A METHOD OF EVALUATING ASSURANCE REQUIREMENTS

Alexandr POTIJ, Dmitrij KOMIN, and Inna REBRIY

Abstract: This paper presents ontological modelling results from the security assurance domain. It examines problems associated with the process of evaluating assurance. Towards this purpose we propose a functional-linguistic approach to the evaluation of security assurance level. The approach is grounded in the ontological modelling of assurance requirements which are liable to evaluation, in the functional modelling of the evaluation process in IDEF0 and IDEF3 notations and in the introduction of linguistic variables to represent qualitative properties. We consider performance requirements on the scope, depth and rigour of the evaluation process and the requirements for objectivity, repeatability, reproducibility, impartiality and comparability of evaluation results. Thus, we propose a method of evaluating assurance requirements that incorporates object-oriented assurance ontological modelling, process-oriented assurance ontological modelling, development of decision criteria, and workflow modelling.

Keywords: Information security, assurance requirements, evaluation process, ontological modelling, assurance level.

Introduction

International standard ISO/IEC 15408 consolidated the general model and security criteria for IT-products evaluation.[1] Wide application of this standard is resulted in necessity of mutual recognition results of security evaluation. Requirements of objectivity, repeatability, reproducibility, impartiality and comparability of the evaluation results are advanced. They can be performed only in case of supporting scope, depth and rigour of evaluation process. In its turn the international standard ISO/IEC 18045 describes the methodology of security evaluation,[2] but it does not contain any formal mechanism for evaluation, which makes performing rigorous evaluation complicated. In this article the approach to the security assurance evaluation, grounded on the functional modelling of evaluation process and on the introduction linguistic variables for the formalization of qualitative TOE properties is considered.

INFORMATION & SECURITY. An International Journal, Vol.28, No. 1, 2012, 108-120.

Ontological Modelling of the Security Assurance Domain

Task of the Domain Ontological Analysis

Domain analysis is the special form of the scientific activities, resulting in domain interpretation model building (in a broad sense). In the analysis process they are divided in the invariant and pragmatic knowledge, their conceptual components present the ontological knowledge of the domain. The system-ontological analysis is the new direction in the means and methods of the domain system analysis. The main idea of the system-ontological approach is the development of ontological system (*OnS*) described by expression (1) and presented domain ontology. *OnS* consists of the object ontology, process ontology and task ontology:[3]

$$OnS = \{O^{Sub}(O^O, O^P), O^T\}, \quad (1)$$

where O^O – object set ontology of the domain, which is considered as classes, subclasses and classes elements of hierarchical structure; O^P – process set ontology of the subject, which is considered as processes, sub-processes, actions and activities in hierarchical structure; O^T – task set ontology, which can be put and solved on the domain and considered as tasks, subtasks, procedures and operators in hierarchical structure.

Object set ontology is a tuple of four sets:

$$O^O = <X, R, F, A(D, Rs)>, \quad (2)$$

where $X = \{x_1, x_2, \ldots, x_i, \ldots, x_n\}$, $i = \overline{1,n}$, $n = Card\ X$ – finite set of domain concepts; $R = \{r_1, r_2, \ldots, r_k, \ldots, r_m\}$, $R: x_1 \times x_1 \times x_2 \times \ldots \times x_n$, $k = \overline{1,m}$, $m = Card\ R$ – finite set of semantically important relations among domain concepts; $F = X \times R$ – finite set of interpretation functions specified by concepts or/and relations; A – finite set of axioms used for writing true statements (definitions and limits).

The primary analysis of regulations and standards,[4] scientific and technical literature [5] has allowed to single out the next objects of the ontological modelling: *term-objects* – assurance, assurance level, assurance criteria, confidence, evaluation program, evaluation methodology, target of evaluation, information security, countermeasures, vulnerability, threat, risk, verdict, overall verdict; term-processes – evaluation, accreditation, certification, activity, action, check, examine, verification.

