IT security evaluation - “hybrid” approach and risk of its implementation

I I Livshitz¹, A V Neklyudov¹, P A Lontsikh²

¹ ITMO University, 49, Kronvekski Str., St. Petersburg, 190000, Russia
² Irkutsk State Technical University, 83, Lermontova Str., Irkutsk, 6644074, Russia

E-mail: Livshitz.il@yandex.ru

Abstract. It is relevant to evolve processes of evaluation of the IT security nowadays. Creating and application of the common evaluation approaches for an IT component, which are processed by the governmental and civil organizations, are still not solving problem. It is suggested to create a more precise and complex assessment tool for an IT security – the “hybrid” method of the IT security evaluation for a particular object, which is based on a range of adequate assessment tools.

1. Introduction
The processes of the evaluation of the IT-security are relevant nowadays. Creation and application of the common approaches to the IT component evaluation remain unsolved. The main criteria for a suitability of the IT component were its passing through a procedure of an independent adequate security conformity assessment. This is a fascinating procedure, because it fosters the fuller comprehension of the IT evolution circumstances today and in a long run. This research proposes performing for the precise object the synthesis of the “hybrid” approach of the IT security evaluation, based on the range of adequate and available assessment tools.

2. The precision as a target
In order to prevent a new essence involvement without emergency, the authors proposed an idea of increasing the IT-security evaluation precision by synthesizing the final adequate assessment tool set on a base of the “hybrid” method, adopted to a concrete IT object. IT evaluation precision is defined by the assessment tool and measuring techniques used. But the most important thing that experience demonstrates is that there should not be too many adequate assessment tools, in conjunction, they should be combined into a basis that has irrespective assessment lines within (this can be compared to a liner vector independence).

3. The expertise
Almost in any domain, all problems can be solved on a basis of these three, quite independent, expertise types:
• Experience (E) – the one, which is gained by the individual himself.
• Requirements (R) – expertise that is fixed on a data carrier like slightly formalized requirements.
• Calculation (C) - expertise that is based on measurement and calculation.
Each type of expertise has its own merits and demerits. In some cases, a problem can be solved both with one type of the expertise or with a random combination. Moreover, as for the historical background, everything starts with the E-type of expertise. However, ideally, it is better to use all three types together, in a harmonious interaction with each other. Graphically it can be imagined as a triangle, where the vertices represent the “poles” of the expertise, and a “body” of a triangle; beyond the vertices – some combination of it, the contribution of each to the proportion is determined by the closeness to the corresponding vertices (Figure 1).

Point A1 represents the expertise contribution before the TCSEC publishing. Point A2 shows expertise combination in a “rainbow series” era, when the security specifications were firstly structured, slightly formalized and were made accessible to a society. Point A3 corresponds to an expertise combination in a Common Criteria (CC) period, when security and assurance specifications were harmonized with the IT evolution level, precisely structured and were brought to a semi-formal style. Exactly at the time of CC, the C expertise type contribution appeared in a expertise proportion, at least because of the risk inclusion in a security concepts list and their correlation investigation.

The aim of the “hybrid” method, as the authors see it, is increasing the C expertise type contribution to the level that will ensure the A1 point in an optimal zone. This approach requires that the IT-security evaluation should be done by calculation, just like the reliability or resistance index of execution of cryptographic primitive estimation.

### 4. The “hybrid” method of evaluation

As an assessment tool for the “hybrid” method, the ISO/IEC 27001 series [1], CC (ISO 15408 allows series substitution [2, 3, 4]) and the Data flow Diagram (DFD) are used. The last one is chosen since, notwithstanding the shift of the emphasis from the structural to object-oriented approach during the analysis and designing the IS, structural notations are widely and effectively used both in business and system analysis. If necessary, DFD might be replaced with another simulation tool, e.g. Unified Modeling Language (UML).

For an industrial automation, evaluation can be useful for such tools as the IEC 61508 [5] or IEC 61511[6], if it requires tying up mutually information and functional security questions. All those assessment tools are uphold in a relevant condition, which is adequate to the up-to-date IT evolution level and consumers demands. And, which is significant, these standards are widely used in practice for a valuation, as DFD is used for a system simulation. In a modern IT belief system, which is stated...
- “all is an object”, the “hybrid” method defines the following types of an object:
  - IT – a production method, in the context of this issue – the way of information processing.
  - IT component – a part of the Information processing method, which, in turn, can be divided into components. When it is necessary to show that the IT component is indivisible, it is called the IT element. IT and its components can be established both on a basis of a hardware and without it.
  - Information Processing System (IPS) – a set of hardware with the specified relations, which is used as a base for IT or IT component establishment.
  - IPS component – a part of IPS that, in turn, can also be divided into parts. To show that the IPS component is indivisible, let us call IPS as an element.

