дату и время регистрации, источник поступления информации об инциденте, первичное описание, категорию, определяющую, на какую подсистему ИС или предоставляемую услугу он оказывает влияние, приоритет, рассчитываемый на основании степени воздействия и требуемой срочности разрешения, а также ряд других. Запись в базе данных инцидентов может не содержать описания последовательности действий, необходимых для его разрешения. Для хранения информации о причинах возникновения и возможных способах разрешения используется база данных проблем. Она содержит не только подробное руководство по разрешению возникающих инцидентов на основе задокументированных ранее в процессе эксплуатации ИС решений, в том числе и обходных, применяющихся для экономии времени и других ресурсов организации, но и рекомендации по устранению первопричин их возникновения.

Проблема, способная одновременно являться как причиной возникновения, так и результатом ранее произошедших в ИС инцидентов, в большинстве случаев связана более чем с одним инцидентом, каждый из которых оказывает сходное влияние на штатное функционирование

ИС [4]. Это означает, что для эффективного многократного использования накопленных знаний базы данных инцидентов и проблем должны быть взаимосвязаны – запись об инциденте должна быть связана со всеми записями о проблемах, которые могли привести к его возникновению, а запись о проблеме – со всеми записями о вызванных ею инцидентах. При этом запись о проблеме может также рассматриваться как самостоятельный источник информации, не зависящий от связанных с ней записей об инцидентах. Например, определение первопричин возникновения инцидента – поиск проблемы и документирование известной ошибки – может продолжаться после успешного разрешения самого инцидента и закрытия соответствующей записи.

В процессе эксплуатации ИС периодически возникают однотипные инциденты, действия для разрешения которых хорошо известны. При регистрации других используется стандартная процедура привязки классификационных данных инцидента к известным ошибкам и записям о проблемах. В случае обнаружения в базе данных записи об инциденте с аналогичным описанием выполняется последовательность ранее зафиксированных и строго регламентированных действий, что позволяет сократить время и значительно упростить процесс его разрешения. Классификация инцидентов и проблем позволяет сотрудникам службы технической поддержки рассматривать базы данных проблем как набор информации, организованный и хранимый таким образом, чтобы к нему можно было оперативно обращаться с помощью ссылок по легко определяемым типичным признакам новых инцидентов.

Во многих программных продуктах, предназначенных для автоматизации процессов управления инцидентами и проблемами, базы данных объединяются в общую постоянно пополняемую базу знаний ИС организации. Такая база содержит информацию о зарегистрированных инцидентах, определенных способах их разрешения, в том числе обходных решениях, а также установленных причинах возникновения, стандартной последовательности действий для их устранения и все существующие связи между ними и объектами управления. Подобные базы знаний могут быть как централизованными, предназначенными для использования в рамках одной организации или организационного подразделения, так и распределенными, предоставляющими интерфейсы для интеграции в открытые репозитории знаний в области управления ИС.

Для определения основных подходов к накоплению и последующему использованию специальных знаний в процессе функционирования ИС был проведен сравнительный анализ ряда специализированных программных продуктов[4]. Анализ проводился по таким критериям как источники наполнения баз данных, наличие предустановленных баз знаний, возможности создания и поддержания в актуальном состоянии связей между записями об инцидентах, проблемах и объектах управления, а также наличие встроенных классификаторов. В результате (фрагмент сравнительного анализа для трех программных продуктов приведен в таблице 1) был выявлен ряд недостатков существующих программных продуктов и применяемых в них методов, в том числе:

- Недостаточная формализация. Собранные знания хранятся в виде самостоятельных, не связанных друг с другом информационных статей, содержащих слабоструктурированную информацию, что не позволяет эффективно использовать информационные технологии для ее поиска и обработки.
- Отсутствие встроенных средств классификации. В большинстве программных продуктов отсутствуют классификаторы, в соответствии с которыми могли бы распределяться новые записи об инцидентах. В результате этого усложняется первоначальная привязка, определение причин возникновения и множества затронутых объектов управления; повышается вероятность появления дублирующихся записей и записей с однотипным содержанием.
- Отсутствие связей. В рассмотренном ПО не реализованы инструменты создания, редактирования и поддержания в актуальном состоянии связей между инцидентами, проблемами и объектами управления. Это приводит к отсутствию у пользователя возможности видеть причинно-следственные связи между событиями, приводящими к нарушению штатного режима функционирования ИС.

