УДК 004.056:061.68

М.А. Колтик

СИСТЕМНО-ОНТОЛОГИЧЕСКИЙ АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ ПРОВЕДЕНИЯ ИСПЫТАНИЙ КСЗИ

Проводится системно-онтологический анализ процесса проведения испытаний комплексной системы защиты информации (КСЗИ). Рассматривается феномен онтологии, методика ее построения, онтологический подхода к анализу предметной области исследования. Проводится анализ онтологических моделей проведения предварительных и экспертных испытаний КСЗИ. Рассматривается фрагмент онтологического графа и глоссарий разрабатываемой онтологии процесса проведения испытаний КСЗИ.

Введение

Огромный интерес вызывают системы, способные без участия человека извлечь какие-либо сведения из текста. Как результат, на фоне вновь возникающих потребностей развиваются новые технологии, призванные решить заявленные проблемы. Наряду с World WideWeb появляется его расширение, Semantic Web, в котором гипертекстовые страницы снабжаются дополнительной разметкой, несущей сведения о семантике включаемых в страницы элементов. Неотъемлемым компонентом Semantic Web является понятие онтологии, описывающее смысл семантической разметки.

В общих чертах под онтологией понимается система понятий некоторой предметной области, которая представляется как набор сущностей, соединенных различными отношениями. Онтологии используются для формальной спецификации понятий и отношений, которые характеризуют определенную область знаний. Преимуществом онтологий в качестве способа представления знаний является их формальная структура, которая упрощает их компьютерную обработку [1, 2].

Цель данной статьи – проведение системно-онтологического анализа предметной области проведения испытаний КСЗИ.

Задача. Построить онтологическую модель представляющую процесс проведения предварительных испытаний КСЗИ и онтологическую модель процесса проведения экспертных испытаний КСЗИ. Разработать фрагмент онтологического графа онтологии проведения предварительных и экспертных испытаний КСЗИ.

Анализ необходимости построения онтологической модели процесса проведения испытаний КСЗИ

Испытания КСЗИ являются одним из важнейших этапов в её создании, дающий возможность оценить уровень защищенности автоматизированной системы, выступающей в качестве объекта испытаний [3]. Данный вид деятельности, как и любой другой вид интеллектуальной деятельности, связан с присущими ему специфичными знаниями.

Анализируя проблемы присущие процессу проведения испытаний КСЗИ описанные в [3], предложен способ их решения, заключающийся в создании программного средства автоматизированной поддержки для проведения испытаний КСЗИ. Специфика анализируемых проблем и самого процесса проведения испытаний КСЗИ, подталкивает к тому, чтобы рассматривать данное программное средство, как интеллектуально-информационную систему, главным компонентом которой является база знаний основанная на онтологии. Следовательно, построение онтологической модели для представления процесса проведения испытаний КСЗИ, является необходимым условием для ее системно-онтологического анализа.

Также, анализ методики технологического процесса проведения испытаний КСЗИ, алгоритма функционирования программного средства [4], рассмотрение по-

следовательности обработки различных видов информации на различных этапах проведения испытаний и их специфики, рассмотрение входных и выходных данных на каждом этапе проведения испытаний [5], говорит о целесообразности использования системно-онтологического подхода для проведения анализа данной предметной области и построения с ее использованием онтологической модели процесса проведения испытаний КСЗИ.

Центральной идеей данного подхода является разработка онтологических средств поддержки решения прикладных задач – полифункциональной онтологической системы [6]. Именно такой подход позволяет говорить об успешной реализации на его основе автоматизированной поддержки проведения испытаний КСЗИ, которая заключается в решении прикладных задач связанных с предоставлением специалисту необходимых знаний, помощи в принятии правильного решения, предоставлении определенных суждений и умозаключений способствующих осуществлению правильных выводов и в общем порождении нового знания относящегося к анализу защищенности конкретного объекта испытаний.

Анализ онтологических моделей предметной области проведения испытания КСЗИ

Анализ предметной области представляет особый вид научной деятельности, в результате которого строится интерпретационная модель предметных знаний (в широком смысле). В процессе анализа последние делятся на инвариантные и прагматичные знания, концептуальные составляющие которых представляют онтологические знания предметной области. Новым направлением в области средств и методов системного анализа предметной области является системно-онтологический анализ. Центральной идеей системно-онтологического подхода является разработка онтологической системы [7].

Под онтологической системой в данной работе будем понимать кортеж множеств $O=(X,R,F)$, где X – конечное множество концептов (понятий) заданной предметной области – процесса проведения испытаний КСЗИ, R – конечное множество отношений между концептами X, F – конечное множество функций интерпретации, заданных на множествах X и/или R. Частным случаем задания множества функций интерпретации F является глоссарий, составленный для множества понятий X. В базовой онтологии примем, что множество F тождественно множеству аксиом A, представляющих истинные высказывания о соответствующих понятиях X [8].

Представленные далее модели, на концептуальном уровне описывают, моделируют онтологическую систему процесса проведения предварительных и экспертных испытаний КСЗИ, с использованием системно-онтологического подхода. Данный подход подразумевает создание онтологии, которая является формализованным представлением знаний используемых в рассматриваемой предметной области.

Создание онтологии подразумевает на первом этапе перечисление всех категорий, обозначающие сущности или явления в моделируемой области. Затем нужно связать эти категории определенными отношениями. И на последнем этапе нужно соотнести категориям набор конкретных экземпляров [1]. Данный подход является упрощенным, но он дает общее представление о разрабатываемой онтологии.

Будим использовать данный подход для построения моделей данной предметной области, за исключением рассмотрения конкретных экземпляров. В связи с тем, что данная онтология подразумевает включение достаточно большого количества конкретных экземпляров, их рассмотрение будет произведено на примере фрагмента онтологического графа данной предметной области.

