Journal of Physics: Conference Series

PAPER • OPEN ACCESS

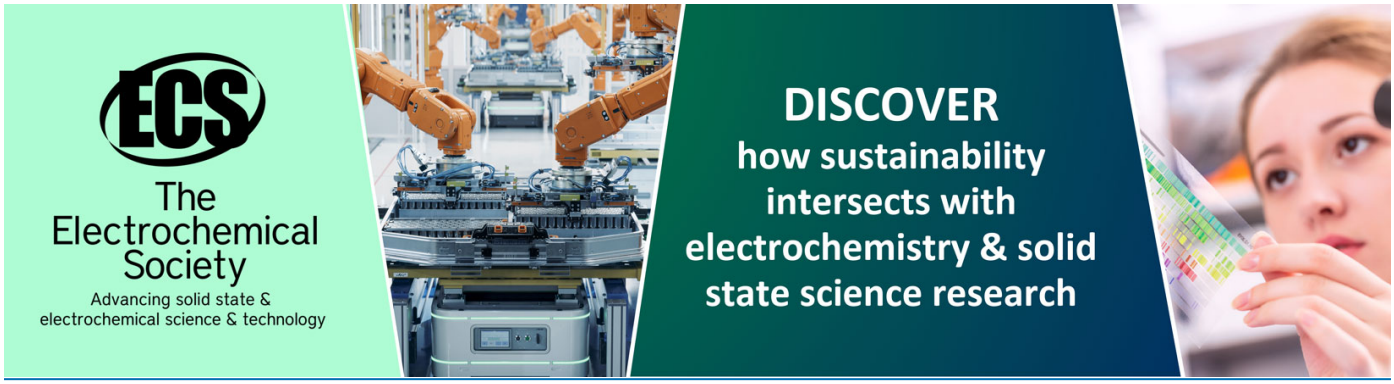
Method of assessing the «usability» characteristic of the functioning quality of information protection systems

To cite this article: A M Kadnova *et al* 2020 *J. Phys.: Conf. Ser.* **1479** 012059

View the article online for updates and enhancements.

You may also like

- Usability assessment of virtual reality as a training tool for oral presentation
M M Daniels
- An Asynchronous Serial Communication Learning Media: Usability Evaluation
D Hariyanto, A C Nugraha, A Asmara et al.
- Assessing the usability of the NDCDB checklist with Systematic Usability Scale (SUS)
N Z A Halim, S A Sulaiman, K Talib et al.



This content was downloaded from IP address 3.144.154.208 on 05/05/2024 at 15:05

IOP Conf. Series: Journal of Physics: Conf. Series **1479** (2020) 012059 doi:10.1088/1742-6596/1479/1/012059

Method of assessing the «usability» characteristic of the functioning quality of information protection systems

A M Kadnova[1], V A Khvostov[2], I G Drovnikova[1]and O A Gulyaev[3]

[1]Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriots Avenue, Voronezh, 394065, Russia
[2] Voronezh State University of Engineering Technologies, 19, Revolution Avenue, Voronezh, 394036, Russia
[3]Voronezh State Technical University, 14, Moskovsky Avenue, Voronezh, 394026, Russia

E-mail: aizhana_kadnova@mail.ru, hvahva1@mail.ru, idrovnikova@mail.ru ptr@utw.su

Abstract. The article is devoted to solving the practical problem of assessing the quality characteristic of the information protection system –«usability». In the course of his/her work, the security administrator of the automated system, built in a secure execution, makes a number of technological operations restricted by regulatory and administrative documents. At this, the prompt of such operations is determined by the characteristics of the interfaces of the software modules of the information protection system (IPS). In this regard, the assessment of the quality characteristic of the IPS «usability» becomes relevant for the category of users - security administrators. A meaningful analysis of the activities of this category users of information systems showed that it is appropriate to assess the "usability" based on operational, temporal and probabilistic indicators. The methodological basis for assessing these indicators is an experimental measurement of the average execution time of each operation by a representative group of users, followed by an analytical prediction of the probability of their execution.