[4] Рассматривалось ПО автоматизации процессов управления инцидентами и проблемами IBM Tivoli Monitoring, Microsoft System Center Service Manager, HP Service Manager, BMC Remedy IT Service Management Suite, OTRS ITSM

Таблица 1 – Сравнительный анализ программных продуктов, применяемых для фиксации специальных знаний в процессе эксплуатации ИС

Название системы	**IBM Tivoli Monitoring**	**Microsoft System Center Service Manager [5]**	**HP Service Manager Knowledge Management [6]**
Формат хранения данных в базе инцидентов	файлы .htm	СУБД	СУБД
Источники наполнения базы инцидентов	поставляется с предустановленным набором типовых инцидентов, может пополняться вручную администратором	системы мониторинга, приложения сторонних производителей, e-mail обращения пользователей, может пополняться вручную администратором	может пополняться вручную администратором или пользователями при наличии необходимых прав
Наличие предустановленного набора типовых инцидентов	да	набор шаблонов для создания записей об инцидентах	нет
Возможность редактирования связей между инцидентами	не предусмотрена	не предусмотрена	не предусмотрена
Графическое отображение инцидентов и связей	нет	нет	нет
Поиск в базе	нет	полнотекстовый поиск	полнотекстовый поиск

инцидентов			по всем документам, преобразованным в HTML
Встроенные классификаторы инцидентов	отсутствуют	отсутствуют	отсутствуют

Как было отмечено выше, повторное использование накопленных специальных знаний позволяет повысить эффективность управления ИС за счет сокращения времени разрешения возникающих инцидентов и принятия управленческих решений, повышения точности этих решений, что в целом позволяет оптимизировать использование временных, финансовых, людских и других ресурсов организации. Однако такое повышение возможно только в случае решения задач формализации и классификации специальных знаний в процессе эксплуатации ИС. Перспективным подходом к их решению является использование онтологий.

Использование онтологий.

Онтология – термин, в интеллектуальных информационных системах и технологиях инженерии знаний обозначающий систему понятий заданной предметной области, представляемой в виде набора значимых сущностей и отношений, возможных между ними. Онтологии используются для формального определения понятий и свойств, формирующих концептуальную модель предметной области.

Появление и стремительное развитие онтологий на сегодняшний день связано с необходимостью перехода на качественно новый уровень поиска и обработки информации при решении таких задач как:

- обработка значительных объемов слабоструктурированной, часто противоречивой информации в различных областях деятельности;
- совместное использование общего хранилища информации специалистами в различных областях, в том числе смежных, для достижения различных целей;

- структуризация совместно используемой информации для представления пользователям;
- сокращение времени поиска требуемой информации и повышение точности, соответствия результатов поиска поисковому запросу.

Существующие определения термина «онтология» значительно различаются и зависят от области применения. Так, с точки зрения информационных систем онтология является базой знаний специального типа, которая может пополняться, использоваться, отчуждаться от разработчика, использоваться совместно с другими базами знаний или разделяться их пользователями [7].

Наиболее распространенное определение, используемое в интеллектуальных системах, описывает онтологию как формальную точную спецификацию совместно используемой концептуализации [8]. В этом определении под концептуализацией подразумевается абстрактная модель определенной предметной области, для которой установлены понятия (концепты), необходимые для описания сущностей, явлений и их взаимосвязей. Формальность означает возможность использования информационных технологий и средств вычислительной техники для автоматизации обработки данных онтологии. Точность подразумевает использование явно определенных типов включенных в состав онтологии понятий и ограничений на область их применения. Совместное использование означает, что онтологии используются для описания общепринятых в определенной группе или сообществе специалистов знаний на основе словаря терминов с объемом, достаточным для их описания.

Для всех определений термина «онтология» общим является наличие словаря имен сущностей, используемого для обмена знаниями в определенной предметной области, и множества связей между ними [9]. Связи могут относиться как к универсальным типам – «часть – целое», «причина – следствие», так и к типам, специфичным для данной предметной области. Сущности, как и связи, могут обладать заданными свойствами, необходимыми для отражения в абстрактной модели значимых свойств и отношений объектов области знаний.

