

ОНТОЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ОЦЕНИВАНИЯ ГАРАНТИЙ В КОНТЕКСТЕ ФУНКЦИОНАЛЬНО-ЛИНГВИСТИЧЕСКОГО ПОДХОДА

Предлагается функционально-лингвистический подход к оцениванию гарантий безопасности. Приводятся методика и результаты онтологического анализа предметной области оценивания гарантий. Обосновывается актуальность применения аппарата онтологического моделирования для задач оценивания безопасности.

Ключевые слова: гарантии, оценивание, онтологическое моделирование, функциональное моделирование, лингвистические переменные.

ВСТУПЛЕНИЕ

Владельцы систем и продуктов информационных технологий (ИТ) хотят быть уверенными в качестве разработки, эффективности функционирования и безопасности приобретенных ИТ-продуктов. Международные [1–4] и национальные [5–7] стандарты в области безопасности информационных технологий определяют функциональные требования безопасности и требования гарантий безопасности, удовлетворение которых позволяет предоставить различные основания для такой уверенности. В ходе активного исследования (оценивания) ИТ-продукта на соответствие требованиям гарантий и формируется уверенность потребителя в корректности реализации функциональных услуг безопасности.

Оценивание ИТ-продуктов проводится аккредитованными испытательными лабораториями на основании программ и методик проведения оценивания. Качественная разработка программы и методики оценивания является важной составляющей при подготовке к проведению оценивания. Сам процесс оценивания подвержен воздействию различных факторов, способных повлиять на итоговый результат оценива-

ния. Поэтому к процессу оценивания выдвигаются требования ширины, глубины и строгости, а к результатам оценивания – требования объективности, повторяемости, беспристрастности, воспроизводимости и сопоставимости.

Обзор научной литературы показал, что моделирование процессов оценивания гарантий безопасности с созданием инструментальных средств для поддержки работы эксперта является актуальной задачей. Однако в основном моделирование направлено на интерактивное представление требований стандарта в виде информационных инструментальных систем. Кроме того, в большинстве работ при моделировании не рассматриваются вышеперечисленные требования.

В работах авторов [8–10] предлагается функционально-лингвистический подход к оцениванию гарантий информационной безопасности, который позволяет разрабатывать программу и методику оценивания и выполнять вышеуказанные требования как к процессу оценивания, так и к результатам оценивания. В данной работе представлены результаты дальнейшего развития функционально-лингвистического подхода и детальное описание первого этапа.

1. КОНЦЕПЦИЯ ФУНКЦИОНАЛЬНО-ЛИНГВИСТИЧЕСКОГО ПОДХОДА

В ходе анализа области оценивания гарантий авторы выдвинули предложение оценивать не сам объект оценивания, а присущие ему *свойства гарантий*. Данные свойства выявляются в ходе анализа требований, выдвигаемых к объекту в нормативных документах на определенном уровне гарантий безопасности. Для доказательства того, что конкретное свойство присуще (имеется в наличии) объекту оценивания (ОО), используются свидетельства, в качестве которых могут выступать сам ОО, его части, документация, результаты испытаний (тестирования). Таким образом, оценивание ИТ-продукта заключается в оценке степени проявления присущих продукту свойств гарантий на основании анализа (исследования) свидетельств. Это является ключевой идеей предлагаемого авторами подхода к оцениванию гарантий безопасности.

Структура функционально-лингвистического подхода представлена на рис. 1. Оценка гарантий безопасности осуществляется в четыре этапа.

На первом этапе проводится онтологический анализ и моделирование предметной области оценивания. Анализ включает в себя исследование множества требований гарантий ($R = \{r_1, r_2, \dots, r_i\}$, $i = \overline{1, N}$), которые выдвигаются к ОО, и выявления (синтез) множества свойств гарантий ($P = \{p_1, p_2, \dots, p_j\}$, $j = \overline{1, L}$), которыми должен обладать ОО. На множестве свойств гарантий P определяются зависимости и взаимосвязи между свойствами. Результаты анализа представляются в виде онтологических графов,

которые точно и однозначно (в принятой нотации) описывают предметную область (т. е. основные понятия (концепты) и отношения между ними). Полнота охвата моделируемой области оценивания гарантий обеспечивается использованием онтологических графов двух видов: объектно-ориентированных и процессно-ориентированных онтологий.

На втором этапе осуществляется функциональное моделирование процесса оценивания гарантий. Целью функционального моделирования является формализованное представление процесса оценивания. В качестве языка моделирования была выбрана нотация IDEF0 [8]. Нотация IDEF0 позволяет однозначно отобразить шаги проведения оценивания (в виде направленного графа), для каждого шага определить оцениваемое свойство гарантий, свидетельства, необходимые для оценивания данного свойства гарантий, субъектов оценивания и нормативное основание проведения оценивания. Если оценке подлежит сложное (составное) свойство гарантий, то каждый шаг (блок IDEF0-диаграммы) может быть декомпозирован для детального описания процедуры оценки подсвойств.

На третьем этапе для каждого свойства p_j вводится лингвистическая переменная $\Omega p_j = \langle \beta, T(\beta), G, M \rangle$ и определяется ее терм-множество β . Применение математического аппарата лингвистических переменных обусловлено тем, что чаще всего степень проявления свойства гарантий не может быть описана с помощью количественных показателей. Поэтому для принятия решения относительно степени проявления свойства гарантий удобно использовать математический аппарат нечеткого логического вывода (НЛВ) на основе заранее подготовленной базы продукционных правил [11]. Применение лингвистических переменных и операций нечеткого логического вывода обеспечивает выполнение требований объективности и повторяемости результатов оценивания гарантий.