Ontological Models of the Security Assurance Domain

In the international standard ISO/IEC 15408 security and evaluation concepts and relationships are closely took. In Figure 1 the ontological model describing the subject of concepts “confidence” and “assurance” is presented. Measure of confidence is assurance level. Assurance level is a set of assurance requirements. Their implemen-

tation are characterized by correctness of the functional requirements realization, IT-product abilities to resist the security threats and provide achievement of the required dependability level in the system. Assurance is a ground for confidence that the IT-product meets its security objectives. Assurance requirements are put forward to the target of evaluation (TOE). TOE is the set of software, firmware and/or hardware possibly accompanied by guidance.

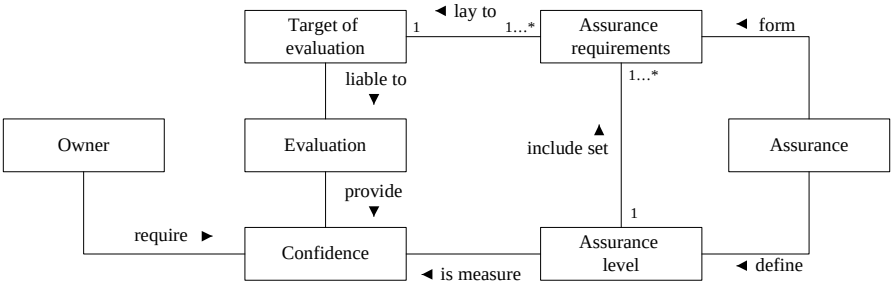

Figure 1: Ontological model of “confidence” and “assurance” concepts.

To define the degree of assurance requirements the implementation of the evaluation process is carried out (Figure 2). The evaluation process is based on the evaluation program and evaluation methodology, within the scope of the TOE certification and according to the evaluation criteria.

Evaluation program is a documental set of assurance requirements, which are checked during the TOE evaluation process. Evaluation methodology means established methods of the assurance requirements evaluation. Certification is a procedure by which the assurance level is approved. Certification may be performed by independent experts. In the evaluation process the next parties are involved: evaluator, validator, owner and developer. Evaluator is an individual person with an appropriate competency to carry out the security evaluation. There are several stages within a TOE lifecycle, there will be several evaluators for each stage. ‘Validator’ is an organization which prepares a validation report.

Evaluation criteria are formal or informal rules for making decision in relation to assurance requirements implementation. The output of the evaluation process is an assurance result. It is a documented quantitative or qualitative characteristic of the TOE. The advanced requirements to evaluation results foresee objectivity, repeatability, reproducibility, impartiality and comparability.

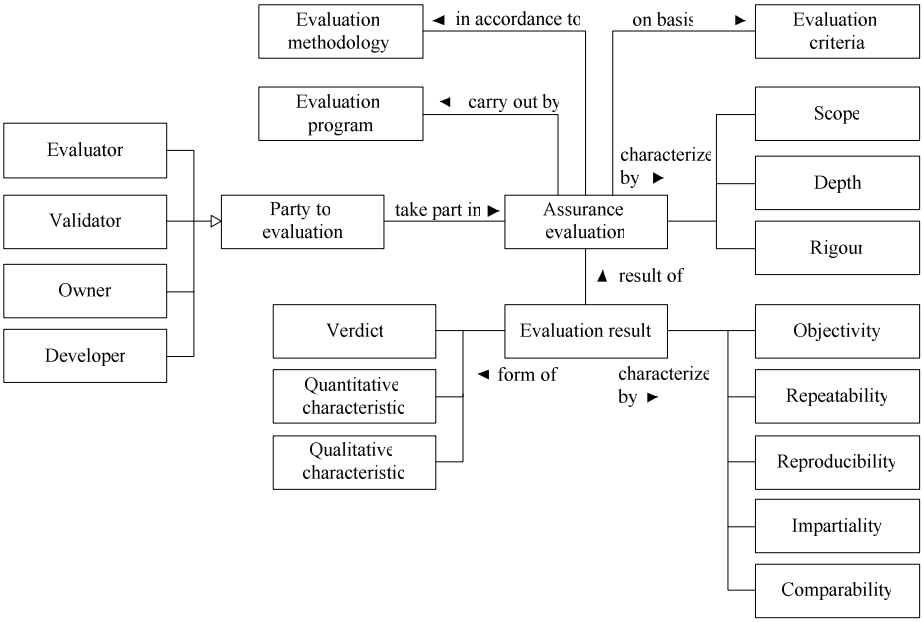

Figure 2: Ontological model of the assurance evaluation.

