Evaluation of IT security – genesis and its state-of-art

I I Livshitz$^1$, A V Neklyudov$^1$, P A Lontsikh$^2$

$^1$ 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 topical to evolve processes of an evaluation of the IT security nowadays. Formation and application of common evaluation approaches to the IT component, which are processed by the governmental and civil organizations, are still not solving problem. Successful processing of the independent evaluation for conformity with a security standard is supposed to be the main criteria of a suitability of any IT component to be used in a trusted computer system. The solution of the mentioned-above problem is suggested through the localization of all research, development and producing processes in a national trusted area (digital sovereignty).

1. Introduction

The fortieth anniversary of an official introduction of «The Department of Defense (DoD) Computer Security Initiative» [1] will be celebrated in 2018. This initiative was the first in the world that puts the worldwide dissemination of trusted computer systems [TCS] as the main purpose. The term «trusted» meant that the system have sufficient security features that allows working over classified and other sensitive information at the same time. «Worldwide dissemination» implied free accessibility of the TCS components on the open market.

It was intended to state TCS security specifications and define a technically founded, reasonable and consistent evaluation routine for these specifications; competent center assistance of governmental TCS security rendered to a worldwide distribution of a trusted TCS by sharing the technology and information support. It was suggested to use an unified approach for evaluation of all TCS developed by governmental organizations or to its demand by its own initiative. The main test for any component to be used in trusted TCS was its passing through the procedure of the security specification evaluation.

2. Genesis of IT evaluation

In 1982, speaking at the fifth seminar «DoD Computer Security Initiative», NSA lieutenant-general Lincoln D. Faurer informed the audience that the DoD Computer Security Center had completed the draft with the security evaluation criteria, which are considered to be the objective base for the assessment of the integrity and reliability of the hardware environment and software (SW) security means [2]. In a few months, it was supposed to be submitted to the USA governmental institutions and IT industry representatives for consideration.

2.1. TCSEC

In 1983, the beginning of the sixth «DoD Computer Security Initiative» seminar coincided with the
signing of the memorandum «Department of Defense Trusted Computer System Evaluation Criteria» (TCSEC) [3]. After this, the DoD and NSA developed a whole set of documents, which are called “rainbow series” and have been unified by one subject – TCS. The last of the books is dated from 1995. However, in spite of an impressive range and wide coverage of different information security aspects, the downsides become evident soon, so it makes it difficult to use it as a mean of the evaluation of perspective IT.

First, rank criteria by TCSEC were not define clearly and universally enough that might not allow one to use them to classify both governmental and civil TCS. Secondly, authors of the TCSEC failed to foresee the IT trends with due precision, so the books of the «rainbow series» assembled later were also not arranged in compliance with those trends. Thus, it turns out that for a number of reasons, the «rainbow series» has limited capabilities to meet the changing conditions. Thirdly, notwithstanding that we can meet the word «risk» in the «rainbow series» of books, neither the single documents, nor the whole series are the example of the risk-oriented approach to the IT security evaluation.

2.2. ITSEC

In 1990 at the 13th National Computer Security Conference [4], ITSEC information was given much attention. It is notable, that the conference was named as «Standards – The Key to the Future». Parties, involved in the USA Department of Defense Initiative, turned out to be inwardly ready to comprehend all those new things that ITSEC contained. It was noted that ITSEC brings some smart ideas.

Firstly, ITSEC contains a unified set of a harmonized criterion for the evaluation of any IT objects. Moreover, it was significant progress, as compared to the TCSEC, which is supposed to be applied for any «computer system», but in practice, they were more or less suitable only for the security evaluation of the computers. Moreover, even then, open market players were pessimistic about using TCSEC for those purposes. With the ITSEC, each customer defines the object of evaluation (OE) and matches the set of criteria on one’s own.

Secondly, ITSEC provided the allocation of the OE security targets and estimation. Security targets define the set of OE security features, while security estimation determines specifications of OE operation environment. Depending on a level of evaluation needed, security targets might be determined by formal, semi-formal or informal style.

Thirdly, ITSEC evaluate the IT security by two figures - security functional and assurance component criteria. The authors of ITSEC said that, as for the specific OE, the set of security functional components more depends on the OE features than on the information value.

Nevertheless, several weaknesses were marked that can make a negative impact on the ITSEC efficiency as an evaluation instrument. Though ITSEC had no limits for an OE to define the set of security functional components, ten common levels of the security functions were fixed. Five of them correspond to TCSEC levels; the rest were fixed for five specific types of systems. This, to some extent, made ITSEC dependent on the TCSEC, which was not a good idea because in that time there was an understanding of a possible replacement of the «rainbow series» with developing ITSEC ideas, which contains more adequate IT evaluation criteria.

2.3. Federal Criteria

In 1992 at the 15th National Computer Security Conference [5], new Federal criteria were mentioned, developed by NIST and NSA (reportedly from November 1991) which contained security functional and assurance component criteria. Thus, the development of the TCSEC ideas began with regard to a newly discovered circumstance named ITSEC. At the same time, NIST and NSA began collaboration on the Federal Information Processing Standards Publications (FIPS).