На четвертом этапе строятся диаграммы потоков работ в нотации IDEF3. Это позволяет однозначно установить порядок и приоритетность выполнения операций (действий) оценивания. Каждый блок диаграммы представляет собой отдельное действие эксперта-оценщика. После каждого блока следует перекресток, который определяет критерий (правило) выбора следующего действия в зависимости от того, какое решение примет эксперт относительно степени проявления оцениваемого свойства. Количество вариантов выбора зависит от количества значений, которые может принимать лингвистическая переменная, описывающая оцениваемое свойство. Диаграммы

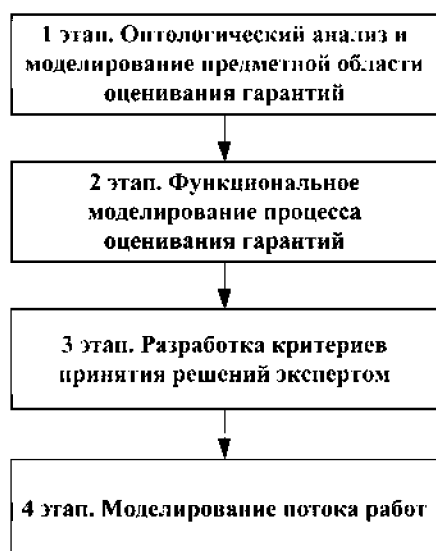


Рис. 1. Функционально-лингвистический подход к оцениванию гарантий

определяют точки, в которых эксперт должен принять решение и вынести вердикт относительно степени проявления того или иного свойства. Построение и применение IDEF3 диаграмм обеспечивает выполнение требования повторяемости результатов оценивания, т. к. для каждой операции оценивания определяется набор вариантов возможных вердиктов (решений) эксперта. Выбор варианта вердикта зависит от того, какие значения принимают лингвистические переменные в ходе оценивания свойств (по сути это выбор эксперта относительно степени проявления свойства).

Таким образом, реализация данного подхода позволяет обеспечить выполнение основных требований к процессу и результатам оценивания гарантий безопасности.

2. ОНТОЛОГИЧЕСКИЙ АНАЛИЗ И МОДЕЛИРОВАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ ОЦЕНИВАНИЯ ГАРАНТИЙ

В ходе онтологического анализа требований гарантий необходимо найти консенсус (баланс) между степенью детализации оцениваемых свойств гарантий и стоимостью процесса оценивания. Чем больше глубина оценивания (выше степень детализации), тем выше точность оценки объекта оценки. Однако при этом увеличиваются стоимостные временные показатели процесса оценивания. Низкая детализация требований удешевляет процесс оценивания, однако может привести к затруднениям при принятии реше-

нии о степени проявления оцениваемых свойств и, как следствие, к неправильным выводам.

2.1. Задачи онтологического анализа и выбор типа онтологии

Основными задачами онтологического анализа требований гарантий являются:

- точное, ясное и однозначное описание предметной области оценивания гарантий информационной безопасности, выделение основных понятий и концептов;
- четкое определение содержания оценивания;
- определение необходимой глубины оценивания;
- преобразование набора статических требований гарантий в динамическую базу для их использования людьми из разных сфер деятельности и понимания области оценивания;
- представление знаний (требований) области оценивания гарантий в форме, которая позволяет создавать ее электронный аналог.

Анализ структуры требований гарантий [3], где ключевыми объектами структуры являются «класс – семейство – компонент – элемент», показал, что для моделирования требований необходимо использовать иерархические объектно-ориентированные графы (онтологии). Пример результата моделирования представлен на рис. 2.

В узлах графа находятся выделенные объекты (класс – семейство – компонент – элемент). Ребра графа показывают связь между объектами. Так, классы гарантий декомпозируются на семейства. Каждое

