УДК 004.056:061.68

М.А. Колтик

ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИИ ДЛЯ ОБЪЕКТА ИСПЫТАНИЙ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИИ ПРОВЕДЕНИЯ ИСПЫТАНИЙ КСЗИ

В данной статье проводится системно-онтологический анализ процесса построения модели угроз и нарушителей информации объекта испытаний. Рассматривается особенности построения модели угроз и нарушителей информации с использованием онтологии проведения испытаний КСЗИ. Проводится описание фрагментов онтологических графов определенных модулей онтологии используемых при построении модели угроз и нарушителей информации для объекта испытаний. Проводится анализ особенностей извлечения специализированных знаний для рассматриваемых онтологических модулей.

Введение

Возможность использования онтологий в качестве узкоспециализированной базы знаний, из которой пользователь может извлечь необходимые для него знания является актуальной задачей. В данном случае, рассматривается вопрос использования онтологии для построения модели угроз и нарушителей информации.

Цель данной статьи – описание модели угроз и нарушителей информации для отдельного объекта испытаний с использованием онтологии проведения испытаний КСЗИ.

Задачи построения фрагментов онтологического графа проведения предварительных и экспертных испытаний КСЗИ, которые используются для разработки модели угроз и нарушителей информации объекта испытаний; анализ особенностей разработки модели угроз и нарушителей информации объекта испытаний с использованием рассматриваемых фрагментов онтологии.

Анализ построения модели угроз и нарушителей с использованием онтологии проведения испытаний КСЗИ

Преимуществом онтологий в качестве способа представления знаний является их формальная структура, которая упрощает их компьютерную обработку [1].

Онтология проведения испытаний КСЗИ относится к онтологиям предметной области или так называемые онтологиям нижней зоны. Онтологии данного типа описывают конкретные предметные области с их спецификой. При этом круг решаемых задач и вопросов, на которые онтология отвечает, ограничен выбранной областью, в данном случае проведением испытаний КСЗИ.

Центральной идеей используемой при разработке онтологии является модульный подход. Каждый из выделенных модулей, отвечает за выполнение отдельных функциональных задач и решение отдельных вопросов [2].

При построении модели угроз и модели нарушителей информации используются следующие онтологические модули: «Характеристика ОИ», «Модель угроз», «Модель нарушителя», характеристика фрагментов которых приведена далее.

Использование данных онтологических модулей предоставляет возможность извлекать специализированные знания, которые позволяют разработчику КСЗИ или эксперту более эффективно обрабатывать сложную и разнообразную информацию, относящуюся к процессу построения модели угроз и нарушителей информации для рассматриваемого объекта испытаний.

Описание фрагмента онтологического графа модуля «Объект испытаний» онтологии предметной области проведения испытания КСЗИ

В соответствии с представленными моделями функционирования онтологии, предметной области проведения испытаний КСЗИ, выделяются отдельные ее модули, на основании тех задач, которые они выполняют на отдельных этапах функционирования онтологии.

Рассматриваемый фрагмент онтографа онтологического модуля «Объект испытаний» онтологии проведения испытаний КСЗИ, предназначен для осуществления поддержки пользователя при проведении им характеристики объекта испытаний и циркулирующей в нем информации и используется на начальном этапе взаимодействия пользователя с базой знаний основанной на разрабатываемой онтологии.

Данный фрагмент онтологического графа, представленный на рис. 1 – это часть онтологического графа модуля «Объект испытаний» описанного в [2], отражающего начальный этап процесса проведения испытаний КСЗИ.