1. Introduction

For the processing of information, the need for protection of which is determined by the legislation of the Russian Federation or by the decision of its owner, automated systems (AS) are created in a secure execution. They implement the requirements for the protection of information in accordance with the current regulatory legal acts. An integral part of such AS is the IPS implementing the specified requirements [1]. In accordance with GOST 28806-90 [2], IPS, as a software tool, has certain quality characteristics. However, this standard does not contain indicators that allow for a quantitative assessment of the quality characteristics specified in it. The analysis of normative documents [3-6] and open literature sources devoted to the quality of software [7-15] showed that today, there are no quantitative indicators of the quality characteristics of software and methods of their assessment. Analysis of program documentation from various IPS [16-19], the guidance documents in the field of information security, as well as operating experience of AS in a secure execution, showed that the primary user interacting with the IPS interface is the security administrator who is decisive and control

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

element of the IPS, significantly affecting the protection effectiveness of circulating information. Therefore, for this category of users, the most relevant is the assessment of the quality characteristic of IPS – «usability» [2]. Thus, the purpose of the article is to develop a system of indicators of quality characteristic of IPS «usability» and methods of their evaluation when designing the AS in a secure execution.

2. Materials and methods

The quality characteristic «usability» should be evaluated by probabilistic, temporal and operational indicators [20]. Evaluation of the listed indicators of software systems can be performed theoretically and experimentally. Since the theoretical evaluation of these characteristics has a number of disadvantages and limitations, it is advisable to make an experimental evaluation.

The process of assessing the quality characteristics of IPS «usability» can be represented as a sequence of four interrelated stages. Before the beginning of the experiment, a specific IPS is selected, in our case – «Guardian NT 3.0», as a platform for this experiment. Using the software documentation [17, 18] and by interviewing the administrators of the IPS, a list of typical operations is compiled that will be performed by the administrators of the IPS «Guardian NT 3.0».

At the first stage, the assessment of the operational indicator «usability» of the quality characteristic of the IPS is carried out by determining the composition of each typical operation from the set list performed by the administrator of the IPS «Guardian NT 3.0». The obtained values of the evaluation of the composition of each typical operation are indicative for further experimental assessment of the indicators of the «usability» quality characteristic of the selected IPS.

At the second stage, representative groups of users of the selected IPS are formed, which will perform typical operations on the IPS use from the compiled list.

At the third stage, which is the main one, the experimental measurement is performed of temporal indicator of the IPS quality feature «usability» by determining the average time to perform typical operations for each group of users who are administrators of the selected IPS. It is advisable to evaluate the time indicator of the quality characteristic «usability» using the mouse-tracking technology. Mouse tracking is a method that allows you to collect information about user cursor positions on the monitor screen. As a tool that implements the mouse-tracking technology, it is advisable to use the IOGraph VI.0.1. application. This application will allow you to experimentally determine the time indicator of the IPS quality characteristic «usability». The block diagram of the software used in the calculations of the IPS quality characteristic «usability» is presented in figure 1.

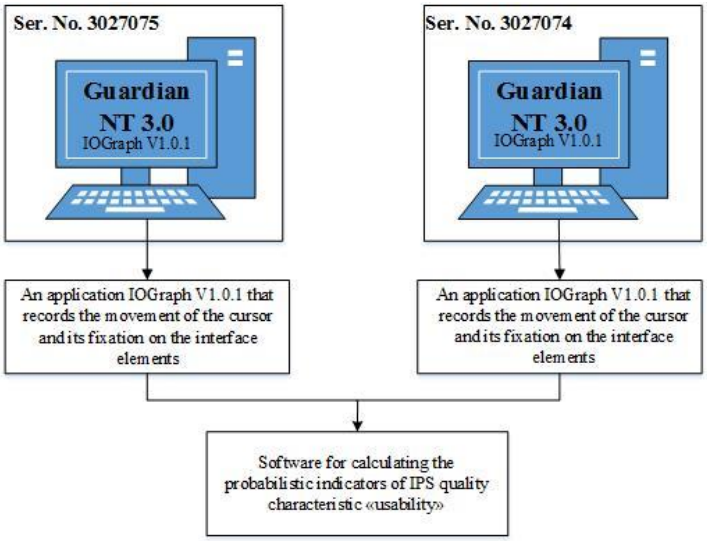


Figure 1. The block diagram of the software used in the calculations of the IPS quality characteristic «usability».