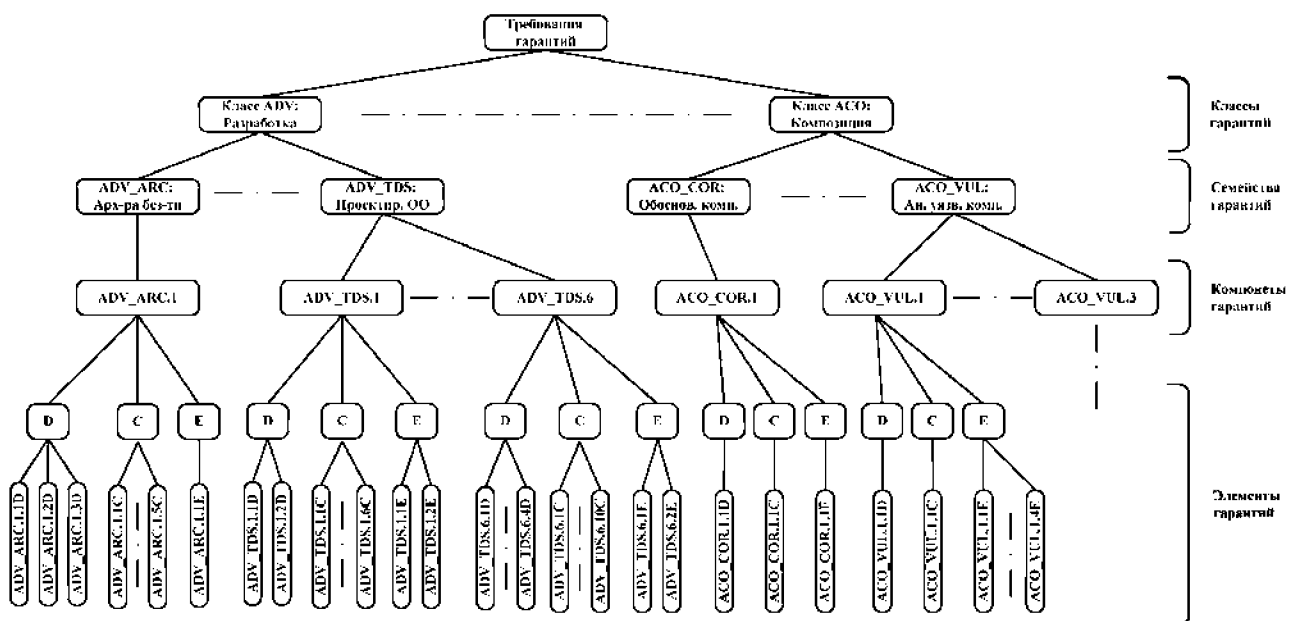


Рис. 2. Иерархическая объектно-ориентированная онтология требований гарантий

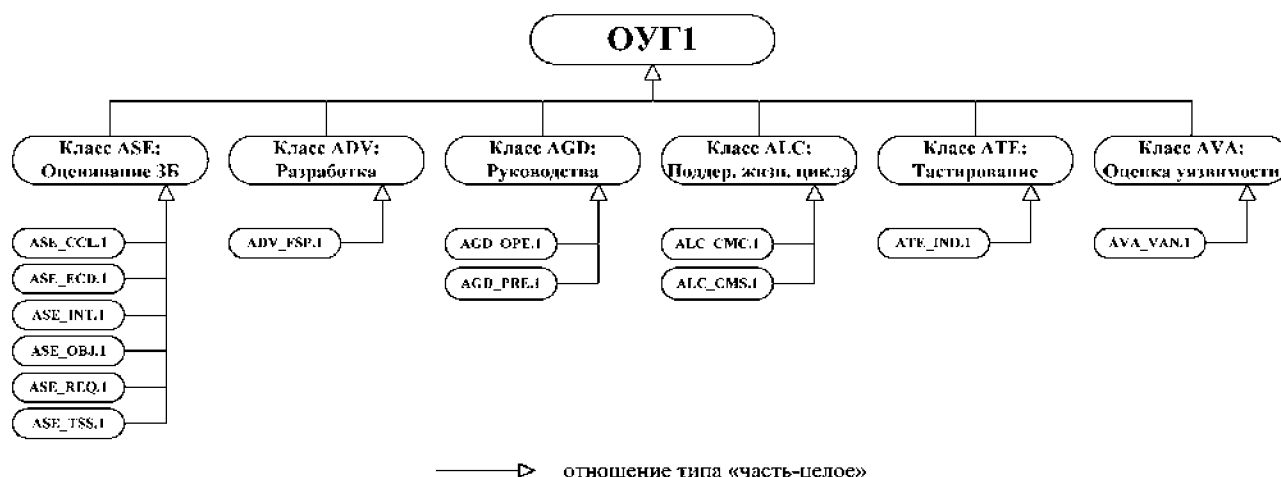


Рис. 3. Иерархическая объектно-ориентированная онтология требования гарантий по ОУГ1

семейство гарантий содержит набор атрибутов, предоставляющих информацию о характеристике, ранжировании компонентов и особенностях применения семейства. Каждое семейство гарантий содержит множество связанных с ним компонентов. При моделировании компоненты могут быть выражены как субсемейства. На уровне компонентов возможны отношения между компонентами как внутри одного класса, так и межклассовые. Каждый компонент содержит элементы гарантий трех типов: элементы действий разработчика, элементы содержания и представления свидетельств, элементы действий оценщика.

Пример иерархической объектно-ориентированной онтологии требований гарантий по оценочному уровню гарантий 1 (ОУГ1) представлен на рис. 3.

2.2. Онтологическая модель области оценивания гарантий

Онтологическая модель области оценивания гарантий включает в себя *объектно-ориентированную онтологическую модель* и *процессно-ориентированную модель* оценивания гарантий информационной безопасности.

2.2.1. Способ построения объектно-ориентированной онтологии области оценивания гарантий

Построение объектно-ориентированной онтологии области оценивания гарантий осуществляется в 3 этапа (рис. 4).

I этап. Строится объектно-ориентированный иерархический граф требований гарантий (G^R). Определяется степень глубины (уровень детализации) требований. Степень детализации требований определяет

мощность множества свойств гарантий объекта оценки. Выявляются отношения зависимости на множестве требований гарантий и определяется их тип (часть – целое, экзистенциальная, каузальная, внутриклассовая, межклассовая и т. д.). Формальная запись графа требований гарантий имеет вид

$$G^R = \langle R, Q_R \rangle, \quad (1)$$

где $R = \{r_1, r_2, \dots, r_i\}$, $i = \overline{1, N}$ – множество требований гарантий, $Q_R = \{Q_f[r_i \leftrightarrow r_j]\}$, $f = \overline{1, F}$ – множество отношений на множестве требований гарантий.