Анализ возможностей онтологического подхода к организации знаний [8,10] позволяет сделать вывод о его применимости к формализации и структурированию экспертных знаний предметной области управления инцидентами, накопленными в ходе эксплуатации ИС.

Следующим шагом в решении поставленных задач является выбор принципов классификации накопленных знаний, в соответствии с которыми они будут организованы в онтологии. В данном исследовании применяются два независимых классификатора объектов предметной области управления ИС. Первый основан на структурном подходе теории информационных систем, позволяющем учитывать универсальные иерархические связи между объектами. Второй использует эталонную модель взаимодействия открытых систем (open systems interconnection, OSI) для определения специфичных для предметной области связей между объектами и их свойств.

Использование структурного подхода.

Структурный подход базируется на утверждении о том, что любая ИС может рассматриваться как совокупность своих подсистем. Примерами таких подсистем являются структурированная кабельная система (СКС), серверное оборудование, виртуальная инфраструктура или почтовая подсистема организации. ИС может состоять из произвольного количества подсистем; одна и та же подсистема может входить в состав ИС многих организаций. Далее в каждой подсистеме выделяется множество программно-аппаратных компонентов, из которых она состоит. Такими компонентами являются физическое или виртуальное оборудование и программное обеспечение. Следующим этапом декомпозиции является выделение в составе каждого аппаратно-программного компонента объектов управления, являющихся атомарными с точки зрения установления взаимосвязей с инцидентами предметной области (в данном случае понятие объектов управления аналогично понятию конфигурационных единиц – configuration items – используемых процессом управления конфигурациями библиотеки ITIL). Атомарный объект либо является причиной возникновения инцидентов, либо оказывается затронутым инцидентами, вызванными другими объектами. При необходимости объекты управления в составе аппаратно-программного комплекса могут объединяться в группы по тем или иным признакам.

На рисунке 1 представлен пример классификации инцидента в ИС с использованием структурного подхода.

Рисунок 1 – Связи инцидента с объектами управления при использовании структурного подхода

Инцидент, вызванный сбоем в работе сетевой службы DNS операционной системы Windows Server 2003, и влияющий на доставку почтовых сообщений серверной задачей Router ПО Lotus Domino связан с соответствующими атомарными объектами. Свойства объектов предметной области и отношения между ними, описываемые в рамках онтологического подхода, могут

использоваться для фиксации знаний как о самом инциденте, так и обо всех инцидентах, с ним связанных.

Эталонная модель OSI предназначена для концептуального определения процесса взаимодействия открытых систем, последовательно рассматривая его на семи уровнях, начиная с физического и заканчивая уровнем приложений. Назначение каждого уровня стандартизируется, определяется набор протоколов, функционирующих в его рамках, описываются интерфейсы, позволяющие передавать данные от одного уровня к другому.

Классификатор, основанный на эталонной модели взаимодействия открытых систем, позволяет логически упорядочить, сгруппировать и распределить инциденты по ее уровням. Распределение инцидентов может выполняться в зависимости как от того, к какому уровню модели относится объект управления, связанный с ними[5], так и от того, на каком уровне было нарушено взаимодействие в результате возникновения инцидента. В качестве примера распределения инцидентов по уровням модели OSI можно привести:

Физический уровень – нарушение целостности оптоволоконного кабеля, соединяющего центры обработки данных.

Канальный уровень – сбой сетевого подключения, вызванный неисправностью сетевого интерфейса сервера.

Сетевой уровень – не найден путь к указанному серверу из-за неверной конфигурации шлюза по умолчанию.

Транспортный уровень – сбой обмена TCP пакетами, вызванный некорректной настройкой параметра MTU (Maximum Transmission Unit, максимальный размер полезного блока данных).

Сеансовый уровень – невозможность установления соединения с удаленным сервером, вызванная использованием различных версий протокола SSH (Secure Shell).

Представительский уровень – ошибка подключения к удаленному рабочему столу при использовании клиентом и сервером несовместимых уровней шифрования.

