УДК 519.766.2

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

АНАЛИЗ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ С ПОМОЩЬЮ МНОГОУРОВНЕВОЙ ОНТОЛОГИИ ОЦЕНКИ РИСКОВ С ПРИМЕНЕНИЕМ МЕТОДОЛОГИИ CORAS

Рассмотрен вопрос описания основных понятий и отношений диаграмм Coras с использованием лингвистического описания зависимостей, характеризующих предметную область. Предложено описание формализованного языка представления знаний для анализа рисков в сложной вычислительной системе. Представлен пример использования многоуровневого онтологического подхода к анализу рисков в вычислительных сетях.

Ключевые слова: *дескрипционная логика, диаграммы Coras, нежелательный инцидент, диаграмма угроз, диаграмма активов, онтология оценки рисков, онтология вычислительной сети, лингвистические переменные, нечеткие множества, необогащенная система логических отношений, многоуровневая онтология, обогащение необогащенной системы логических отношений*

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

ANALYSIS OF COMPUTER NETWORKS WITH MULTI-LEVEL RISK ASSESSMENT ONTOLOGIES USING CORAS METHODOLOGY

The problem of describing the basic concepts and relationships Coras charts with the use of linguistic description of dependencies arising in the subject field were explored. Introduced a description of the formal knowledge representation language for the analysis of risks in complex computational system. The example of using multi-level ontological approach to risk analysis in computer networks were shown.

Keywords*: description logic, diagrams Coras, unwanted incident, chart threats, diagram of assets, risk assessment ontology, ontology of computer networks, linguistic variables, fuzzy sets, unenriched logical relationship system, multi-level ontology enrichment of unenriched logical relationship system*

Н. Б. Копитчук, д-р техн. наук,
П. М. Тішін, канд. фіз-мат. наук,
М. В. Цюрупа

АНАЛІЗ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ З ДОПОМОГОЮ БАГАТОРІВНЕВОЇ ОНТОЛОГІЇ ОЦІНКИ РИЗИКІВ З ВИКОРИСТАННЯМ МЕТОДОЛОГІЇ CORAS

Розглянуто питання опису основних понять і відношень діаграм Coras з використанням лінгвістичного опису залежностей, що виникають у предметній області. Запропоновано опис формалізованої мови подання знань для аналізу ризиків у складній обчислювальній системі. Представлений приклад використання багаторівневого онтологічного підходу до аналізу ризиків в обчислювальних мережах.

Ключові слова: *дескипційна логіка, діаграми Coras, небажаний інцидент, діаграма загроз, діаграма активів, онтологія оцінки ризиків, онтологія обчислювальної мережі, лінгвістичні змінні, нечіткі множини, незбагачена система логічних відносин, багаторівнева онтологія, збагачення незбагаченої системи логічних відносин*

Введение. В данной статье представлен разработанный авторами модульный подход к созданию моделей онтологий оценки рисков в корпоративных сетях с применением методологии оценки рисков Coras. Построенная модель онтологии подразумевает создание необогащенной системы логических соотношений, которая описывает параметры и неизвестные переменные (целостность сети, частота отказов устройств, воздействие на проводящую среду и т.д.), входящие в онтологии оценки рисков по методологии Coras, как и в работах [1, 2]. Каждое логическое соотношение имеет содержательное толкование, а вся система в целом является представлением концептуализации, которое понимается как множество ситуаций и множество систем знаний предметной области [3, 4].

Разработанный подход предусматривает создание многоуровневой модели онтологии

в виде совокупности модулей, представленной на рис. 1.

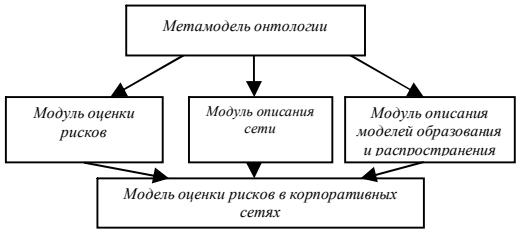


Рис. 1. Многоуровневая модель онтологии оценки рисков

Многоуровневая онтология. Базовым модулем на 3-м уровне иерархии является метамодель онтологии. Каждый модуль второго уровня описывает терминологию соответствующего раздела предметной области. Модуль оценки рисков (обозначаемый далее T_1), модуль описания сети (обозначаемый далее T_2) и модуль описания моделей образования и распространения угроз (обозначаемый далее T_3).