II этап. Строится объектно-ориентированный иерархический граф свойств гарантий (G^P), которые необходимо оценить. Между иерархиями требований и свойств гарантий устанавливаются отношения (зависимости) ($D[R \leftrightarrow P]$). На основе анализа зависимостей Q_R определяются зависимости свойств гарантий Q_P . Зависимости могут как повторяться, так и возникать новые. Определяются сложные свойства гарантий, т. е. такие свойства, для оценки которых необходимо проверить или исследовать множество субсвойств. Формальная запись графа свойств гарантий имеет вид

$$G^P = \langle P, Q_P \rangle, \quad (2)$$

где $P = \{p_1, p_2, \dots, p_i\}$, $i = \overline{1, N}$ – множество свойств гарантий, $Q_P = \{Q_s[p_i \leftrightarrow p_j]\}$, $s = \overline{1, S}$ – множество отношений между свойствами гарантий.

III этап. Строится иерархический граф множества свидетельств (G^E), которые получены путем декомпозиции объекта оценки. Для каждого элементарного свойства $p_i \in P$ определяется множество свидетельств $E_{p_i} = \{e_1, e_2, \dots, e_i\}$, $i = \overline{1, N}$, которые необходимо исследовать для оценки данного свойства. За-

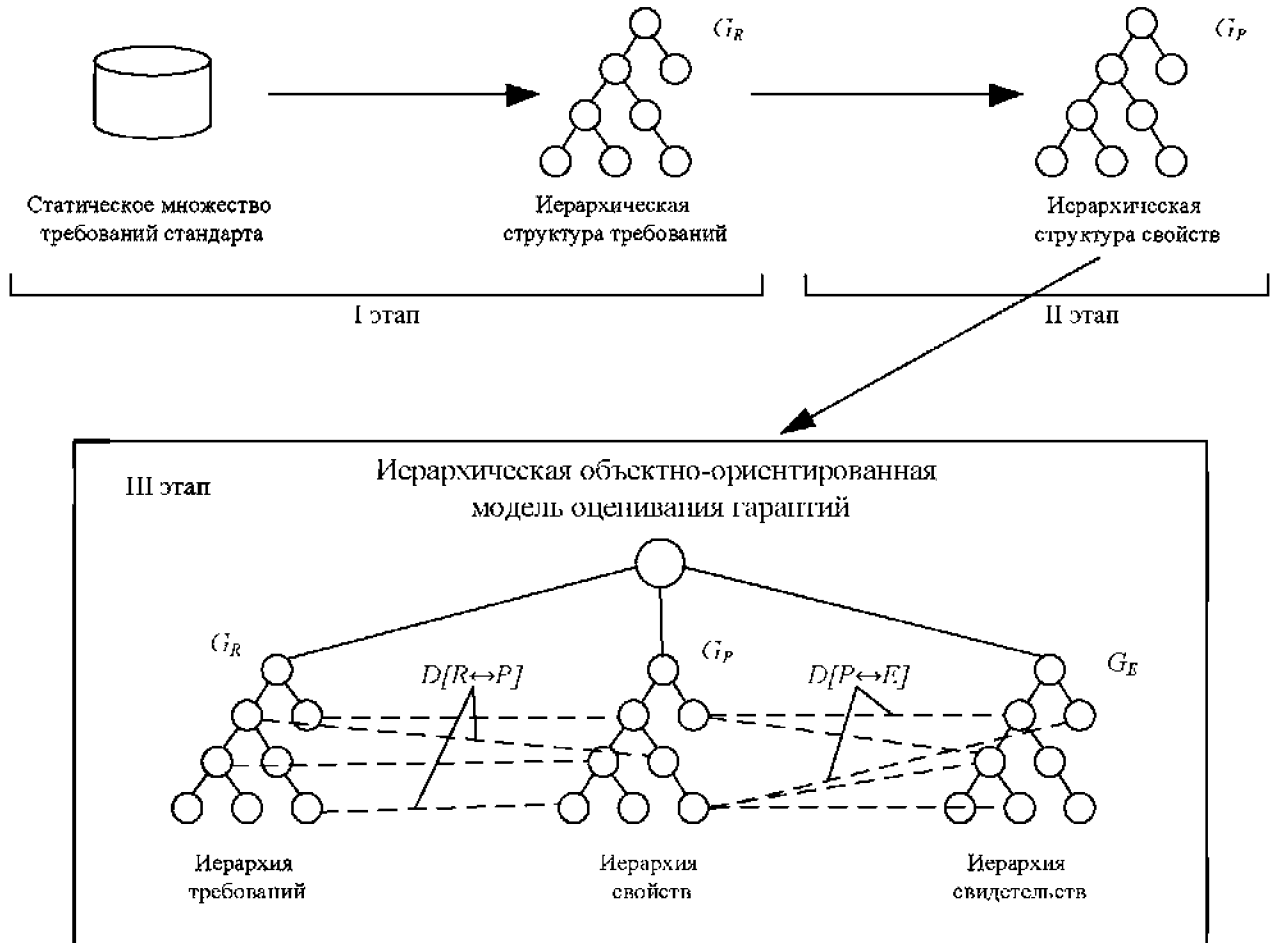


Рис. 4. Объектно-ориентированная модель области оценивания гарантий

висимости между графами G^P и G^E показываются в виде отношений типа «свойство – свидетельство» $D[PE]$. Формальная запись графа свидетельств имеет вид

$$G^E = \langle E, Q_E \rangle, \quad (3)$$

где $E = \{e_1, e_2, \dots, e_z\}$, $z = \overline{1, Z}$ – множество свидетельств, $Q_E = \{Q_y[e_i \leftrightarrow e_j]\}$, $y = \overline{1, Y}$ – множество отношений между свидетельствами.