Рассматриваемые модели отражают общую методику процесса проведения предварительных и экспертных испытаний КСЗИ, состав фрагментов онтологии, характер взаимосвязей фрагментов онтологии, задачи, решаемые на каждом этапе данными фрагментами онтологий и полученный результат в процессе функциони-

рования рассматриваемой технологической линии.

В состав представленных моделей входят элементы четырех категорий: понятия, отношения, аксиомы, отдельные экземпляры. Они группируются вокруг отдельно выделенных категорий – сущностей, которые выступают в качестве родового понятия и формируют отдельные фрагменты онтологии, которые являются составляющими частями общей онтологии.

Каждый фрагмент онтологии, представляет собой набор классов и подклассов понятий, конкретных экземпляров данных классов связанных между собой отношениями как таксономического, так и функционального значения. С помощью отношений устанавливаются связи как между классами понятий, понятиями так и отдельными экземплярами. Каждый фрагмент онтологии содержит перечень уникальных для него аксиом и глоссарий терминов.

Характеристика онтологической модели технологического процесса проведения предварительных испытаний КСЗИ

Характеристика фрагментов онтологической модели. Данная модель представляет, с использованием онтологического подхода, описание технологического процесса проведения предварительных испытаний КСЗИ, с помощью, которого реализуется проектирования КСЗ в соответствии с заявленными требованиями и оценка данных требований на соответствие национальным критериям защищенности информации в соответствии с [9].

В состав онтологической модели технологического процесса проведения предварительных испытаний КСЗИ входят следующие ее фрагменты, а именно:

– анализ объекта испытаний и циркулирующей в нем информации;

– анализ модели угроз и нарушителей;

– требования по защите информации;

– критерии оценки защищенности информации в компьютерных системах от НСД;

– уровни функционального профиля защищенности ОИ;

– механизмы и средства защиты объекта испытаний.

Для фрагмента онтологии «**Анализ объекта испытаний и циркулирующей в нем информации**» родовой сущностью является категория «Объект испытаний». Данный фрагмент онтологии предназначен для предоставления пользователю знаний относительно характеристики объекта испытаний и определения объектов защиты.

Часть онтологического графа данного фрагмента онтологии, будет рассмотрена в качестве примера далее.

Для фрагмента онтологии «**Анализ модели угроз и нарушителей**» родовыми сущностями является две равнозначные категории «Угроза» и «Нарушитель». В данном фрагменте онтологии целесообразно рассматривать две данные родовые сущности, поскольку анализ технологии проведения предварительных испытаний КСЗИ показывает, что они являются тесно взаимосвязанными и обладают большим количеством функциональных отношений, которые связывают между собой многие классы понятий, понятия и отдельные экземпляры понятий данных рассматриваемых сущностей. Данный фрагмент онтологии предназначен для предоставления пользователю знаний для корректного определения перечня потенциальных угроз и потенциальных нарушителей информационной безопасности объекта испытаний и проведения их классификации.

Для фрагмента онтологии «**Требования по защите информации**» родовой сущностью является категория «Требования». Данный фрагмент онтологии предназначен для предоставления пользователю знаний относительно характеристики требований для обеспечения необходимого уровня информационной безопасности объекта испытаний и их классификации.

Для фрагмента онтологии «**Критерии оценки защищенности информации в компьютерных системах от НСД**» ро-

довой сущностью является категория «Критерии». Данный фрагмент онтологии предназначен для предоставления пользователю знаний относительно структуры критериев и их описания в соответствии с нормативным документом НД ТЗИ 2.5 – 004 – 99. Данный фрагмент онтологии используется для предоставления знаний относительно корректного формирования требований информационной безопасности, а также характеризует уровни функционального профиля защищенности анализируемого объекта испытаний.

Для фрагмента онтологии «**Уровни функционального профиля защищенности ОИ»** родовой сущностью является категория «Уровень ФПЗ». Данный фрагмент онтологии предназначен для предоставления пользователю знаний, необходимых для корректного определения и формирования функционального профиля защищенности соответствующего уровня, в соответствии с заявленными требованиями и на основе критериев оценки защищенности информации в компьютерных системах от НСД.

Для фрагмента онтологии «**Механизмы и средства защиты объекта испытаний**» родовыми сущностями является две равнозначные категории «Механизмы защиты» и «Средства защиты». В данном фрагменте онтологии целесообразно рассматривать две данные родовые сущности, поскольку анализ технологии проведения предварительных испытаний КСЗИ показывает, что они являются тесно взаимосвязанными и обладают большим количеством функциональных отношений, которые связывают между собой многие классы понятий, понятия и отдельные экземпляры понятий данных рассматриваемых сущностей. Данный фрагмент онтологии предназначен для предоставления пользователю знаний необходимых для корректного определения перечня механизмов и средств защиты объекта испытаний от потенциальных угроз, реализованных потенциальными нарушителями, в соответствии с заявленными требованиями и на основе сформированного функционального профиля защищенности.

Характеристика функциональных отношений онтологической модели. Рассматриваемая онтологическая модель включает следующие **функциональные отношения** между фрагментами онтологии:

– «Определяет объекты защиты»;
– «Классификация угроз и нарушителей»;
– «Формируются»;
– «Характеризуются»;
– «Включают набор»;
– «Являются мерой»;
– «Предъявляются к».

Функциональное отношение «**Определяет объекты защиты**» устанавливающее связь между соответствующими фрагментами онтологии, отражая общую концепцию отношений между ними, представляет характер отношения между сущностями «Объект испытаний» и «Угроза», «Нарушитель», а также, решаемую задачу, соответствующим фрагментом онтологии на данном этапе взаимодействия с пользователем.

Функциональное отношение «**Классификация угроз и нарушителей**» устанавливающее связь между соответствующими фрагментами онтологии, отражая общую концепцию отношений между ними, представляет характер отношения между сущностями «Угроза», «Нарушитель» и «Требования», а также, решаемую задачу, соответствующим фрагментом онтологии на данном этапе взаимодействия с пользователем.

