УДК 519.766.2

Н. Б. Копытчук, д-р техн. наук,
П. М. Тишин, канд. физ-мат. наук,
К. В. Ботнарь, канд. техн. наук,
М. В. Цюрупа

РАЗРАБОТКА ФОРМАЛИЗОВАННОГО ЯЗЫКА АНАЛИЗА РИСКОВ НА ОСНОВЕ ДЕСКРИПЦИОННОЙ ЛОГИКИ

Аннотация. *Рассмотрен вопрос разработки формализованного языка представления знаний для анализа рисков в сложной технической системе. Описаны основные понятия диаграмм рисков CORAS и языка дескрипционной логики ALC. Введены концепты и роли, описывающие основные понятия языка CORAS на языке ALC, и соответствующие аксиомы. Приведен пример диаграммы активов и описание данной диаграммы с помощью понятий разработанного языка анализа рисков.*

М. Б. Копитчук, д-р техн. наук,
П. М. Тішин, канд. физ-мат. наук,
К. В. Ботнар, канд. техн. наук,
М. В. Цюрупа

РОЗРОБКА ФОРМАЛІЗОВАНОЇ МОВИ АНАЛІЗУ РИЗИКІВ НА ОСНОВІ ДЕСКРИПЦІЙНОЇ ЛОГІКИ

Анотація. *Розглянуто питання розробки формалізованої мови представлення знань для аналізу ризиків у складній технічній системі. Описано основні поняття діаграм ризиків CORAS і мови дескрипціонної логіки ALC. Введено концепти і ролі, що описують основні поняття мови CORAS мовою ALC, і відповідні аксіоми. Наведено приклад діаграми активів і опис даної діаграми за допомогою понять розробленої мови аналізу ризиків.*

N. B. Kopytchuk, ScD,
P. M. Tishin,PhD,
K. V. Botnar, PhD,
M. V. Tsyurupa

THE DEVELOPMENT OF A FORMALIZED LANGUAGE OF RISK ANALYSIS DESCRIPTION LOGIC BASED

Abstract. *The development of formalized knowledge representation language for risk analysis in complex technical systems is considered. The basic concepts of CORAS risk diagrams and basic definitions of description logic language ALC are described. The concepts and the role describing the basic concepts of language CORAS with language ALC and the corresponding axioms are introduced. An example of assets diagram and a description of this diagram using the concepts of developed language of risk analysis are shown.*

Введение. В настоящее время возрастает важность методов анализа рисков, что обусловлено применение данной области знания при оценке технических систем. Под анализом рисков в некоторой технической системе подразумевается оценка возможности перехода системы в некоторое нежелательное состояние, например, отказ системы, потеря данных или сбой в функционировании и т.п. Описание такой возможности может осуществляться с помощью вероятностных величин либо с помощью набора некоторых лингвистических значений. Результатом анализа обычно является набор мероприятий, который направлен на уменьшение рисков в системе. Выбор таких действий часто неоднозначен и достаточно сложен. При этом решения часто приходится прини

мать в условиях жестких временных ограничений.

В связи с перечисленными трудностями возникает потребность в интеллектуальных системах поддержки принятия решений реального времени (ИСППР РВ), которые смогли бы помочь лицам, принимающим решения, выбрать наилучшие варианты снижения рисков в технической системе.

По сути, ИСППР РВ является системой распределенного искусственного интеллекта семиотического типа [3], которая включает набор взаимодействующих между собой интеллектуальных модулей, выполняющих соответствующие интеллектуальные функции. Как правило, различные функции требуют различных моделей представления и оперирования знаниями или соответствующих их сочетаний.

Говоря о задаче анализа рисков, данные модели должны давать возможность описы-

вать состояния системы, оценивать возможные риски и предлагать решения по снижению выявленных рисков. Это порождает задачу описания знаний о технической системе, для которой проводится анализ рисков, с помощью некоторого формализованного языка, на основе которого можно делать логический вывод. При этом от степени выразительности, точности и универсальности языка представления знаний (ЯПЗ) во многом зависит полезность описанной на нем онтологии как инструмента оперирования с информационными ресурсами и знаниями. С помощью ЯПЗ можно описать параметры технической системы и их значения, факторы, влияющие на значения параметров, и состояния, в которых анализируемая система может пребывать.

Целью работы, некоторые результаты которой изложены в данной статье, является разработка формализованного ЯПЗ на основе дескрипционной логики для анализа рисков в сложной технической системе с использованием диаграмм рисков языка *CORAS*.