Данное описание позволяет расширять многоуровневую модель онтологии оценки рисков в корпоративных сетях за счет введения новых модулей, которые могут соответствовать новым разделам такой сложной и структурированной предметной области, как описание и оценка рисков [5, 6].

Онтология оценки риска. Для определения модуля "Модель онтологии рисков в корпоративных сетях" воспользуемся понятием гомоморфизма между необогащенными системами логических соотношений и понятием произведения необогащенных систем логических соотношений [3, 7]. Если ς – некоторое обогащение [3] необогащенной системы O, то $S =< O,\varsigma >$ есть O, обогащенная ς. На множестве всех возможных обогащений необогащенной системы O определяется отношение эквивалентности и множество классов эквивалентности всех возможных обогащений, которое будем обозначать $En(O)$. Если $k \in En(O)$ – некоторый класс эквивалентности множества всех возможных обогащений необогащенной системы O, то O определяет множество эквивалентных обогащенных систем логических соотношений $\{< O,k > | k \in En(O)\}$. Обогащенную систему логических соотношений S_2 будем называть гомоморфным образом обогащенной системы S_1, если существует всюду определенное однозначное отображение $h()$ множества решений системы S_1 в множество решений системы S_2.

Необогащенную систему логических соотношений O_2 будем называть гомоморфным образом необогащенной системы логических соотношений O_1, если существует всюду определенное однозначное отображение $h()$ множества $En(O_1)$ во множество $En(O_2)$ такое, что для всех $k \in En(O_1)$ система $S_2 =< O_2, h(k) >$ является гомоморфным образом системы $S_1 =< O_1, k >$.

В соответствии с введенными определениями обогащенную систему логических соотношений S будем называть произведением обогащенных систем логических соотношений S_1, S_2,..., S_m, если существуют гомоморфизмы $h_i : S \to S_i, i = \overline{1,m}$ такие, что для любых α_1, α_2 принадлежащих множеству решений S имеет место соотношение

$$\alpha_1 \neq \alpha_2 \Rightarrow$$
$$< h_1(\alpha_1), h_2(\alpha_1), ..., h_m(\alpha_1) > \neq < h_1(\alpha_2), h_2(\alpha_2), ..., h_m(\alpha_2) > .$$

Необогащенную систему логических соотношений O будем называть произведением необогащенных систем логических соотношений O_1, O_2,..., O_m, если существуют гомоморфизмы $h_i : O \to O_i, i = \overline{1,m}$ такие, что для любых $k_1, k_2 \in En(O)$ можно записать

$$k_1 \neq k_2 \Rightarrow$$
$$< h_1(k_1), h_2(k_1), ..., h_m(k_1) > \neq < h_1(k_2), h_2(k_2), ..., h_m(k_2) >$$

и для всех $k \in En(O)$ система $< O, k >$ является произведением систем

$$< O_1, h_1(k) >, < O_2, h_2(k) >, ..., < O_m, h_m(k) >$$

что обозначим следующим образом:

$$O = O_1 \otimes O_2 \otimes ... \otimes O_m .$$

В рамках введенных определений модуль "Модель онтологии рисков в корпоративных сетях" будет являться произведе-

нием необогащенных систем логических соотношений T_i, $i=\overline{1,3}$,

$$T = T_1 \otimes T_2 \otimes T_3 .$$

Онтология 3-го уровня представляет собой необогащенную систему логических отношений

$$O^3 =< \Phi^3, P^3, C^3 >,$$

где Φ^3 – множество предложений прикладной логической теории; P^3 – параметры онтологии 3-го уровня; C^3 – определения конструктов сортов 3-го уровня.

Введем следующие обозначения:

R, I, N, L – множество вещественных чисел (целых чисел, имен, логических значений [true, false]);

{}, множество элементов типа, указанного после скобок;

TS – типы сущностей, не пустое множество названий типов сущностей предметной области;

TSCom – типы компонентов сущности;

TSM – подмножества компонентов сущности;

D – множества значений;

OB3 – область возможных значений;

M – множество сущностей, термин обозначающий множество сущностей всех типов.

