Stages and procedures for forming a method to assess reliability of the information security systems in automated systems and main areas of its implementation in the normative-technical documentation

O I Bokova¹, O M Bulgakov², A S Etepnev¹ and E A Rogozin¹

¹ The Voronezh institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriotov prospect, Voronezh, 394065, Russia
² The Krasnodar university of the Ministry of Internal Affairs of the Russian Federation, 128, Yaroslavskaya street, Krasnodar, 350005, Russia

E-mail: electronag@gmail.com, o.i.bokova@gmail.com, eacg@mail.ru, evgenirogozin@yandex.ru

Abstract. The article completes the cycle the articles by the authors assessing reliability of information security systems from the unauthorized access to automated systems. In includes previously unpublished materials. The article discloses main directions to improve methods and procedures for assessing reliability of the information security systems from the unauthorized access to automated systems. There is modification of the traditional static method to assess the functional reliability of the information security systems from the unauthorized access to investigate their operation in the dynamic (real) functioning mode and to quantify reliability of the information security systems, including development of adequate indicators, models and algorithms. Main stages and procedures for forming the reliability assessment method were developed as a technological scheme with demonstration of the main stages to implement the proposed methods in the current normative-technical documentation.

1. Introduction

One of the key problems in the theory and practice of protecting the confidential information resource in the automated systems (AS) at objects of information critical practice (OICP) is the quality (efficiency) functioning assessment of the tools and systems for the security of information (SI) in them. It is related to the fact that at design and operation of the security information tools and systems from the unauthorized access (UAA) significant computation resources of automated systems are to be diverted in real time which is not acceptable to perform the functional task by the systems (processing, storing and transmitting the confidential information). To find a compromise solution for the stated...
task it is needed to comply with the requirements of the guiding documents provided by the Federal service for the technical and expert control (FSTEC) of Russia [1], and also international and domestic standards in protection of information from the unauthorized access in automated systems [2]. In particular, in part 3.6 of the guiding document provided by the FSTEC of Russia "The concept to protect computation tools and automated systems from the unauthorized access" there is the need to assess efficiency of the information security tools and systems, as reflected in GOST R ISO /IEC 15408-3-2013 "Information technology. Methods and tools to provide security. Security assessment criteria. Part 3. Security confidence components". Consequently, the task related to the quality (efficiency) functioning assessment of information security tools and systems (IS) at objects of information critical practice (OICP) is rather relevant and important. Since the efficiency is a sub-characteristic of the information security system reliability, then the task to assess the information security system quality (efficiency) reliability from the unauthorized access is also very relevant. The current method to assess the functioning reliability of the information security system has a static character and reflects its functional depending on the automated system security classes, that does not allow investigating the information security system from the unauthorized access in the dynamic (real) mode of the their functioning. It requires a significant refinement of the current method to assess the functioning reliability of the information security system from the unauthorized access for investigating their operation in the dynamic (real) mode and also the reliability quantifying assessment including development of adequate indicators, models and algorithms.

Thus, development of the method including specific methods to assess the functional reliability of the information security systems from the unauthorized access for providing confidentiality, integrity and information accessibility is a relevant problem to provide the information security of the automated systems in the secured operation at OICP, what this article is about.

Analysis of the normative documents concerning the PS quality proved that now in the Russian Federation to substantiate the requirements to PS (data base management systems (DBMS), operation systems, development tools, etc) are guided by [3, 4]. In such GOST there are formalized terms and definitions for PS quality, introduced group characteristics of PS quality, specific quality indicators, characterizing main program properties. PS quality indicators, determined by these standards, include the following:

1. PS reliability indicators;
2. Maintenance indicators;
3. Usability indicators;
4. Efficiency indicators;
5. Universality indicators;
6. Correctness indicators.

Quality indicators are recommended for the lifecycle stages of development, commissioning and operation. At that in GOST [4] there are the following PS types:

- OS (expansion modules and additional utilities);
- DBMS;
- Program tools (interpreters and translators);
- Network utilities;
- Programs to service computation planning;
- Programs to perform service functions;
- ECM service utilities;
- Applied software for researches;
- SAPR;
- Tools to manage technological processes and equipment;
- Economic program packages.

