УДК 629.735

Д.С. Комин, М.В. Мурзин, С.В. Шварчук, И.Ю. Гридасов

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

ФОРМАЛИЗАЦИЯ КАЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ ОЦЕНКИ УРОВНЯ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются основные качественные характеристики, оцениваемые экспертом в ходе экспертизы систем защиты информации. Представлена формализация показателей полноты описания и достаточности с позиции решения задач системного анализа. Описываются критерии принятия решений по оценке показателей полноты описания и достаточности на основе уровня информированности эксперта.

Ключевые слова: *требования гарантий, экспертиза, качественные показатели.*

Введение

Неотъемлемой частью любой информационной технологии (ИТ), особенно там, где обрабатывается конфиденциальная информация, является комплекс мероприятий, связанный с обеспечением и защитой конфиденциальности, целостности и доступности информации. Для этого разрабатываются и внедряются в ИТ системы защиты информации (СЗИ).

Для оценки качества используемой СЗИ проводится экспертиза с привлечением соответствующих организаций и компетентных экспертов. Неотъемлемой частью экспертизы СЗИ является оценка уровня гарантий (уровня корректности реализации в СЗИ функций безопасности). В [1 – 3] предложен подход и разработан метод оценки гарантий информационной безопасности (ИБ) по требованиям стандартов [4 – 6]. Одной из основных проблем, которые существуют в сфере оценки гарантий ИБ, является тот факт, что для больше части требований гарантий в качестве показателей оценки могут быть использованы только качественные значения. В данной статье на основе применения метода оценки гарантий ИБ к требованиям гарантий уровня 1 и 2 приводятся типовые характеристики объекта, которые проверяются экспертом в ходе экспертизы объекта оценки (СЗИ), и разрабатываются способы их оценки с позиции решения задач системного анализа.

Основной материал

1. Показатели информированности эксперта при оценивании гарантий ИБ

На сегодняшний день отсутствует принятая система показателей оценки качественных характеристик информации. С позиции решения задач системного анализа существенно значимыми качественными свойствами информации являются: неопределенность, неточность, неполнота, нечеткость, несвоевременность, недостоверность, противоречивость [7, 8]. Определения данных свойств были учтены при формировании показателей информированности эксперта, проводящего оценку уровня гарантий.

Анализ свойств гарантий, выявленных в ходе применения метода оценивания гарантий ИБ к требованиям гарантий уровня 1 и 2, позволил сформировать следующие основные показатели информированности эксперта в части оценивания уровня гарантий: наличие (предоставление), согласованность (соответствие), полнота описания, достаточность.

Наличие (*предоставление*) – свойство ($I_Н$), которое характеризует факт существования и использования в целях экспертизы достоверной и своевременной информации (свидетельств). Данное свойство является бинарным, т.е. по результатам его оценки эксперт принимает решение либо о наличии, либо об отсутствии чего-либо.

Согласованность (*соответствие*) – свойство ($I_С$), которое свидетельствует о том, что информация из одного источника (свидетельства) не противоречит любой другой информации (другому свидетельству). Оценка согласованности может быть отдельным направлением научных исследований. В данном контексте принята бинарная оценка согласованности, при которой определяется наличие непротиворечивости двух свидетельств с использованием значений: согласованно либо не согласованно.

Полнота описания – свойство ($I_П$), которое характеризует соответствие количества получаемой экспертом информации той информации, которая необходима для принятия решения. При оценке свойств гарантий по такому показателю используется метод исследования, который предполагает выполнение углубленного анализа содержания материалов на предмет соответствия выдвинутым требованиям. Для оценки свойства полноты может быть использована многомерная шкала, в которой используются промежуточные значения между мерами описание отсутствует и описание полное, такие как описание недостаточно полное, описание почти полное и др.

Достаточность – свойство ($I_Д$), которое определяет наличие всех необходимых условий для соответствия заданным требованиям. Данный показатель используется для оценки сложных (комплексных) свойств гарантий и предполагает многомерную шкалу по результатам исследования (проверки) под-

свойств. Таким образом, решение по оценке свойства достаточности принимается путем агрегирования, т.е. объединения решений по подсвойствам из которых оно состоит.