At the fourth stage, the evaluation of the probabilistic indicator of the IPS quality characteristic «usability» is carried out by constructing the time distribution functions of typical operations by the administrators of the IPS «Guardian NT 3.0». The result of the experimental evaluation and calculations are the values of timeliness of typical operations performed by administrators of IPS.

3. Results and their discussion

The idea of the experiment was to observe the users and their interaction with the software system in the conditions closest to real. For this purpose the list of typical tasks defined by program documentation [17, 18] and presented in table 1 was chosen. The choice of the list of typical tasks is determined by typical actions of the IPS administrator, regularly performed in the daily activity (the context of use of the program according to [21,22]).

Table 1. The list of typical operations performed by security administrators in the operation of IPS «Guardian NT 3.0».

Name of the typical operation performed by the administrator of the IPS «Guardian NT 3.0»
Adding and removing the registered data carriers
Editing the parameters of the system audit
Creating, deleting, and renaming users
Assignment of «classified» status
Setting the parameters of integrity, check of the integrity
Editing properties for groups of devices
Opening and saving the event log
Security system testing

All of the above operations performed by the administrators of the IPS contain a regulated order of actions described below

The operation «Adding and removing the registered data carriers» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «Carriers accounting». In the case of a computer running an operating system (OS) older than MS Windows XP, and enabling user account control, a window will appear on the screen in which the administrator presses the «Yes» button. To add carrier to the list of registered users, the administrator selects in the menu item «Carrier» | «Add carrier...» or calls the context menu in the users list area and selects «Add carrier...». At the same time, on the screen appears a wizard for adding the carrier in which the administrator selects one of the carriers and clicks the «Next» button. In the dialog box, the administrator specifies the registration data of the selected carrier: carrier account number (fills the window with characters), the name of the responsible user (fills the window with characters), the «classified» status of carrier (chooses from the options). Then presses the «End» button, after which the carrier will be registered. To remove the carrier from the list, the administrator selects in the menu item «Carrier» | «Delete carrier» or calls the context menu, in which he/she selects the «Delete carrier» item.

The operation «Edit system audit parameters» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «File manager». In the window that appears, the administrator selects the «Properties» item from the context menu of the selected object. In the properties window that appears, the administrator selects the «Security» tab and clicks the «Additionally» button, then selects the «Audit» tab. If the administration mode is enabled, the administrator presses the «Edit» button, otherwise – the «Continue» button, and a window will appear

on the screen displaying a list of the system audit of the selected object. In the window that appears, the administrator selects an object from the list and presses the «Edit» button. Next, the administrator changes the audit elements that he/she considers necessary.

The operation «Creating, deleting and renaming users» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «Users manager». In the case of a computer running an operating system older than MS Windows XP, and enabling users account control, a window will appear on the screen in which the administrator presses the «Yes» button. To create a user, the administrator selects the menu item «Computer», then «New user» or the menu item «Domain», then «New user» or calls the context menu by right-clicking in an empty area of the users list and selects the item «New user...». After that, a dialog appears on the screen, in which the administrator enters the user name, full name, description, as well as his password and permission. To create a user, the administrator clicks the «Create» button. If the administrator needs to create a user in the domain, then it is possible to place the user account in an Active Directory container other than the default container. To do this, in the above dialog, the administrator presses the «Select...» and in the window that appears, selects the required AD container. When the administrator selects the checkbox «Create user profile on this computer», after the user has been successfully created, on this computer his/her local profile is formed. To delete a user, the administrator selects him/her in the list of users and selects the menu item «User», then «Delete» or selects the «Delete» item from the context menu. To rename a user, the administrator selects him/her in the list of users and selects the menu item «User», then «Rename» or selects the «Rename» item from the context menu. After that, the administrator enters a new user name and presses the «Enter» key.