From the content analysis of [4] it may be concluded that the information security systems from the unauthorized access, used in automated systems as the objects justifying requirements to their quality
are not given in the standards [4]. Accordingly computation methods and reliability indicators in the information security systems from the unauthorized access, regulated by these documents are not suitable for the practical use to justify the requirements to the reliability of the information security systems from the unauthorized access.

PS quality management system now is formed by the international system of standards to develop the qualitative software. The quality management system is based on the main standard provisions of ISO series 9000. As the main standard providing the program quality matters is the standard ISO 9126:1991 – "Information technology. Assessment of the software product. Characteristics of the quality and guidance to use them". The standard includes a set of requirements to the software quality indicators. According to them, the quality indicators should meet the following principles:

- Clarity and measure of the indicator value;
- No overlap between the used indicators;
- Compliance with standardized concepts and established terminology;
- Possibility of detail and further specification;
- Division into characteristics providing the assessment of the software consumer and constructive quality.

In standard ISO 9126 there are 6 group characteristics of the software quality. For each group characteristics the following features are detailed:

1. For the functional suitability there are the detailed indicators of suitability for use, accuracy, security, ability to interact and coherence with the unified system for design documentation;
2. Reliability is recommended to be characterized by the completion level indicators (no errors), error resistance and restart ability;
3. Applicability is characterized by indicators of comprehension, learning and application use;
4. Efficiency is characterized by the temporary and resource efficiency;
5. Maintenance is characterized by indicators of analysis convenience, variability, stability and testability;
6. Portability is proposed to reflect adaptability, structure, substitution and implementation.

In standard ISO 9126 there are three parts. The first part includes the general concept to use group indicators and software quality indicators at different lifecycle stages. The second part determines the software quality characteristics to assess quality of the information security systems from the unauthorized access by consumers. The third part gives intra-system characteristics of the software quality used at development. In terms of the methods to access reliability of the information security systems from the unauthorized access ISO 9126 has some shortages. First, group characteristics and characteristics are determined in the standard without recommendations for their use. Second, the standard is reference. The main shortage is the lack of recommendations to choose the items and order (ranking) of characteristics for the information security systems. Reliability indicators lack the methods of assessment, measurement and abilities to compare with specification requirements as well as recommendations, for what stage of the program lifecycle there are to be used. Description of the reliability indicators is focused on the use both by qualified system analysts and software customers. These specialists can choose the required items of the reliability characteristics in the information security systems.

Standardization of reliability requirements in the Russian Federation is regulated by the System of State Standards "Reliability in technology" (SSNT), described by GOST 27.001—81. In standards SSNT series 27.xxx there are the following indicators:

1. Reliability rationing;
2. Methods to calculate reliability;
3. Methods to provide reliability;
4. Reliability testing and control;
5. Collecting and processing information of reliability.

The most important information security standards SSNT are given in Table 1.
Table 1. Main system standards "Reliability in Technology".

| GOST    | Name                                                                 |
|---------|----------------------------------------------------------------------|
| 27.002—83 | Terms and definitions                                               |
| 27.003—83 | Choosing and rationing of reliability standards. General provision   |
| 27.103—83 | Failure and limit state criteria. General provisions                 |
| 27.104—84 | Classification features of failures and limit states. General provisions |
| 27.201—81 | Assessment of reliability indicators at small number of observations using additional information. General provisions |
| 27.301—83 | Prediction of the product reliability at design. General provisions   |
| 27.410—83 | Methods and plans of the statistic control for the reliability indicators by the alternative basis |
| 27.502—83 | Reliability in technology. The system to collect and process information. Observation planning |

The standards listed in Table 1 determine the main terms in reliability and also the related issues, a set of basic theoretical dependencies, recommended calculation formulas, methods of calculating, assessing and testing of reliability objects. Standards are mostly for planning and providing reliability of the computer technology means.