Функциональное отношение «**Включают набор**» представляет характер отношения между сущностями «Требования» и «Уровень ФПЗ», устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

Функциональное отношение «**Предъявляются к**» представляет характер отношения между сущностями «Требования» и «Механизмы защиты», «Средства защиты», устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

Функциональное отношение «**Формируются**» представляет характер отношения между сущностями «Требования» и «Критерии», устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

Функциональное отношение «**Характеризуются**» представляет характер отношения между сущностями «Уровни ФПЗ» и «Критерии» устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

Функциональное отношение «**Являются мерой**» представляет характер отношения между сущностями «Уровни ФПЗ» и «Механизмы защиты», «Средства защиты» устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

В качестве результата работы должно быть предоставлено заключение, с возможными количественными и качественными характеристиками, относительно достаточности выбранных механизмов и средств защиты, для защиты информации от потенциальных угроз, в соответствии с заявленными требованиями.

Онтологическая модель, которая описывает предметную область процесса проведения предварительных испытаний КСЗИ, показана на рис. 1.

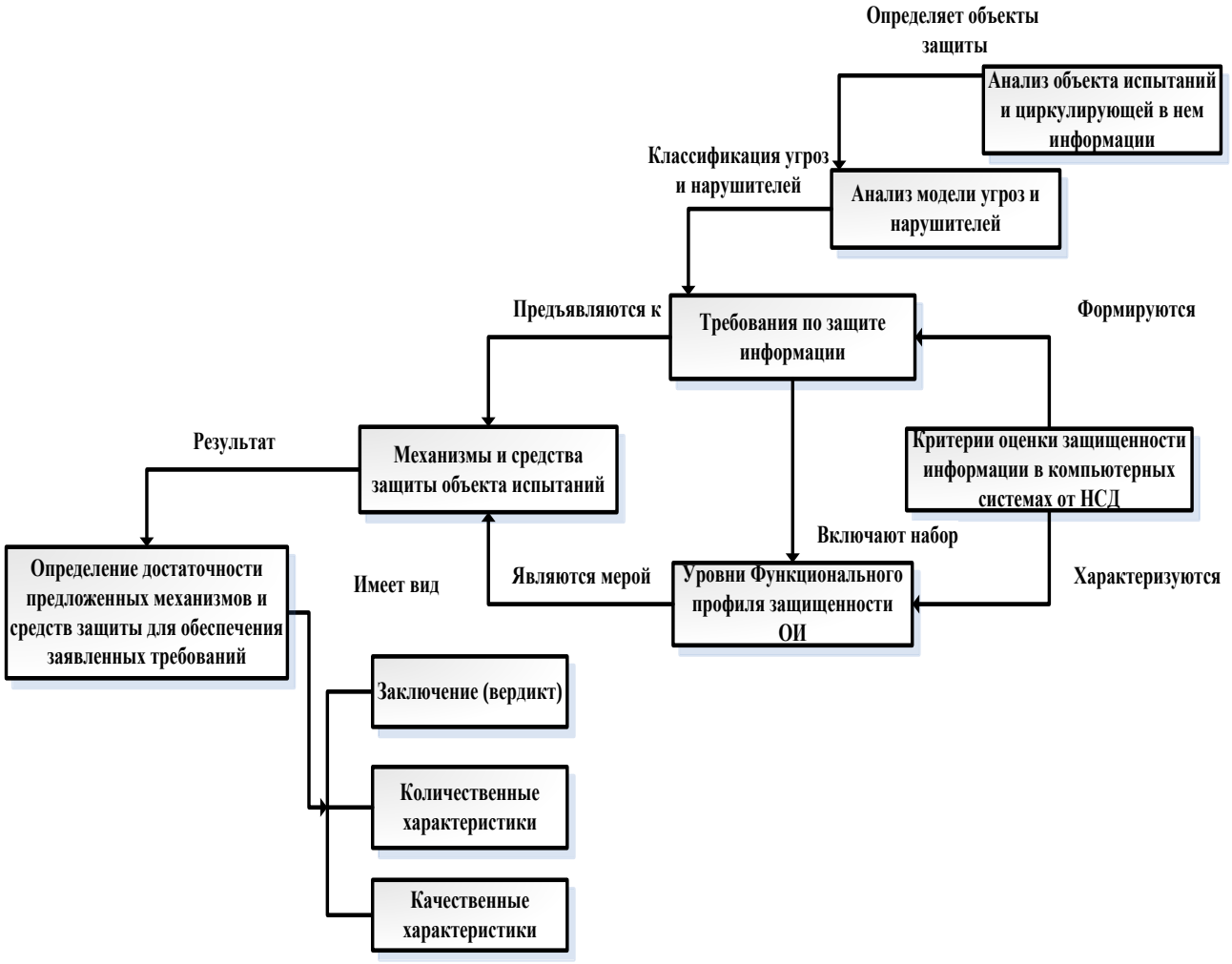

Рис. 1. Онтологическая модель представления процесса проведения предварительных испытаний КСЗИ

Характеристика онтологической модели технологического процесса проведения экспертных испытаний КСЗИ

Характеристика фрагментов онтологической модели. Данная модель представляет, с использованием онтологического подхода, описание технологического процесса проведения экспертных испытаний КСЗИ, с помощью, которого реализуется оценивание уровня защищенности объекта испытаний.

В состав онтологической модели технологического процесса проведения экспертных испытаний КСЗИ входят следующие ее фрагменты, а именно:

– анализ объекта испытаний и циркулирующей в нем информации;

– анализ модели угроз и нарушителей;

– анализ состава и структуры реализованного комплекса средств и механизмов защиты;

– критерии оценки защищенности информации в компьютерных системах от НСД;

– уровни требуемого функционального профиля защищенности;

– уровни реализованного функционального профиля защищенности;

– оценивание соответствия реализуемого и требуемого функционального профиля защищенности;

– определение требуемых механизмов и средств защиты объекта испытаний.