Objectivity is a property supposed that the evaluation requirements results must be actual, i.e. not to be undergone to sense influence or expert (evaluator) opinions. Repeatability is a property which provides the identity of the evaluation results during a re-evaluation of the same TOE held by the same program and methodology of security requirements evaluation by the same expert (evaluator). Repeatability is a property which provides the identity of evaluation results during the re-evaluation of the same TOE held on the same program and methodology of security requirements evaluation by another expert (evaluator). Impartiality is a property which provides the assurance requirements evaluation not prejudiced towards any specific evaluation result. Comparability is a property which provides matching the evaluation results obtained during the evaluation of the TOE developed by the same protection profile on different (or the same) program and evaluation methodology by another (or the same) expert (evaluator).

Concept of Functional-Linguistic Approach to Evaluating Security Assurance

During the analysis of assurance evaluation domain authors advanced a proposal to evaluate not the TOE, but its inherent assurance properties. These properties are de-

tected during the requirements. Thereby, IT-product evaluation consists of manifestation degree assessment of assurance properties inherent to the product. This is the key idea of the approach to the assurance evaluation proposed by authors.

Functional-linguistic approach structure is shown in Figure 3. Assurance evaluation is implemented in four phases. In the *phase 1* the ontological analysis and modelling of the domain evaluation are carried out. Analysis includes the research of the assurance requirements set ($R=\{r_1, r_2,...,r_i\}$, $i = \overline{1, N}$) advanced to the TOE, and detection the assurance properties set ($P=\{p_1, p_2,...,p_j\}$, $j = \overline{1, L}$) the TOE must possess. The assurance properties set P defines dependences and relations among properties. Analysis results are shown in form of ontological graphs, that exactly and unambiguously (in accepted notation) describe the domain (notably the main concepts and relations among them). Complex coverage of domain modelling is ensured by ontological graphs of two types: object-oriented and process oriented. The idea of Common Criteria requirements modelling was suggested by Seok Won Lee and co-authors.[6]

In the *phase 2* the functional modelling of the assurance evaluation process is implemented. Functional modelling goal is the formalized presentation of the evaluation process. IDEF0 notation was selected as a modelling language. IDEF0 notation makes it possible to defined evaluation steps unambiguously. If it necessary to evaluate complex property each step (diagram box) can be decomposed for the detail description of sub-properties evaluation.

In the *phase 3* for each property p_j the linguistic variable $\Omega p_j = <\beta, T(\beta), G, M>$ and its term-set $T(\beta)$ is defined. The application of linguistic variables can be explained by impossibility of quantitative characteristics usage for most assurance properties. Therefore for making decision on inherent degree of assurance properties it is convenient to use mathematical techniques of fuzzy inference conclusion on the ground of production rules basis.[7] Application of linguistic variables and fuzzy logic operations are provide the requirements implementation of objectivity and repeatability of assurance evaluation results.

In the *phase 4* workflow diagrams in IDEF3 notation are constructed.[8] It makes it possible to define the order and priority of evaluation actions implementation. Each diagram box represents the separate evaluator action. Each box is followed by the node, which defines the rule for chose the next action according to evaluator decision about inherent degree of evaluated property. Applications of IDEF3 diagrams ensure the requirements implementation of evaluation results repeatability.

During the ontological analysis of assurance requirements it is necessary to find the balance between the detail degree of evaluated properties and the cost of it evaluation process. The deeper the evaluation the more accurate the target of evaluation (TOE) assessment. However it can increase the cost-time factor of evaluation process. Low

detail evaluation reduces the cost of evaluation process, but can led to difficulties in decision making about inherent degree of assurance property and effect the wrong overall evaluation results.