Прикладной уровень – запрашиваемая пользователем Web-страница недоступна из-за ошибки сервера.

[5]Штатное функционирование которого, как объекта управления, было нарушено инцидентом, либо само привело к возникновению инцидента

Использование классификатора, основанного на семиуровневой модели взаимодействия OSI, позволяет организовывать и соответствующим образом распределять накопленные знания о причинах возникновения и способах разрешения, а также существующих взаимосвязях между инцидентами. Это дает специалисту, работающему с онтологией, возможность последовательно просматривать уровни, начиная с физического и заканчивая уровнем приложений в поисках корневой причины возникновения инцидента (рисунок 2).

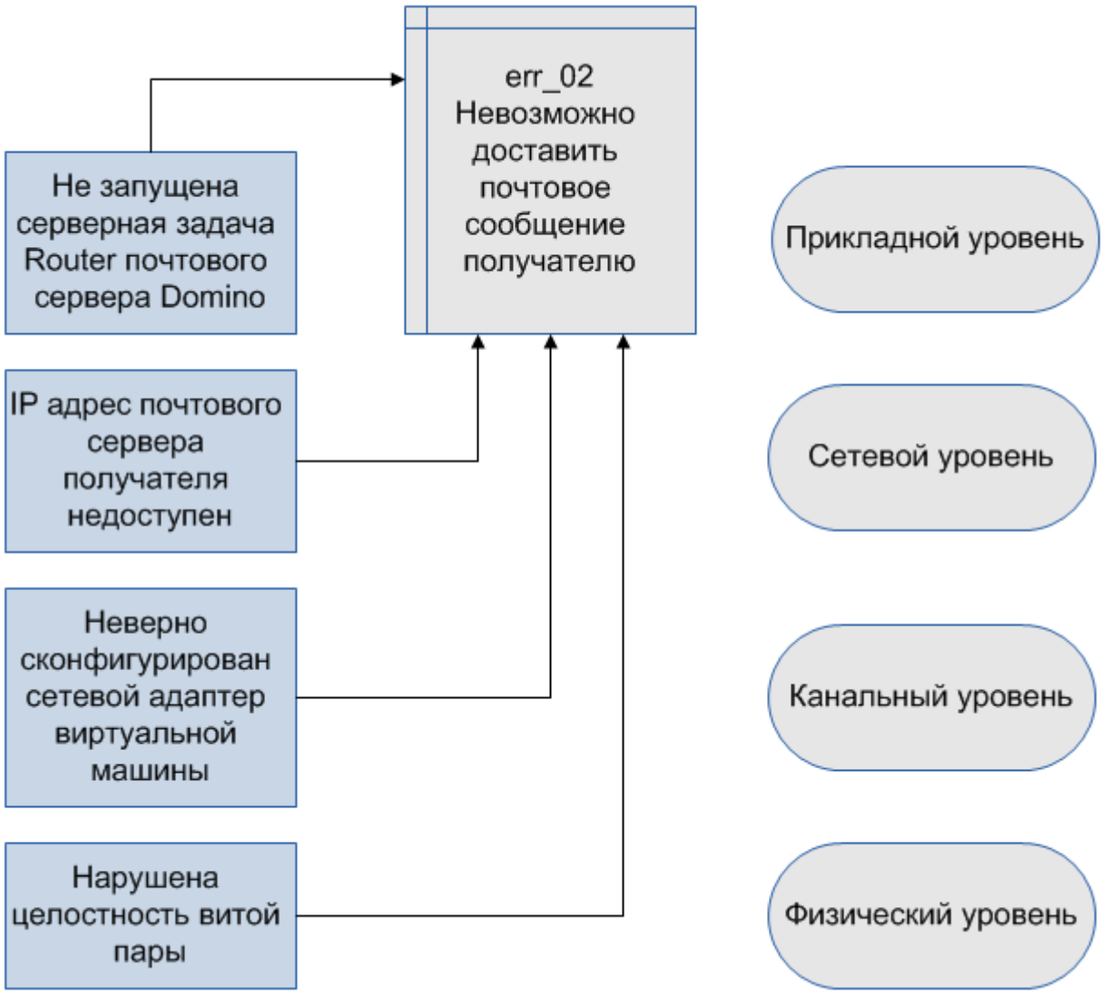

Рисунок 2 – Распределение причин возникновения инцидента по уровням модели OSI

В качестве инструмента построения и графического отображения инцидентов и связей между ними в данной работе используется комплект средств разработки Thinkmap [11]. Он обеспечивает поддержку ряда современных технологий (Java EE, HTML5, CSS, XML) и