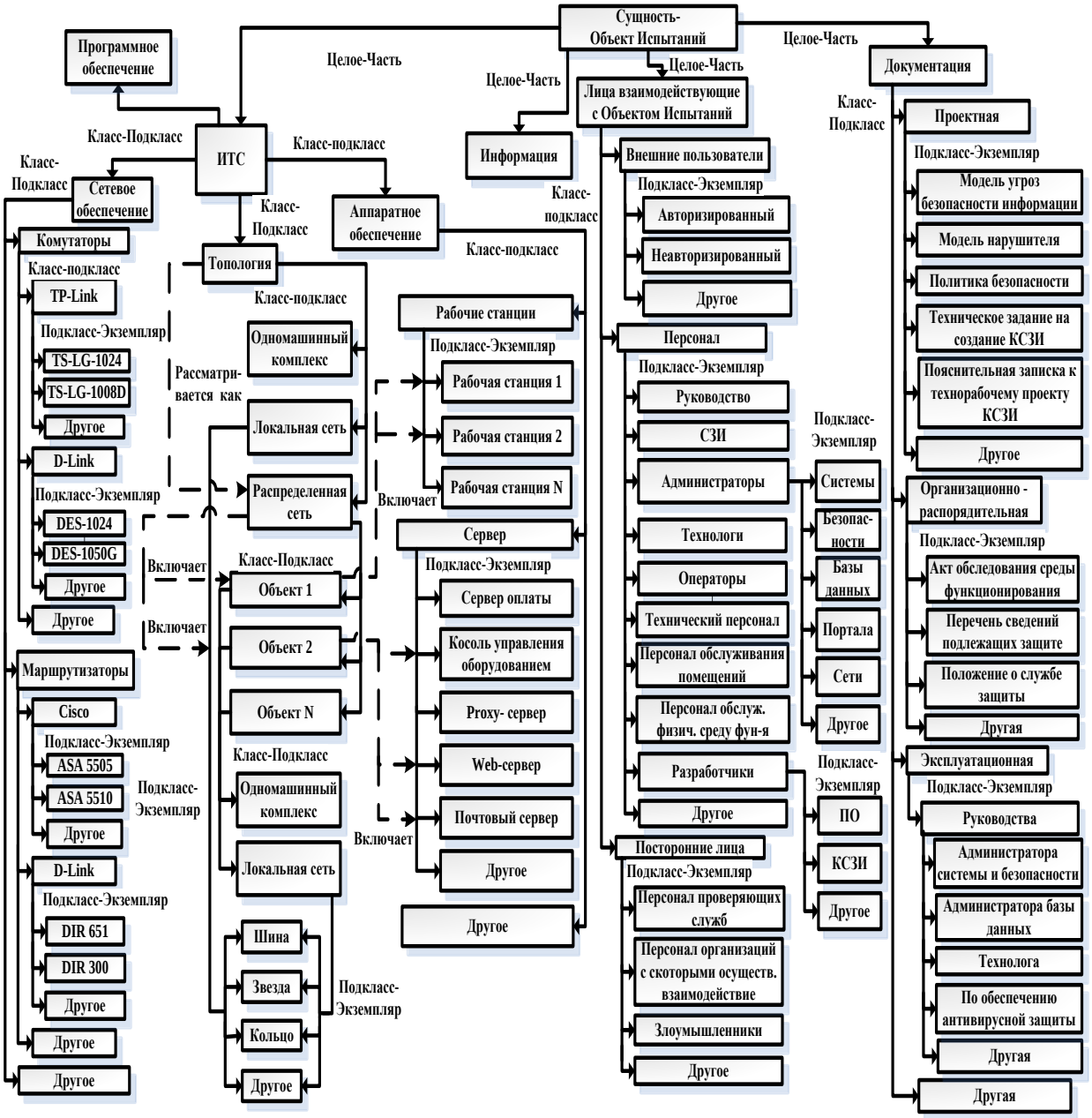

Рис. 1. Фрагмент онтографа модуля «Объекта испытаний» онтологии предметной области проведения испытаний КСЗИ

Фрагмент онтографа модуля «Объект испытаний», онтологии предметной области проведения испытания КСЗИ, предоставляет возможность получения знаний и осуществления умозаключений в процессе проведения характеристики объекта испытаний и определения объектов защиты, которые являются компонентами рассматриваемого объекта испытаний.

В состав фрагмента онтографа модуля «Объект испытаний» входят понятия, показанные на рис. 1, которые находятся в структурированном порядке обобщенного отношения выше – ниже.

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: «***рассматривается как***», «***включает***», 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 – рассматривается как включает.

Выделенные отношения позволяют находить необходимые пользователю зависимости между компонентами онтологии.

Представление фрагмента онтографа «Объект испытаний» онтологии предметной области проведения испытаний КСЗИ.

Представленный на рис. 1 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.

Описание фрагмента онтологического графа модуля «Модель угроз» онтологии предметной области проведения испытания КСЗИ

В онтологии предметной области проведения испытания КСЗИ выделяется модуль «Модель угроз» на основании выделения отдельного комплекса задач, которые выполняются с его использованием.

Общая схема взаимодействия модулей данной онтологии представлена в [2].