The operation «Assignment of «classified» status to objects» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «File manager». In the window that appears, the administrator selects the menu item «File» | «Administration» or presses the «Administration» button on the toolbar. In the case of a computer running an operating system older than MS Windows XP, and enabling users account control, a window will appear on the screen in which the administrator presses the «Yes» button. To assign a «classified» status, the administrator calls the context menu of the selected object, in which he/she selects the «Properties» item and in the appeared properties window selects the «Classified status» tab. Next, in the «Classified status:» field, the administrator selects the appropriate value from the drop-down list and presses the «OK» or «Apply» button to save the changes.

The operation «Setting the parameters of integrity, check the integrity» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «File manager». In the window that appears, the administrator selects the menu item «File» | «Administration» or presses the «Administration» button on the toolbar. In the case of a computer running an operating system older than MS Windows XP, and enabling users account control, a window will appear on the screen in which the administrator presses the «Yes» button. To set integrity parameters, the administrator selects an object, calls its context menu, in which he/she selects «Properties», and in the window that appears, selects the «Integrity» tab. To check the integrity, the administrator selects the file, calls its context menu, in which selects the item «Check integrity». A message about the results of the check will appear on the screen.

The operation «Editing properties for groups of devices» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «Device manager». In the case of a computer running an operating system older than MS Windows XP, and enabling users account control, a window will appear on the screen in which the administrator presses the «Yes» button. A dialog box appears on the screen. To view and edit permissions, the security administrator selects a group in the top left, then selects the menu item «Devices» | «Properties» and in the dialog box that appears selects the «Security» tab.

The operation «Opening and saving the event log» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «Event log». A dialog appears that displays the local computer event log. To open another log file, the administrator selects

the menu item «Log» | «Open log file...» and in the dialog box that appears selects the required log file. To save the event log to a file, the administrator selects the menu item «Log» | «Save log as ...» and in the dialog that appears enters the name of the log file.

The operation «Security system testing» contains the following composition. The security administrator selects in the «Programs» menu item | «Guardian NT» | «Security system testing». In the case of a computer running an operating system older than MS Windows XP, and enabling users account control, a window will appear on the screen in which the administrator presses the «Yes» button. A dialog box appears on the screen. In the list of computers, the administrator selects those on which the checks will be performed. In the list of available checks for each selected computer, the administrator selects the necessary checks.

An important step in assessing the quality characteristics of the IPS «usability» is the selection of test participants. In this case, the main requirement is a representative sample of prospective users of IPS. In accordance with [21-23], in the presence of a small number of subjects, it is necessary to involve in the experiment the participants most suitable for the description of the «average user of IPS». In the case of a significant number of participants in the experiment, it is necessary to select representatives of several different subgroups into which all users of the IPS can be stratified (for example, experienced users and beginners, representatives of different age groups, etc.).

During the experimental evaluation of the IPS quality characteristic «usability», there were involved 5th year students in the number of 79 people trained in the course 08.01.01 – «Economic security», and studying in accordance with the curriculum discipline «Information security of the organization». During the study of this discipline, there is provided a course of laboratory works with the IPS «Guardian NT 3.0», «Dallas Lock 8.0 c», «Dallas Lock 8.0 k», «Shell».

During the preparation of the experiment, in the course of the preliminary interviewing, all participants were divided into three approximately equal groups. The first group included users who had already worked with security systems for various purposes before (experienced users). The second group included users who did not use the IPS directly, but have experience with the AS in a secure execution, and are confident users of text and table editors and Windows OS (middle-level users). The third group included users who did not consider themselves to be confident users of the AS, but who attended a lecture course of the discipline «Information security of the organization» (entry-level users). The composition of the entire group of users involved in the pilot evaluation included 52 women and 27 men. In this case, all users were of the same age 22-24 years.