Для фрагментов онтологий «**Анализ объекта испытаний и циркулирующей в нем информации**», «**Анализ модели угроз и нарушителей**», «**Критерии оценки защищенности информации в компьютерных системах от НСД**» предназначение данных фрагментов онтологий совпадает с описанным в онтологической модели технологического процесса проведения предварительных испытаний КСЗИ.

Для фрагмента онтологии «**Анализ состава и структуры реализованного комплекса средств и механизмов защиты**» родовыми сущностями является две равнозначные категории «Механизмы защиты» и «Средства защиты». В данном фрагменте онтологии целесообразно рассматривать две данные родовые сущности, поскольку анализ технологии проведения предварительных испытаний КСЗИ показывает, что они являются тесно взаимосвязанными и обладают большим количеством функциональных отношений, которые связывают между собой многие классы понятий, понятия и отдельные экземпляры понятий данных рассматриваемых сущностей. Данный фрагмент онтологии предназначен для предоставления пользователю знаний для корректного определения состава и структуры реализованного комплекса средств и механизмов защиты информации рассматриваемого объекта испытаний.

Для фрагмента онтологии «**Требуемые механизмы и средства защиты объекта испытаний**» родовыми сущностями является две равнозначные категории «Механизмы защиты» и «Средства защиты». В данном фрагменте онтологии целесообразно рассматривать две данные родовые сущности, поскольку анализ технологии проведения предварительных испытаний КСЗИ показывает, что они являются тесно взаимосвязанными и обладают большим количеством функциональных отношений, которые связывают между собой многие классы понятий, понятия и отдельные экземпляры понятий данных рассматриваемых сущностей. Данный фрагмент онтологии предназначен для предоставления пользователю знаний необходимых для корректного определения перечня требуемых механизмов и средств защиты объекта испытаний.

Необходимо отметить, что в данном технологическом процессе фрагменты онтологии «Анализ состава и структуры реализованного комплекса средств и механизмов защиты» и «Требуемые механизмы и средства защиты объекта испытаний», логически необходимо рассматривать как два разных фрагмента, хотя, по сути, фрагмент онтологии один, поскольку

родовые категории – сущности одни «Механизмы защиты» и «Средства защиты». Технологический процесс предусматривает их отдельное рассмотрение, поскольку задачи данных частей одного фрагмента онтологии отличаются. В данном фрагменте онтологии с сущностями «Механизмы защиты» и «Средства защиты», технологически предусмотрено построение двух иерархических деревьев классов, каждое предназначено для выполнения своей задачи. То есть, с точки зрения технологии использование одного фрагмента онтологии будет проводиться дважды. Сначала для анализа реализованного комплекса средств и механизмов защиты, а затем для определения требуемых механизмов и средств защиты.

Для фрагмента онтологии «**Уровни требуемого функционального профиля защищенности ОИ**» родовой сущностью является категория «Уровень ФПЗ». Данный фрагмент онтологии предназначен для предоставления пользователю знаний, необходимых для корректного определения и формирования функционального профиля защищенности соответствующего уровня, в соответствии с определенным перечнем угроз и нарушителей, на основе критериев оценки защищенности информации в компьютерных системах от НСД.

Для фрагмента онтологии «**Уровни реализованного функционального профиля защищенности ОИ**» родовой сущностью является категория «Уровень ФПЗ». Данный фрагмент онтологии предназначен для предоставления пользователю знаний, необходимых для корректного определения и формирования функционального профиля защищенности соответствующего уровня, в соответствии с проведенным анализом состава и структуры реализованного комплекса средств и механизмов защиты ОИ и на основе критериев оценки защищенности информации в компьютерных системах от НСД.

Необходимо отметить, что в данном технологическом процессе фрагменты онтологии «Уровни требуемого функционального профиля защищенности ОИ» и «Уровни реализованного функционального профиля защищенности ОИ», логически необходимо рассматривать как два разных фрагмента, хотя, по сути, фрагмент онтологии один, поскольку родовая категория – сущность одна «Уровень ФПЗ». Технологический процесс предусматривает их отдельное рассмотрение, поскольку задачи данных частей одного фрагмента онтологии отличаются. В данном фрагменте онтологии с сущностью «Уровень ФПЗ», технологически предусмотрено построение двух иерархических деревьев классов, каждое предназначено для выполнения своей задачи. То есть, с точки зрения технологии использование одного фрагмента онтологии будет проводиться дважды. Сначала для анализа реализованного функционального профиля защищенности, а затем для определения требуемого функционального профиля защищенности.

Для фрагмента онтологии «**Оценивание соответствия реализуемого и требуемого функционального профиля защищенности**» родовой сущностью является категория «Уровень ФПЗ». Данный фрагмент онтологии предназначен для предоставления пользователю знаний, необходимых для корректного проведения оценивания соответствия реализуемого и требуемого функционального профиля защищенности и формирования соответствующих выводов, относительно сохранения, добавления или удаления отдельно рассматриваемых функций в реализованном функциональном профиле защищенности, для приведения его в соответствие с требуемым функциональным профилем защищенности.

Необходимо отметить, что в данном технологическом процессе фрагмент онтологии «Оценивание соответствия реализуемого и требуемого функционального профиля защищенности», логически необходимо рассматривать как отдельный фрагмент, хотя, по сути, он относится к фрагменту онтологии с родовой категорией – сущностью «Уровень ФПЗ». В рассматриваемой модели целесообразно поэтапное и отдельное рассмотрение, разных решаемых задач одного фрагмента онтологии. В данном фрагменте онтоло-

гии технологически предусмотрено как построение двух иерархических деревьев классов, каждое из которых предназначено для выполнения своей задачи, так и оценка соответствия одного иерархического дерева другому, устанавливая соответствующие отношения между ними, что также является отдельной задачей. На основе проведения данного оценивания строятся соответствующие выводы. То есть, с точки зрения технологии при использовании данного фрагмента онтологии будет проводиться оценивание его классов, понятий и сущностей (установка отношений), что в соответствии с технологией целесообразно рассматривать как отдельную логическую часть построения фрагмента онтологии.