The most important of the methodological standard in SSNT series is GOST 27.301-95 "Reliability in technology. Reliability calculation. General provisions". This standards determines the general order to calculate reliability. GOST includes requirements to formulation of the reliability calculation goals, general scheme of calculations, identification of reliability objects and calculation methods. Moreover, there are requirements for submitting calculation results.

It should be noted that there is a set of standards for individual reliability aspects excluded from SSNT which are relevant for providing the information safety. For instance, 24.701-83. "Reliability. Automated systems to manage technological processes. General provisions"[11].

Analysis of the popular domestic and foreign literature, research results, various authors shows that a significant number of sources is dedicated to the information security, design and development of automated systems, information security from information security threats of various nature and the software reliability.

Methods to protect information-computing and automated systems from implemented information security threats (including computer attacks), as special software, hardware or software-hardware tools are described by research results of the following authors: D. Y. Gamayunov, Y. V. Borodaky, S. N. Grinyaev, V. M. Zima, A. A. Moldavyan, N. A. Moldavyan, M. A. Ivanov , I. V. Kotenko, S. M. Klimov, М. P. Sychev, A. V. Astrakhov, Y. V. Grechishnikov , I. B. Sayenko [8,9,10].

Possible ways to implement the information security threats, methods of simulation, assessment and provision of information security in automated information systems from various information - technological attacks are described in research results of the following authors: S. N. Grinyaev, V. I. Yemelin, A. A. Boyko, S. A. Budnikov, V. P. Zhumaty, N. V. Parshin, M. A. Kotsynyak, I. A. Kuleshov, A. M. Kudryavtsev, O. S. Lauta, A. G. Korchenko, S. I. Makarenko, G. A. Ostapenko, P. I. Tutubalin, V. S. Moiseyev, K. V. Ivanov.

Methods, models and methodology to design and develop the information security systems in automated information systems under implementation of various information security threats and also methods to provide safety operation of the automated information systems from the information attacks are given in research results of the following authors: R. M. Alguliyev, Y. V. Borodaky, S. A. Budnikov, N. V. Parshin, A. N. Burenin, K. Y. Legkov, O. Yu. Gatsenko, V. Y. Dementyev, Y. I. Starodubtsev, M. A. Kotsynyak, V. V. Domarev, I. V. Kotenko, D. P. Zegzhda, O. V. Kazarin, S. M. Klimov, Y.A. Rogozin, V.A. Khvostov, O. V. Lukinova, S. N. Novikov, V. G. Kulakov, V. G. Kobyshev, V. V. Zima, A. G. Lomako, M. M. Kotsynyakov, A. S. Markov, A. A. Moldavyan, Y. A. Rogozin, A. Y. Shcherbakov.

Some scientific-theoretical provisions justifying development methods of information security
systems and methods of providing the information security are disclosed by research results of the following authors: G. A. Ostapenko, V. I. Belonozhkin, V. A. Gerasimenko, A. A. Grusho, Y. Y. Timonina, P. N. Devyanin, D. P. Zegzhda, A. M. Ivashko, S. A. Petrenko, D. D. Stupin, A. P. Rosenko, P. D. Zegzhda.

Constructive, production and operation factors significantly affecting the reliability indicators of the soft-and hardware complex in the automated information system, consequences of these factors and prevention methods preventing failures and extension of operation are included into research results of the following authors: B.E. Berdichevsky, V.V. Lipayev [5, 6, 7], B. Boem.

Theoretical approaches to develop reliability models of individual (recoverable and unrecoverable) elements, to calculate parameters of continuous work and recovery as well as to develop the models to control and diagnostics are disclosed in research results of the following authors: B.V. Gnedenko, I.A. Ushakov, A.M. Polovko, N.A. Severtsev, L.P. Glazunov, V.P. Grabovetsky, O.V, Shcherbakov, G.V. Druzhinin etc.