2.4. Common Criteria

In 1993 during the 16th National Computer Security Conference [6], the «Federal Criteria for Information Technology Security» (FC) draft was widely discussed. It was mentioned that FC, undoubtedly, is the great step ahead as compared to TCSEC and it syncretizes with ITSEC quite well.
The result of this FC draft consideration was the decision to make the FC project international and to develop this to Common Criteria (CC), which are supposed to be harmonized with all existent criteria by the means of the USA at the conference with Canada and European union. The start was allocated on the fall of 1993, and in spring it was expected to get the first results. It must be mentioned that this term is too short for the work of such scale and complexity.

In 1994, during the 17th National Computer Security Conference [7], the community was brought up to date of the CC state of affairs. The international expert group examined the preliminary version of the CC in 1994 (Version 0.6, April 1994). It was assumed that using CC would facilitate the broadening of the IT trusted product market and mutual acceptance of the evaluation results by the national laboratories. The official version of CC after its publishing was supposed to became a base for a corresponding international standard. During CC development in every new version, consumers found it to be more and more useful for the IT security assurance and less useful because it might impose some limits on using the CC for the particular evaluation object. CC Version 1 ((Version 1.0, January 1996), after receiving the results of its using, was intended to pass to ISO as a base for the international standard [8].

3. Harmonization criteria of evaluation

It turns out that during a creation process, CC were harmonized not so much with all existing security evaluation criteria as it was planned firstly, but with the present IT evolution level and with the most advanced views on the IT matter and its security. Moreover, it played a significant role while CC became a self-contained document without any references to the documents with which CC was harmonized. The fact is that CC began considering the IT security question not as a detached direction but as a part of IT. This point of view on the IT-security problem allowed CC to develop naturally and without conflict with a speed of the IT evolution.

3.1. FISMA

However, even a creation of a suitable for practical using version of CC did not solve all the problems in IT security evaluation sphere, because, in some reasons, the decision to replace the «rainbow series» by the CC has not been completely made. Practically, CC replace the «rainbow series» only in security evaluation. This is especially strange because development of the «rainbow series» at that moment was frozen and, to authors’ mind, the last book of this series was dated by 1995. In 2002 The Federal Information Security Management Act of 2002 (FISMA) was adopted, which is, with the Paperwork Reduction Act of 1995 and Information Technology Management Reform Act of 1996, clearly determined adequate and profitable security policy based on risk assessments. In January 2003 NIST begun the FISMA Implementation Project, realization of which was elaborated by the FIPS and the Special Publications (SP) 800-30, SP800-37 and SP800-53 [9,10,11]. These documents contained the Risk Management Framework (RMF) description.

3.2. RFM

Like a CC, RMF uses a universal approach to an arbitrary chosen object named as «Information System» (IS). This approach is risk-oriented and object-oriented at the same time. An IS concept range in the RMF is shorter than that of an «evaluation object» in CC, but, in spite of this, there is much wider evaluation range possibility in a RMF context than it was with the «rainbow series» as whole, not to mention the TCSEC itself. RMF shows an original approach to the risk assessment. First of all, IS are classified by the apprehended damage level, then there are security and privacy controls options, which corresponded to the chosen IS level; after this, security measures are taken and only at the end the risk evaluation is realized.

This process differs from the classic one (ISO 27005 series); the estimation is taken twice: the first one - before the security measures selection, and the second one - right after they were chosen and taken. This difference does not mean that the RMF approach is better or worse than the “classic” one, it is just varied. In some way, RFM save some continuity with TCSEC in a field of an object classification
and an accident control measure selection from the terminal catalog. Moreover, if in TCSEC the object classification is determined most likely by the internal regulations of the USA Ministry of Defense, in RMF the same classification was regulated by the FIPS 199, which is the part of RFM and is used as a criterion of the apprehended damage level. The same situation is with an accident control measure catalog, in TCSEC it is only inner one, but RFM has two units – short FIPS 200 and advanced SP800-53. And it is necessary to take into consideration that the RFM authors were well informed that the trusted CS era began that gives an opportunity to optimize the risk assessment approach.

3.3. ISO/IEC 15408 Series
An extremely high expert level of a participant that developed and actualized CC and RFM raised the IT security documents standard to significant levels. As a result, all other IT security, normative documents are less in significance and it was the most notable in industry documents, which have been repeatedly developed by the industry agents but have not obtained any acceptable results. It must be noted that both CC and RFM now continue its evolution and have elaborated procedures to keep them in actual state, which is relevant to the IT evolution level and customer expectations. The Federal Information Security Modernization Act of 2014 was the addition to the FISMA of 2002, and the last edition of the CC of 13.11.2017 is the CC v3.1 Release 5. Each CC version became the base for the development of the ISO/IEC 15408 standard edition («Information technology. Security techniques. Evaluation criteria for IT security») by the International Organization for Standardization, ISO.