Далее будет рассмотрена формализация показателей полноты описания и достаточности.

2. Формализация показателя полноты описания

Количественно полноту описания будем характеризовать показателем полноты описания $I_П$ [7]:

$$I_П = \frac{П - П^-}{П^+ - П^-}, \qquad (1)$$

где $П^+$, $П^-$ – максимально целесообразный и минимально допустимый объем информации, необходимый для принятия решения в определенных условиях; $П$ – объем информации, полученный экспертом в конкретной ситуации.

Величина $I_П$ определяет уровень полноты описания в том смысле, что показывает, на сколько относительный объем полученной информации превышает минимально допустимый объем для принятия решения, т.е. этот показатель количественно характеризует уровень полноты описания, исходя из минимально допустимого объема информации $П^-$. Исходя из того, что величина $I_П = 0$ при $П = П^-$, где $П^- > 0$, следует, что за начало отсчета уровня полноты информированности берут такое значение, которое соответствует определенному минимально допустимому объему информации в реальных условиях, т.е. в условиях проведения экспертизы. Величина $П$ характеризует объем информации для определенной ситуации из прогнозируемого множества ситуаций. При этом каждой k-й ситуации соответствует собственное значение $П_k$. А значения $П^+$ и $П^-$ – едины для всех ситуаций из исследуемого множества.

Особое внимание следует уделить понятию максимально целесообразный объем информации, необходимый для принятия решения. На первый взгляд может показаться, что увеличение объема информации обуславливает повышение обоснованности решения. Однако на практике это часто не оправдано, поскольку обоснованность решения повышается в случае получения не любой информации, а только полезной с точки зрения принятия решения. Поэтому существуют определенные количественные ограничения на максимально целесообразный объем информации для принятия решения, поскольку с увеличением объема возрастает время, необходимое на обработку данной информации.

Также следует отметить, что под значением $П^-$ понимается нижняя граница объема информации в том смысле, что решение можно принимать при условии $П \geq П^- + \varepsilon$, где ε – достаточно малая величина, поскольку для $П = П^-$ имеем $I_П = 0$. Взаимосвязь величин, которые характеризуют полноту описания $I_П$, можно изобразить в виде схемы (рис. 1).

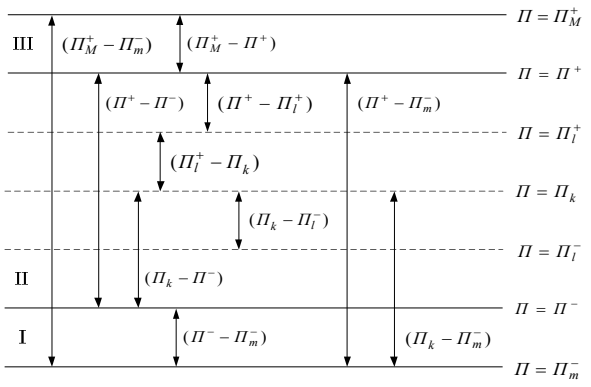

Рис. 1. Схема взаимосвязи величин, характеризующих полноту описания $I_П$

На рис. 1 введены такие обозначения: $П = П_m^-$ – уровень полного отсутствия информации об объекте оценивания; $П = П^-$ – уровень минимально допустимого объема информации об объекте оценивания; $П = П^+$ – уровень максимально целесообразного объема информации для принятия решения в определенных условиях; $П = П_M^+$ – уровень максимально полной информации об объекте оценивания; $П = П_k$ – уровень, соответствующий k-му объему полученной информации.

На рисунке выделены следующие области:

– область I соответствует уровню информации в интервале $[П_m^-, П^-]$, который определяет область недостаточной полноты информации об объекте оценивания. При данном уровне информированности эксперт примет решение «описание отсутствует»;

– область II соответствует уровню информации в интервале $[П^-, П^+]$, который определяет область рациональной полноты информации об объекте оценивания. При данном уровне информированности эксперт получает все необходимые свидетельства для их исследования на соответствие заданным требованиям;

– область III соответствует уровню информации в интервале $[П^+, П_M^+]$, который определяет область чрезмерной полноты информации об объекте оценивания. При данном уровне информированности эксперт получает избыточную информацию, затрудняющую анализ и исследование свидетельств на соответствие конкретному требованию, для оценки соответствия которому данная информация не нужна. В данном случае увеличивается временные рамки проведения экспертизы.