Рассматриваемые фрагменты онтографа рис. 2 и 3 онтологического модуля «Модель угроз» онтологии проведения испытаний КСЗИ, предназначены для осуществления поддержки пользователя, которая выражается в получении им знаний и умозаключений в процессе построения модели угроз для рассматриваемого объекта испытаний с помощью использования базы знаний, которая основана на разрабатываемой онтологии.

Для каждого класса, подкласса или экземпляра понятий модуля «Объект испытаний» определяются потенциальные характерные угрозы, путем установления соответствующих межмодульных отношений с экземплярами класса «Перечень угроз» модуля «Модель угроз». Данные отношения позволяют устанавливать логические связи между понятиями, на основе которых формируются соответствующие суждения и умозаключения об объекте испытаний и его модели угроз информационной безопасности.

Взаимодействие характеризуется, также, межмодульными аксиомами, которые дают возможность построения умозаключений и вывода отдельных знаний о рассматриваемом объекте испытаний.

В состав онтологического модуля «Модель угроз» входят понятия, представленные на рис. 2 и 3, которые находятся в структурированном порядке обобщенного отношения выше – ниже.

В представленном фрагменте онтологического графа выделяются **таксономические отношения**, которые

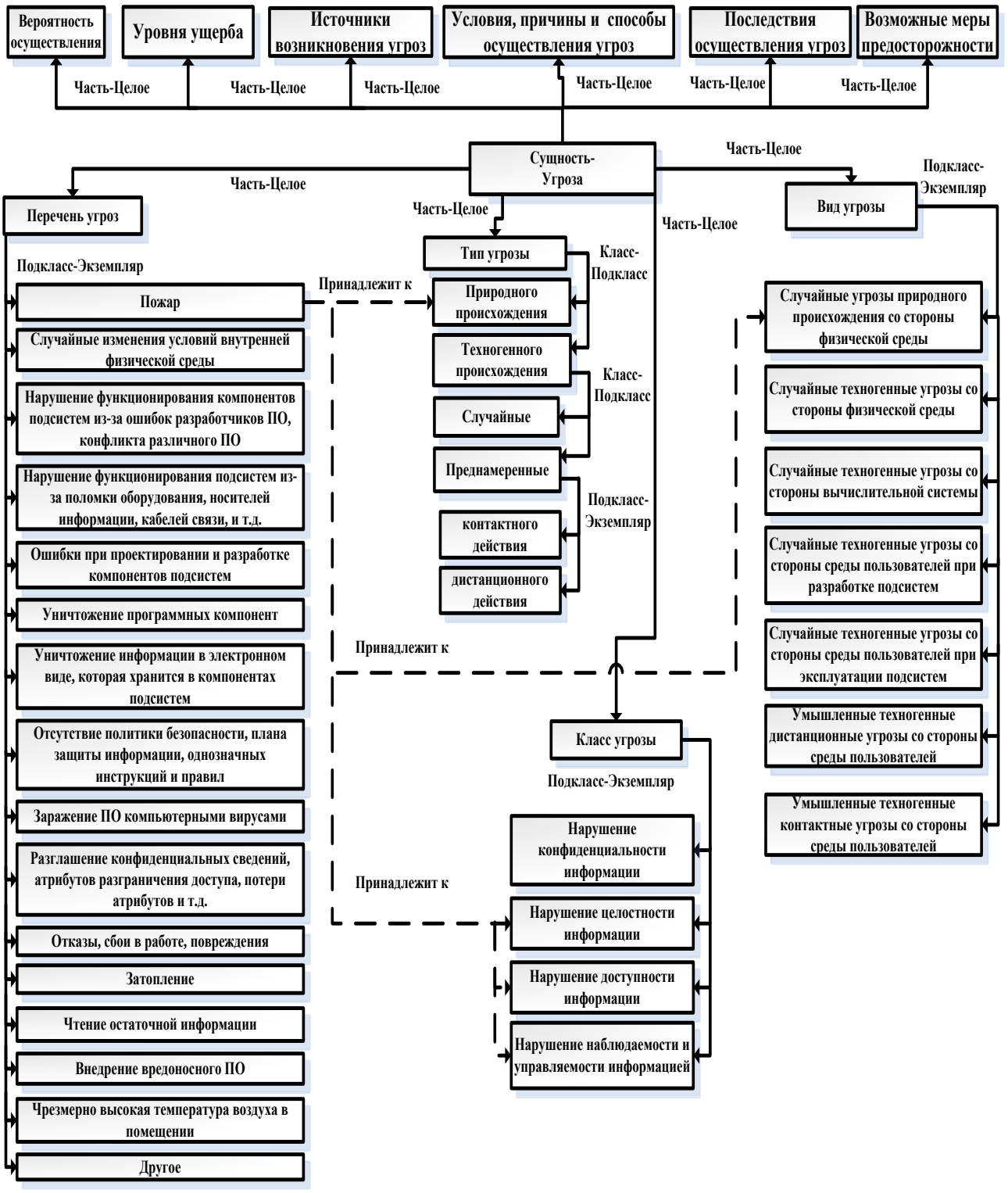

Рис. 2. Фрагмент онтографа модуля «Модель угроз»
онтологии предметной области проведения испытаний КСЗИ (1)

определяют иерархию и структуру классов понятий, подклассов понятий, понятий и конкретных экземпляров.

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

В представленном фрагменте онтологического графа, также выделяются **функциональные отношения**, которые описываются заданными объектными сво-

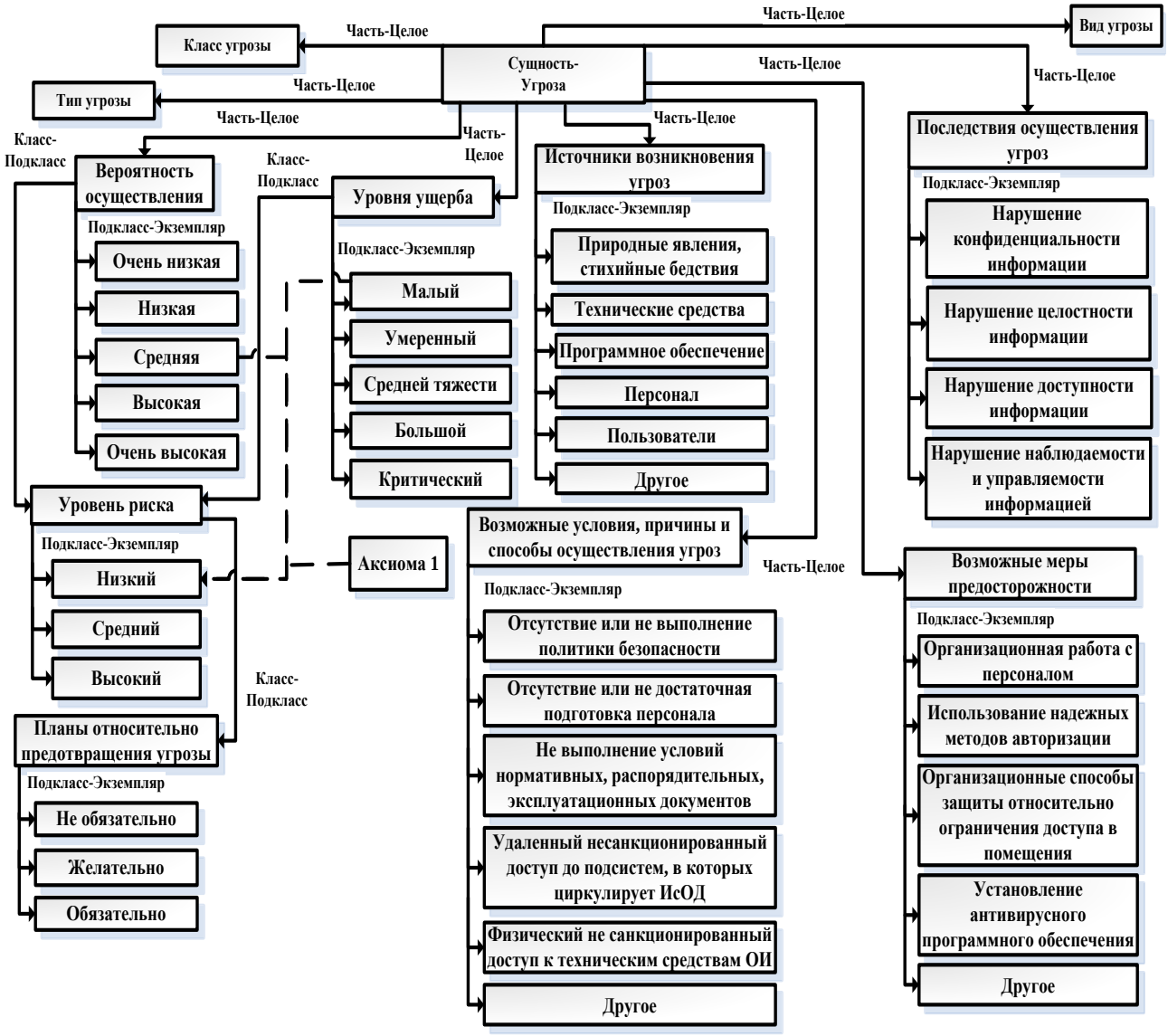

Рис. 3. Фрагмент онтографа модуля «Модель угроз»
онтологии предметной области проведения испытаний КСЗИ (2)

йствами, такими как: «***принадлежит к***» которые описывают функциональные отношения между понятиями.

