
Alexandr POTIJ and Dmitrij KOMIN

Department of Radio-Electronic Systems of Air Force Control Centers, Kharkiv Air Force University, Ukraine

Abstract: The functional-linguistic approach to the security assurance evaluation is proposed. Methodic and results of the assurance evaluation ontological analysis are given. Ontological modeling application to the security evaluation is grounded.

Keywords: Assurance requirement, Evaluation, Ontological modeling, Functional modeling

1. Introduction

Owners of information technology products (IT-products) want to have confidence in development quality, effectiveness of operations and security of IT-products. Regulations [1-4] in domain of security information technique define functional requirements and assurance requirements. Implementation of these requirements can give ground for that confidence. During the IT-product evaluation of assurance requirements implementation the consumer confidence in correctness of functional requirements realization is formed.

IT-product evaluations conduct by accredited testing labs according to evaluation program and method. Qualitative development of evaluation program and method is important component in the preparation time to evaluation. Evaluation process undergo by influence of different factors, which ability to effect on overall evaluation result. Therefore, requirements of scope, depth and rigour are advance to evaluation process, and requirements of objectivity, repeatability, comparability, reproducibility and impartiality are advanced to evaluation results.

Review of research literature shown that the assurance evaluation modeling and evaluation tools creation is the actual scientific task [9-14]. But generally modeling directed to the interactive representation of standard requirements in the form of informational tools. In addition in most papers at the modeling above-listed requirements are not regard.

In articles [5-7] the functional-linguistic approach to the assurance evaluation is proposed. Methods that used in the approach are broadly application in different branch of knowledge. Among them: ontological modeling [15], fuzzy technique [16-19] etc. It makes it possible to develop evaluation program and method, and implement above-listed requirements to the evaluation process and evaluation results. In the article represented results of further progress of functional-linguistic approach and it detail describing.

2. Conception of functional-linguistic approach

During the analysis of assurance evaluation domain authors advanced a proposal to evaluate not the TOE, but its inherent assurance properties. These properties are detected during the requirements analysis that advanced to the TOE in the regulation documents in the defined assurance level. As arguments of the property inherent to the TOE use evidences kind of all TOE, part of TOE, TOE documentations, TOE testing documentations etc. Thereby, IT-product evaluations consist in manifestation degree assessment of assurance properties that inherent to the product. This is the key idea of the approach to the assurance evaluation that proposed by authors.

Functional-linguistic approach structure is shown on figure 1. Assurance evaluation has implemented in four phases.
In the phase 1 the ontological analysis and modeling of the domain evaluation are carried out. Analysis is include the research of the assurance requirements set 

\[ R = r_1, r_2, ..., r_i, i = 1, N \] 

that advanced to the TOE, and detection the assurance properties set \( P = p_1, p_2, ..., p_j, j = 1, L \) which the TOE must possess. On the assurance properties set \( P \) dependences and relations between properties are defined. Analysis results are shown in the form of ontological graphs, that exactly and unambiguously (in accepted notation) describing the domain (notably the main concepts and relations between them). Completeness coverage of domain modeling is ensured by ontological graphs of two types: object-oriented and process oriented.

In the phase 2 the functional modeling of the assurance evaluation process is implemented. Functional modeling goal is the formalized presentation of the evaluation process. As modeling language was selected IDEF0 notation. IDEF0 notation makes it possible to unambiguously defined evaluation steps, for each step defined assurance property that evaluation, defined evidences which is necessary to given property evaluation, defined evaluation parties and regulations. If it necessary to evaluate complex property, that to each step (diagram box) can be decomposed for the detail description of subproperties evaluation.

In the phase 3 for each property \( p_j \) the linguistic variable \( \Omega p_j = \{0, T(\beta), G, M, F\} \) and its term-set \( T(\beta) \) is defined. Mathematical techniques application of linguistic variables is conditional by impossibility of used quantita-

tive characteristic for most assurance property. Therefore to decision making about inherent degree of assurance properties it is convenient to use mathematical techniques of fuzzy inference conclusion on the ground of production rules basis \[ 8 \]. Application of linguistic variables and fuzzy logic operations are provided the requirements implementation of objectivity and repeatability of assurance evaluation results.