The monograph proposes a formalized model and develops the methods of synthesis for security functions of the information security systems, proposes an approach to justify the required security level from the unauthorized access. There are analyzed methods to improve efficiency of the debugged program text for information security systems for the quantitative reduction. The research proposes the concept of "control and information security mechanism". There is the standard scheme to process information, the indicative error graph is used. The proposed concepts are intended for the formal analysis of data flows as objects with the provided reliability and accessibility characteristics.

The monograph proposes possible solutions to prevent the information security implemented threats in critically relevant information resources. The research is focused on implementation of the open segment in the National Computer Attack Early Warning System.

In the monograph there is the proposed methodological approach to assess the confidential information security in terms of the information security threats. The research proposes a mathematical model to assess the impact of information security threats on the information security indicators. The evaluation model is based on integrated application of the mathematical apparatus of the Markov random processes with discrete states, game theory and simulation modeling [17].

The research solves the problems of computer systems security from malicious software. The work determines a conceptual device related to the security concept, develops the classification scheme and gives examples of realizing the information security threats using malicious software. The developed computation system model and the formal task of analyzing the software security determined the formal methods to provide the information security: in the program (logic-analytical method) and in relationships (control - testing method).

The most important research is the software system quality. The research solves the problem and offers methods to assess the software quality at all stages of its development. There are indicators providing detection of software errors at the early development stage. The concepts are introduced such as "Software general usefulness" and "Reliability impact on overall usefulness."

In [20] there is the metric theory of the program quality. The metric theory of quality is intended to assess the costs on the software development depending on the complexity, realized functions, number of developers and other factors. Mathematical expressions to assess the impact of various factors on the cost, time of development and reliability of the programs provides formation of the methodological complex to assess the software costs.

From Russian researches of the software quality it is needed to note [21]. In [21] there are the software indicators and analyzed factors determining their value. The methods are developed to calculate complexity, correctness and reliability of the software. Recommendations are given to improve the software quality at all their lifecycle stages.

The works [19, 20, 21] focus on the project quality analysis (quality, as the major part or the structure of the project, for example, software architecture, program structure and interface design structure). Therefore the choice of indicator, model and assessment algorithm is differed from indicators, models and algorithms to assess the user's quality (automated system quality perceived by
the users and measured in terms of the software operation results). The practical use of methods to provide the program system quality does not depend on the architecture and work of the automated system. Methods to analyze the software quality have an abstract general theoretic character. It is impossible to assess reliability of the information security systems from the unauthorized access by using the methods to assess reliability, as it is in [19, 20, 21]. It is needed to develop a new (perspective) method to assess reliability of the information security systems from the unauthorized access.

2. Materials and methods
Analysis of architecture and operation features of the information security systems from the unauthorized access proved that as the object to provide reliability this class of the software can be characterized by the following.

In the information security systems the error is related to failure of one or several security functions. Failed information security is an error in the program code of the information security systems. Reliability of the information security systems is determined by the probable work without failures in the set time period, calculated in terms of the occurred losses for each failure category, and the readiness to perform the security function in response to the actual threat of the information security aimed at violating the confidentiality, integrity and information availability.

Important findings from these properties are the following:
1. The software reliability is related to external system operation conditions.
2. The software reliability characterizes both the software internal properties and the external system expectations.

Practice demand in the automated system development for the secured version is the need to formulate requirements to reliability of the information security systems from the unauthorized access as quantitative values of the indicators characterizing such properties of the information security systems, as reliability, recovery, durability, persistence, which determine reliability of the information security systems in general. The numerical reliability indicators according to GOST [11], are set based on reliability calculation results during the technical-economic study performed for the development of the information security systems using the methods.

However, analysis of the normative documentation and popular literature both in provision of the information security and reliability proved that now there is neither the well-defined system of indicators nor the methods to assess reliability of the information security systems.