5. The main idea of the “hybrid” method

A primary intent of the suggested “hybrid” method of the IT-security evaluation is a facility to make secure assessment with a preset refinement level of the random object of evaluation (OE) that can be any IT or its separate component. This method becomes “exclusive” due to a simple, but effective solution – building a model of the operation system and attention span to security questions in places that can bring effective solution with the limited number of trusted boundaries points (TB). Exactly within the TB, control is realized by the security functions or functional environment, specified in CC notation. IT-Security management measures in the 27001 notation are provided exactly for TB. Thus, IT-security evaluation quality will be determined largely by a validity of the OE model. On the one hand, the need for creation of an adequate IT model for OE can cause some difficulties for persons who have not enough skills; but on the other hand, it must be mentioned that it cannot be satisfactorily examined without IT as a whole or its components models.

The “hybrid” method does not provide the development of a united requirement list for the Security Target (ST), or for the range of the ST, as it should be done if the CC doctrine is followed dogmatically. However, at the same time, some structure and forming procedures are adopted partially from the ST. In the first case, this is done not to involve new essences over the existed ones, but in the other – to ensure “hybrid” method users with sets of materials, compatible with the ST parts, which might be useful for users if they will decide to develop ST and certify the OE by the CC. The operation sequence is provided by the “hybrid” method:
  - IT structuring.
  - Device space structuring.
  - IPS modelling.
  - Security issue defining.
  - Security target identification.
  - Short specification of the valuation object.

5.1. Step 1. IT structuring

All IT that provide business process automation are being divided into a few realms. The number of realms and their content are determined as convenient and effective to work with. The concentration of the IT ensures automation of the organization business processes, similar in some criteria, in one area borders, and attainability of the evaluation targets also has an impact on the number of realms and their content. The realm can be a composite and tiered hierarchical structure, which contains nested realms.

5.2. Step 2. Device space structuring.

The device space, which is occupied by an organization, is structured into a few locations (L). The number of it depends on the actual position of the organization assets in a device space, its working convenience and efficiency and attainability of the evaluation targets. The location also can be a composite and tiered hierarchical structure, which contains a nested location.
5.3. Step 3. IPS modelling
The IPS model patterning, which is the base for the IT, is realized in terms of DFD. The number of models patterned is defined as convenient to work with, to bear a comprehensive picture with a detailed elaboration given and to ensure the accomplishment of the evaluation targets. If necessary, it is possible to develop more than one model per system, as well as only one model can be designed for several systems, similar to each other. It is possible to see the IPS model for a real object (from the author’s practical experience) in Figure 2.

![IPS model for real evaluation object](image)

**Figure 2.** IPS model for real evaluation object

5.4. Step 4. Defining security issue.
The defining of the security issue consists of logical determination of the IT-security threats, organization security policy and assumptions for the operation environment. Keeping in mind an Albert Einstein’s quotation that “Everything should be made as simple as possible, but not simpler”, let us try to avoid extra detailed elaboration of the security threat information. In the authors’ opinion, it is necessary and enough to determine the security threats information on the IPS model to get the optimal detailed elaboration to keep going from the DFD objects to its realization tools – practically to the IPS components, considering IPS components as a finite automaton.

The necessity appears because the one of the assessment tools, which are used in a CC evaluation, keeps security specifications that practically appear in a semi-formal style, but it is necessary to use formal ones indeed for a height level of confidence. One must note that the real height levels of the EAL, from 5 and higher, mean that all possible controls with the mathematical methods are done. For example, Integrity-178B RTOS, the EAL6+ level system is a military operation system (which was
used for the fighting machine automation control and for the NASA space shuttle). To do the CC usage as an assessment tool, it is more efficient and reasonable to apply it to pretty formalized items; the IPS model, undoubtedly, is the formal one.

5.5. **Step 5. Security target identification**

Security targets are the brief and abstract statement of the assumed solution of the issue, already appointed. They have three roles:

- To present a height-level issue solution description.
- To divide this solution into two pieces (one for the evaluation object and the second for a function environment), which reflects that each essence solves its own part of an issue.
- To show that all these parts are arranged in solving the absolute problem.

Defining the security targets is processed as it is recommended in CC. The conclusion is made on a basis of security targets and their substantiation that if all security targets are reached, which means that the security issue, appointed earlier, is solved. That, in its turn, means that all threats are reacted to properly and the security assumptions are executed.

5.6. **Step 6. Short specification of the valuation object**

In this short description, the OE user can find information about how the certain object meets all security function, assurance and IT management specifications. The correspondence between the IPS model and the real respective system is described by a natural language. Each DFD notation in a model fits to a certain IPS component, data channel, TB implement means. Therewith, the following points are considered for each TB:

- TB implement means;
- Security function and assurance specifications in a CC notation;
- IT management specifications in 27001 notation.