Для сложных свойств соответствие между свидетельствами и свойствами может быть представлено в табличном (табл. 1) или матричном виде (4).

Таблица 1. Соответствие свидетельств и свойств

$e_i p_j$	Сложное свойство, P		
	p_1	p_2	p_3
e_1	1	1	1
e_2	0	1	0
e_3	1	0	0

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \quad (4)$$

В ячейки таблицы соответствия ставится «1» тогда, когда свидетельству e_i (строки таблицы) присуще свойство p_j (столбцы таблицы), то есть когда для оценки свойства p_j , записанного в столбце, необходимо использовать свидетельство e_i . В ячейке таблицы записывается «0», если между свидетельством и свойством нет взаимосвязи (соответствия).

Заполнение таблицы соответствия упорядочивает (систематизирует) знания об объекте оценки и позволяет уточнять характеристику оцениваемых свойств. Это в конечном итоге оказывает влияние на объективность оценки свойств гарантий.

Мощность множества требований (свойств, свидетельств), отображаемых с использованием онтологий иерархического типа, может быть определена по формуле

$$W = \sum_i \sum_h \sum_l G^i \cdot S_{h,l}, \quad (5)$$

где G^i – онтограф i -го множества, $i = \overline{1, 3}$; $S_{h,l}$ – степень вершины, равная числу исходящих из нее ребер, $h = \overline{1, H}$ – количество уровней онтологического графа, $l = \overline{1, L_h}$ – номер вершины на соответствующем (h -м) уровне онтологического графа.

Формально, объектно-ориентированная онтология области оценивания гарантий Ω_{ASO} имеет вид

$$\Omega_O = \langle G^R, G^P, G^E, D \rangle, \quad (6)$$

где G^R – объектно-ориентированный онтологический граф множества требований гарантий; G^P – объектно-ориентированный онтологический граф множества свойств; G^E – объектно-ориентированный онтологический граф множества свидетельств; $D = \{D[R \leftrightarrow P], D[P \leftrightarrow E]\}$ – множество отношений типа «требование – свойство» и «свойство – свидетельство».

Таким образом, для каждого свойства гарантий однозначно определяется требование, с которым оно связано, и свидетельство (одно или множество), необходимое для оценки данного свойства.

Пример объектно-ориентированной онтологии по оцениванию документации, которая описывает процедуры установки, генерации и запуска (ПУГЗ), представлен на рис. 5.

2.2.2. Способ построения процессно-ориентированной онтологии области оценивания гарантий

Процессно-ориентированная онтология оценивания гарантий строится на основе требований международного стандарта ISO/IEC 18045 [4]. Целью ее построения является определение взаимосвязи между оцениваемыми свойствами и действиями по оценке гарантий безопасности. Построение процессно-ориентированной онтологии осуществляется с учетом результатов, полученных при построении объектно-ориентированной онтологической модели. В качестве входов для выполнения процедуры построения процессно-ориентированной онтологии выступают, в частности, онтологический граф требований G^R , онтологический граф свойств гарантий G^P и множество отношений между ними $D[R \leftrightarrow P]$.

I этап. Строится онтологический граф действий по оценке гарантий G^A , определенных в стандарте ISO/IEC 18045 [4]. Определяется множество отношений зависимости Q_A на множестве действий A . Формальная запись графа действий имеет вид

$$G^A = \langle A, Q_A \rangle, \quad (7)$$

где $A = \{a_1, a_2, \dots, a_i\}$, $i = \overline{1, N}$ – множество действий по оценке гарантий, $Q_A = \{Q_s[a_i \leftrightarrow a_j]\}$, $s = \overline{1, S}$ – множество отношений между действиями по оценке гарантий.

II этап. Определяется множество зависимостей $D[R \leftrightarrow A]$ между онтологическими графами действий G^A и требований G^R . Взаимосвязь между структурными компонентами требований гарантий и структурой действий по стандарту ISO/IEC 18045 представлена на рис. 6.

III этап. Определяется множество зависимостей $D[A \leftrightarrow P]$ между онтологическими графами действий по оценке гарантий G^A и свойств гарантий G^P . Т. к. напрямую данные зависимости определить нельзя, они определяются косвенным путем, т. е. через требования гарантий (рис. 7).

IV этап. Строится онтология субъектов G^B , вовлеченных в процесс оценивания гарантий информационной безопасности. Формальная запись графа заинтересованных субъектов имеет вид

$$G^B = \langle B, Q_B \rangle, \quad (8)$$

где $B = \{b_1, b_2, \dots, b_i\}$, $i = \overline{1, N}$ – множество заинтересованных субъектов, $Q_B = \{Q_f[b_i \leftrightarrow b_j]\}$, $f = \overline{1, F}$ – множество взаимосвязей между субъектами.

Онтология субъектов, которые принимают участие в процессе обеспечения и оценивания гарантий безопасности, представлена на рис. 8 [13].

Таким образом, формальная запись процессно-ориентированной онтологии оценивания гарантий безопасности Ω_{ASP} имеет вид

$$\Omega_P = \langle G^R, G^P, G^A, D, G^B \rangle, \quad (9)$$

где G^R – онтологический граф множества требований гарантий; G^P – онтологический граф множества свойств; G^A – онтологический граф множества действий по оценке гарантий; $D = \{D[R \leftrightarrow P], D[R \leftrightarrow A], D[A \leftrightarrow P]\}$ – множество отношений типа «требование – свойство», «требование – действие» и «действие – свойство»; G^B – онтологический граф субъектов, вовлеченных в процесс оценивания гарантий.