So, approach realization makes it possible to implement requirements to assurance evaluation process and evaluation results. The approach can use for development of assurance evaluation program and methodology. These program and methodology can be used for IT-products evaluation of critical infrastructures which are influence on business and country safety and security.

A Method of evaluating Security Assurance

Method of the Object-Oriented Assurance Ontological Modeling

The process-oriented assurance ontological modeling is implemented into three phases (Figure 4). IDEF5 has been used as a modeling notation.

Phase 1. The object-oriented hierarchical graph of the assurance requirements (G^R) is constructed. Depth degree (specification level) of requirements is defined. Depth degree of requirements is defined by the power of the TOE assurance requirements set. Dependence relations on assurance requirements set are detected. Their mode (part, existential, causal, intra-class, interclass etc.) are defined. Formal description form of the assurance requirements graph is:

$$G^R = <R, Q_R>, \quad (3)$$

where $R=\{r_1, r_2,\ldots,r_i\}$, $i = \overline{1,N}$ – assurance requirements set, $Q_R=\{Q_f[r_i \leftrightarrow r_j]\}$, $f = \overline{1,F}$ – relations (dependences) set among assurance requirements.

For ontological modeling it is necessary to introduce the formal notation for each graph node. Formal note will be of form $R_i^{\{j\}}$, where i – graph node number of current level, $\{j\}$ – set, which values are graph node numbers according to level from top level to level previous to current, it is a decomposition way for node R_i of current level. This formal note has been used in all graphs of the security assurance evaluation method.

Phase 2. The object-oriented hierarchical graph of the assurance properties *(G^P)* is constructed. Dependences (relations) between requirements graph and properties graph *($D[R\leftrightarrow P]$)* are detected. The set of properties dependences Q_P grounded on Q_R dependences analysis is defined. Dependences can be repeated or arise as new ones. Complex assurance properties are defined. Complex is a property for evaluation of which it is necessary to check or examine the sub-properties set. Formal description form of the assurance properties graph is:

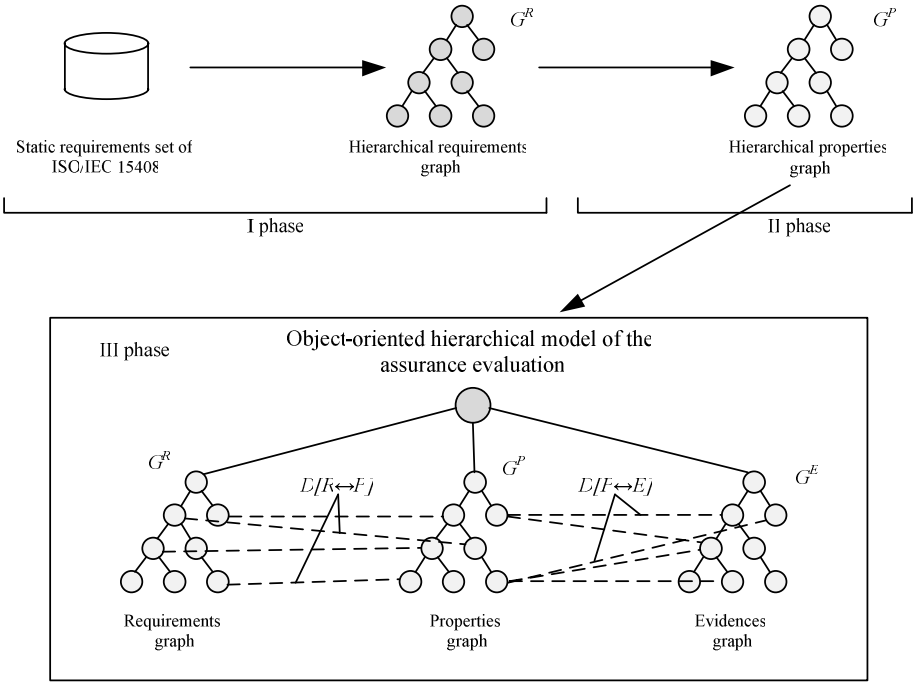

Figure 4: Object-oriented ontological model of the assurance evaluation domain.

$$G^P = <P, Q_P>, \tag{4}$$

where $P=\{p_1, p_2,...,p_i\}$, $i = \overline{1,N}$ – assurance properties set, $Q_P=\{Q_s[p_i \leftrightarrow p_j]\}$, $s = \overline{1,S}$ – relations (dependences) set among assurance properties.