At the main third stage, the estimation is carried out of time of performing the listed standard operations by each group of users. During each operation, the IOGraph V1.0.1 tool, which implements the mouse-tracking method, recorded the cursor path of each security administrator and the time he/she performed the operation.

As an example, figure 2 shows a map of the movement and fixation of the cursor of the user of the group «Users of the middle level» on the interface elements of the program «User manager» of IPS «Guardian NT 3.0», performing a typical operation «Create user» as a security administrator, built using the software IOGraph V1.0.1.

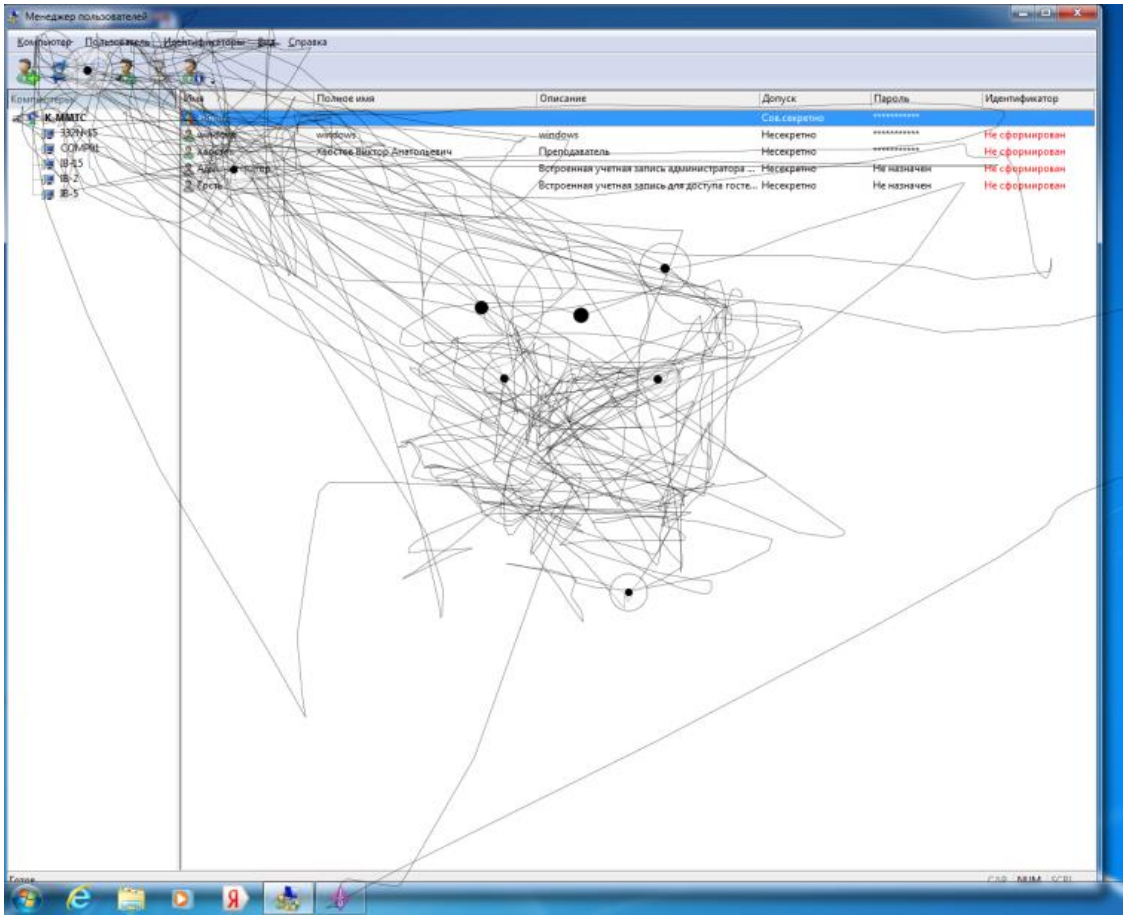


Figure 2. The interface of the program «User manager» of the IPS «Guardian NT 3.0», map of the movement and fixation of the cursor on the interface elements.