Пример процессно-ориентированной онтологии по оцениванию документации, которая описывает ПУГЗ, представлен на рис. 9.

ЗАКЛЮЧЕНИЕ

Исследование требований гарантий с использованием аппарата онтологического моделирования дает более глубокое понимание предметной области оце-

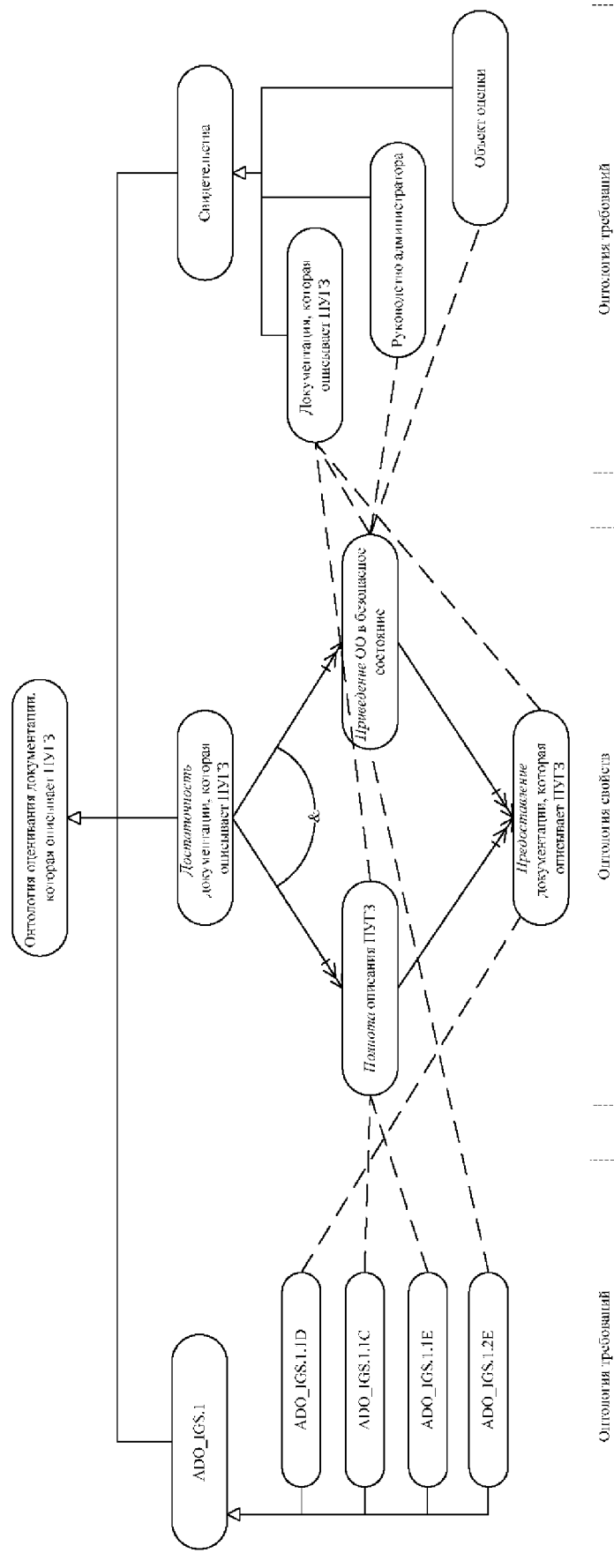


Рис. 5. Об'єктно-орієнтована онтологія по оцінюванню документації, яка описує ПУГЗ

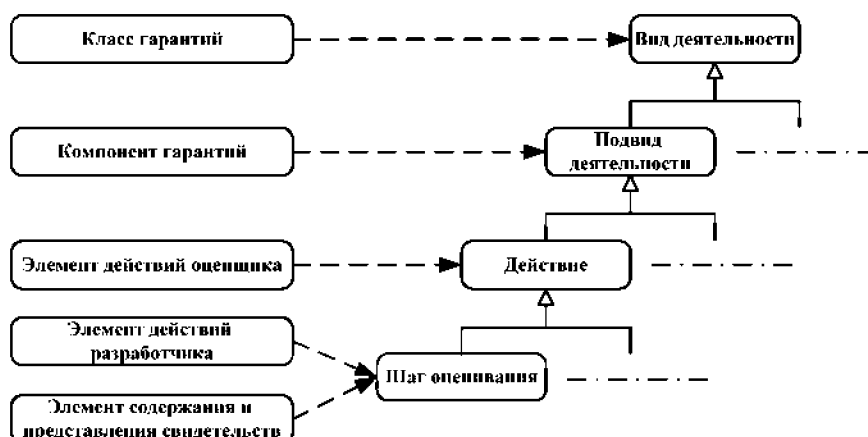


Рис. 6. Соответствие между компонентами требований гарантий и действиями по их оценке

