УДК 629.735

А.В. Потий, Д.С. Комин

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

ОЦЕНКА ГАРАНТИЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРИМЕНЕНИЯ ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ

Предлагается подход к оценке уровня гарантий на основании построения функциональных моделей процесса оценивания и введения лингвистических переменных для оценивания качественных свойств, характеризующих уровень гарантий безопасности. На примере моделирования процесса оценивания по первому уровню гарантий демонстрируется возможность применения предложенного подхода.

Ключевые слова: *гарантии безопасности, оценивание, лингвистические переменные.*

Введение

Международный стандарт ISO/IEC 15408 [1, 2] закрепил общую модель и критерии оценки безопасности систем информационных технологий (ИТ). Широкое применение стандарта привело к необходимости взаимного признания результатов оценивания безопасности. К результатам оценивания выдвигаются требования объективности, повторяемости и сопоставимости, которые могут быть удовлетворены путем обеспечения глубины, ширины и строгости процесса оценивания [3]. В свою очередь, международный стандарт ISO/IEC 18045 [4] описывает методологию оценки безопасности, однако он не содержит формализованного аппарата проведения оценивания, что затрудняет обеспечение требования строгости процесса оценивания.

В данной статье предлагается подход к оценке гарантий безопасности, базирующийся на функциональном моделировании процессов оценивания и применения лингвистических переменных для характеристики и принятия решения относительно свойств объектов оценки.

1. Общий подход к оценке уровня гарантий

Результаты, представленные в данной работе, относятся к решению задачи обеспечения глубины и строгости оценивания. Глубина оценивания гарантий определяется степенью детальности рассматриваемых материалов об объекте оценивания. Стро-

гость оценивания определяется уровнем формализации применяемых методов оценивания и качеством инструментальных средств оценки [3].

Под объектом оценки (ОО) понимается ИТ-продукт или ИТ-система и связанные с ними руководства и документация (в частности задание по безопасности (ЗБ) или техническое задание, проектная документация, конструкторская документация и т.д.) [1]. Отдельные части ОО называют свидетельствами. Методология предполагает оценивание именно отдельных свидетельств, по результатам оценки которых и формируется соответствующее мнение (вердикт) и общий вывод об уровне гарантий.

На рис. 1 представлена общая схема, характеризующая подход к оценке уровня гарантий безопасности.

Рис. 1. Общий подход
к оценке гарантий безоасности

Глубина оценивания достигается путем анализа ОО, четкого определения множества свидетельств и однозначного выделения множества свойств ОО, подлежащих оценке. Для этого предлагается использовать процедуру декомпозиции ОО. В результате декомпозиции формируется конечное множество свидетельств оценки и соответствующее им конечное множество свойств, т.е. получаем множество пар вида «свидетельство-свойство». Декомпозиция свойств, в сочетании с четко определенными свидетельствами, и соответствующее представление результатов декомпозиции (например, в виде графов, матриц) позволяет убедительно продемонстрировать степень детализации ОО и даже дать количественную оценку глубины оценивания. Это позволит объективно судить о степени удовлетворения требования глубины оценивания.

С целью обеспечения строгости оценивания в работе предлагается формализовать процесс оценивания. Поскольку методология оценивания гарантий, определенная стандартом ISO/IEC 18045 [4], имеет вид вербального описания процесса проведения оценивания (прежде всего как деятельности эксперта), то задачу формализации оценивания предлагается решить путем использования методологии функционального моделирования процессов [5 – 8]. Под моделированием будем понимать процесс создания точного, достаточного, лаконичного, удобного для восприятия и анализа описания процессов оценивания, как совокупности взаимодействующих компонент и взаимосвязей между ними. Результаты анализа описания процессов оценки в стандарте ISO/IEC 18045, особенности описания и представления результатов оценки показали, что для описания процесса оценивания целесообразно использовать функциональное моделирование в нотациях IDEF0 и IDEF3 [5 – 7].

Одним из важных и труднодостижимых свойств является объективность результатов оценивания. Достижение требуемой степени объективности усложняется тем, что в большинстве случаев оценка свойств, характеризующих гарантии безопасности, осуществляется на основе субъективного мнения эксперта.