Phase 3. The hierarchical graph of the evidences set (G^E) is constructed. Evidences are getting from the TOE decomposition. For each elementary property $p_i \in P$ the set of evidences $Ep_i=\{e_1, e_2, \dots, e_i\}$, $i = \overline{1,N}$ is defined. Dependences between graphs G^P and G^E are shown in the form of relations kind of "property - evidence" $D[P \leftrightarrow E]$. Formal description form of the evidences graph is:

$$G^E = <E, Q_E>, \tag{5}$$

where $E=\{e_1, e_2,...,e_z\}$, $z = \overline{1,Z}$ – evidences set, $Q_E=\{Q_y[e_i \leftrightarrow e_j]\}$, $y = \overline{1,Y}$ – relations set among evidences.

The power of requirements (properties, evidences) set shown by hierarchical ontology graph can be defined by formula:

$$W = \sum_{i} \sum_{h} \sum_{l} G^{i} \cdot S_{h,l} \tag{6}$$

where G^i – ontological graph of the i-th set, $i = \overline{1,3}$; $S_{h,l}$ – point degree of graph, equal to the number proceed from it lines, $h = \overline{1,H}$ – levels quantity of the ontological graph, $l = \overline{1,L_h}$ – point number on corresponding (h) level of the ontological graph.

Formal description form of the object-oriented ontological model by assurance evaluation domain is:

$$\Omega_O = < G^R, G^P, G^E, D >, \tag{7}$$

where G^R – the object-oriented ontological graph of assurance requirements set; G^P – the object-oriented ontological graph of assurance properties set; G^E – the object-oriented ontological graph of evidences; $D = \{D[R \leftrightarrow P], D[P \leftrightarrow E]\}$ – the relations set kind of "requirement-property" and "property-evidence."

Thereby, for each assurance property the associated requirement and necessary for evaluation evidence (one or set) are defined unambiguously.

Method of the Process-Oriented Assurance Ontological Modeling

Process-oriented assurance ontology is constructed on the ground of ISO/IEC 18045 requirements. The main reason of this ontology working out is the necessarily of relations identification between properties and evaluation actions. As inputs for process-oriented assurance ontological modeling the assurance requirements graph G^R, the assurance properties graph G^P and the relations set between them $D[R \leftrightarrow P]$ are used.

Phase 1. Evaluation assurance actions ontological graph (G^A) is constructed. Dependence relations set (Q_A) on actions set A is defined. Formal description form of the actions graph is:

$$G^A = <A, Q_A>, \tag{8}$$

where $A=\{a_1, a_2, \ldots, a_i\}$, $i = \overline{1,N}$ – evaluation assurance actions set, $Q_A=\{Q_s[a_i \leftrightarrow a_j]\}$, $s = \overline{1,S}$ – dependence set among evaluation assurance actions.

Phase 2. Dependences set ($D[R \leftrightarrow A]$) between ontological graphs of actions (G^A) and requirements (G^R) is constructed. Interdependences between structural components of assurance requirements and assurance actions by ISO/IEC 18045 are shown in Figure 5.