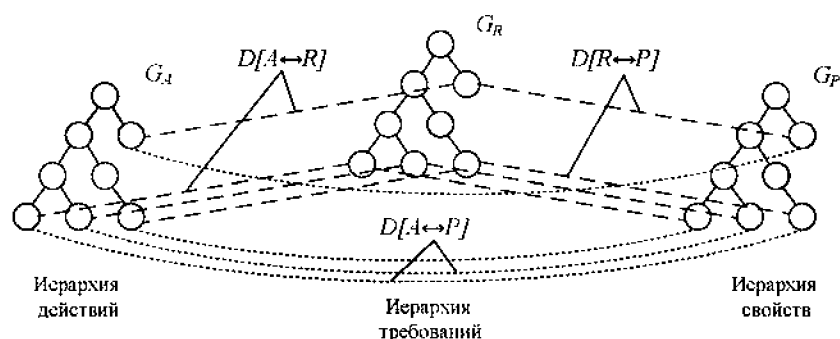


Рис. 7. Модель соответствия действий по оценке и свойств

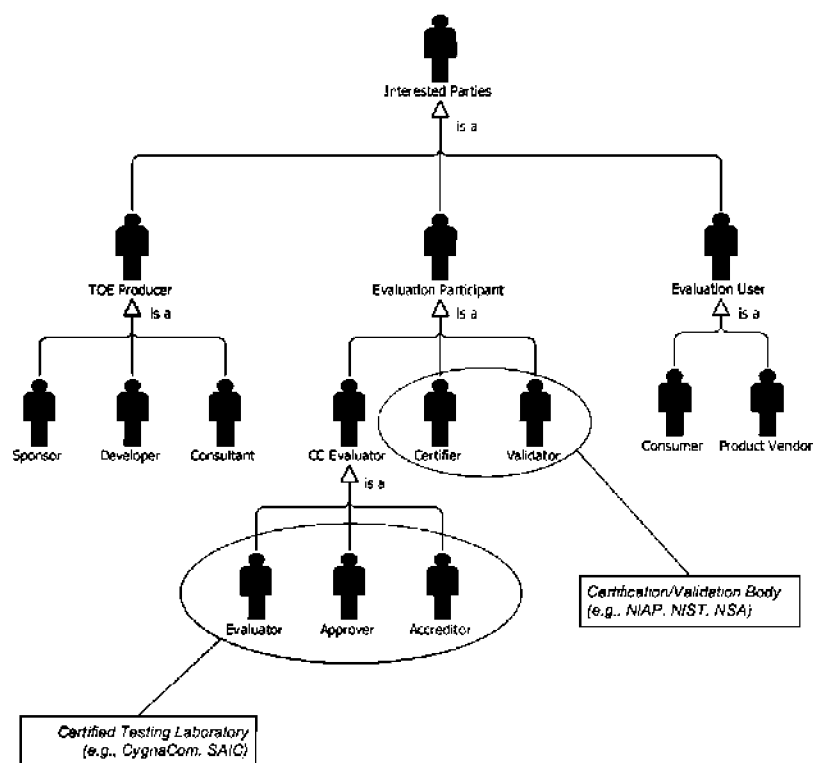


Рис. 8. Онтология субъектов, вовлеченных в процесс оценивания гарантий

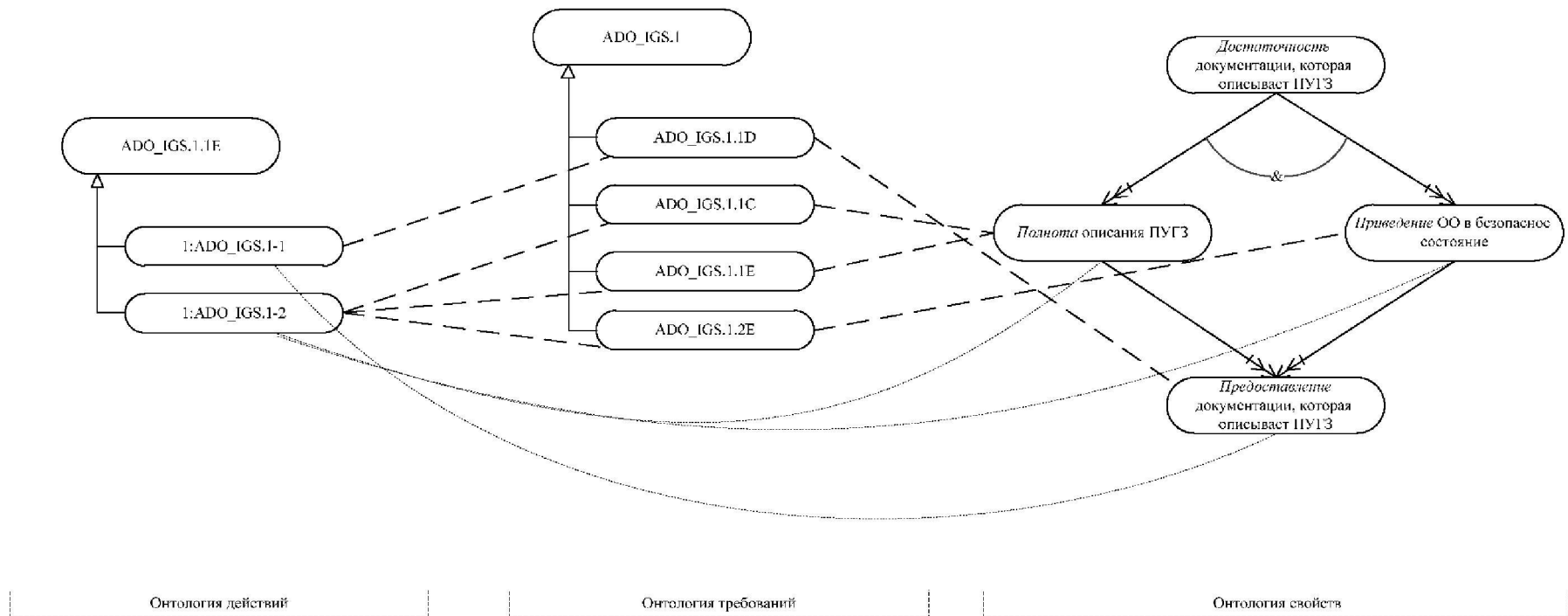


Рис. 9. Процессно-ориентированная онтология по оцениванию документации, которая описывает ПУГЗ