В предлагаемом подходе для обеспечения объективности результатов оценки предлагается ограничить свободу выбора эксперта, как лица принимающего решение. То есть эксперту предлагается осуществлять выбор (в частности давать оценку о степени проявления того или иного свойства) из заранее обоснованного и конечного множества альтернатив. Это достигается путем четкого и ясного описания оцениваемого свойства (характеристики) ОО и формального его представления в виде лингвистической переменной (в частности для описания множества возможных значений степени проявления оцениваемого свойства, из которого и осуществляет выбор эксперт).

Введение лингвистических переменных (ЛП) позволил применить соответствующий математический аппарат для разработки продукционных правил формирования промежуточных и окончательных вердиктов относительно степени проявления оцениваемых свойств, и, как итог, общего вердикта об уровне гарантий безопасности.

2. Применение предложенного подхода на примере оценки по уровню гарантии 1

Подход, представленный на рис. 1, был на практике применен для формального описания процесса оценивания на соответствие требованиям уровня гарантии 1.

1 этап. На данном этапе был проведен анализ требований гарантий, выдвигаемых при оценке по уровню гарантии 1. Это позволило выделить множество свидетельств, подлежащих оцениванию: {задание по безопасности (ЗБ), функциональная спецификация (ФС), руководство администратора (РА), руководство пользователя (РП), процедуры установки, генерации и запуска (ПУГЗ), непосредственно объект оценки (ОО)}.

2 этап. Процедура декомпозиции позволила сформировать множество свойств, присущих соответствующим свидетельствам, и выявить отношения зависимости на множестве свойств. В частности для рассматриваемого примера установлено, что оценке подлежит *достаточность* документации, описывающей ПУГЗ, которая в свою очередь зависит, например, от *полноты* неформального описания ФС и других свойств. Декомпозиция позволяет определить, что для оценивания какого-либо свойства ОО может потребоваться одно или несколько свидетельств, а также определить сложные свойства, т.е. такие свойства, для оценки которых необходимо оценить несколько подсвойств. Так, для оценки достаточности документации, описывающей ПУГЗ, необходимо проверить или исследовать множество свидетельств {ПУГЗ; РА; ОО}, и оценить множество подствойств – {Предоставление; Полнота описания; Приведение}. Результаты декомпозиции могут быть представлены в виде графа (например, граф отношений, таксономия и т.д) и в табличном виде (табл. 1).

Таблица 1

Декомпозиция свойства достаточности документации, описывающей ПУГЗ

Свидетельства	Характеристика	Свойство
ПУГЗ	Предоставление процедур, необходимых для безопасной установки, генерации и запуска	Предоставление
Описание ПУГЗ	Полнота описания шагов, необходимых для безопасной установки, генерации и запуска ОО	Полнота описания
ОО, РА, ПУГЗ	Приведение ОО в состояние «безопасная конфигурация"	Приведение

3 этап. На третьем этапе осуществляется моделирование процесса оценивания. Моделирование осуществляется в соответствии с нотацией IDEF0. При моделировании используются результаты предыдущих этапов, для того чтобы определить названия блоков IDEF0-диаграмм, входные, выходные потоки, управления. Названия блоков диаграмм точно определяют оцениваемое на данном шаге свойство. Входами блоков являются свидетельства, которые подлежат оцениванию, а выходом – вердикт об оценке оцениваемого свойства.

4 этап. На данном этапе для формализации записи вербально представленных свойств ОО, подлежащих оценке, вводится множество ЛП. Под ЛП будем понимать переменную, значением которой являются нечеткие подмножества, выраженные в форме слов или предложений на естественном или искусственном языке [9].

Формально ЛП задается кортежем

$$\{b,T,X,G,M\},$$

в котором b – название ЛП; T – совокупность ее лингвистических значений (терм-множество), областью определения каждого из которых является множество X; G – синтаксическое правило, порождающее термы множества T; M – семантическая процедура, позволяющая превратить каждое новое значение ЛП, образуемое процедурой G, в нечеткую переменную. Например, для оценки достаточности документации, описывающей ПУГЗ, была введена ЛП «*Достаточность*», которая может принимать множество значений: *Достаточность = {Достаточно, Вполне достаточно, Недостаточно}*.

5 этап. Построенные диаграммы оценивания гарантий в нотации IDEF0 дополняют диаграммы в нотации IDEF3. Нотация моделирования IDEF3 позволяет однозначно описать порядок действий эксперт, который может изменяться в зависимости от значений, которые будут принимать ЛП в ходе оценивания (по сути это выбор эксперта). Построенные диаграммы позволяют определить точки, в которых эксперт должен принять решение и вынести вердикт относительно оценки того или иного свойства.