В каждом конкретном случае уровень полноты информации будет зависеть от того, какому значению будет соответствовать уровень информации $П_k$. Как видно из схемы, показатель полноты описания $I_П$ целесообразно использовать для характеристики области II. Поэтому для областей I и III введем дополнительные показатели:

– показатель избыточной полноты описания I_{Π}^{+}:

$$I_{\Pi}^{+} = \left(\Pi_{M}^{+} - \Pi^{+}\right) \Big/ \left(\Pi^{+} - \Pi^{-}\right); \qquad (2)$$

– показатель дефицита полноты описания I_{Π}^{-}:

$$I_{\Pi}^{-} = \left(\Pi^{-} - \Pi_{m}^{-}\right) \Big/ \left(\Pi^{+} - \Pi^{-}\right). \qquad (3)$$

Запишем множество ситуаций S_0 по оценке i-го свойства в виде

$$S_0 = \{S_k \mid k = \overline{1, N_S}\}. \qquad (4)$$

Из множества ситуаций S_0 по оценке i-го свойства выделим подмножества ситуаций по оценке полноты описания S_{Π} для каждой из введенных областей:

$$S_{\Pi_1} = \left\{S_{k_1} \in S_0 \mid \Pi_{m}^{-} \le \Pi_{k_1} < \Pi^{-}, k_1 = \overline{1, N_{\Pi_1}}\right\};$$

$$S_{\Pi_2} = \left\{S_{k_2} \in S_0 \mid \Pi^{-} \le \Pi_{k_2} \le \Pi^{+}, k_2 = \overline{1, N_{\Pi_2}}\right\}; \qquad (5)$$

$$S_{\Pi_3} = \left\{S_{k_3} \in S_0 \mid \Pi^{+} < \Pi_{k_3} \le \Pi_{M}^{+}, k_3 = \overline{1, N_{\Pi_3}}\right\};$$

$$N_{\Pi_1} + N_{\Pi_2} + N_{\Pi_3} = N_{\Pi_S},$$

где S_{Π_1}, S_{Π_2}, S_{Π_3} – подмножества ситуаций, для которых уровень полноты описания определяют области I, II и III соответственно.

Более детально проанализируем область II, поскольку в данной области при значениях полноты информации $\Pi_k \in [\Pi^{-}, \Pi^{+}]$ может быть реализована одна из следующих альтернатив: описание полное; описание почти полное; описание неполное.

Для этого проанализируем множество S_{Π_2}, которое соответствует области II, и выделим подмножества, характеризующие количество полученной полезной информации в ходе экспертизы:

$$S_{\Pi_{21}} = \left\{S_{k_{21}} \in S_{\Pi_2} \mid \Pi^{-} \le \Pi_{k_{21}} < \Pi_{I}^{-}, k_{21} = \overline{1, N_{\Pi_{21}}}\right\};$$

$$S_{\Pi_{22}} = \left\{\begin{matrix} S_{k_{22}} \in S_{\Pi_2} \mid \Pi_{I}^{-} \le \Pi_{k_{22}} < \Pi_{I}^{+}, \\ k_{22} = \overline{1, N_{\Pi_{22}}}; \end{matrix}\right\}; \qquad (6)$$

$$S_{\Pi_{23}} = \left\{S_{k_{23}} \in S_{\Pi_3} \mid \Pi_{I}^{+} \le \Pi_{k2_3} \le \Pi^{+}, k_{23} = \overline{1, N_{\Pi_{23}}}\right\},$$

где $S_{\Pi_{21}}$ – множество ситуаций, при котором объем полученной экспертом информации k_{21} соответствует альтернативе «описание неполное»; $S_{\Pi_{22}}$ – множество ситуаций, при котором объем полученной экспертом информации k_{22} соответствует альтернативе «описание почти полное»; $S_{\Pi_{23}}$ – множество ситуаций, при котором объем полученной экспертом информации k_{23} соответствует альтернативе «описание полное».