Характеристика функциональных отношений онтологической модели. Рассматриваемая онтологическая модель включает следующие **функциональные отношения** между фрагментами онтологии:

– «Определяет объекты защиты»;
– «Классификация угроз и нарушителей»;
– «Определяет функции КСЗ»;
– «Характеризуют»;
– «Подлежат»;
– «Предоставляют возможность».

В представленной модели, выделенные функциональные отношения описывают характер связей между и внутри фрагментов онтологии.

Функциональное отношение «**Определяет объекты защиты**» устанавливающее связь между соответствующими фрагментами онтологии, отражая общую концепцию отношений между ними, представляет характер отношения между сущностями «Объект испытаний» и «Угроза», «Нарушитель», а также, решаемую задачу, соответствующим фрагментом онтологии на данном этапе взаимодействия с пользователем.

Функциональное отношение «**Классификация угроз и нарушителей**» устанавливающее связь между соответствующими фрагментами онтологии, отражая общую концепцию отношений между ними, представляет характер отношения между сущностями «Угроза», «Нарушитель» и «Уровни ФПЗ», а также, решаемую задачу, соответствующим фрагментом онтологии на данном этапе взаимодействия с пользователем.

Функциональное отношение «**Определяет функции КСЗ**» представляет характер отношения между сущностями «механизмы защиты», «Средства защиты» и «Уровень ФПЗ», устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

Функциональное отношение «**Характеризуют**» представляет характер отношения между сущностями «Уровни ФПЗ» и «Критерии» устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

Функциональное отношение «**Подлежат**» представляет характер отношения между построенными различными деревьями классов, внутри фрагмента онтологии с родовой сущностью «Уровни ФПЗ» отражая общую концепцию отношений между ними.

Функциональное отношение «**Предоставляют возможность**» представляет характер отношения между сущностями «Уровни ФПЗ» и «Механизмы защиты», «Средства защиты», устанавливая связь между соответствующими фрагментами онтологии и отражая общую концепцию отношений между ними.

В качестве результата работы должно быть предоставлено заключение относительно уровня защищенности объекта испытаний от НСД, проведено определение недостатков, полноты и достаточности реализованного ФПЗ, предоставлены предложения по изменению реализуемого ФПЗ в соответствии с требуемым ФПЗ. Проведено представление механизмов и средств защиты ОИ, исходя из требуемых изменений ФПЗ. Проведено обоснование требуемых изменений.

Онтологическая модель, описывающая предметную область процесса проведения экспертных испытаний, показана на рис. 2.

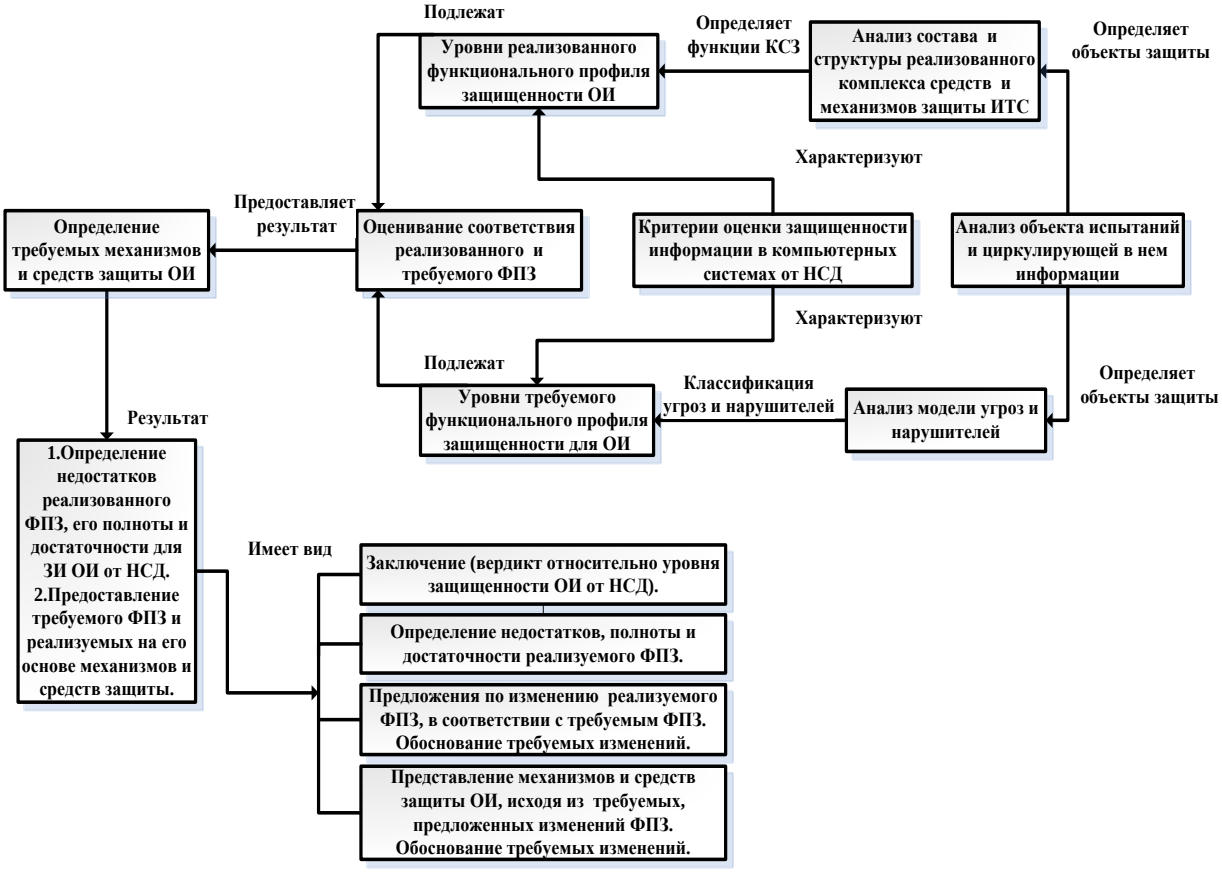

Рис. 2. Онтологическая модель представления процесса автоматизированной поддержки экспертных испытаний КСЗИ