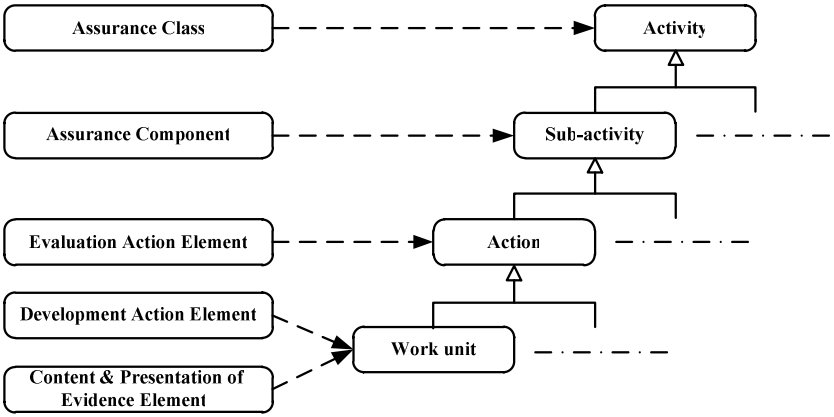

Figure 5: Interdependences between structural components of assurance requirements and assurance actions.

Phase 3. Dependences set ($D[A \leftrightarrow P]$) between ontological graphs of evaluation actions (G^A) and properties (G^P) are defined. These dependences are identified in indirect way, because it is impossible to do this directly. Correspondence model between actions and properties is shown on Figure 6.

Phase 4. Interested parties ontology (G^B) of the assurance evaluation process is constructed. Formal description form of the parties graph is:

$$G^B = <B, Q_B>, \tag{9}$$

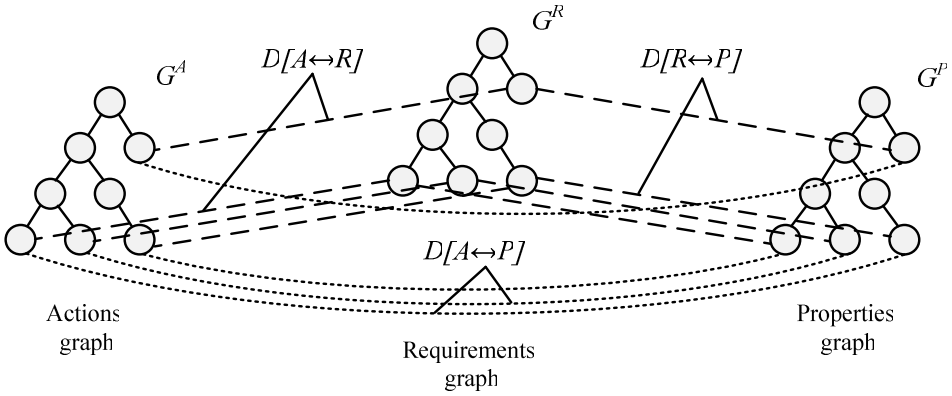

Figure 6: Correspondence model between actions and properties.

where $B=\{b_1, b_2, ..., b_i\}$, $i = \overline{1,N}$ – interested parties set, $Q_B=\{Q_f[b_i \leftrightarrow b_j]\}, f = \overline{1,F}$ – relations set among parties. Thereby, formal description form of the process-oriented ontological model by assurance evaluation domain is:

$$\Omega_P = < G^R, G^P, G^A, D, G^B >, \quad (10)$$

where G^R – ontological graph of the assurance requirements set; G^P – ontological graph of the assurance properties set; G^A – ontological graph of the evaluation actions set; $D = \{D[R \leftrightarrow P], D[R \leftrightarrow A], D[A \leftrightarrow P]\}$ – relations set kind of "requirement – property," "requirement - action" and "action - property"; G^B – ontological graph of interested parties that participate in the evaluation process.

Functional Modeling of Assurance Requirements Evaluation

Input data for functional modeling are results of object-oriented and process oriented ontological modeling of assurance requirements liable for evaluation. It's reasonable to present these data as a table:

Property	*Requirement*	*Action*	*Evidence*	*Evaluation parties*	*Evaluation method*
$P_i^{\{j\}}$	$R_i^{\{j\}}$	$A_m^{\{n\}}$	$\{E\}^{P_i^{\{j\}}}$	$\{B\}^{P_i^{\{j\}}}$	$U(P_i^{\{j\}})$

General form of functional box for assurance activity modeling is shown in Figure 7.