предназначен для автоматизации обработки и визуализации (в том числе построения графических интерфейсов приложений) как формализованных, так и описываемых с помощью естественных языков данных. Модели предметной области, построенные с использованием Thinkmap, учитывают связи и различные типы взаимодействия объектов, а также их свойства. В качестве источника данных используются XML файлы, файлы данных (flat file) или реляционные СУБД; данные могут располагаться на выделенном сервере или локально на компьютере пользователя.

Определения структур данных.

Использование классификатора, основанного на выделении подсистем в составе ИС, требует определения структур данных, используемых для описания каждого уровня вплоть до атомарных объектов управления. Примером такой структуры для аппаратно-программного компонента в формате XML является:

```
<nodetype name="COMPONENT" >
        <property name="compname"   type="String"    />
        <property name="vendor"   type="String"    />
        <property name="comment"   type="String"    />
</nodetype>
```

Свойство compname используется для хранения названия серии и модели оборудования или названия и версии ПО; vendor – компании-производителя. Свойство comment содержит подробную характеристику, позволяющую специалисту, незнакомому с тем или иным компонентом ИС, быстро определить его тип и принадлежность к определенной подсистеме.

Далее приведен пример записи о коммутаторе Cisco как аппаратном компоненте подсистемы «активное сетевое оборудование».

```
<node type="COMPONENT" id="121" >
        <property name="compname"  value="Catalyst 3750G" />
        <property name="vendor"  value="Cisco" />
        <property name="comment"  value="Коммутатор" />
</node>
```

Основным типом сущностей в рассматриваемой онтологии предметной области управления ИС является инцидент. Приведенные выше классификаторы используются в первую очередь для организации и привязки к соответствующим объектам управления (узлам классификаторов) записей об инцидентах. Структура инцидента описывается в данной работе следующим образом [12]:

```
<nodetype name="INCIDENT" >
        <property name="code"   type="String"    />
        <property name="message"   type="String"    />
        <property name="severity"   type="String"    />
        <property name="type"   type="String"    />
        <property name="event"   type="String"    />
        <property name="action"   type="String"    />
        <property name="osi"   type="Float"    />
        <property name="comment"   type="String"    />
</nodetype>
```

Свойство code здесь предназначено для хранения идентификатора инцидента, отображаемого в графическом интерфейсе пользователя, построенного с использованием средств разработки Thinkmap. Свойство message содержит стандартное сообщение об ошибке, генерируемое соответствующим объектом управления. Поле severity определяет приоритет инцидента, вычисляемый на основании степени его воздействия на ИС организации и требуемой срочности разрешения. Поле type позволяет определить, с какой подсистемой, группой решаемых задач или аппаратно-программным компонентом связан инцидент. Свойства event и action содержат, соответственно, подробное описание самого инцидента и руководство по его разрешению, представляющую собой рекомендуемую последовательность действий, выполненных и зафиксированных при первоначальном разрешении инцидента. Поле osi является служебным и определяет принадлежность инцидента к заданному уровню в соответствии с

классификатором, основанным на эталонной модели взаимодействия открытых систем. Свойство message содержит краткое описание инцидента, также доступное в графическом интерфейсе.