Характеристика фрагмента онтологического графа «Объект испытаний» предметной области проведения испытания КСЗИ

Задача представленного фрагмента онтографа. В общем случае методика проектирования онтологии включает три этапа:

– предварительный анализ заданной предметной области;

– построение вручную онтографа предметной области. Под онтографом понимается ориентированный граф, вершинами которого являются понятия ПдО, а дугами – связи, отношения между ними;

– графическое (визуальное) проектирование онтографа ПдО и составление формализованного описания онтологии ПдО [2].

Задача в построении онтологического графа порождается методикой в разработке онтологии предметной области.

Представленный онтологический граф является частью фрагмента онтологического графа «Объект испытаний» отражающего начальный этап процесс проведения испытаний КСЗИ. Фрагмент онтографа «Объект испытаний», предоставляет суждения и умозаключения для осуществления характеристики объекта испытаний и определения объектов защиты, которые являются компонентами рассматриваемого объекта испытаний.

Характеристика понятий. В состав представленного фрагмента онтографа входят следующие понятия, представленные в структурированном порядке обобщенного отношения выше-ниже:

1. Объект испытаний.

2. Информационно-телекоммуникационная система (ИТС).

2.1. Программное обеспечение.

2.1.1. Системное программное обеспечение.

2.1.1.1. Базовое программное обеспечение.

2.1.1.1.1. Операционные системы.

2.1.1.1.1.1. Windows.

2.1.1.1.1.1.1. Server 2003.

2.1.1.1.1.1.2. 2000.

2.1.1.1.1.1.3. XP.

2.1.1.1.1.1.4. NT.

2.1.1.1.1.1.5. Другое.

2.1.1.1.1.2. Unix.

2.1.1.1.1.3. Linux.

2.1.1.1.1.4. Macintosh.

2.1.1.1.1.5. Другие.

2.1.1.1.2. Оболочки.

2.1.1.1.3. Сетевые операционные системы.

2.1.1.2. Сервисное программное обеспечение (утилиты).

2.1.1.2 1. Утилиты диагностики ОС.

2.1.1.2 2. Архивирования.

2.1.1.2 3. Обслуживания носителей.

2.1.1.2 4. Обслуживания сети.

2.1.1.2 5. Другое.

2.1.2. Прикладное программное обеспечение.

2.1.2.1. Общего назначения.

2.1.2.1.1. Текстовые процессоры.

2.1.2.1.2. Графические редакторы.

2.1.2.1.3. Электронные таблицы.

2.1.2.1.4. Web-браузер.

2.1.2.1.5. СУБД.

2.1.2.1.6. Интегрированное ПО.

2.1.2.1.7. Другое.

2.1.2.2. Специального назначения.

2.1.2.2.1. Экспертные системы.

2.1.2.2.2. Мультимедиа.

2.1.2.2.3. Гипертекстовые системы.

2.1.2.2.4. Другое.

2.1.2.3. Профессионального назначения.

2.1.2.3.1. САПР.

2.1.2.3.2. АРМ.

2.1.2.3.3. АСУ.

2.1.2.3.4. АСУ ТП.

2.1.2.3.5. Другое.

2.1.3. Системы программирования.

2.1.3.1. Трансляторы.

2.1.3.2. Среды разработки программ.

2.1.3.3. Библиотеки справочных программ, функций, процедур.

2.1.3.4. Отладчики.

2.1.3.5. Другое.

2.2. Аппаратное обеспечение.

2.3. Сетевое обеспечение.

2.4. Топология ИТС.

3. Информация.

3.1. Категории информации.

3.1.1. Открытая информация.

3.1.2. Информация ограниченного доступа (Конфиденциальная).

3.2. Виды информации.

3.2.1. Технологическая.

3.2.2. Финансовая.

3.2.3. Статистическая.

3.2.4. Другая.

3.3. Требуемые свойства информации.

3.3.1. Конфиденциальность информации.

3.3.2. Целостность информации.

3.3.3. Доступность информации.

3.3.4. Наблюдаемость информации.

4. Пользователи.

5. Документация.

Характеристика отношений. В представленном фрагменте онтологического графа выделяются **таксономические отношения**, которые определяют иерархию и структуру классов понятий, подклассов понятий, понятий и конкретных экземпляров.

В представленном фрагменте онтологического графа, также выделяются **функциональные отношения**, которые описываются заданными объектными свойствами, такими как: «Является», «Требует обеспечения», которые описывают функциональные отношения между понятиями.

Множество **таксономических отношений** состоит из следующего перечня отношений: целое – часть, класс – подкласс, подкласс – экземпляр,

Множество **функциональных отношений** состоит из следующего перечня отношений – является.

Выделенные отношения позволяют находить необходимые пользователю зависимости между компонентами онтологии.

Характеристика аксиом. Данные аксиомы задают условия соотнесения понятий и отношений, они выражают очевидные утверждения, связывающие понятия и отношения. Данные аксиомы можно понимать как утверждения, вводимые в онтологию в готовом виде, из которых могут быть выведены другие утверждения.

В представленном онтографическом графе в качестве примера выделяются две аксиомы, которые представлены далее.