Множество Φ^3 представим в виде

1. $D \equiv$ R $\cup$ I $\cup$ N $\cup$ L $\cup$({}(R $\cup$ I $\cup$ N $\cup$ L)\∅).
2. Кортежи $D \equiv (\cup$(n:I[1,∞)) $D \Uparrow n$).
3. Сорт TS : {} N\O.
4. Кортежи $TS \equiv (\cup$(n:I[1, ∞))) ($TS \Uparrow n$).
5. $M \equiv (\cup(x: TS)$ j(x)).
6. Тип сущности ≡ ($\lambda(x:M)$ $\tau(y: TS))(x \in$ j(y)).
7. Сорт $TSCom: (TS \rightarrow$ {} TS).
8. $(x: TS)$ $x \notin TSCom(x)$.
9. Сорт TSM (($x \rightarrow TS$, $y \rightarrow TSCom(x)) \rightarrow$ {}N).
10. ($x: TS$, $y: TSCom(x)$) (элемент: $TSM(x, y)$)

сорт элемент: (j(x) → {}{(v: M) TS (v)= y }\∅).

11. (Тип: TS) Сорт Тип: {}(R $\cup$ I $\cup$ N $\cup$ L) $\cup$ Кортежи D.
12. ($x:TS$) ($y:TS \setminus \{x\}$) j(x)$\cap$ j(y) = ∅.

Параметрами P^3 онтологии 3-го уровня являются сорта: TS, $TSCom$. Конструкторами сортов онтологии 3-го уровня C^3 являются:

1. Компоненты сущностей ≡ ($\lambda(x: TS)(y: TSCom(x))$(j($x$) → {}{v: M) Тип сущности(v) = y } \ ∅).
2. Свойства сущностей ≡ ($\lambda(x: TS)$($\lambda(OB3:\{\}(D \cup \{\}$Кортежи $D))$) (j(x) → $OB3$)).
3. Свойства компонентов сущностей указанного типа ≡ ($\lambda(x: TS)$ ($y:TSCom(x)$) ($\lambda(OB3:$ {}(D $\cup$ {} Кортежи D)) ($O_1 \rightarrow$j(x), $O_2 \rightarrow$ Компонент сущности(x, y)(O_1) → $OB3$)).
4. Совместные свойства сущностей ≡ ($\lambda(x:$ {} Кортежи TS)($\lambda(OB3:\{\}(D \cup \{\}$Кортежи D) (i:I[1, length(x)]) {($O_1: M$) Тип сущности(O_1) = π (i, x)} → $OB3$).
5. Общие свойства сущности и компонента ≡ ($\lambda(x:TS)(y:TSCom(x))(\lambda(OB3:\{\}(D \cup \{\}$ Кортежи D)) (j(Тип сущности) $\cup O_1 \rightarrow$j(x), $O_2 \rightarrow$ Компонент сущности(x, y)(O_1) → $OB3$).

Необогащенные системы логических отношений 2-го уровня строятся посредством задания обогащения k^3 необогащенной системы логических отношений O^3. В общем случае k^3 представимо в следующем виде:

$$k^3 =< P^2, \varnothing, O^2, K^2, \varnothing >,$$

где P^2 – значения параметров 3-го уровня, O^2 – множества ограничений, K^2 – определения конструкторов сортов 2-го уровня.

В общем случае обогащение позволяющее получить необогащенные логические соотношения T_1 имеет довольно громоздкое представление, поэтому в рамках данной статьи приведем упрощенную не-

обогащенную систему логических отношений, представляющая T_1.

В этом случае параметрами P^3 онтологии 3-го уровня являются сорта *TS* , *TSCom* и требуется задать значения этих параметров (т.е. множество P^2) для определения T_1. Построенное множество P^2 имеет следующий вид:

TS ≡ {диаграмма, диаграмма угроз, актив, угроза, сценарий угрозы, сценарий исправления, риск, нежелательный инцидент, вершина, предумышленная угроза, случайная угроза, не человеческая угроза, уязвимость, связь };

TSCom ≡ λ(Тип: { диаграмма, диаграмма угроз, актив, угроза, сценарий угрозы, сценарий исправления, риск, нежелательный инцидент, вершина, предумышленная угроза, случайная угроза, не человеческая угроза, уязвимость, связь [8, 9, 19]}).