Далее приведен пример записи об инциденте в соответствии с рассмотренной структурой в формате XML:

```
<node type="INCIDENT" id="171021" >
    <property name="code" value="INC_0038" />
    <property name="message" value="The remote procedure call timed out and was canceled" />
    <property name="severity" value="Средняя" />
    <property name="type" value="Администрирование ОС" />
    <property name="event" value="При попытке выполнения удаленного вызова процедуры Active Directory (репликация изменений) время ожидания истекло, вызов отменен" />
    <property name="action" value="Установите значение параметра реестра RPC Replication Timeout (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters), равное 45 минутам" />
    <property name="osi" value="7" />
    <property name="comment" value="Ошибка репликации изменений службы каталогов Active Directory" />
</node>
```

Для описания связи атомарного объекта управления с одним или несколькими инцидентами используется следующая структура данных:

```
<edgetype name="OBJECT_INCIDENT" from="OBJECT" to="INCIDENT" >
    <property name="issuedby" type="Boolean" />
    <property name="affect" type="Boolean" />
    <property name="comment" type="String" />
</edgetype>
```

Здесь поля issuedby и affect определяют, стал ли объект управления причиной возникновения инцидента или, в свою очередь, было ли его функционирование нарушено

возникшим инцидентом. Свойство comment содержит текстовое пояснение, доступное в графическом интерфейсе.

Работа прототипа системы управления инцидентами.

На рисунке 3 представлен общий вид пользовательского интерфейса прототипа системы управления инцидентами, разработанной с использованием инструмента Thinkmap.