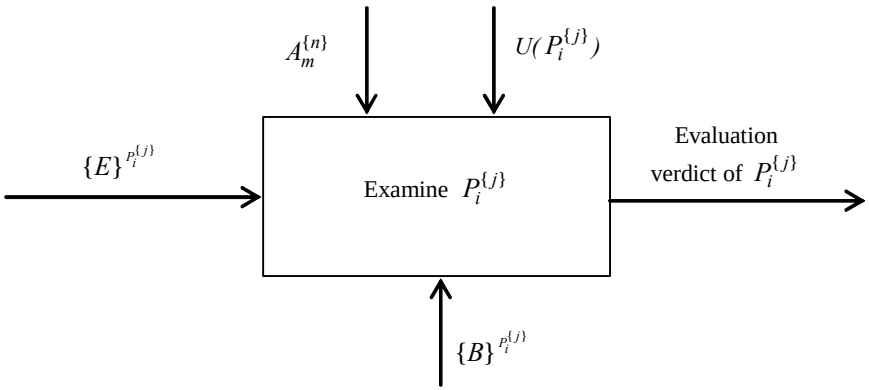

Figure 7: General form of functional box.

Where $P_i^{\{j\}}$ is a property liable for evaluation; $\{E\}^{P_i^{\{j\}}}$ is an evidence set necessary for property $P_i^{\{j\}}$ evaluation; $A_m^{\{n\}}$ is an action of property $P_i^{\{j\}}$ evaluation; $\{B\}^{P_i^{\{j\}}}$ is a set of interested parties participating in property $P_i^{\{j\}}$ evaluation; $U(P_i^{\{j\}})$ is a property $P_i^{\{j\}}$ evaluation method.

Method of Decision Criteria Development and Workflow Modeling

1. The linguistic variable for each property is introduced. Their term-sets and membership functions are defined;
2. Evaluation criteria for complex properties are developed. For example, define percentage value of linguistic variable (affirmative, intermediate, negative) for making decision about pass or fail verdict is defined;
3. According to evaluation criteria for each complex property the base of productional rules for decision making about evaluation of this complex property is developed. Productional rules are represented in the form of: IF … THEN…;
4. Algorithm of fuzzy logic inference is chosen. For example, Mamdani algorithm, Sugeno algorithm, Larsen algorism etc.;
5. If the evaluation results of some properties (simple or complex) must be represented in overall verdict, the verdict variants for each linguistic variable value are developed;
6. Order of simple properties evaluation is defined;
7. Workflow diagrams are developed. For example, modeling in IDEF3 notation.

Conclusion

Assurance evaluation is necessary condition of functional requirements implementation and information security maintenance. Today exist certain approaches and guidelines about assurance requirements choice and assurance level substantiation for the TOE. However, there are unresolved tasks (in theoretical and practical sense) of requirements implementation advanced to the assurance evaluation process and to evaluation results. Considering that assurance requirements have more informal type, objects of their application are mostly organizational and technological processes (design, development, production) and for the assurance level evaluation it is necessary to use various system-analysis techniques.

Application of the functional-linguistic approach for assurance level evaluation makes it possible to perform requirements to the evaluation process (scope, depth,

rigor) and to the evaluation results (objectivity, repeatability, comparability). The approach can use for IT-products evaluation of critical infrastructures which are influence on business and country safety and security.

Assurance requirements research using the instrument of ontological modeling gives deeper understanding of domain evaluation and makes it concepts more concrete. Ready-built ontological models show different types of relations and dependences among domain concepts (among assurance requirements). Ontological modeling of assurance requirements is directed to evaluation requirements implementation of scope and depth. Results of ontological analysis can be used as a ground for the assurance requirements evaluation program development. Results of functional modeling in IDEF0 and IDEF3 notations can be used as grounds for assurance requirements evaluation methodology development. The approach is referred to creation methodological mechanism of assurance evaluation. Method of security assurance evaluation is developed.