(Тип = диаграмма $\Rightarrow$ {диаграмма угроз }.

Тип = диаграмма угроз $\Rightarrow$ {актив, предумышленная угроза, случайная угроза, не человеческая угроза, участник, сценарий угрозы нежелательный инцидент, набор уязвимостей, связь }).

Определение конструкторов сортов второго уровня для упрощенной необогащенной системы логических соотношений выполняется с использованием конструкторов сортов третьего уровня, следующим образом:

{не человеческая угроза, случайная угроза, предумышленная угроза}

≡ Компоненты сущностей (угроза);

{актив, угроза, участник, сценарий угрозы, сценарий исправления, риск, нежелательный инцидент, уязвимость} ≡ Компоненты сущностей (вершина);

свойства активы ≡ Свойства сущностей (активы);

свойства угроз ≡ Свойства сущностей (угроз);

свойства сценарии угроз ≡ Свойства сущностей (сценарии угроз);

свойства нежелательный инцидент ≡ Свойства сущностей (нежелательный инцидент);

свойства связи ≡ Свойства сущностей (связь);

содержит ≡ Общие свойства сущности и компонента (диаграмма, вершина);

{отношение косвенного ущерба, отношение воздействия, отношение инициации, отношение защиты, отношение исправления, отношение следствия}

≡ Совместные свойства сущностей (вершина, вершина).

Онтология вычислительной сети. По аналогии с тем, как ранее была получена необогащенная система логических отношений T_1, получаем и T_2. В этом случае для параметров P^3 онтологии 3-го уровня построенное множество P^2 имеет следующий вид:

TS ≡ { Сетевой адаптер, Устройство, Проводящая среда, Передача, Сеть, Окружающая среда [11]};

TSCom ≡ λ (Тип: {Сетевой адаптер, Устройство, Проводящая среда, Передача, Сеть, Окружающая среда});

(Тип = Сеть $\Rightarrow$ { Сетевой адаптер, Устройство, Проводящая среда, Передача };

Тип = Окружающая среда $\Rightarrow \varnothing$).

По аналогии с тем, как это делалось для T_1, определяются конструкторы сортов второго уровня для T_2 с использованием конструкторов сортов третьего уровня.

Пример. В качестве примера рассмотрим произведение $T = T_1 \otimes T_2$ двух необогащенных систем логических отношений T_1, и T_2. Необогащенная система логических отношений T строится с учетом введенного соответствия E между параметрами модели онтологии оценки риска T_1 и модели онтологии сети T_2. Если через $k_1 \in En(T_1)$ и $k_2 \in En(T_2)$ обозначить введенные обогащения T_1 и T_2, то построенное соответствие должно удовлетворять условию $k_2 = E(k_1)$.

В рассматриваемой задаче описываемое соответствие задается с помощью следующих соотношений:

k_1.Угрозы = k_2.(Сетевой адаптер, Устройство, Проводящая среда, Передача, Окружающая среда, Сеть);

k_1. Нежелательный инцидент = k_2.(Сетевой адаптер, Устройство, Проводящая среда, Передача, Окружающая среда, Сеть);

k_1. Сценарии угроз = k_2.(Сетевой адаптер, Устройство, Проводящая среда, Передача, Окружающая среда, Сеть).

Таким образом, термины, введенные в T_2, могут быть связанны с сущностями, введенными в T_1, и использоваться при оценке рисков в качестве угроз, а другие сущности, такие как термины, описывающие в модели онтологии риска нежелательные инциденты или сценарии угроз.

Рассмотрим нежелательный инцидент «Фрагментирование сетевого адаптера», представленный на рис. 2.

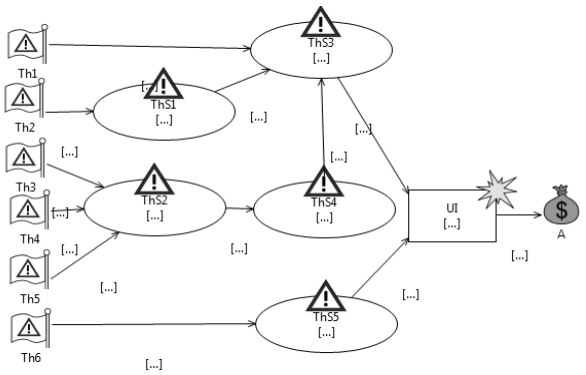


Рис. 2. Диаграмма угрозы «Фрагментирование сетевого адаптера»

Необогащенная логическая система T_1, соответствующая этому примеру, будет содержать ThD – диаграмму угрозы, $Th_i, i=\overline{1,6}$ - угрозы, $ThS_j, j=\overline{1,5}$ – сценарии угроз, UI - нежелательный инцидент, A – актив.