Review of the cursor movement records showed that, during the implementation by security administrator of the typical operation «Create user», application IOGraph V1.0.1 recorded six 5-seconds stops and two 15-seconds stops of the cursor on the dialog window of the IPS program «User manager» of the «Guardian NT 3.0». Thus, the average time of the operation «Create user» by security administrator of the group «Users of the middle level» in the IPS «Guardian NT 3.0» is 60 seconds.

For each group of users, the average execution time of each of these operations was calculated, the results are presented in table 2.

Table 2. The results of the evaluation of the time indicator of the IPS «Guardian NT 3.0» quality characteristic «usability».

Name of the typical operation performed by the administrator of the IPS «Guardian NT 3.0»	Value of the time indicator of a typical operation, s		
	Users group «Entry level users»	Users group «Middle level users»	Users group «Experienced users»
Adding and removing the registered data carriers	95	60	55
Editing the parameters of the system audit	70	40	35
Creating, deleting, and renaming users	100	60	60
Assignment of «classified» status	60	35	35
Setting the parameters of integrity, check of the integrity	55	45	45
Editing properties for groups of devices	120	110	110
Opening and saving the event log	45	35	30
Security system testing	75	50	50

The obtained experimental values of the statistical characteristics of the typical operations, presented in table 2, were the initial data for the evaluation of the probabilistic indicator of the IPS «Guardian NT 3.0» quality characteristic «usability» presented in table 3. In this case, according to [24], a truncated normal distribution was used to describe the statistical characteristics of typical operations performed by a group of users in the practical evaluation.

Table 3. The results of the evaluation of the probabilistic indicator of the IPS «Guardian NT 3.0» quality characteristic «usability».

Name of the typical operation performed by the administrator of the IPS «Guardian NT 3.0»	Value of the execution time of a typical operation by the administrator of the IPS «Guardian NT 3.0», s	Probability of performing a typical operation by the administrator of the IPS «Guardian NT 3.0»		
		Users group «Entry level users»	Users group «Middle level users»	Users group «Experienced users»
Adding and removing the registered data carriers	40	-	0.0227	0.0667
	50	-	0.1586	0.3084
	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 the parameters of the system audit	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	-	-
Creating, deleting, and renaming users	40	-	0.0227	0.0227
	50	-	0.1586	0.1586
	60	-	0.4999	0.4999

Name of the typical operation performed by the administrator of the IPS «Guardian NT 3.0»	Value of the execution time of a typical operation by the administrator of the IPS «Guardian NT 3.0», s	Probability of performing a typical operation by the administrator of the IPS «Guardian NT 3.0»		
		Users group «Entry level users»	Users group «Middle level users»	Users group «Experienced users»
	70	0.0013	0.8412	0.8412
	80	0.0227	0.9771	0.9771
	90	0.1586	0.9986	0.9986
	100	0.4999	-	-
	110	0.8412	-	-
	120	0.9771	-	-
	130	0.9986	-	-
Assignment of «classified» status to the objects	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	-	-
Setting the parameters of integrity, check the integrity parameters	30	0.0061	0.0667	0.0667
	40	0.0667	0.3084	0.3084
	50	0.3084	0.6914	0.6914
	60	0.6914	0.9331	0.9331
	70	0.9331	-	-
	80	0.9937	-	-
Editing properties for groups of devices	80		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	-	-
Opening and saving the event log	30	0.0677	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
Security system testing	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	-	-

4. Summary

Thus, in the article, on the basis of experiment, the assessment was carried out of the IPS quality characteristic «usability», namely the assessment of its operational, temporal and probabilistic indicators. Evaluation of the operational indicator was carried out by determining the composition of typical operations performed by the safety administrator during the operation of the IPS. The estimation of the time indicator was carried out by determining the average time of typical operations by several groups of users who are security administrators of the selected IPS. The estimation of the probabilistic indicator was carried out by constructing the distribution functions of the time of execution of typical operations by the security administrators of the selected IPS. The result is the values of timeliness of typical operations performed by the security administrators of the IPS.