The lack of reliability indicators at the early stages of automated systems development for the information security systems and their evaluation methods results in the following problems:
1. The purpose and functional requirements and requirements to the customers reliability of the information security systems can't be realized in full volume;
2. Low reliability of the primary reliability assessments of the information security systems can't calculate the required budget, time and resources to develop the automated system at design of the technical task;
3. The automated system development process is poorly controlled which results in no set reliability for the finished product, violated calendar plans;
4. The lack of reliability system indicators for the information security systems provides no formation of correspondent items in the technical task and the section of reliability on the sketch and technical projects according to GOST 27.003-2016.

Due to that there is the practical relevant task to develop the methods for assessing reliability indicators for the information security systems from the unauthorized access, characterizing them as the automated system subsystem operating under multiple implemented information security threats and their determined work conditions.

The need to solve the practical task made it necessary to find a solution for justifying the indicators characterizing reliability of the information security systems from the unauthorized access and development of their assessment methods.
Thus development of indicators characterizing reliability of the information security systems, and also methods and algorithms of their assessment, at the design stage of the information security systems in the automated secured system – “Formation of the technical task” is a relevant task.

For that it is needed to solve the following problems:
1. Analysis of the current regulated methodological approach to assess reliability in the information security systems in automated systems.
2. Development of indicators characterizing reliability of the information security systems, in terms of the current norms and requirements in the software quality, reliability of the technical systems, features of their architecture and performance of functions to protect information.
3. Development of methods and algorithms to assess reliability indicators at solving the task to provide its confidentiality, integrity and information availability.
4. Approbation of developed methods to assess reliability of the information security systems, functioning under the typical operation conditions in structure of the secured automated systems.

Main stages and procedures to form the methods of assessing reliability of the information security systems from the unauthorized access in automated systems are given in Figure 1.

---

**Figure 1.** Main stages and procedures to form a method to assess reliability of the information security systems from the unauthorized access in automated systems.
3. Results and their discussion

The method based on the methodology to assess reliability indicators of the information security systems from the unauthorized access in automated systems is reasonable to use as supplementary procedures at design of the information security subsystem when developing the automated secured systems regulated by the current norms in the secured information. In RD FSTEC [12, 13] and "General criteria ..." there is a sequence of steps at design of the information security systems. Features to use the developed methods to assess reliability indicators of the information security systems at using them in context of the normatively stated development procedures of the information security systems can be given as in Figures 2 and 3.

Refining of the design methods which is factually a cascade model to design a complex program system presupposes modernization in terms of reliability indicators assessment of the information security systems. Jointly with the standard set in "General criteria" in paragraph 4.2 first part and paragraph 3 "Security concepts of CET and AS from the unauthorized access to information" [12] branches "Technical task to develop AS - Security class (Task on security) — Functional requirements (requirements to security trust)" and "Security to AS technical characteristics - Structural scheme of the information security systems, typical sequence of the user's interaction with the system" is supplemented by the block "Assessment of reliability parameters for the information security systems", including "Assessed probability of the trouble-free work", "Assessed readiness factor", "Assessed average work time for failure".

Stages 1 and 2 in Figure 3 factually correspond to the specific GOST [14 - 16] and RD FSTEC first branch of methods to form requirements to the information security systems. Stage 3 is supplementary in relation to specific GOST [14 - 16] RD FSTEC branches and they provide application used and developed in the second chapter of the mathematical maintenance for assessment of the information security systems and the use of calculated characteristics in sections "Requirements to reliability in the information security systems" in the Technical task and "Programs to secure reliability" in explanatory notes to sketch and technical projects.

![Figure 2. Improved methodology to develop AS security system in secured mode using designed methods to assess the information security system from unauthorized assess.](image-url)
Figure 3. Improved model to develop a maintenance automated subsystem in a secured mode using the developed methods to assess reliability of the information security systems from the unauthorized access.
4. Conclusion

The article provides analysis of the current principles, methods and operation features of the information security systems from the unauthorized access in automated systems as reliable assessment objects both at design and operation of the system, discloses their main shortages and methods of their improvement. For the first time the technological scheme is developed including main stages and procedures to form a new (perspective) method to assess reliability of the information security systems from the unauthorized access in automated systems.