Соответствие терминов обогащения [12, 13] необогащенной системы логических соотношений T_1 и T_2 тогда можно записать в следующем виде:

Th_1 = Частота отказов (Сетевой адаптер);

Th_2 = Модель (Сеть);

Th_3 = Выходная мощность (Устройство);

Th_4 = Мощность (Передача);

Th_5 = Максимальная нагрузка (Сетевой адаптер);

Th_6 = Интерференция (Сеть, Окружающая среда);

ThS_1 = Физическое влияние;

ThS_2 = Перегрузка сетевого адаптера;

ThS_3 = Внутреннее влияние;

ThS_4 = Электрическое влияние;

ThS_5 = Внешнее влияние;

UI = Фрагментирование сетевого адаптера;

A = Целостность сети.

Вывод. Подобный подход к построению многоуровневой модели онтологии оценки рисков в корпоративных сетях, позволяет получить множество взаимосвязанных онтологий при описании сложных технических систем. Необогащенные системы логических отношений упрощают создание конкретных онтологий для проведения анализа рисков в этой системе. Введение онтологий позволяет быстро производить запросы к построенным базам знаний для поиска и анализа источников риска.

Список использованной литературы

1. Копытчук, Н. Б. Разработка формализованного языка анализа рисков на основе дескрипционной логики [Н. Б. Копытчук, П. М. Тишин, К. В. Ботнарь, М. В. Цюрупа] – Одесса : / Электротехнические и компьютерные системы. – 2011. – С. 103 – 108.

2. Копытчук, Н. Б. Применение нечеткой дескрипционной логики при разработке формализованного языка анализа рисков [Копытчук Н. Б., Тишин П. М., Ботнарь К. В., Цюрупа М. В.] – Одесса : / Электротехнические и компьютерные системы. – 2011. – С.168 – 176.

3. Клещев, А. С. Необогащенные системы логических соотношений / А. С. Клещев, И. Л Артемьева // Научно-техническая информация. – 2000. – № 7. – С.18 – 28.

4. Андреева, Н. В. Онтологический анализ стандартов информационной безопасности / Н. В. Андреева, А. В. Любимов. // Региональная информатика. – 2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Материалы конференции СПОИСУ. – СПб : – 2008. – С. 91 – 92.

5. Артемьева, И. Л. Системы логических соотношений с атомарными объектами / И. Л. Артемьева, Т. Л. Гаврилова, А. С. Клещев. – СПб. : НТИ. – 1996. – № 1. – С. 11 – 18.

6. Артемьева, И. Л. Системы логических соотношений с параметрами / И. Л. Артемьева, Т. Л. Гаврилова, А. С. Клещев. – СПб. : НТИ. Сер. 2. – 1997. – № 7. – С.19 – 23.

7. Клещев, А. С Онтологий и обработки знаний / А. С Клещев, И. Л. Артемьева // Технический доклад. – Владивосток : IACP, FEBRAS, 1999. – 25 с.

8. Seehusen, F. Tool-supported risk modeling and analysis of evolving critical infrastructures / F. Seehusen, S. Bjornar // In Multidisciplinary Research and Practice for Information Systems (CD-ARES), LNCS 7465. – 2012. – С. 562 – 577с.

9. Lund, M. S. Risk analysis of changing and evolving systems using CORAS / M. S. Lund, B. Solhaug, K. Stolen. Foundations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science. – Springer 2011. – P. 231 – 274.

10. Dahl H. E. I. The CORAS method for security risk analysis // Tutorial presentation at 7-th Estonian Summer School on Computer and Systems Science in cooperation with the Nordic Network On DEpendable Systems (NODES). – Otepaa, Estonia : – 2008. – P.24 – 29.

11. Stuphorn, J. Iterative Decomposition of a Communication-Bus System using Ontological Analysis – Bielefeld, 2005.

12. Ricciulli, L. Modeling Correlated Alarms in Network Management / L. Ricciulli, N.Shacham. – Computer Science Laboratory, 1996.