Исходя из свойств областей I – III, можно сделать вывод, что подмножество $S_{\Pi_{21}}$ по своим свойствам совпадает с множеством S_{Π_1} в том смысле, что свойство полноты описания не обеспечивается для $S_k \in S_{\Pi_{21}}$ и $S_k \in S_{\Pi_1}$. Множество S_0 по системе признаков, определенных выражениями (5) и (6), можно разделить на два подмножества S_{Π}^{+} и S_{Π}^{-}, где S_{Π}^{+} – подмножество, для элементов которого возможно обеспечение свойства полноты описания; S_{Π}^{-} – подмножество, для элементов которого свойство полноты описания не обеспечивается. Учитывая свойства введенных ранее подмножеств, можно записать

$$S_{\Pi}^{+} = S_{\Pi_3} \cup S_{\Pi_{22}} \cup S_{\Pi_{23}}; \; S_{\Pi}^{-} = S_{\Pi_1} \cup S_{\Pi_{21}}. \qquad (7)$$

Таким образом, оценивание показателя полноты описания сводится к определению объема полученной информации и решению задачи распознавания, а именно определению для каждой конкретной ситуации, к какому из введенных ранее множеств она относится.

3. Формализация показателя достаточности

Еще одним важным показателем, введенным для оценки свойств гарантий, является показатель достаточности. Особенностью его является то, что он описывает только сложные свойства и показывает уровень соответствия заданным требованиям, обусловленный влиянием ряда факторов – неполноты, несогласованности, неточности и неопределенности исходной информации, т.е. информации о результатах оценки подсвойств. Анализ данного показателя по различным уровням достаточности представлен на рис. 2.

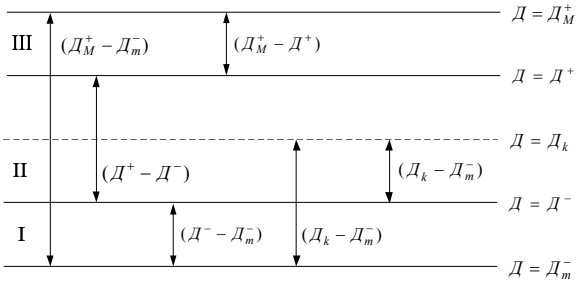

Рис. 2. Схема различных уровней достаточности $I_Д$

На схеме введены следующие обозначения: $Д_m^-$ – уровень, который соответствует полному отсутствию информации о результатах оценки подсвойств; $Д_M^+$ – уровень, который соответствует максимальной информированности о результатах оценки подсвойств, причем каждое из них имеет максимальный уровень соответствия оцениваемым требованиям; $Д^+$ – уровень, которому соответствует информированность о результатах оценки всех подсвойств, при котором интегральная оценка подсвойств может быть вынесена как «достаточная»; $Д^-$ – уровень, которому соответствует информированность о результатах оценки всех подсвойств, при котором каждое из подсвойств имеет минимально достаточный уровень соответствия оцениваемым требованиям; $Д_k$ – значение достаточности для k-й ситуации из заданного множества ситуаций.

Можно выделить три области:

– область I соответствует интервалу $Д \in [Д_m^-, Д^-]$ и определяет область *недостаточного* соответствия заданным требованиям;

– область II соответствует интервалу $Д \in [Д^-, Д^+]$ и определяет область *умеренно достаточного* соответствия заданным требованиям;

– область III соответствует интервалу $Д \in [Д^+, Д^+_M]$ и определяет область *достаточного* соответствия заданным требованиям.

Для каждой области введем показатель достаточности.

Для области I введем показатель уровня дефицита достаточности:

$$I^-_Д = \left(Д^- - Д^-_m\right) \Big/ \left(Д^+ - Д^-\right). \quad (8)$$

Для области II введем показатель уровня умеренной достаточности:

$$I_Д = \left(Д_k - Д^-\right) \Big/ \left(Д^+ - Д^-\right). \quad (9)$$

Для области III введем показатель уровня полной достаточности:

$$I^+_Д = \left(Д^+_M - Д^+\right) \Big/ \left(Д^+ - Д^-\right). \quad (10)$$

Исходя из введенных обозначений, множество ситуаций S_0, определенное соотношением (4), запишем таким образом, чтобы введенные подмножества ситуаций имели свойства, определенные областями I, II и III по показателю достаточности.