Аксиома 1. Аксиома, описывающая отношение между экземпляром «Windows Server 2003» класса «ОС Windows» и экземпляром «Конфиденциальная информация» класса «Категории информации» (табл. 1).

Таблица 1

Понятие	Значение понятия
X	Экземпляр – Windows Server 2003 класса «ОС Windows» базового системного программного обеспечения
Y	Конфиденциальная информация

Аксиома: «Если **X** является **Y**, тогда **X** объект защиты».

Данная **аксиома 1** задает условие соотнесения экземпляров «Windows Server 2003 SP2», «Конфиденциальная информация» и отношения между ними – «Является» и выражают очевидное утверждение связывающие понятия и отношение. Данная аксиома предоставляет возможность суждения относительно того, что ОС Windows Server 2003 SP2 – это объект защиты.

Необходимо отметить, что онтология предоставляет возможность определить все экземпляры, входящие в состав ИТС ОИ и являются ли они носителями конфиденциальной информации.

Данное суждение может выводится для пользователя в качестве умозаключения на экран и являться результатом работы вывода нового знания с помощью данного фрагмента онтологии.

Аксиома 2. Аксиома, описывающая отношение между экземпляром «Технологическая информация» класса «Вид информации» и экземпляром «Конфиденциальная информация» класса «Категории информации» (табл. 2).

Таблица 2

Понятие	Значение понятия
X	Экземпляр – Технологическая информация класса «Вид информации» обрабатываемой в объекте испытаний;
Y	Конфиденциальная информация;

Аксиома: «Если **X** является **Y**, тогда **X** информация с ограниченным доступом».

Данная **аксиома 2** задает условие соотнесения экземпляров «Технологическая информация», «Конфиденциальная информация» и отношения между ними – «Является» и выражают очевидное утверждение связывающие понятия и отношение. Данная аксиома предоставляет возможность суждения относительно того, что технологическая информация является информацией с ограниченным доступом.

Необходимо отметить, что онтология предоставляет возможность определить все экземпляры, входящие в состав ИТС ОИ и определить являются ли они информацией с ограниченным доступом.

Данное суждение может выводиться для пользователя в качестве умозаключения на экран и являться результатом работы вывода нового знания с помощью данного фрагмента онтологии.

Представление фрагмента онтографа «Объект испытаний» онтологии предметной области проведения испытаний КСЗИ. Представленный фрагмент онтографа предметной области проведения испытаний КСЗИ может быть в дальнейшем использован, как составной компонент более полного онтологического графа онтологии проведения испытаний КСЗИ, а также для его формализации при разработке онтологии данной предметной области.

Фрагмент онтографа «Объект испытаний» онтологии предметной области проведения испытаний КСЗИ показан на рис. 3.