Выделенные отношения позволяют находить необходимые пользователю зависимости между компонентами онтологии.

Описание фрагмента онтологического графа модуля «Модель нарушителя» онтологии предметной области проведения испытания КСЗИ

В онтологии предметной области проведения испытания КСЗИ выделяется модуль «Модель нарушителя» на основании выделения отдельного комплекса задач, которые выполняются с его использованием.

Общая схема взаимодействия модулей данной онтологии представлена в [2].

Рассматриваемые фрагменты онтографа рис. 4 онтологического модуля «Модель нарушителя» онтологии проведения испытаний КСЗИ, предназначены для осуществления поддержки пользователя, которая выражается в получении им знаний и умозаключений в процессе построения модели нарушителя для рассматриваемого объекта испытаний с помощью использования базы знаний, которая основана на разрабатываемой онтологии.

Рассматриваемый онтологический

модуль «Модель нарушителя» взаимодействует с другими модулями данной онтологии, такими как «Объект испытаний». Взаимодействие характеризуется межмодульными отношениями и аксиомами, которые дают возможность построения умозаключений и вывода отдельных знаний о рассматриваемом объекте испытаний.

Параметры модуля «Модель нарушителя» определяются для предварительно выбранных экземпляров класса понятий «Лица взаимодействующие с объектом испытаний» модуля «Объект испытаний» рис. 1. Каждое лицо взаимодействующее с объектом испытаний рассматривается как потенциальный нарушитель информационной безопасности.

Построение модели нарушителя с помощью рассматриваемого онтологического модуля «Модель нарушителя» и «Объект испытаний» подразумевает установление отношений между выбранными экземплярами класса «Лица взаимодействующие с объектом испытаний» модуля «Объект испытаний» рис. 1 и экземплярами всех классов модуля «Модель нарушителя» рис. 4.

В состав фрагмента онтографа представленного на рис. 4, в соответствии с [3–5], входят следующие понятия, представленные в структурированном порядке обобщенного отношения выше – ниже:

1. Нарушитель.

2. Категорирование нарушителя по отношению к контролируемой зоне:

2.1. Внешние нарушители;

2.2. Внутренние нарушители.

3. Категорирование по цели совершения нарушений:

3.1. ЦД1 – получение необходимой информации в нужном объеме и составе;

3.2. ЦД2 – получение возможности вносить изменения в информацию в соответствии со своими намерениями (интересами, планами);

3.3. ЦД3 – причинение убытков собственнику и пользователям АС путем уничтожения (повреждения) материальных и информационных ценностей.

4. Категорирование по мотиву совершения нарушений:

4.1. МН1 – ошибочность действий;

4.2. МН2 – безответственность;

4.3. МН3 – самоутверждение;

4.4. МН4 – корыстный интерес.

5. Категорирование по уровню знаний:

5.1. ЗН1 – владеют информацией о функциональных особенностях технических и программных средств компонентов АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеют пользоваться штатными средствами;

5.2. ЗН2 – обладают высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

5.3. ЗН3 – обладают высоким уровнем знаний в области вычислительной техники и программирования, проектирования и эксплуатации АС;

5.4. ЗН4 – обладают информацией о функциях и механизмах действия средств защиты АС.

6. Категорирование по уровню возможностей (каждый следующий уровень содержит функциональные возможности предыдущего):

6.1. УВ1 – возможность запуска фиксированного набора задач (программ), которые реализуют заранее предусмотрены функции обработки информации;

6.2. УВ2 – возможность создания и запуска собственных программ с новыми функциями обработки информации;

6.3. УВ3 – возможность управления функционированием компонентов АС, т. е.

влиянием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования (возможно создание или использование специальных технических средств);

6.4. УВ4 – возможность осуществления проектирования, реализации, сопровождения программно-аппаратного обеспечения компонентов АС, которые могут включать в состав АС собственные средства с новыми функциями обработки информации.