$$S_{Д_1} = \left\{S_{k_1} \in S_0 \mid Д^-_m \le Д_{k_1} < Д^-, k_1 = \overline{1, N_{Д_1}}\right\};$$

$$S_{Д_2} = \left\{S_{k_2} \in S_0 \mid Д^- \le Д_{k_2} \le Д^+, k_2 = \overline{1, N_{Д_2}}\right\}; \quad (11)$$

$$S_{Д_3} = \left\{S_{k_3} \in S_0 \mid Д^+ < Д_{k_3} \le Д^+_M, k_3 = \overline{1, N_{Д_3}}\right\};$$

$$N_{Д_1} + N_{Д_2} + N_{Д_3} = N_{Д_S}.$$

Таким образом, оценивание показателя достаточности сводится к определению уровня информированности о результатах оценки подсвойств и решению задачи распознавания, а именно определению для каждой конкретной ситуации, к какому из введенных ранее множеств она относится.

Выводы

Применение подходов системного анализа позволило формализовать показатели полноты описания и достаточности и аргументировано описать критерии принятия решений по данным показателям. Использование приведенных материалов в сочетании с математическим аппаратом лингвистических переменных и нечеткого логического вывода в контексте метода оценивания гарантий ИБ будет способствовать обеспечению объективности экспертизы и выполнению требований повторяемости и воспроизводимости результатов экспертизы.

Подобный подход по формализации показателей оценки уровня гарантий ИБ может быть применен и к вновь выявленным показателям. Дальнейшие исследования будут направлены на разработку количественных оценок по критериям многомерных шкал показателей полноты описания и достаточности.

Список литературы

1. Потий А.В. Формальное описание процесса оценивания гарантий информационной безопасности / А.В. Потий, Д.С. Комин, В.И. Новиков // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ НІУ», 2011. – Вип. 4(20). – С. 246-249.

2. Потий А.В. Оценка гарантий информационной безопасности на основе функционально-лингвистического подхода / А.В. Потий, Д.С. Комин // Прикладная радиоэлектроника. – 2010. – Том 9 (№3). – С. 421-435.

3. Potij A.V. A Method of Evaluating Assurance Requirements. Information & Security / A.V. Potij, D.S. Komin, I.N. Rebriy // An International Journal. – 2012. – Vol. 28, No. 1. – P. 108-120.

4. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

5. ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

6. ISO/IEC 15408-3:2008, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement.

7. Згуровський М.З. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К. : Видавнича група BHV, 2007. – 544 с.

8. Потій О.В. Основи теорії систем та системного аналізу. Навчальний посібник / [Потій О.В., Медіченко М.П., Лєншин А.В., Комін Д.С.] – Х. : ХУПС, 2012. – 232 с.

Поступила в редколлегию 1.02.2013

Рецензент: д-р техн. наук, проф. А.В. Потий, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ФОРМАЛІЗАЦІЯ ЯКІСНИХ ПОКАЗНИКІВ ОЦІНКИ РІВНЯ ГАРАНТІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Д.С. Комін, М.В.Мурзін, С.В.Шварчук, І.Ю.Грідасов

Розглядаються основні якісні характеристики, що оцінюються експертом в ході експертизи систем захисту інформації. Наведена формалізація показників повноти опису та достатності з позиції рішення задач системного аналізу. Описуються критерії прийняття рішень по оцінці показників повноти опису та достатності на основі рівня інформованості експерта.

Ключові слова: *вимоги гарантій, експертиза, якісні показники.*

FORMALIZATION OF QUALITATIVE CHARACTERISTICS OF ASSURANCE EVALUATION

D.S. Komin, M.V. Murzin, S.V. Shvarchuk, I.U. Gridasov

Basic qualitative characteristics of information protection systems which are evaluated by an expert are considered. Characteristics formalization of description completeness and sufficiency for system analysis is proposed. Decision criteria according to the evaluation of description completeness and sufficiency on the basis of expert's informational level are characterized.

Keywords: *requirements of guarantees, examination, high-quality indexes.*