In the phase 4 workflow diagrams in IDEF3 notation are constructed. It makes it possible to unambiguously define the order and priority of evaluation actions implementation. Each diagram box is represented the separate evaluator action. After each box is followed the junction, which define the rule for chose the next action according to evaluator decision about inherent degree of evaluated property. Number of alternative is depended on number of value that can take the linguistic variable which describing the evaluated property. Diagrams are defined points in which the evaluator must to make decision and pass the verdict about inherent degree of evaluated property. Build and application of IDEF3 diagrams are ensured the requirements implementation of evaluation results repeatability, because for each action define the set of evaluator verdicts. Chose the variant of verdict depend on value of linguistic variable which define during the evaluation.

Thereby, approach realizations make it possible to implement requirements of assurance evaluation process and evaluation results.

3. Ontological analysis and modeling of the assurance evaluation domain

During the ontological analysis of assurance requirements it is necessary to find the balance between details degree of evaluated properties and cost of it evaluation process. The more depth of evaluation the better accuracy of assessment target of evaluation (TOE). However thus increase the cost-time factor of evaluation process. Low detail of requirements reduce the cost of evaluation process, but can led to difficulty decision making about inherent degree of assurance property and as effect to the wrong overall evaluation results.

Ontological model of the security assurance domain is included an object-oriented ontological model and a process-oriented ontological model.
3.1. Method of the assurance object-oriented ontological modeling

The process-oriented assurance ontological modeling is implemented into 3 phase (fig. 2).

**Phase I.** 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 the power of the TOE assurance requirements set. Dependence relations on assurance requirements set are detected. Theirs mode (part of, existential, causal, intraclass, interclass etc.) are defined. Formal description form of the assurance requirements graph is:

$$G^R = <R, Q^R>, \quad (1)$$

where $R = \{r_1, r_2, \ldots, r_d\}, i = 1, N$ – assurance requirements set, $Q^R = \{Q^IR, \leftrightarrow r_f\}, f = 1, F$ – relations (dependences) set between assurance requirements.

**Phase II.** 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 repeated or arise new. Complex assurance properties are defined. Complex is a property for which evaluation it is necessary to check or examine the subproperties set. Formal description form of the assurance properties graph is:

$$G^P = <P, Q^P>, \quad (2)$$

where $P = \{p_1, p_2, \ldots, p_d\}, i = 1, N$ – assurance properties set, $Q^P = \{Q^IP, \leftrightarrow p_f\}, s = 1, S$ – relations (dependences) set between assurance properties.

**Phase III.** 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 $Ep_i = \{e_1, e_2, \ldots, e_z\}, i = 1, N$ is defining. 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:

$$G^E = <E, Q^E>, \quad (3)$$

where $E = \{e_1, e_2, \ldots, e_z\}, z = 1, Z$ – evidences set, $Q^E = \{Q^IE, \leftrightarrow e_y\}, y = 1, Y$ – relations set between evidences.

![Fig. 2. Object-oriented ontological model of the assurance evaluation domain](image-url)
For complex properties corresponding between evidences and properties can be shown in the form of table (table 1) or matrix (4).

Table 1. – Correspondence between evidences and properties

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
A = \begin{pmatrix}
1 & 1 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
\end{pmatrix}
\] (4)

In the table cell put “1” when to the evidence \(e_i\) (table rows) inherent the property \(p_j\) (table columns), that is when to the property \(p_j\) it is necessary to use evidence \(e_i\). If property \(p_j\) and evidence \(e_i\) have non-interconnection then in the table cell put “0”.

Table filling sort and systematize the knowledge about TOE and enable to specify evaluation property. In the final, it is influence on the assurance evaluation objectivity.