13. Lodderstedt, T. A UML-based modeling language for model-driven security / T. Lodderstedt, D. A Basin, J. Doser. // 5nd International Conference on the Unified Modeling Language, UML'02. Lecture Notes in Computer Science – Springer, Berlin : – 2004: – Vol. 2460. – P.426 – 441.

Получено 05.04.2013

References

1. Kopytchuk, N. B. Development of a formalized language risk analysis on the basis of the description logic [Kopytchuk, N. B. Hush P. M., Botnari K. V., Tsyurupa M. V.]. – Odessa : // Electrotechnic and Computer Systems. – 2011. – P.103 – 108[in Russian].

2. Kopytchuk, N. B. The use of non-explicit description logic in the development of a formalized language of risk analysis [Kopytchuk, N .B., Tishin, P. M., Botnari, K. V., Tsyurupa, M. V.]. – Odessa : // Electrjtechnic and Computer Systems. – 2011. – P.168 – 176 [in Russian].

3. Kleschev, A. S. Unenriched logical relationship systems / A. Kleshchev, IL. Artemyev. // Scientific and technical information but the number in July 2000. – P.18 – 28 [in Russian].

4. Andreeva, N. Ontological analysis standards informatsionnoybe-rity / N.V. Andreeva // Love mov-AV // Regional informatics-2008 (RI 2008). XI St. Petersburg International Conference. Materials SPOISU conference. – St. Petersburg : – 2008. – 3. 91 – 92 [in Russian].

5. Artemyev, I. L. Systems of logical relations with atomic objects / I. L. Artemyev, T. L. Gabriel Island, A. S. Kleshchev – St.Petersburg : – NTI. – № 1. – 1996. – P.11 – 18 [in Russian].

6. Artemyev, I. L. Systems of logical relations with the / I. L. Artemyev, T. L. Gavrilova, A. S. Kleshchev – St. Petersburg. : NTI. Ser. 2. – 1997. – № 7. P.19 – 23 [in Russian].

7. Kleshchev, A. S. Ontology and knowledge processing / A.S. Kleshchev, I. L. Altemeva // Technical Report. – Vladivostok : IACP, FEBRAS, 1999. – 25p [in Russian].

8. Seehusen, F. Tool-supported risk modeling and analysis of evolving critical infra-

structures / F. Seehusen, S. Bjornar // In Multidisciplinary Research and Practice for Information Systems (CD-ARES), LNCS 7465. – 2012. – P. 562 – 577 [in English].

9. Lund, M. S. Risk analysis of chang-ing and evolving systems using CORAS / M. S. Lund, B. Solhaug, K. Stolen // Foun-dations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science. – Springer, 2011. – P. 231 – 274 [in English].

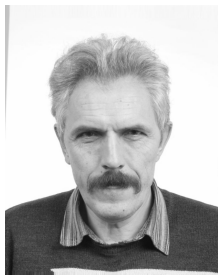
10. Dahl, H. E. I. The CORAS me-thod for security risk analysis // Tutorial presentation at 7-th Estonian Summer School on Computer and Systems Science in cooperation with the Nordic Network On DEpendable Systems (NODES). – Otepaa, Estonia : – 2008. – P.24 – 29 [in English].

10. Stuphorn, J. Iterative Decomposi-tion of a Communication-Bus System using Ontological Analysis / J. Stuphorn – Bielefeld, 2005 [in English].

11. Ricciulli, L. Modeling Correlated Alarms in Network Management / L. Ricciulli, N. Shacham // Computer Science Laboratory. – 1996 [in English].

12. Lodderstedt, T. A UML-based modeling language for model-driven se-curity / T. Lodderstedt, D. A Basin, J. Doser // 5-nd International Conference on the Unified Modeling Language, UML'02. Lecture Notes in Computer Science, vol. 2460 – Springer, Berlin : – 2004. – P. 426 – 441 [in English].

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



Тишин Петр Метталинович, канд. физико-математ. наук, доц. Одесского нац. политехн. ун-та,
м/т: 098-805-0448

Цюрупа Марат Владимирович, аспирант Одесского нац. политехн. ун-та,
м/т.: 093-645-4288