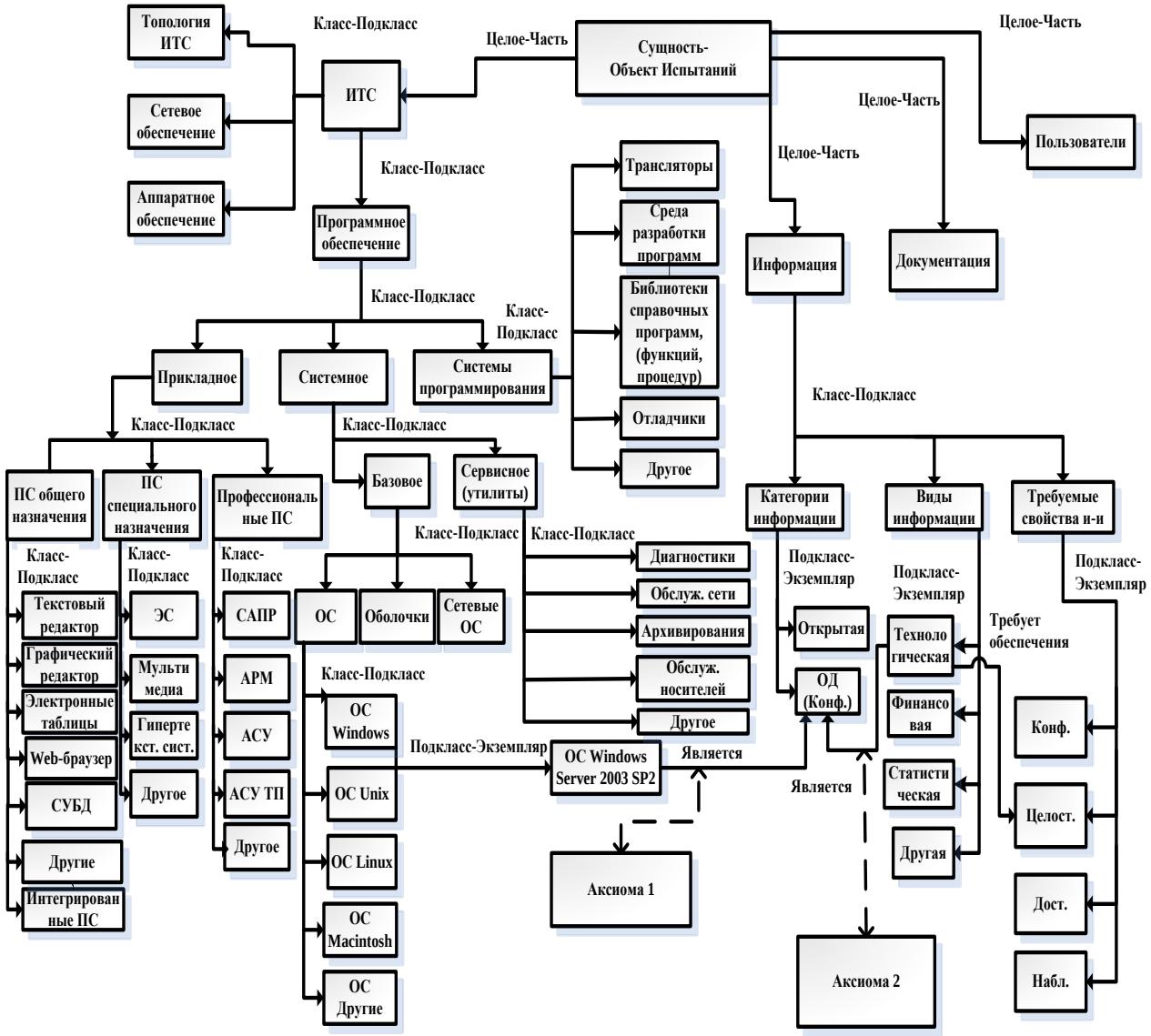

Рис. 3. Фрагмент онтографа «Объекта испытаний» предметной области «Проведение испытаний КСЗИ»

Построение глоссария основных терминов для фрагмента онтологии «Объект испытаний» предметной области проведения испытания КСЗИ

Для заданной предметной области создается глоссарий, который включает термины характерные для рассматриваемой предметной области и их естественно – языковое описание. Фрагмент глоссария приведен в табл. 3.

Таблица 3. Фрагмент глоссария терминов для фрагмента онтологии «Объект испытаний» предметной области проведения испытания КСЗИ

Термин	Описание
Объект испытаний	автоматизированная система (АС) как организационно-техническая система, реализующая информационную технологию и объединяет вычислительную систему, персонал и информацию которая обрабатывается и для которой разрабатывается или оценивается комплекс средств защиты
Вычислительная система	совокупность программно-аппаратных средств, предназначенных для обработки информации
Информационно-телекоммуникационная система (ИТС)	совокупность взаимосвязанных каналами дальнего приема и передачи информации аппаратно-программных и технических средств, объединенных в единое целое из территориально-разнесенных элементов для обеспечения технологического цикла обработки (поиска, сбора, хранения, переработки, редактирования) информации и выдачи потребителю в требуемой форме результатов такой обработки
Информация	совокупность сведений (сообщений) об окружающем мире (событиях, лицах, явлениях, процессах, фактах и их взаимосвязях), представленных в виде, пригодном для передачи одними людьми и восприятия другими, используемых в целях получения знаний и принятия решений
Пользователь	(user) физическое лицо, которое может взаимодействовать с ИТС через предоставленный ею интерфейс; лицо, использующее действующую систему для выполнения конкретной функции
Программное обеспечение	совокупность всех программ и подготовленных определенным образом данных, обеспечивающих использование компьютера в интересах его пользователя
Системное ПО	(system software) комплекс программ, обеспечивающих управление компонентами компьютерной системы, такими как процессор, оперативная память, устройства ввода-вывода, сетевое оборудование, выступая как «Межслойный интерфейс», с одной стороны которого аппаратура, а с другой – приложения пользователя
Прикладное ПО	(application software) программа, предназначенная для выполнения определенных пользовательских задач и рассчитанная на непосредственное взаимодействие с пользователем
Системы программирования	система для разработки новых программ на конкретном языке программирования

Выводы

Создание онтологий является перспективным направлением современных исследований по обработке информации, представляемой на естественном языке и

применению данных разработок в сфере информационной безопасности, в частности при проведении испытаний КСЗИ.

В рамках работы дано определение понятию онтология, проведен системно-онтологический анализ предметной области проведения испытаний КСЗИ. Предоставлена разработанная онтологическая модель процесса проведения предварительных и экспертных испытаний КСЗИ. На ее основе предложен общий поход к построению онтологии рассматриваемой предметной области. В статье представлен разработанный фрагмент онтологического графа и глоссария для онтологии проведения предварительных и экспертных испытаний КСЗИ. Рассмотрены основные особенности построения онтологии данной предметной области.

Необходимо отметить, что представленная онтологическая модель – это первый необходимый шаг на пути к построению АС поддержки проведения испытаний КСЗИ.

В дальнейшем планируется провести более детальную и полную разработку онтологического графа предметной области проведения испытаний КСЗИ, а также рассмотреть различные аспекты формализации и способов их проведения, при построении онтологии данной предметной области. Разработанная база знаний на основе онтологии, будет рассматриваться как основной компонент интеллектуальной информационной системы предназначенной для реализации автоматизированной поддержки при проведении предварительных и экспертных испытаний КСЗИ.

1. *http*://window.edu.ru/resource/795/58795/files/68352e2-st08.pdf
2. *http*://archive.nbuv.gov.ua/portal/natural/Kzms/2011/2011_st1.pdf
3. *Колтик М.А.* Проблемы массового построения КСЗИ и пути их решения // Проблеми програмування «ИПС» НАН Украины. – 2011. – № 3. – С. 72–81.
4. *Колтик М.А.* Методы и способы реализации автоматизированной поддержки проведения испытаний КСЗИ // Проблеми програмування. – 2013. – № 1. – С. 85 – 99.
5. *Баровская Е.Н., Колтик М.А.* Характеристика информационных потоков программных модулей входящих в состав программного средства для автоматизированной поддержки проведения испытаний КСЗИ // Проблеми програмування. – 2013. – № 3. – С. 86–99.
6. *http*://www.aduis.com.ua/books/1.pdf
7. *http*://archive.nbuv.gov.ua/portal/natural/Rks/2010_5/Potij.pdf
8. *http*://paws.kettering.edu/~pstanche/ibs-15-p02-KDS2-Palagin_et_al.pdf
9. *НД* ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

Получено 23.05.2013

Об авторе:

Колтик Максим Анатолиевич,
аспирант.

Место работы автора:

Институт программных систем
НАН Украины,
03187, Киев-187,
Проспект Академика Глушкова, 40.
Тел.: 067 218 2809.
E-mail: maxfaktor@ua.fm