Дескрипционный язык *ALC* (*attributive language with complement*) является расширением языка *AL* (*attributive language*), введенного в 1991 г. [1]. Язык является одним из базовых языков дескрипционных логик (ДЛ). Выбор в качестве основы ЯПЗ языка *ALC* обосновывается тем, что *ALC* является основой для многих других дескрипционных языков, которые получаются в результате добавления к *ALC* таких свойств, как функциональность, транзитивность, иерархичность и других. Это значит, что, добавляя соответствующие свойства к разработанному базовому ЯПЗ, можно будет получить более развитые и соответствующие поставленным задачам языки представления знаний.

В основе *ALC* лежат понятия «концепт» и «роль», задающие множество индивидов и бинарные отношения между ними соответственно. Относительно предикатной логики концепты могут рассматриваться как одноместные, а роли – как двуместные предикаты.

Для описания некоторой предметной области с помощью *ALC* вводятся атомарные концепты, на основе их, используя конструкторы, можно получить более сложные описания реальных объектов. Атомарность концепта подразумевает, что он не может быть описан через другие концепты с применением заданных конструкторов. Далее в описании будем применять символы A и R – для описания атомарных концептов и атомарных ролей соответственно, символы C и D – для описания составных концептов, а символ S – для описания составных ролей. Используя введенные обозначения, опишем синтаксические правила языка *ALC*:

– всякий атомарный концепт A является концептом;

– выражения top и bottom, которые обозначают универсальный концепт, включающий в себя все понятия предметной области, и пустой концепт соответственно являются концептами;

– дополнение концепта $\neg C$ является концептом;

– пересечение C□D и объединение C□D концептов – концепты;

– выражения $\forall R.C$ и $\exists R.C$ – концепты, где $\forall$ – квантор всеобщности, а $\exists$ – квантор существования.

Тут концепт $\forall R.C$ определяет множество таких объектов, для которых все объекты, состоящие с исходными в отношении R, являются объектами концепта C. Концепт $\exists R.C$ определяет множество таких объектов, для которых существует хотя бы один объект концепта C, состоящий с исходными в отношении R.

Семантика ДЛ задается путем интерпретации ее атомарных концептов как множеств объектов (индивидов), выбираемых из некоторого фиксированного множества предметной области (домена), а семантика атомарных ролей – как множеств пар индивидов, т.е. бинарных отношений на домене. Формально интерпретацией I называется пара

$$I = (\Delta^I, \bullet^I), \qquad (1)$$

состоящая из непустого множества Δ^I (домен), а также интерпретирующей функции $\bullet^I$, которая сопоставляет каждому атомарному концепту A некоторое подмножество $A^I \subseteq \Delta^I$, а каждой атомарной роли R – некоторое подмножество $R^I \subseteq \Delta^I \times \Delta^I$. Интерпретирующая функция I распространяется на составные концепты и роли *ALC* согласно следующим правилам:

$$
\begin{aligned}
&(top)^I = \Delta^I;\\
&(bottom)^I = \varnothing;\\
&(\neg A)^I = \Delta^I \setminus A^I;\\
&(C \sqcap D)^I = C^I \cap D^I;\\
&(C \sqcup D)^I = C^I \cup D^I;\\
&(\forall R.C)^I = \left\{a \in \Delta^I \mid \forall b.(a,b) \in R \to b \in C^I\right\}\\
&(\exists R.C)^I = \left\{a \in \Delta^I \mid \exists b.(a,b) \in R \wedge b \in C^I\right\}\\
&(*nR)^I = \left\{a \in \Delta^I \mid \left|\{b \mid (a,b) \in R\}\right| * n\right\},\\
&* \in \{<, \le, >, \ge\}.
\end{aligned}
\qquad (2)
$$

Концепты, роли и конструкторы позволяют описывать сложные объекты реального мира и отношения между ними. Для описания же отношений между концептами и ролями внутри языка используется набор аксиом, который в общем случае можно описать соотношениями

$$C \equiv D \ (R \equiv S), \qquad (3а)$$

$$C \sqsubseteq D \ (R \sqsubseteq S); \qquad (3б)$$

Аксиомы вида (3а) называются аксиомами эквивалентности, а аксиомы вида (3б) – аксиомами включения. Семантика данных аксиом подразумевает, что интерпретация I удовлетворяет аксиомам эквивалентности и включения, если $C^I = D^I$ и $C^I \subseteq D^I$ соответственно.

На основе синтаксиса и семантики *ALC* позволяет строить утверждения (обозначим их через α), которые являются выражениями типа $C(a)$ (a – это индивид C) или $R(a,b)$ (a соотносится к b с помощью R). Семантика утверждения определяется тем, что утверждение $C(a)$ (соответственно $R(a,b)$) справедливо в интерпретации I тогда и только тогда, когда $a^I \subseteq C^I$ (соответственно $(a^I, b^I) \subseteq R^I$).