The problem of instrumental tools development for evaluator support in assurance evaluation is really actual. The approach presented can serve as a ground for designing such tools.

Notes:

[1] ISO/IEC 15408, *Informational technology – Security techniques – Evaluation criteria for IT security*, Part 1: Introduction and general model (2009) and Part 3: Security assurance requirement (2008).

[2] ISO/IEC 18045:2008, *Informational technology – Security techniques – Methodology for IT security evaluation*.

[3] A.V. Palagin, N.G. Petrenko, "System-ontological analysis of domain," *USiM* 4 (2009): 3-14.

[4] ISO/IEC 15408; ISO/IEC 18045:2008; Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, Final, CCMB-2009-07-003, July 2009; Common Methodology for Information Technology Security Evaluation – Evaluation methodology, Version 3.1, Revision 3, Final, CCMB-2009-07-004, July 2009.

[5] See for example A.P. Trubachev, *Assessment Security of Information Technology* (Moscow: SIP RIA, 2001), 14-138; M.V. Grajvoronskij, O.M. Novikov, *Security of Information and Computing Systems* (Kiev: VNV, 2009), 120-325.

[6] Deepak S. Yavagal, Seok Won Lee, Gail-Joon Ahn, and Robin A. Gandhi, "Common Criteria Requirements Modeling and its Uses for Quality of Information Assurance (QoIA)," Proceedings of the 43rd Annual ACM Southeast Conference ACMSE '05 (Kennesaw, Georgia, 2005), Vol. 2, pp. 130-135; Seok-Won Lee, Divya Muthurajan, Robin A. Gandhi, Deepak Yavagal, and Gail-Joon Ahn, "Building Decision Support Problem Domain Ontology from Natural Language Requirements for Software Assurance," *International Journal*

of Software Engineering and Knowledge Engineering 16:6 (2006): 851-84; Robert K. McNally, Seok-Won Lee, Deepak Yavagal, Wei-Ning Xia, "Learning the critical infrastructure interdependencies through an ontology-based information system," *Environment and Planning B: Planning and Design* 34:6 (2007): 1103-24.

[7] Lotfi A. Zadeh, "The Concepts of a Linguistic Variable and its Application to Approximate Reasoning," *Informational Sciences* 8 (1975): 199-249.

[8] Richard J. Mayer, Christopher P. Menzel, Michael K. Painter, Paula S. deWitte, Thomas Blinn, and Benjamin Perakath, *Information Integration for Concurrent Engineering,* IDEF3 Process Description Capture Method Report (September 1995).

ALEXANDR POTIJ, Colonel. Doctor of Technical Sciences, Associated Professor, Head of Department of Radioelectronic Systems for Air Force Command Posts of Kharkov Kozhedub Air Force University. Graduated of the Kharkov Higher Military School of Rocket Forces as an engineer in radioelectronics in 1993. In 1996 he got a PhD degree in automatic control systems. In 2008 he received a Doctor of Sciences degree in Information Security Systems. Over 80 articles dealing with problems of Information Security and Cryptography. *E-mail*: potav@ua.fm. *Address for Correspondence*: Ivanova 12/16 str, app. 61, Kharkov, Ukraine, 61002.

DMITRIJ KOMIN, Senior Lieutenant, with a specialist degree in radio engineering from Kharkov Kozhedub Air Force University (2007) and a degree in economics from Kharkov National Academy of Municipal Economy (2010). Postgraduate at Kharkov Kozhedub Air Force University and a PhD candidate in technical sciences. His current research interests include systems analysis methods of information security process and security evaluation methods. *E-mail*: dimakomin@mail.ru.

INNA REBRIY is Associate Professor at the Department of Foreign Languages of Kharkov Kozhedub Air Force University. Graduated from the School of Foreign Languages at Kharkiv State University. Teaches English and German. Since 1998 she has participated as a translator in training programs for foreign officers. Research interests in Social Philosophy for military purposes. Author of more than 15 publications. Currently works at her PhD thesis. *E-mail*: rebriy@vega.com.ua.