7. Категорирование по месту совершения действия:

7.1. МД1 – без получения доступа на контролируемую территорию АС;

7.2. МД2 – с получением доступа на контролируемую территорию, но без доступа к техническим средствам АС;

7.3. МД3 – с получением доступа к техническим средствам пользователей АС;

7.4. МД4 – с получением доступа к местам хранения данных (носителей, архивов и т. п.);

7.5. МД5 – с получением доступа к средствам администрирования АС и средствам управления КСЗ.

8. Категорирование по времени совершения действия:

8.1. ВД1 – во время перерывов в работе компонентов системы (в нерабочее время, во время плановых перерывов в работе, перерывов для обслуживания и ремонта и т. п.);

8.2. ВД2 – во время функционирования АС (или компонентов системы);

8.3. ВД3 – при создании системы.

9. Категорирование по методам и способам совершения нарушений:

9.1. МСН1 – используются агентурные методы получения сведений;

9.2. МСН2 – используются пассивные технические средства перехвата информации;

9.3. МСН3 – используются штатные средства компонентов АС или недостатки проектирования КСЗИ для реализации попыток НСД;

9.4. МСН4 – используются способы и средства активного воздействия на технические и программные средства компонентов АС, изменяющие конфигурацию системы (несанкционированное подключения дополнительных или модификация штатных технических средств, внедрение и использование специального программного обеспечения).

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

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

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

Данные функциональные отношения представляются как межмодульные отношения устанавливаемые между выбранными экземплярами классов «Лица взаимодействующие с объектом испытаний» модуля «Объект испытаний» рис. 1 и экземплярами всех классов модуля «Модель нарушителя» рис. 4.

Выделенные отношения позволяют находить необходимые пользователю зависимости между компонентами онтологии.