Множество утверждений и аксиом, которое называют базой знаний, обозначим через Σ. Интерпретация I называется выполнимой (является моделью) в Σ тогда и только тогда, когда I выполняется для каждого элемента в Σ. Будем записывать, что $\Sigma \models \alpha$, если в любой модели утверждение α истинно.

Для дескрипционных логик БЗ некоторой предметной области разделяют на терминологическую базу (*TBox*) и базу утверждений (*ABox*). *TBox* содержит словарь концептов и ролей рассматриваемого домена, в то время как *ABox* содержит утверждения об индивидах домена, составленные на основе словаря.

Описание диаграмм рисков *CORAS* на языке *ALC*. Для описания понятий о рисках в некоторой предметной области, воспользуемся языком анализа риска *CORAS*. Данный язык является графическим, предназначен для описания коммуникаций, документаций, анализа угроз и сценариев рисков. Он адаптирует и комбинирует такие методы проведения анализа рисков, как *Event-Tree-Analysis*, *HazOp* и *FMECA*. *CORAS* использует технологию *UML* и базируется на австралийском/ново-зеландском стандарте «*AS/NZS* 4360 Менеджмент риска», выпущенном в 1999 г., и стандарте «*ISO*/*IEC*17799-1 Свод правил по управлению защитой информации», принятом в 2000г. В стандарте учтены рекомендации, изложенные в техническом регламенте «*ISO*/*IEC TR* 13335-1 Методы и средства обеспечения безопасности» (2001г.) и в стандарте «*IEC* 61508 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (2000г.).

Системы в *CORAS* рассматриваются как сложные комплексы, в которых учтены разнообразные факторы (в том числе и человеческий). Язык *CORAS*, в частности, предназначен для поддержки использования мозгового штурма с целью определения и оценки рисков безопасности. Такой мозговой штурм характеризуется участием людей с глубокими знаниями в отдельных областях и отчасти дублирующих один другого в некоторых аспектах анализа объекта. Методология *CORAS* позволяет подойти к анализу рисков с различных сторон и поддерживает несколько видов диаграмм (активов, угроз, рисков, исправлений, обзора исправлений), каждая из которых описывает свой конкретный аспект исследуемой системы.

Для реализации объектов диаграмм *CORAS* зададим набор концептов *ALC*, которые будут отображать следующие множества объектов предметной области: вершина (*Vertex*), актив (*Asset*), участник (*Party*), риск (*Risk*), сценарий (*Scenario*), сценарий угрозы (*Threat_scenario*), сценарий исправления

(*Treatment_scenario*), угроза (*Threat*), случайная угроза (*Accidental_threat*), предумышленная угроза (*Deliberate_threat*), не человеческая угроза (*Non_human_threat*), нежелательное событие (*Unwanted_inci-dent*), уязвимость (*Vulnerability*), диаграмма (*Diagrams*), диаграмма Активов (*Asset_diagram*), диаграмма Угроз (*Threat_diagram*), диаграмма Рисков (*Risk_diagram*), диаграмма Исправлений (*Treatment_diag-ram*), диаграмма Обзора Исправлений (*Treatment_overview_diagram*).

Введенный таким образом набор концептов предоставляет возможность для создания онтологии предметной области, которая может использоваться для соответствующих ИСППР с учетом решения задач анализа рисков.

Учитывая структуру объектов языка *CORAS*, введем следующие аксиомы:

$Asset \sqsubseteq Vertex$, $Party \sqsubseteq Vertex$,

$Scenario \sqsubseteq Vertex$, $Threat \sqsubseteq Vertex$,

$Unwanted\_incident \sqsubseteq Vertex$,

$Vulnerability \sqsubseteq Vertex$, $Risk \sqsubseteq Vertex$,

$Threat\_scenario \sqsubseteq Scenario$,

$Treatment\_scenario \sqsubseteq Scenario$,

$Accidental\_threat \sqsubseteq Threat$,

$Deliberate\_threat \sqsubseteq Threat$,

$Non\_human\_threat \sqsubseteq Threat$,

$Asset\_diagram \sqsubseteq Diagrams$,

$Threat\_diagram \sqsubseteq Diagrams$,

$Risk\_diagram \sqsubseteq Diagrams$,

$Treatment\_diagram \sqsubseteq Diagrams$,

$Treatment\_overview\_diagram \sqsubseteq Diagrams$.