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

\[
W = \sum_i \sum_h \sum_l G_i^h \cdot S_{h,l}
\]

(5)

where \(G_i^h\) – ontological graph of the \(i\)-th set, \(i = 1, 3\);

\(S_{h,l}\) – point degree of graph, equal to the number proceeded from it lines, \(h = 1, H\) – levels quantity of the ontological graph, \(l = 1, L_h\) – point number on corresponding \((l)\) level of the ontological graph.

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

\[
\Omega_d = <G^R, G^P, G^E, D>,
\]

(6)

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; \(D = \{D[R\rightarrow P], D[P\rightarrow E]\}\) – 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.

3.2. Method of the assurance process-oriented ontological modeling

Process-oriented assurance ontology is constructed on the ground of ISO/IEC 18045 requirements. Its buildings claim is the relations identification between properties and evaluation actions. Construct of the process-oriented assurance ontology is implemented with take results from object-oriented assurance modeling. As inputs for process-oriented assurance modeling are acted assurance requirements graph \(G^R\), assurance properties graph \(G^P\) and relations set between them \(D[R\rightarrow P]\).

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

\[
G^A = <A, Q_s>,
\]

(7)

where \(A = \{a_1, a_2, ..., a_t\}, i = 1, N\) – evaluation assurance actions set, \(Q_s = \{Q_s[a_1 \leftrightarrow a_j]\}, s = 1, S\) – dependence set between evaluation assurance actions.

Phase II. Dependences set \((D[R\rightarrow A])\) between ontological graphs of actions \((G^A)\) and requirements \((G^R)\) is constructed. Interdependencies between structural components of assurance requirements and assurance actions by ISO/IEC 18045 are shown on fig. 3.
Fig. 3. Interdependences between structural components of assurance requirements and assurance actions

**Phase III.** Dependences set \((D/A \rightarrow P)\) between ontological graphs of evaluation actions \((G^A)\) and properties are defined \((G^P)\). These dependences are identifying by indirectly way, that is throw assurance requirements, because by directly way it is impossible (fig. 4).

**Phase IV.** Interested parties ontology \((G^R)\) of the assurance evaluation process is constructed. Formal description form of the parties graph is:

\[
G^R = <B, Q^R>,
\]

where \(B = \{b_1, b_2, \ldots, b_i\}, i = 1, N\) – interested parties set, \(Q^R = \{Q[b_i \leftrightarrow b_j]\}, f = \{F\} – relations set between parties.

Figure 5 provides a hierarchical decomposition of the interested parties. Interested parties are individuals and organizations that participate in the CC Evaluation Process. The hierarchy shows three main classes of participants and examples of organization membership for some of the participants (fig. 5) [9].

Fig. 5. Interested parties ontology

Thereby, formal description form of the process-oriented ontological model by assurance evaluation domain is:

\[
\Omega_{e} = \langle G^R, G^P, G^A, D, G^0 \rangle,
\]

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”; \(G^0\) – ontological graph of interested parties that participate in the evaluation process.

Fig. 4. Correspondence model between actions and requirements
4. Conclusion

Assurance requirements research with use the instrument of ontological modeling give more deep understanding of evaluation domain and make more concrete it concepts. Ready-built ontological models show different types of relations and dependencies between domain concepts (between assurance requirements). Ontological modeling of assurance requirements directed to evaluation requirements implementation of scope and depth. Results of ontological analysis can be used as ground for develop program of assurance requirements evaluation.

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).

Actual stay problem of develop instrumental tools for evaluator support during the assurance evaluation. Introduced approach can be ground for designing such tools. Further research can be direct on extend and specification approach phase, it development and practical realization.

References
lands, 2005.


Alexandr Y. POTIJ, Colonel

Dmitrij KOMIN, senior lieutenant
He received the specialist degree in Radio Engineering from the Kharkov Air Force University in 2007, and the Specialist Degree in Economics from the Kharkov National Academy of Municipal Economy in 2010. He has served his Postgraduate term at the Kharkov Air Force University. He has got the degree of a Doctoral Candidate in Technical Sciences (PhD). His present research interests include Systems Analysis Methods of Information Security Process, Security Evaluation Methods of Information Objects, among others.