References

[1] State Standard R 51583-2014 Protection of information. Order of creation of automated systems in the secure execution. General provisions. Available at: http://docs.cntd.ru/document (accessed 15 December 2019).
[2] State Standard 28806-90 Quality of software. Terms and definitions. Available at: http://docs.cntd.ru/document (accessed 15 December 2019).
[3] FSTEC (Federal Service for Technical and Export Control) of Russian Federation Guidance document. Computer aids. Protection against unauthorized access to information. Indicators of protection against unauthorized access to information. Available at: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativ-nye-dokumenty (accessed 15 December 2019).
[4] FSTEC (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. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty (accessed 15 December 2019).
[5] 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». Available at: http://www.consultant.ru/document (accessed 15 December 2019).
[6] About the scope and content of organizational and technical measures for ensuring safety of personal data at their processing in information systems of personal data: the order of FSTEC of Russia of 18.02.2013 No. 21. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy (accessed 15 December 2019).
[7] ISO/IEC 15408-2:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components». Available at: https://www.iso.org/standard (accessed 15 December 2019).
[8] ISO/IEC 17000:2004 Conformity assessment – Vocabulary and general principles Available at: https://www.iso.org/ru/standard (accessed 15 December 2019).
[9] State Standard 28195-89. Quality of software. Terms and definitions. Available at: http://docs.cntd.ru/document (accessed 15 December 2019).
[10] State Standard R ISO/IEC 9126-93. Information technology. Evaluation of software products. Quality characteristics and guidelines for their application. Available at: http://docs.cntd.ru/document (accessed 15 December 2019).
[11] B W Boehm, M Lipow, G J MacLeod, J R Brown and H Kaspar 1978 Characteristics of Software Quality (Amsterdam: North-Holland) p 208.
[12] B W Boehm 1981Software engineering economics (USA: Prentice Hall) p 512.
[13] Lipaev V V 1983 Quality software (Moscow: Finance and Statistics) p 250.
[14] Kadnova A M, Bokova O I, Rogozin E A and Serpilin A S 2019 System of indicators of quality of functioning at creation of system of information security on object of informatization of Internal Affairs Department *Devices and systems. Management, control, diagnostics* **1** pp 32-39.
[15] The system of information protection from unauthorized access «Dallas Lock 8.0». Operation manual. Available at: https://www.dallaslock.ru/products/szi-dallas-lock (accessed 15 December 2019).
[16] The system of information security «Guardian of NT 3.0». Administrator's Guide. Available at: https://www.guardnt.ru/doc (accessed 15 December 2019).
[17] The system of information protection from unauthorized access «Guardian of NT 3.0».

Application description. Available at: http://www.rubinteh.ru/public (accessed 15 December 2019).
[18] Information security tool «Secret Net 7». Administrator's Guide. Available at: https://www.securitycode.ru/upload/documentation/secret_net (accessed 15 December 2019).
[19] 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.
[20] Plumbaum T, Stelter T and Korth A 2009 Semantic Web Usage Mining: Using Semantics to Understand User Intentions. Proceedings of the 17th International Conference on User Modeling, Adaptation, and Personalization: formerly UM and AH Trento, Italy pp 391-396.
[21] Couper M P, Tourangeau R, Conrad F G and Crawford S D 2004 What they see is what we get: response options for web surveys, *Social Science Computer Review* **22** pp 111-127.
[22] N Nakamichi, K Shima, M Sakai and K Matsumoto 2006 Detecting low usability web pages using quantitative data of users' behavior, Proceedings of the 28th international conference on Software engineering, Shanghai, China pp 569-576.
[23] Druzhinin G V 1977 Reliability of automated systems (Moscow: Energy) p 536.