Для описания взаимосвязей между концептами диаграмм и остальными введенными концептами введем в рассмотрение бинарное отношение (роль), названное «*Contains*» (Содержит). Тогда можно построить следующие соотношения:

для концепта *Asset_diagram* (диаграмма активов) –
Contains(*Asset_diagram*, *Asset*),
Contains(*Asset_diagram*, *Party*);

для концепта *Threat_diagram* (диаграмма угроз) –
Contains(*Treat_diagram*, *Threat*),
Contains(*Treat_diagram*, *Threat_scenario*),
Contains(*Treat_diagram*, *Asset*),
Contains(*Treat_diagram*, *Vulnerability*),
Contains(*Treat_diagram*, *Unwanted_inci-dent*);

для концепта *Risk_diagram* (диаграмма рисков) –
Contains(*Risk_diagram*, *Threat*),
Contains(*Risk_diagram*, *Risk*),
Contains(*Risk_diagram*, *Asset*);

для концепта *Treatment_diagram* (диаграмма исправлений) –
Contains(*Treatment_diagram, Threat*),
Contains(*Treatment_diagram*, *Threat_scenario*),
Contains(*Treatment_diagram*, *Asset*),
Contains(*Treatment_diagram*, *Vulnerability*),
Contains(*Treatment_diagram*, *Unwanted_incident*),
Contains(*Treatment_diagram*, *Treament_scenario*);

для концепта *Treatment_overview_diagram* (диаграмма обзора исправлений) –
Contains(*Treatment_overview_diagram*, *Risk*),
Contains(*Treatment_overview_diagram*, *Asset*),
Contains(*Treatment_overview_diagram*, *Threat*),
Contains(*Treatment_overview_diagram*, *Treatment_scenario*).

Для ссылки на индивидов соответствующих концептов в таблице в соответствии с работой [2] приведены их обозначения.

Для каждого класса введем бинарные отношения, описанные в рамках структурной семантики языка *CORAS*:

Отношение косвенного ущерба (*Indirect_harm_relation – Ihr*) – отражает зависимость между двумя активами, в смысле того как, ущерб, нанесенный первому активу, вызывает возможный косвенный ущерб для других активов:

$$Ihr(a,a).$$

Отношение воздействия (*Impact*) – описывает воздействие нежелательного инцидента или сценария угроз на актив, который пострадает в результате этого воздействия. Каждое отношение воздействия может быть связано с последствием:

$$Impact(TUR,a),$$

при этом справедливо утверждение $TUR:(Threat\_scenario \sqcup Unwanted\_incident \sqcup Risk)$.

Отношение инициации (*Initiate*) – описывает взаимосвязь некоторой угрозы и сценария угрозы, нежелательного события или риска:

$$Initiate(t,TUR).$$

Отношение защиты (*Protect*) – выводит отношения присущее определению актива, т.е. то, что актив представляет ценность для заинтересованной в его защите стороны (участника):

$$Protect(p,a).$$

Обозначения индивидов

Концепт	Индивид
вершина (*Vertex*)	v
актив (*Asset*)	a
участник (*Party*)	p
риск (*Risk*)	r
сценарий угрозы (*Threat_scenario*)	Ts
сценарий исправления (*Treatment_scenario*)	Trs
угроза (*Threat*)	t
предумышленная угроза (*Deliberate_threat*)	dt
не человеческая угроза (*Non_human_threat*)	nht
случайная угроза (*Accidental_threat*)	at
нежелательное событие (*Unwanted_incident*)	Ui
уязвимость (*Vulnerability*)	$vn = \{vn\} = vn_1$
набор уязвимостей (*Vulnerability_set*)	$Vn = \{vn_1, \dots, vn_n\}$
диаграмма	d
диаграмма активов (*Asset_diagram*)	ad
диаграмма угроз (*Threat_diagram*)	thd
диаграмма рисков (*Risk_diagram*)	rd
диаграмма исправлений (*Treatment_diagram*)	td
диаграмма обзора исправлений (*Treatment_overview_diagram*)	tod

Отношение исправления (*Treatment*) – описывает связь сценария исправления с любым другим элементом диаграммы, кроме участника и сценария исправления:

$$Treatment(ts,w),$$

где w:($Vertex \sqcap \neg Party \sqcap \neg Treatment\_scenario$).

Отношение следствия (*Leads_to*) – отражает некоторую причинно-следственную связь между сценарием угрозы, нежелательным событием и рисками:

$$Leads\_to(TUR,TUR).$$

Отношение исправления может подразумевать следующие подотношения:

- избежание ($Avoid(ts,w)$) – позволяет избежать риска;
- уменьшение вероятности ($Decrease\_likelihood(ts,w)$) – уменьшает вероятность риска;
- уменьшение последствия ($Decrease\_consequence(ts,w)$) – уменьшает последствия риска;
- деление ($Share(ts,w)$) – делит риск;
- удержание ($Retain(ts,w)$) – удержание риска на некотором уровне.

