Innovative technologies for evaluating user interfaces of information security systems in the digital educational environment

O I Bokova¹, A M Kadnova², A V Barabanov³, T V Meshcheryakova² and M Yu Kalinin⁴

¹Ltd Kaskad, 2, Ferganskaya Street Avenue, Moscow, 109444, Russia
²Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriots Avenue, Voronezh, 394065, