Method and model for quantitative assessment of the performance indicator of information security systems against unauthorized access in automated systems based on a computational experiment

O M Bulgakov¹, A M Kadnova²,³, V A Meshcheryakov³ and D N Kuznetsov⁴

¹Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, 128, Yaroslavskaya Street, Krasnodar, 350005, Russia
²Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriots Avenue, Voronezh, 394065, Russia
³Central branch of the Russian State University of Justice, 72, Koltsovskaya Street, Voronezh, 394006, Russia
⁴Air Force Academy named after Professor N.E. Zhukovsky and Yu. A. Gagarin, 53 a, Starykh Bolshevikov street, Voronezh, 394064, Russia
⁵Author to whom any correspondence should be addressed

E-mail: ombfrier@yandex.ru, aizhana_kadnova@mail.ru, digitprof@yandex.ru, vrnh@bk.ru

Abstract. The article is devoted to the solution of the practical problem of a quantitative assessment of the quality characteristic «usability» of information security systems against unauthorized access in automated systems in the secure version. The main operator who interacts with the information security system against unauthorized access during its operation is a security administrator. This interaction is carried out through the interface of the security program. Therefore, for this category of users, the most relevant assessment is the characteristic «usability» of the quality of functioning of the information security system against unauthorized access. The method of evaluating this characteristic involves assessment of the operation code, probabilistic and time indicators, based on the experiment. The obtained values of these indicators can be further used in the comparative analysis of the «usability» characteristic of information security systems against unauthorized access of various classes, during the development of work plans for information security services, and the justification of requirements for the organization and structure of information security services.

1. Introduction

Restricted access information that circulates in any automated system (AS) in a secure version is subject to a variety of risks and threats that are of a different nature. The function of protecting such information in an AS in a secure version is performed by the information security system (ISS) from unauthorized access (UA), which is an independent software or software-hardware that is installed as a part of the secure AS at the stage of technical implementation [1, 2]. In accordance with the standards of the Russian Federation – GOST P 50922-2006 [3] and GOST P ISO/IEC 25010:2015 [4], the interstate standard GOST 28806-90 [4] and the international standard ISO/IEC 25010:2011 [6] ISS
from UA as a software tool has a number of characteristics. However, these standards do not contain methods that can be used to quantify these characteristics. Analysis of various regulatory documents [3-8] and open literature sources [9-11] devoted to the quality of software tools has shown that today there are no quantitative indicators of the quality characteristics of software tools and methods for their evaluation. Thus, the purpose of the article is to develop a system of indicators for characterizing «usability» of ISS against UA in AS in the security version and methods for their assessment.

2. Materials and methods
The experience of operating a variety of ISS against UA to AS in a secure version, analysis of software documentation [12-14] and guidance documents in the field of information security [7-11] allow us to conclude that the main operator interacting with ISS against UA via the interface, is the administrator of security [1,4-8], who has a direct impact on the effectiveness of the security of the information circulating in the AS in a secure version. Therefore, for this category of users, the most relevant assessment is the quality characteristics of the functioning of ISS against UA – «usability» [5].

Evaluation of the functional quality characteristic «usability» of ISS against UA can be carried out theoretically (for example, analytical and expert methods, the survey method) and experimentally [1-5]. The theoretical assessment has some disadvantages and limitations, so it is advisable to conduct an experimental assessment.

The experimental evaluation of usability features is carried out in three stages and consists of an assessment of three indicators, namely, the operation code, time, and probability, which characterize any operation performed by the ISS security administrator against UA in an AS in a secure version.

Before the experiment, we selected the ISS against UA, which was the platform of the experiment, in our case, it was the «Guardian NT 3.0». Further, in accordance with the software documentation [13] and the survey administrators of ISS against UA, we determined the list of typical operations that prospective administrators of ISS against UA would perform. Then groups of users were formed, which, as administrators of the ISS against UA, would perform operations from the compiled list.

The experiment involved students of the 5th year in the number of 81 people with the speciality 10.05.01 «Computer Security». All participants were divided into groups depending on the level of proficiency in «Guardian NT 3.0».

At the first stage, the «operation code» indicator and the «usability» characteristic were evaluated by decomposing each operation performed by security administrators into elementary actions. At the second stage, a time indicator of the «usability» characteristic was evaluated by determining the average time and execution of all operations by each group of security administrators. They used the application IOGraph V1.0.1 [16] as a tool, which implements mouse-tracking technology (cursor movement tracking technology).

At the third stage, the probabilistic indicator of the «usability» characteristic was evaluated by constructing functions for allocating the execution time of typical operations by the security administrators. The results of the experimental evaluation and calculations were the values of the timeliness of performing standard operations by the security administrators of «Guardian NT 3.0».

3. Results and discussion
The peculiarity of this experiment was to create conditions closest to real ones for the interaction of operators with the selected ISS against UA.

Participants of the experiments performed the following typical operations as ISS administrators of «Guardian NT 3.0»: «Editing properties for media groups in «Media Accounting»; «Adding and removing registered media in «Media Accounting»; Editing media properties in «Media Accounting»; «Viewing the password and list of user IDs in «User Manager»; «Changing the user's password in the «User Manager»; «Viewing and editing user properties in «User Manager»; «Generating personal identifiers in «User manager»; «Reading and clearing identifiers in «User Manager»; «Changing the owner of file resources in «File Manager»; «Editing the system audit parameters in «File Manager»;
«Editing properties for device groups in «Device Control»; «Adding an event group in «Event Log»; «Testing the security system in «Testing the Security System»; «Unlocking the computer».

Each of the above operations can be decomposed into a sequence of elementary actions, which, in turn, is an indicator of the quality characteristic of the functioning of the ISS «Guardian NT 3.0» «usability» – «operation code». As an example, let us consider the composition of a typical operation «Editing system audit parameters in «File Manager».

The operation «Editing system audit parameters in «File Manager» has the following structure. The security administrator selects the menu item «Programs» | «Guardian NT» | «File Manager». In the window that opens, the administrator selects the «Properties» item in the context menu of the selected object. In the properties window that appears, the administrator selects the «Security» tab and clicks the «Advanced» button, then selects the «Audit» tab. If administration mode is enabled, the administrator clicks the «Edit» button, otherwise - the «Continue» button and a window will appear on the screen that displays a list of system audits of the selected object. In the window that opens, the administrator selects an object from the list and clicks the «Edit» button. Next, the administrator changes the audit elements that he/she considers necessary.

The results of evaluating the time indicator of the «usability» characteristic are presented in Table 1.

Table 1. Results of evaluating the time indicator of the quality of functioning characteristic «usability» of ISS against UA «Guardian NT 3.0».

| Name of a typical operation performed by the administrator of «Guardian NT 3.0» | Time of execution of a typical operation by the ISS against UA «Guardian NT 3.0» administrator, s |
|---|---|
| | Group «Entry-level users» | Group «Middle-level users» | Group «Advanced users» |
| Editing properties for media groups in «Media Accounting» | 120 | 75 | 70 |
| Adding and removing registered media in «Media Accounting» | 95 | 60 | 55 |
| Editing media properties in «Media Accounting» | 180 | 105 | 95 |
| Viewing the password and list of user IDs in «User Manager» | 55 | 35 | 40 |
| Changing the user's password in «User Manager» | 80 | 65 | 60 |
| Viewing and editing user properties in “User Manager”» | 65 | 60 | 50 |
| Creating personal identifiers in «User Manager» | 70 | 55 | 50 |
| Reading and clearing identifiers in «User Manager» | 70 | 45 | 40 |
| Changing the owner of file resources in «File Manager» | 45 | 35 | 30 |
| Editing system audit parameters in «File Manager» | 70 | 40 | 35 |
| Editing properties for device groups | 120 | 110 | 110 |
Table 1. Results of evaluating the time indicator of the quality of functioning characteristic «usability» of ISS against UA «Guardian NT 3.0».

| Name of a typical operation performed by the administrator of «Guardian NT 3.0» | Time of execution of a typical operation by the ISS against UA «Guardian NT 3.0» administrator, s |
|---|---|
| Adding a group of events in «Event Log» | Group «Entry-level users» | 340 |
| | Group «Middle-level users» | 290 |
| | Group «Advanced users» | 280 |
| Testing the security system in «Testing the Security System» | | 75 |
| | | 50 |
| Unlocking the computer | | 45 |
| | | 30 |
| | | 30 |

Based on the obtained values of the time indicator for performing typical operations by the user groups presented in Table 1, we obtained an estimate of the probabilistic indicator of the quality characteristic «usability» of the functioning of ISS against UA «Guardian NT 3.0».

To calculate the probability that an administrator performs typical operations in a given time, we assumed that the probability density \( f(t) \) is a Gaussian function with an average value \( t_0 \) and variance \( \Delta t^2 \):

\[
f(t) = \frac{1}{\Delta t \sqrt{2\pi}} \exp\left(-\frac{(t-t_0)^2}{2\Delta t^2}\right)
\]

The probability that the administrator performs typical operations in a given time \( t \), \( t_0 > 3\Delta t \) is equal to the distribution function \( F(t) \), which can be expressed in terms of the error function \( \text{erf}(x) \) as follows:

\[
F(t) = \int_{-\infty}^{t} f(t) \, dt = \frac{1}{2} \left[ 1 + \text{erf}\left(\frac{t-t_0}{\sqrt{2\Delta t^2}}\right)\right]
\]

\[
\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_{0}^{x} e^{-z^2} \, dz
\]

To improve the accuracy of calculating probabilistic characteristics, we can take into account the restriction on the possible values of the operation execution time \( t \in (0, \infty) \). In this case, instead of the normal distribution, it is necessary to use a truncated normal distribution [1-7], which determines the probability of a normally distributed random variable \( t \) falling into the range from \( t_1 \) to \( t_2 \). The distribution function of a truncated normal distribution has the form:

\[
F(t) = \text{erf}\left(\frac{t-t_0}{\sqrt{2\Delta t^2}}\right) - \text{erf}\left(\frac{t_1-t_0}{\sqrt{2\Delta t^2}}\right)
\]

\[
f(t) = c f(t) = \frac{c}{\Delta t \sqrt{2\pi}} \exp\left(-\frac{(t-t_0)^2}{2\Delta t^2}\right)
\]

\[
c = \int_{t_1}^{t_2} f(t') \, dt' = \frac{1}{2} \left[ \text{erf}\left(\frac{t_2-t_0}{\sqrt{2\Delta t^2}}\right) - \text{erf}\left(\frac{t_1-t_0}{\sqrt{2\Delta t^2}}\right)\right]
\]
The probability that an administrator will perform typical operations in a given time $t$ when using a truncated normal distribution is equal to:

$$
\overline{F(t)} = \int_{-\infty}^{t} f(t')dt' = \frac{\pi}{2} \left[ 1 + \text{erf} \left( \frac{t-t_0}{\sqrt{2}\Delta t^2} \right) \right] = \frac{1}{4} \left[ 1 + \text{erf} \left( \frac{t-t_0}{\sqrt{2}\Delta t^2} \right) \right] \left[ \text{erf} \left( \frac{t_2-t_0}{\sqrt{2}\Delta t^2} \right) - \text{erf} \left( \frac{t_1-t_0}{\sqrt{2}\Delta t^2} \right) \right]
$$

(4)

Taking into account the restriction $t_1 = 0$, $t_2 = \infty$, the probability is equal to:

$$
\overline{F(t)} = \frac{1}{4} \left[ 1 + \text{erf} \left( \frac{t-t_0}{\sqrt{2}\Delta t^2} \right) \right] \left[ 1 + \text{erf} \left( \frac{t_0}{\sqrt{2}\Delta t^2} \right) \right]
$$

(5)

When the «three sigmas» condition $t_0 > 3\Delta t$ is met, the truncated normal distribution (3) practically coincides with the normal distribution (1). For the typical operations under consideration, it is more than 30 seconds, so the «three sigmas» condition takes the form $\Delta t < 10$ sec.

For the typical operations under consideration, this condition is met, so formula (2) is used for calculations.

The algorithm for calculating the probability of the operator performing the i-th operation in time $t$ is as follows:

1. Enter the average operation execution time $t_i$ and standard deviation $\Delta t_i$.
2. If the «three sigmas» condition $t_0 > 3\Delta t$ is met, go to point 3, otherwise to point 4.
3. Calculate the probability of performing an operation in a time of no more than $t$ $P(t) = \overline{F(t)}$ according to formula (2).
4. Calculate the probability of performing an operation in a time of no more than $t$ $P(t) = \overline{F(t)}$ according to formula (5).
5. Derive the probability $P(t)$. 
Figure 1. Algorithm for calculating the probability of an operator performing the \( i \)-th operation in time \( t \).

The results of calculations of the probability of performing a typical operation by the «Guardian NT3.0» administrator in time not exceeding the set time is shown in Table 2.

Table 2. Results of the evaluation of the probabilistic indicator of the quality of functioning characteristic «usability» of ISS against UA «Guardian NT 3.0».

| Name of a typical operation performed by the «Guardian NT 3.0» administrator | Value of the required time for performing a typical operation by the «Guardian NT 3.0» administrator, s. | Probability of performing a typical operation by the «Guardian NT 3.0» administrator |
|---|---|---|
| | Group «entry-level users» | Group «mid-level users» | Group «advanced users» |
| Editing properties for media groups in «Media Accounting» | 30 | 0.0061 | 0.3083 | 0.1586 |
| | 40 | 0.0667 | 0.6913 | 0.4999 |
| | 50 | 0.3084 | 0.9330 | 0.8412 |
| | 60 | 0.6914 | 0.9936 | 0.9771 |
| | 70 | 0.9331 | - | 0.9986 |
| | 80 | 0.9937 | - | - |
| Adding and deleting registered media in | 40 | - | 0.0227 | 0.0667 |
| | 50 | - | 0.1586 | 0.3084 |
| Name of a typical operation performed by the «Guardian NT 3.0» administrator «Media Accounting» | Value of the required time for performing a typical operation by the «Guardian NT 3.0» administrator, s. | Probability of performing a typical operation by the «Guardian NT 3.0» administrator | Group «entry-level users» | Group «mid-level users» | Group «advanced users» |
|---|---|---|---|---|---|
| «Media Accounting» | 60 | 0.0001 | 0.4999 | 0.6914 |
| | 70 | 0.0061 | 0.8412 | 0.9331 |
| | 80 | 0.0667 | 0.9771 | 0.9937 |
| | 90 | 0.3081 | 0.9986 | 0.9998 |
| | 100 | 0.6914 | 0.9999 | - |
| | 110 | 0.9332 | - | - |
| | 120 | 0.9937 | - | - |
| «Editing media properties in «Media Accounting»» | 70 | - | 0.0003 | 0.0061 |
| | 90 | - | 0.0807 | 0.3084 |
| | 110 | - | 0.7256 | 0.9331 |
| | 130 | - | 0.9952 | 0.9998 |
| | 150 | 0.0013 | 0.9999 | - |
| | 170 | 0.1586 | - | - |
| «Viewing a password and a list of user IDs in «User Manager»» | 40 | - | 0.0061 | 0.0227 |
| | 60 | 0.0227 | 0.3084 | 0.4999 |
| | 80 | 0.4999 | 0.9331 | 0.9771 |
| | 100 | 0.9998 | 0.9998 | 0.9995 |
| «Changing the user's password in «User Manager»» | 30 | 0.0013 | 0.3083 | 0.3083 |
| | 40 | 0.0227 | 0.6913 | 0.6913 |
| | 50 | 0.1586 | 0.9330 | 0.9330 |
| | 60 | 0.4999 | 0.9936 | 0.9936 |
| | 70 | 0.8412 | - | - |
| | 80 | 0.9771 | - | - |
| «Viewing and editing user properties in «User Manager»» | 40 | 0.0061 | 0.0227 | 0.1586 |
| | 60 | 0.3084 | 0.4999 | 0.8412 |
| | 80 | 0.9331 | 0.9771 | 0.9986 |
| | 100 | 0.9998 | 0.9995 | - |
| «Creating personal identifiers in «User Manager»» | 40 | 0.0013 | 0.0667 | 0.1586 |
| | 60 | 0.1586 | 0.6914 | 0.8412 |
| | 80 | 0.8412 | 0.9937 | 0.9986 |
| | 100 | 0.9986 | 0.9999 | - |
| «Reading and clearing» | 30 | 0.0013 | 0.0067 | 0.1586 |
Table 2. Results of the evaluation of the probabilistic indicator of the quality of functioning characteristic «usability» of ISS against UA «Guardian NT 3.0».

| Name of a typical operation performed by the «Guardian NT 3.0» administrator | Value of the required time for performing a typical operation by the «Guardian NT 3.0» administrator, s. | Probability of performing a typical operation by the «Guardian NT 3.0» administrator |
|---|---|---|
| IDs in «User Manager» | | |
| 40 | 0.0013 | 0.3084 | 0.4999 |
| 60 | 0.1586 | 0.9331 | 0.9771 |
| 80 | 0.8412 | 0.9998 | 0.9999 |
| 100 | 0.9986 | - | - |
| Changing the owner of file resources in «File Manager» | | |
| 30 | 0.0667 | 0.3083 | 0.4999 |
| 40 | 0.3084 | 0.6913 | 0.8399 |
| 50 | 0.6914 | 0.9330 | 0.9758 |
| 60 | 0.9331 | 0.9936 | 0.9973 |
| Editing system audit parameters in «File Manager» | | |
| 30 | 0.0013 | 0.1586 | 0.3083 |
| 40 | 0.0013 | 0.4999 | 0.6913 |
| 60 | 0.1586 | 0.9771 | 0.9936 |
| 80 | 0.8412 | 0.9999 | - |
| 100 | 0.9986 | - | - |
| Editing properties for device groups in «Device Control» | | |
| 80 | 0.0013 | 0.0013 | 0.0013 |
| 100 | 0.0227 | 0.1586 | 0.1586 |
| 120 | 0.4999 | 0.8412 | 0.8412 |
| 140 | 0.9771 | 0.9986 | 0.9986 |
| 160 | 0.9999 | - | - |
| Adding a group of events in «Event Log» | | |
| 270 | - | 0.0227 | 0.1586 |
| 290 | - | 0.4999 | 0.8412 |
| 310 | 0.0013 | 0.9771 | 0.9986 |
| 330 | 0.1586 | 0.9999 | - |
| 350 | 0.8412 | - | - |
| 370 | 0.9986 | - | - |
| Testing the security system in «Testing the Security System» | | |
| 40 | 0.0001 | 0.1586 | 0.1586 |
| 50 | 0.0061 | 0.4999 | 0.4999 |
| 60 | 0.0667 | 0.8412 | 0.8412 |
| 70 | 0.3084 | 0.9771 | 0.9771 |
| 80 | 0.6914 | - | - |
| 90 | 0.9331 | - | - |
| Unlocking the computer | | |
| 30 | 0.0667 | 0.4999 | 0.4999 |
| 40 | 0.3084 | 0.8399 | 0.8399 |
Table 2. Results of the evaluation of the probabilistic indicator of the quality of functioning characteristic «usability» of ISS against UA «Guardian NT 3.0».

| Name of a typical operation performed by the «Guardian NT 3.0» administrator | Value of the required time for performing a typical operation by the «Guardian NT 3.0» administrator, s. | Probability of performing a typical operation by the «Guardian NT 3.0» administrator, |
| --- | --- | --- |
| 50 | 0.6914 | 0.9758 |
| 60 | 0.9331 | 0.9973 |

4. Conclusion

Thus, the article develops a method for quantifying probabilistic and temporal indicators of the quality characteristic «usability» of the functioning of ISS against UA in a secure version based on information obtained during interaction with the security administrator. The proposed method of a quantitative assessment of indicators of usability of ISS against UA, in contrast to existing methods (analytical, expert), provides an increase in objectivity, information content and accuracy, also allows us to effectively compare different ISS against UA and calculate quantitative indicators dynamically when the operating conditions of ISS against UA in the automated system in a secure version change.

References

[1] State Standard R 51583-2014 Protection of information. Order of creation of automated systems in the secure execution. General provisions Retrieved from: http://docs.cntd.ru/document

[2] Kadnova A M, Makarov O Yu, Mishin S A, Rogozin E A 2019 Algorithm of the creation of the protected automated systems. Information technology security 26 pp 93–100

[3] State Standard R 50922-2006 Protection of information. Key terms and definitions Retrieved from: http://docs.cntd.ru/document/1200058320

[4] State Standard R ISO/IEC 25010-2015 Information technology. Systems and software engineering. Systems and software Quality Requirements and Evaluation. System and software quality models Retrieved from: http://docs.cntd.ru/document/1200121069

[5] State Standard 28806-90 Quality of software. Terms and definitions Retrieved from: http://docs.cntd.ru/document

[6] ISO/IEC 25010:2011 Systems and software engineering. Systems and software Quality Requirements and Evaluation Retrieved from: https://www.iso.org/standard/35733.html

[7] Federal Service for Technical and Export Control of Russian Federation Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information security requirements Retrieved from: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty

[8] Resolution of the government of the Russian Federation of 01.11.2012 No. 1119 «About the approval of requirements to protection of personal data at their processing in information systems of personal data» Retrieved from: http://www.consultant.ru/document

[9] B W Boehm, M Lipow, G J MacLeod, J R Brown and H Kaspar 1978 Characteristics of Software Quality (Amsterdam: North-Holland) p 208

[10] B B W Boehm 1981 Software engineering economics (USA: Prentice Hall) p 512

[11] Lipaev V V 1983 Quality software (Moscow: Finance and Statistics) p 250

[12] The system of information protection from unauthorized access «Dallas Lock 8.0». Operation manual Retrieved from: https://www.dallaslock.ru/products/szi-dallas-lock/szi-ot-nsd-dallas-lock-8-0-s
[13] The system of information security «Guardian of NT 3.0». Administrator's Guide. Retrieved from: https://www.guardnt.ru/doc/gnt_30_admin_guide.pdf

[14] Information security tool «Secret Net 7». Administrator's Guide. Retrieved from: https://www.securitycode.ru/upload/documentation/secret_net/Secret_Net_Admin_Guide_Construction_Principles.pdf

[15] Kadnova A M, Bokova O I, Barabanov A V, Meshcheryakova T V, Kalinin M Yu 2020 Innovative technologies for evaluating user interfaces of information security systems in the digital educational environment. IOP Conf. Series: Journal of Physics: Conf. Series 1691 pp 012104

[16] Kadnova A M 2019 Methodical approach to evaluation of probabilistic indicator of timeliness of typical operations by the administrator of the information security system of the automated system. Bulletin of the Dagestan State Technical University 3 pp 87-96

[17] Druzhinin G V 1977 Reliability of automated systems (Moscow: Energy) p 536