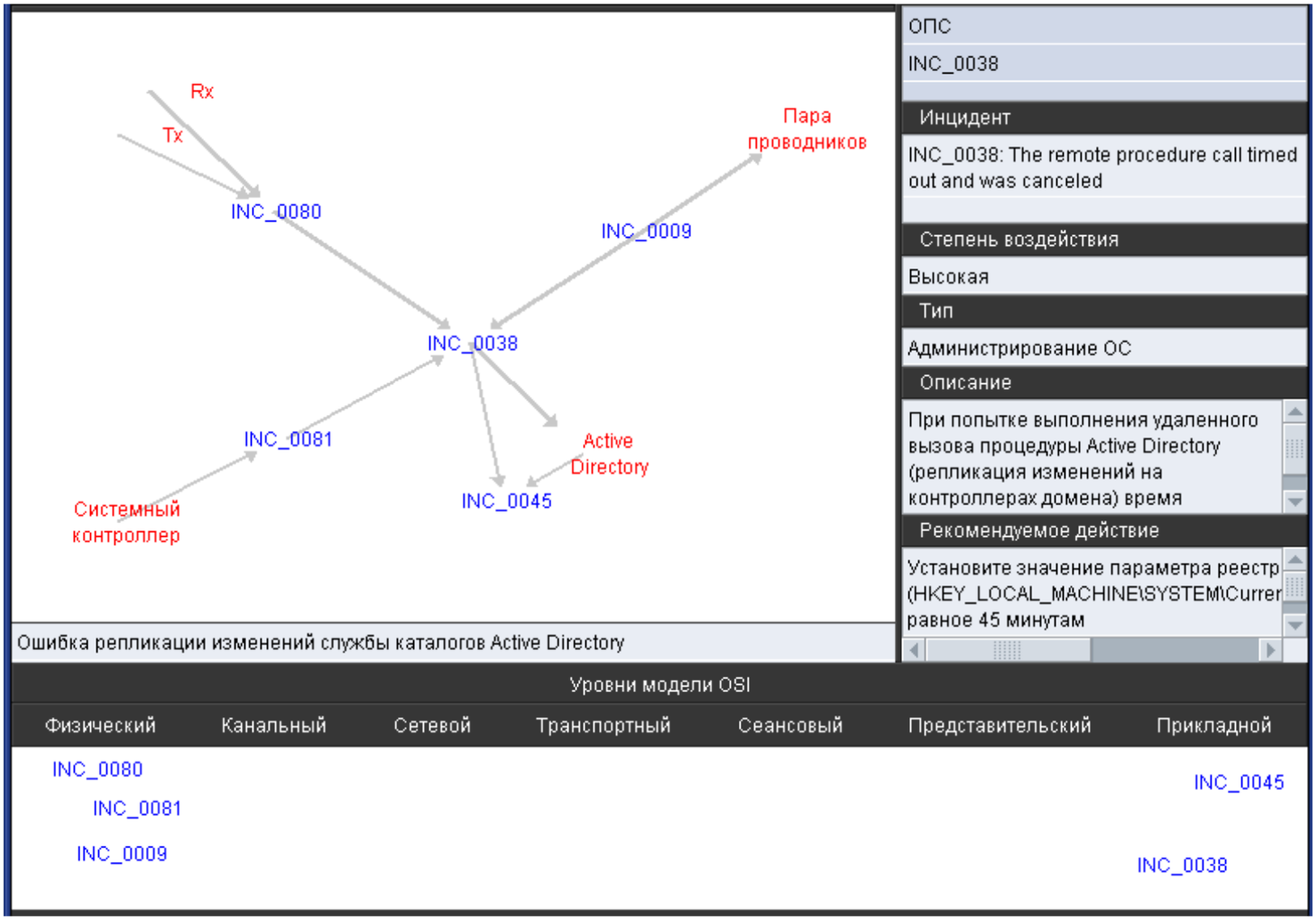

Рисунок 3 – общий вид инцидентов, объектов управления и связей между ними в пользовательском интерфейсе прототипа системы управления инцидентами

В рабочей области расположены инциденты, обозначенные идентификаторами, хранящимися в поле code соответствующей записи, связи между ними и объектами управления и

сами объекты управления, отобранные в зависимости от текущего представления. Для выбранного инцидента в правой панели отображается подробная информация в соответствии со структурой записей об инцидентах. В нижней панели отображаются инциденты текущего представления, распределенные по уровням эталонной модели взаимодействия открытых систем OSI.

Заключение

Применение онтологического подхода и разработанных классификаторов объектов предметной области управления инцидентами ИС позволяет разработать инструмент, учитывающий недостатки существующих систем управления и предоставляющий пользователю функции, в них не реализованные. Такими функциями являются классификация и разрешение инцидентов с учетом выявленных причинно-следственных связей, а также возможность получать информацию о причинах, структуре и уровне их возникновения в соответствии с эталонной моделью OSI.

Разработанный прототип системы может использоваться для накопления и формализации экспертных знаний, полученных в процессе эксплуатации ИС. Их использование позволит повысить эффективность управления за счет сокращения времени классификации и разрешения возникающих в системе инцидентов и повышения точности принимаемых управленческих решений.

Литература

1. http://www.itil-officialsite.com/
2. Глоссарий терминов и определений ITIL V3/ ITIL V3 Glossary / Пер. с англ. ITIL V3 Translation Project. – М.: itSMF Russia, 2009. – 146 с.
3. Поддержка услуг: библиотека ITIL. – М.: Компания “Ай-Теко”, 2006. – 395 с.
4. IT Service Management (ITSM) Implementation Workshop Student Guide. – Houston: BMC Software Inc., 2008. – 508 p.
5. URL: http://www.microsoft.com/ru-ru/server-cloud/system-center/service-manager.aspx

6. URL: http://h20195.www2.hp.com/V2/GetPDF.aspx%2F4AA1-6148ENW.pdf

7. Константинова, Н.С. Онтологии как системы хранения знаний / Н.С. Константинова, О.А. Митрофанова. – СПб.: Санкт-Петербургский государственный университет, 2009. – 54 с.

8. Болотова, Л.С. Системы искусственного интеллекта: модели и технологии, основанные на знаниях / Л.С. Болотова. – М.: Финансы и статистика, 2012. – 664 с.

9. Соловьев, В.Д. Онтологии и тезаурусы: учебно-методическое пособие / В.Д. Соловьев, Б.В. Добров, В.В. Иванов, Н.В. Лукашевич. – Казань: Издательство Казанского государственного университета, 2006. – 157 с.

10. Гаврилова, Т.А. Формирование прикладных онтологий / Т.А. Гаврилова // КИИ-2006: труды X национальной конференции по искусственному интеллекту, Обнинск, 25-28 сентября 2006 г. М.: Физматлит, 2006. – Том 2

11.URL: http://www.thinkmap.com

12. Карасёв, А.А. Определение структуры инцидента в системе управления инцидентами на основе онтологического подхода и семиотического моделирования / А.А. Карасев, В.А. Старых, С.С. Смирнов //Труды XX Всероссийской научно-методической конференции «Телематика’2013». Том 1. – СПб.: «Университетские телекоммуникации», 2013. – с. 93-94.