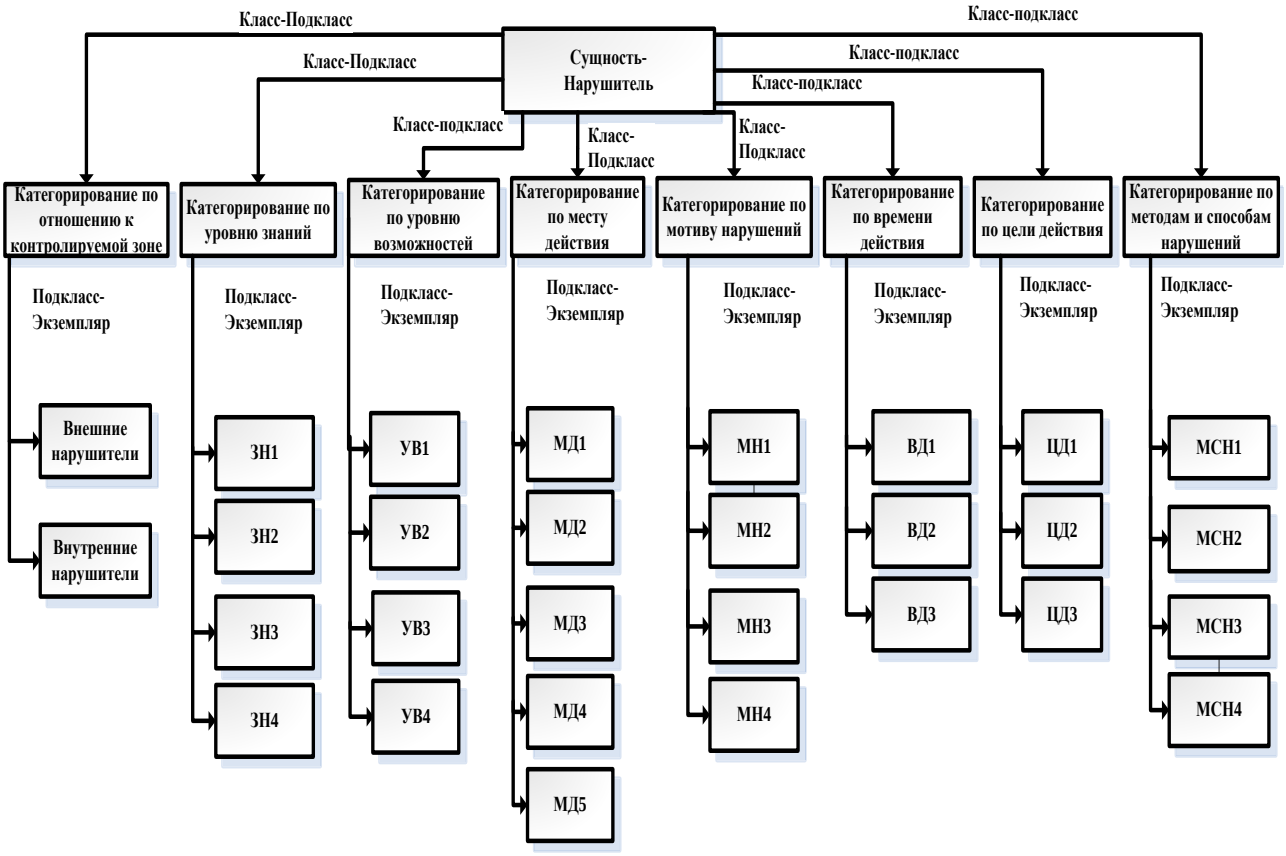

Рис. 4. Фрагмент онтографа модуля «Модель нарушителей» онтологии предметной области проведения испытаний КСЗИ

Анализ особенностей извлечения специализированных знаний из онтологии предметной области проведения испытаний КСЗИ

Извлечение знаний при использовании онтологии предметной области проведения испытаний КСЗИ и предоставление их пользователю, является основной задачей средства автоматизированной поддержки проведения испытаний КСЗИ, главным компонентом которого является рассматриваемая онтология.

Предоставляемые пользователю знания можно классифицировать по их функциональному предназначению, а именно:

– знания, характеризирующиеся как подсказка, в процессе решения отдельно взятой задачи;

– знания, выступающие в виде получения готового результата (построения модели угроз и модели нарушителя информационной безопасности объекта испытаний).

Извлечение знаний, в виде получения подсказки, в процессе решения отдельно взятой задачи

Извлечение знаний, которые выступают в качестве подсказки пользователю, реализуются с помощью 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 рассматриваемом онтологическом графе выделяются два вида аксиом: внутримодульные и межмодульные.

К внутримодульным относятся аксиомы, которые формируются с использованием понятий и отношений входящие в состав одного из рассматриваемых модулей, в данном случае: «Объект испытаний», «Модель угроз», или «Модель нарушителя».

К межмодульным относятся аксиомы, которые формируются с использованием понятий и отношений входящие в состав двух и более модулей, в данном случае: «Объект испытаний», «Модель угроз», «Модель нарушителя».

Характеристика внутримодульных аксиом

В онтографическом графе «Модель угроз» рис. 3, в качестве примера внутримодульной аксиомы выделяется Аксиома 1, которая представлена далее.

Аксиома 1, – описывающая отношение между экземпляром «**Малый**» класса «Уровень ущерба», экземпляром «**Средняя**» класса «Вероятность осуществления» и экземпляром «**Низкий**» класса «Уровень риска» табл. 1.

Аксиома 1. «Если уровень ущерба **– X** является «Малый», а вероятность осуществления угрозы – **Y** является «Средняя», тогда риск, который несет угроза для объекта испытаний – низкий.

Таблица 1

Понятие	Значение понятия
X	Экземпляр – «Малый» класса «Уровень ущерба»
Y	Экземпляр – «Средняя» класса «Вероятность осуществления»

Данная **аксиома 1** задает условие соотнесения экземпляров «Малый», «Средняя», «Низкий» и отношения между ними – «Является», и выражают очевидное утверждение, связывающие понятия и отношение. Данная аксиома предоставляет возможность суждения относительно того, что: «Если угроза несет **малый» уровень ущерба** и имеет **среднюю вероятность осуществления угрозы** то **уровень риска**, который несет угроза, для объекта испытаний является «**низкий»**.

В данной аксиоме используются качественные шкалы и таблица определения уровня риска информационной безопасности описанные в статье [5].

Характеристика межмодульных аксиом

Аксиома 2, – описывающая отношение между экземпляром «**Администратор системы**», подкласса «Администратор», подкласса «Персонал», класса «Лица взаимодействующие с объектом испытаний», модуля «Объект испытаний» с подклассом «**Персонал**» класса «Лица взаимодействующие с объектом испытаний» модуля «Объект испытаний» и экземпляром «**Внутренний нарушитель**» класса «Категорирование по отношению к контролируемой зоне» модуля «Модель нарушителя» табл. 2.