6 этап. На данном этапе для каждой контрольной точки (перекрестка) IDEF3 диаграмм было сформировано множество шаблонов вердиктов (вариантов выбора эксперта). Выбор одного из шаблонов зависит от значения, которое принимает ЛП при оценке текущего свойства. Для вынесения окончательных вердиктов были сформированы продукционные правила. Окончательный вердикт может быть либо положительным, либо отрицательным. Ниже приводится вариант положительного вердикта по оцениванию достаточности документации, описывающей ПУГЗ.

Вердикт: *Достаточно = {Представлено, Полное, Приводит}*. Представленная документация, в которой описываются ПУГЗ ОО, является достаточной для обеспечения ПУГЗ ОО, а ПГУЗ приводят к безопасной конфигурации ОО. Проверено, что в документации представлено описание ПУГЗ. Представленное описание является полным. В ходе исследования установлено, что ПУГЗ приводят к безопасной конфигурации ОО.

Заключение

К процессам оценивания гарантий безопасности выдвигаются требования ширины, глубины и строгости. В существующих стандартах и нормативных документах [1, 2, 4] способы выполнения данных требований не определены, что затрудняет обеспечение объективности, сопоставимости и повторяемости результатов оценки.

Предлагаемый в данной работе подход позволяет обеспечить требования глубины и строгости оценивания за счет применения методов декомпозиции объектов оценивания свойств гарантий, функционального моделирования процессов оценки и принятия рений о степени проявления свойств гарантий на основе использования лингвистических переменных. В контексте данного подхода проводится анализ объекта оценки и его декомпозиция на свидетельства. Свидетельства используются для оценки множества свойств ОО. Для каждого свойства вводятся ЛП. Формально процесс и порядок оценивания представляется в виде IDEF0 и IDEF3 моделей.

Нерешенным остается вопрос определения функций принадлежности для введенных лингвистических переменных. Применение предложенного подхода может послужить основой для создания современных инструментальных средств и систем проведения оценивания гарантий безопасности.

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 15408-3:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.

3. Оценка безопасности информационных технологий / А.П. Трубачев и др. – М.: СИП РИА, 2001. – 356 с.

4. ISO/IEC 18045:2005, Informational technology – Security techniques – Methodology for IT security evaluation.

5. Методы и модели информационного менеджмента / Под ред. А.В. Кострова. – М.: Финансы и статистика, 2007. – 336 с.

6. Методология функционального моделирования IDEF0. Руководящий документ. – М.: Госстандарт России, 2000. – 75 с.

7. Марка Д.А. SADT — методология структурного анализа и проектирования / Д.А. Марка, К. МакГоуэн. – М.: Метатехнология, 1993. – 245 с.

8. Моделирование бизнеса. Методология ARIS: практическое руководство / М. Каменнова, А. Громов, М. Ферапонтов, А. Шматалюк. – М.., 2001. – 333 с.

9. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л.А. Заде. – М: Мир, 1976. – 165 с.

Поступила в редколлегию 17.03.2010

Рецензент: д-р техн. наук, проф. А.С. Петров, Восточно-украинский национальный университет им. Владимира Даля, Луганск.

ОЦІНЮВАННЯ ГАРАНТІЙ БЕЗПЕКИ НА ОСНОВІ ЗАСТОСУВАННЯ ЛІНГВІСТИЧНИХ ЗМІННИХ

О.В. Потій, Д.С. Комін

Пропонується підхід до оцінки рівня гарантій на основі побудови функціональних моделей процесу оцінювання та введення лінгвістичних змінних для оцінювання якісних властивостей, що характеризують рівень гарантій безпеки. На прикладі моделювання процесу оцінювання за першим рівнем гарантій демонструється можливість застосування запропонованого підходу.

Ключеві слова: *гарантії безпеки, оцінювання, лінгвістичні змінні.*

THE SECURITY ASSURANCE EVALUATION ON THE BASIS OF APPLICATION OF LINGUISTIC VARIABLES

O.V. Potij, D.S. Komin

The approach to the security assurance evaluation s on the basis of construction of functional models of evaluation process and introduction of linguistic variables for the qualitative properties evaluation is offered. On an example of evaluation process modeling on the first assurance level possibility of application of the approach is shown.

Keywords: *safe conducts, evaluation, linguistic variables.*