Очевидно выполнение следующих аксиом:

$$Avoid(ts,w) \sqsubseteq Treatment(ts,w),$$

$$Decrease\_likelihood(ts,w) \sqsubseteq Treatment(ts,w),$$

$$Decrease\_consequence(ts,w) \sqsubseteq Treatment(ts,w),$$

$$Share(ts,w) \sqsubseteq Treatment(ts,w),$$

$$Retain(ts,w) \sqsubseteq Treatment(ts,w).$$

Таким образом, введены все объекты, которые требуются для описания всех пяти диаграмм *CORAS*.

Опишем простой пример, в котором покажем, как, используя ДЛ, можно описать знания, представленные диаграммами *CORAS*. Для этого рассмотрим диаграмму рисунке.

Обозначим описанную диаграмму через D, p_1 и p_2 – участники, a_1, a_2, a_3 – активы. Тогда для представленной диаграммы справедливы следующие утверждения:

$Asset\_diagram(D)$; $Asset(a_1)$, $Asset(a_2)$, $Asset(a_3)$; $Party(p_1)$, $Party(p_2)$;

$Contains(D, a_1)$, $Contains(D, a_2)$, $Contains(D, a_3)$, $Contains(D, p_1)$, $Contains(D, p_2)$; $Protect(p_1,a_1)$, $Protect(p_1,a_3)$, $Protect(p_2,a_2)$, $Protect(p_2,a_3)$; $Ihr(a_1,a_2)$, $Ihr(a_1,a_3)$.

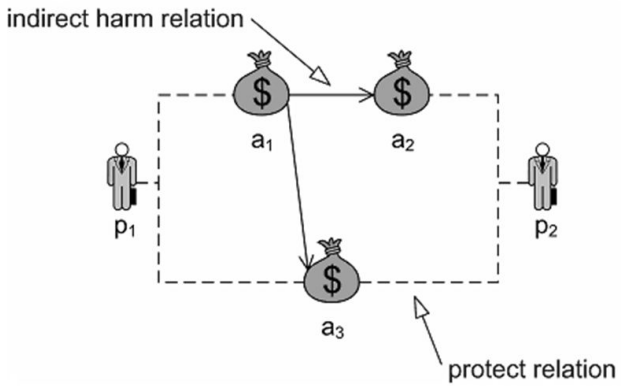


Рис. Пример диаграммы активов

Выводы. В статье описаны основные понятия и отношения языка *CORAS* в виде концептов и ролей языка *ALC*. Введенные понятия являются частью терминологии разрабатываемого ЯПЗ. Описанные в статье результаты могут быть использованы при создании онтологии некоторой технической системы, что позволит проводить более эффективный анализ риска за счет формировании запросов и логического вывода на основе имеющихся знаний.

Список использованной литературы

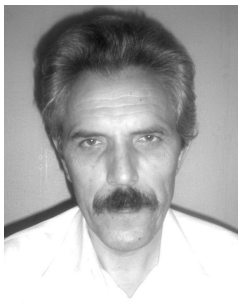
1. Baader F. The Description Logic Handbook: Theory, Implementation, and Applications. / Franz Baader, Diego Calvanese, Deborah McGuinness, Daniele Nardi, Peter F. Patel-Schneider // Cambridge University Press, 2003.

2. Dahl Heidi E. I. Structured semantics for the CORAS security risk modelling language. / Heidi E. I. Dahl, Ida Hogganvik, Ketil Stolen // Technical Report A970, SINTEF ICT, 2007.

3. Eremeev A.P. A real-time decision support system prototype for management of a power block. / A.P. Eremeev, // International Journal "Information Theories & Applications" Vol.10, 2003, pp 248-255.

Получено 22.02.2011

Копытчук
Николай Борисович, д-р техн. наук, проректор Одесск. нац. политехн. ун-та, пр. Шевченко 1



Тишин
Петр Метталинович, кандидат физико-математ. наук, доцент Одесск. нац. политехн. ун-та,
пр. Шевченко 1,
моб: 098-805-0448

Ботнарь
Константин Васильевич, канд. техн.наук, Одесск. нац. политехн.ун-т,
моб.: 095-302-0265

Цюрупа
Марат Владимирович, аспирант Одесск. нац. политехн. ун-та,
пр. Шевченко 1,
моб.: 093-645-4288