Аксиома 2. «Если **X** относится к подклассу **Y**, тогда **X** является внутренним нарушителем.

Таблица 2

Понятие	Значение понятия
X	Экземпляр – «**Администратор системы**» подкласса «Персонал» класса «Лица взаимодействующие с объектом испытаний» модуля «Объект испытаний»
Y	Подкласс «**Персонал**» класса «Лица взаимодействующие с объектом испытаний» модуля «Объект испытаний»

Данная **аксиома 2** задает условие соотнесения экземпляра «**Администратор системы**», подкласса «**Персонал**» и отношения между ними – «Относится к» и выражают очевидное утверждение связывающие понятия и отношение. Данная аксиома предоставляет возможность суждения относительно того, что: «Администратор системы является внутренним нарушителем по отношению к контролируемой зоне объекта испытаний».

Извлечение знаний в виде получения готового результата

Извлечение знаний в виде получения готового результата подразумевает получение разработанной модели угроз информационной безопасности для рассматриваемого объекта испытаний.

Знания предоставляются пользователю при использовании онтологических модулей – «Объект испытаний», «Модель угроз» онтологии проведения испытаний КСЗИ.

Построение модели угроз предусматривает определение, структурирование и систематизацию следующих видов информации в соответствии с [6–8]:

– типизация угроз информационной безопасности рассматриваемого объекта испытаний;

– классификация угроз информационной безопасности рассматриваемого объекта испытаний;

– распределение угроз информационной безопасности рассматриваемого объекта испытаний по видам;

– определение источников возникновения угроз;

– определение условий, причин и способов осуществления угроз;

– определение последствий осуществления угроз;

– определение возможных мер предосторожности;

– оценка вероятности осуществления угроз (наступления последствий осуществления угроз);

– оценка потенциального уровня ущерба от осуществления угроз (наступления последствий осуществления угроз);

– оценка уровня риска реализации угроз;

– определение планов относительно предотвращения угроз.

Извлечение знаний в виде получения готового результата, также, подразумевает получение разработанной модели нарушителя информационной безопасности для рассматриваемого объекта испытаний.

Данные знания предоставляются пользователю при использовании онтологических модулей – «Объект испытаний», «Модель нарушителей» онтологии проведения испытаний КСЗИ.

Установление соответствующих отношений позволяет осуществить для каждого из потенциальных или явных нарушителей определение следующих видов информации:

– категорирование нарушителей по отношению к контролируемой зоне;

– категорирование нарушителей по уровню знаний;

– категорирование нарушителей по уровню возможностей;

– категорирование нарушителей по месту действия;

– категорирование нарушителей по мотиву нарушений;

– категорирование нарушителей по времени действия.

Выводы

В статье представлены разработанные фрагменты онтологического графа проведения предварительных и экспертных испытаний КСЗИ, которые используются для построения модели угроз и нарушителей информации объекта испытаний, предоставлена их характеристика и функциональное предназначение. Рассмотрены особенности построения модели угроз и модели нарушителей информационной безопасности, для отдельного объекта испытаний с использованием онтологии проведения предварительных и экспертных испытаний КСЗИ.

Необходимо отметить, что разработка онтологического графа и выявление особенностей его построения, является необходимым шагом на пути к построению онтологии проведения предварительных и экспертных испытаний КСЗИ.

Рассмотрены особенности извлечения специализированных знаний, из онто-

логии проведения предварительных и экспертных испытаний КСЗИ, которые относятся к процессу создания модели угроз и модели нарушителей информационной безопасности.

В дальнейшем планируется провести более детальную и полную разработку онтологического графа предметной области проведения испытаний КСЗИ, связанную с анализом его структуры, взаимосвязи его компонентов, анализом их функционального предназначения и выполняемых задач. Также, планируется рассмотреть аспекты, связанные с программной реализацией 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. *Константинова Н.С., Митрофанова О.А.* «Онтологии, как системы хранения знаний». http://window.edu.ru/resource/795/58795/files/68352e2-st08.pdf
2. *Колтик М.А.* «Системно-онтологический анализ предметной области проведения испытаний КСЗИ» // Проблеми програмування. – 2014. – № 1. – С. 62–75.
3. *НД* ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999. № 22.
4. *НД* ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
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. – № 4. – С. 86–100.
6. *НД* ТЗИ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
7. *НД* ТЗИ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
8. *НД* ТЗИ 1.6-003-04. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

Получено 14.07.2014

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