Actually at this stage, security issue consideration for each TB is held and that is exactly what provides height security assessment precision of such complicated OE as IT.

6. **IT security risk assessment**

For the interfacing and the risk assessment procedure using the “hybrid” method of IT-security evaluation, one can take the IPS model, validity of which is approved with the IT-security evaluation, as a base for the risk assessment, and estimate the threat impact probability. In addition, in the process, the probability of a successful impact of a definite threat to a concrete object in the IPS model calculated as a multiplication of a probability of data flow (DF) occurrence by the threat source, between itself and a target object, with a probability of a DF overcoming each TB along its way.

It is necessary to mention that all threat impact probabilities, calculated by the method given below, are a probability a-priori, so the assessment of an apprehended damage by the threat impact is also a-priori. For that reason, the risks, which are calculated as a multiplication of the a-priory probability by the a-priori assessment of damages still a-priori themselves. However, practice is a truth criterion and the authors believe that it is useful to repeat evaluation of posterior risks with some intervals, using posterior (actual) damage assessment that fits these incidents. For calculation of the security posterior incident probability, the authors recommend using a calculation formula of a recovered object failure probability, applied during the reliability calculation.

7. **Example of Hybrid method implementation**

Authors have an experience in comparison of the real IT-security assessments, received in 2016-2017 using different methods for the unique and complex industrial facilities (CIF) [7, 8]. To ensure a scale identity, the IT security assessment was shown as a risk measure. In order to bring it to a ten-to-one scale, risk figures are multiplied by a normalized factor (risk measures are from 1 to 10); the loss of risk is 0. Table 1 shows a result of comparison of a-priori risks based on different methods.
Table 1. The risk assessment for “hybrid” method (for a-priori risk)

| Realm   | Hybrid method (15408 + 27001) | FSTEC Russia 31 | FSTEC Russia 21 | STO Gazprom 4.2-2-002-2009 | STO Gazprom 4.2-2-001-2010 | STO Gazprom 4.2-3-003-2009 | STO Gazprom 4.2-3-003-2009 |
|---------|--------------------------------|-----------------|-----------------|----------------------------|----------------------------|----------------------------|----------------------------|
| R1.1    | 2.50                           |                 |                 |                            |                            |                            |                            |
| R1.2    | 2.50                           |                 |                 |                            |                            |                            |                            |
| R1.3    | 2.50                           |                 |                 |                            |                            |                            |                            |
| R1.4    | 2.50                           |                 |                 |                            |                            |                            |                            |
| R2.1    | 1.67                           | 3.33            |                 | 6.67                       |                            | 6.67                       | 6.67                       |
| R2.2    | 1.67                           | 3.33            |                 | 6.67                       |                            | 6.67                       | 6.67                       |
| R2.3    | 0.83                           |                 |                 |                            |                            |                            |                            |
| R3.1.1  | 2.50                           | 10.00           |                 | 10.00                      |                            | 10.00                      | 10.00                      |
| R3.1.2  | 2.50                           | 10.00           |                 | 10.00                      |                            | 10.00                      | 10.00                      |
| R3.1.3  | 2.50                           | 10.00           |                 | 10.00                      |                            | 10.00                      | 10.00                      |
| R3.1.4  | 2.50                           | 10.00           |                 | 10.00                      |                            | 10.00                      | 10.00                      |
| R3.2    | 2.50                           | 10.00           |                 | 10.00                      |                            | 10.00                      | 10.00                      |
| R3.3    | 2.50                           | 10.00           |                 | 10.00                      |                            | 10.00                      | 10.00                      |

That high risk level using all methods except the “hybrid” was received only since all these methods provided, in principle, the definition procedure of the threat impact probability with a sufficient precision. Comparison of A-priori risks results on a ten-to-one scale using different methods is shown in Figure 3.

8. Conclusion
Nowadays, IT components with the security features that meet the civil society demands are available. All these components were evaluated by their competence and are suitable for building security capacity. A new method was suggested to create a more precise IT-security evaluation tool for the
particular object – the ‘hybrid’ method of IT-security assessment on a base of the set of adequate assessment tools.

References
[1] ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013
[2] ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
[3] ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components
[4] ISO/IEC 15408-3:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components
[5] IEC 61508-1:2010 Functional safety of electrical, electronic, programmable electronic safety-related systems — Part 1: General requirements
[6] IEC 61511-1:2003 Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements
[7] Livshitz I 2016 The Methods of optimization audit program for Integrated Management Systems. SPIIRAS Proceedings 5 52–68 https://dx.doi.org/10.15622/sp.48.3
[8] Livshitz I, Yurkin D, Minyaev A 2016 Formation of the instantaneous information security audit concept. Distributed computer and communication networks. Communications in Computer and Information Science Series 678 314–324 https://dx.doi.org/10.1007/978-3-319-51917-3_28