The use of proposed methods allows developing sections of the design documentation ("Explanatory note to the technical design") at projection of information security systems from the unauthorized access, including reliability calculations. The resultant assessed reliability indicators for average characteristics of information security systems can be the basis to justify requirements to the operation system of information security systems from the unauthorized access in automated systems by subdivisions to provide the information security, and also used as requirements to reliability, contained in the normative documentation jointly with technical requirements of information security.

References

[1] FSTEC of the Russian Federation Guidance document *Basic model of personal data threats at their processing in information systems of personal data* (app on 15 February 2008) p 69  (in Russian)
[2] FSTEC of the Russian Federation Guidance document *Methodology to detect information security threats in information systems* (app on 15 August 2015) p 43  (in Russian)
[3] GOST 28195-89 1990 *Assessed software quality. General provisions* (Moscow: Standardinform) p 32  (in Russian)
[4] GOST 28806-89 1992 *Software quality . Terms and definitions* (Moscow: Standardinform) p 8  (in Russian)
[5] Abbasov A E, Abbasov T E 2015 *Assessed software quality for modern systems of information processing. Information -technological bulletin* (Information technology Bulletin, – Moscow: MRTU) p 15  (in Russian)
[6] Senthil Pandian P 2019 *Adopting security checks in business transactions using formal-oriented analysis processes for entrepreneurial students.* International Journal of Electrical Engineering Education pp 101-112
[7] Shchennikov A N 2018 *Quality of information systems.* (Moscow: ITNOU) pp 53-62 (in Russian)
[8] Kotenko I V, Sayenko I B 2012 *Development of intellectual services system to secure information under cyber-confrontation conditions.* (Saint-Petersburg: Works of SPIIRAS) pp 84-100  (in Russian)
[9] Sayenko I B, Ageyev S A 2015 *Method of intellectual multi-agent management of information security risks in secured multi-service networks of special designation* (Moscow: Telecommunications and transport) pp 5-10 (in Russian)
[10] Sayenko I B, Kiy A V, Bushuyev S N 2016 *Methods to control an access to information resources based on the application activity analysis.* In volume: Science today: facts, tendencies, forecasts (Vologda: Science today: facts, trends, forecasts) p 69 (in Russian)
[11] GOST 24.701-86 2009 *Reliability. Automated management systems of technological processes. General provisions* (Moscow: Standardinform) p 12 (in Russian)
[12] Rui Zhu,Yali Zeng, Li Xu, Xun Yi 2019 *Lightweight Privacy Preservation for Securing Large-Scale Database-Driven Cognitive Radio Networks with Location Verification.* Security and Communication Networks p 12
[13] Mehran Alidoost Nia, Mehdi Kargahi, Behnam Baharak, Benjamin Fabian 2019 *Detecting New Generations of Threats Using Attribute-Based Attack Graphs.* IET Information Security p 293 303
[14] Yakovina V S, Fedasyuk D V, Mamrokha N M 2010 *Analysis of the use of aspect-oriented programming as a means of improving software reliability.* Software engineering p 24
[15] GOST R ISO/IEC 15408-2013 2014 *Methods and means of security assessment Criteria of information technology security* (Moscow: Standartinform) p 161 (in Russian)
[16] National vulnerability database
[17] Conto J 2015 *MPjobs — a tool to run PSSe scripts in parallel* p 5
[18] Bokova O I, Drovnikova I G, Yetepnev A S, Rogozin Y A, Khvostov V A 2019 *Methods to assess reliability of information security systems from unauthorized access in automated systems.* (Saint-Petersburg: Works of SPIIRAS) pp 1301-1332 (in Russian)
[19] Lipayev B B 1983 *Software quality* p 250 (in Russian)
[20] Boem B 1981 *Software quality characteristics* p 208
[21] Belyaev Y K, Bogatyrev V A, Bolotin V V 1985 *Reliability of technical systems: Reference book* (Moscow: Radio and communications) p 608 (in Russian)