4. State-of-the-art of IT security evaluation
However, CC and RMF are the «top of creation» today in the sphere of IT security normative documents; there are some peculiarities of its using that need to be reconsidered for a more exact understanding of the current IT situation and choosing the further ways of development of the security evaluation tools. What can be said about RMF? It exists and is oriented to a IS and organizations. However, the authors did not know any cases of IS and organization evaluation by RMF. But at the same time, the SP 800-53 document has an application which determines correspondence between the functional safety specifications and security assurance requirements of ISO 15408, and also between the security and privacy controls of SP 800-53 and ISO/IEC 27001 («Information technology. Security techniques. Information security management systems. Requirements») [12]. An interesting picture shows up – it seems like there are no evidences of the security evaluation by the RMF, but, at the same time, SP 800-53 sets up a correspondence with clauses (ISO/IEC 15408 and 27001 series) which are often used for security evaluation.

4.1. ISO/IEC 27001 Series
In authors’ opinion, this situation might arise because the wide availability of the IT components that have been evaluated by ISO 15408, so the IS, created from these components, have all chances to satisfy the requirements of RMF. The requirements for organizations are satisfied by the evaluation of IT-security management systems (ISMS) specified by ISO/IEC 21001. Potential partners will likely be interested in a certificate of the official independent evaluation of the ISMS competence to the ISO 27001 requirements than in security evaluation assessment by the RMF.

It is possible to say that ISO 15408 also focuses on a target of evaluation that can be anything from the IT field, since ISO 15408 sets no limits in this question, but only requires the clear understanding on the matter, which the user deals with. But in practice, ISO 15048 is used to evaluate relatively simple and local objects like programs, hardware and so on, which shows a necessity of widening and adaptation of the ISO 15408 requirements for evaluation of a much more complicated and large structure as IS or IT.

4.2. ISO/IEC TR 19791
ISO even developed the ISO/IEC TR 19791 «Information technology. Security techniques. Security assessment of operational systems», which is the ISO 15408 addendum for evaluation of more
complicated and large objects as «operational systems», which are, in the context of ISO 19791, better in calling «information systems».

At the same time, one should remember that ISO 15408 is a CC «replica» in fact, and thus it is addendum to the CC. It should be added here that the authors had no evidences of using the ISO 19791 for the security evaluation, but only the fact of its creation shows the necessity of the more precise and flexible tool of the IS security evaluation than RMF. However, ISO 19791 has one principally irremovable defect – it is independent, but not all-sufficient document, whose live-cycle is need, is to be maintained. Moreover, if the ISO 15408 life-cycle maintenance is not so expensive for ISO because it is a CC “replica”, ISO 19791 can rely only on its own resources.

4.3. IEC 61508 and IEC 61511 Series

The authors propose using widely additional standards of the functional security during the IS security evaluation, for example, IEC 61508 and IEC 61511 series [13,14]. Some practice for integrated application of several standards was shown in research [15,16]. For the IT-security evaluation solutions, several target controls can be used in cooperation, at each stage of the research, development and production processes within the national trusted jurisdiction. It can satisfy increased demands of the civil and governmental institutions and insure digital sovereignty.

5. Conclusion

Nowadays, IT components with the security features that meet the civil society demands are easily available. All those components have been passed through the evaluation of its competence and are fit for building security capacity.

It can be mentioned that today there are no difficulties with security; there are problems with the confidence. These questions can be solved only with focus on the research, development and production processes within the national trusted jurisdiction (digital sovereignty). This allows satisfying the increased demands of the civil and governmental institutions.

References

[1] Proceedings of the seminar on the DoD computer security initiative program National bureau of standards Gaithersburg, Maryland, July 17-18, 1979
[2] Proceedings of the fifth seminar on the DoD computer security initiative program National bureau of standards Gaithersburg, Maryland, May 24-26, 1982
[3] Proceedings of the sixth seminar on the DoD computer security initiative program National bureau of standards Gaithersburg, Maryland, November 15-17, 1983
[4] 13th National Computer Security Conference, Omni Shoreham Hotel, Washington D.C., October 1-4, 1990
[5] 15th National Computer Security Conference, Baltimore Convention Center Baltimore, MD, October 13-16, 1992
[6] 16th National Computer Security Conference, Baltimore Convention Center, Baltimore, MD, September 20-23, 1993
[7] 17th National Computer Security Conference, Baltimore Convention Center, Baltimore, MD, October 11-14, 1994
[8] 19th National Information Systems Security Conference Proceedings, Baltimore, MD, October 22-25, 1996
[9] NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments
[10] NIST Special Publication 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
[11] NIST Special Publication 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations
[12] ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013
[13] IEC 61508-1:2010 Functional safety of electrical, electronic, programmable electronic safety-related systems — Part 1: General requirements

[14] IEC 61511-1:2003 Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements

[15] Livshitz I 2014 Approaches to the Application of the Integrated Management System Model for Carrying out Audits for Complex Industrial Objects – Airport Facilities. SPIIRAS Proceedings. 6 72–94

[16] 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.