нивания и позволяет конкретизировать основные ее понятия и концепты. Построенные онтологии отображают различные типы связей и зависимостей между концептами области (между требованиями гарантий). Построение онтологических моделей требований гарантий направлено на выполнение требований ширины и глубины оценивания гарантий. Результаты онтологического анализа служат основой для разработки программы оценивания требований гарантий.

Применение функционально-лингвистического подхода для оценивания уровня гарантий безопасности позволяет удовлетворить требования как к процессу оценивания (ширина, глубина и строгость), так и к результатам оценивания (объективность, повторяемость, сопоставимость).

Актуальным вопросом остается разработка инструментальных средств поддержки работы эксперта по проведению оценивания гарантий. Предложенный подход служит основой для проектирования таких инструментальных средств. Дальнейшие исследования могут быть направлены на углубление и уточнение этапов подхода, его развитие и практическую реализацию.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 15408-1:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
2. ISO/IEC 15408-2:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
3. ISO/IEC 15408-3:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement.
4. ISO/IEC 18045:2005, Informational technology – Security techniques – Methodology for IT security evaluation.
5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. – [Чинний від 1999-04-22]. – К.: ДСТСЗІ СБ України, 1999. – 53 с. – (Нормативний документ системи технічного захисту інформації).
6. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-009-09. – [Чинний від 2009-07-24]. – К.: Адміністрація держспецзв'язку, 2009. – 171 с. – (Нормативний документ системи технічного захисту інформації).
7. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-010-09. – [Чинний від 2009-07-24]. – К.: Адміністрація держспецзв'язку, 2009. – 131 с. – (Нормативний документ системи технічного захисту інформації).
8. Потій, А. В. IDEF модели процесса оценки уровня гарантий безопасности / А. В. Потий, Д. С. Комин // Труды Научно-технической конференции с международным участием «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2010), Харьков, 18–21 мая 2010 г. – Х.: ХНУ, 2010 – С. 284–287.
9. Потий, А. В. Функционально-лингвистический подход к оценке гарантий информационной безопасности / А. В. Потий, Д. С. Комин // Тезисы докладов XIII Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах», Киев, 18–21 мая 2010 г. – К.: ГСССЗП, 2010 – С. 88.
10. Потий, А. В. Застосування функціонально-лінгвістичного підходу для оцінювання гарантій інформаційної безпеки / А. В. Потій, Д. С. Комін // Спеціальні телекомунікаційні системи та захист інформації. – 2010. – № 1(17). – С. 24–31.
11. Потий, А. В. Нечеткий логический вывод в задачах оценки уровня гарантий безопасности / А. В. Потий, Д. С. Комин // Тези доповідей V Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій», Запоріжжя, 22–24 вересня 2010 р. – Запоріжжя: ЗНТУ, 2010 – С. 121–123.
12. Information Integration for Concurrent Engineering (IICE). IDEF5 Method Report [Електронний ресурс] / Knowledge Based Systems, Inc. – Електрон. дан. – Texas: Knowledge Based Systems, 1994. – Режим доступу: <http://www.idef.com/pdf/Idef5.pdf>, вільний. – Англ.
13. Prieto-Diaz, R. The Common Criteria Evaluation Process. Process Explanation, Shortcomings, and Research Opportunities [Електронний ресурс] / Ruben Prieto-Diaz. – Електрон. дан. – Harrisonburg: Commonwealth Information Security Center, 2002. – (Commonwealth Information Security Center Technical Report Series / Series Editor Samiuel T. Redwine, Jr.) – Режим доступу: <https://users.cs.jmu.edu/prietorx/Public/CEvaluationProcessesTR03-5.pdf>, вільний. – Англ.

Надійшла 17.11.2010

Потій О. В., Комін Д. С.

ОНТОЛОГІЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ ОЦІНЮВАННЯ ГАРАНТІЙ В КОНТЕКСТІ ФУНКЦІОНАЛЬНО-ЛІНГВІСТИЧНОГО ПІДХОДУ

Пропонується функціонально-лінгвістичний підхід до оцінювання гарантій безпеки. Наводяться методика та результати онтологічного аналізу предметної області оцінювання гарантій. Обґрунтовується актуальність застосування апарату онтологічного моделювання для завдань оцінювання безпеки.

Ключові слова: гарантії, оцінювання, онтологічне моделювання, функціональне моделювання, лінгвістичні змінні.

Potij A. V., Komin D. S.

ONTOLOGICAL MODELING OF ASSURANCE EVALUATION IN THE CONTEXT OF FUNCTIONAL-LINGUISTIC APPROACH

The functional-linguistic approach to security assurance evaluation is proposed. The procedure and results of assurance evaluation ontological analysis are described. Ontological modeling application to security evaluation is justified.

Key words: assurance, evaluation, ontological modeling, functional modeling, linguistic variables.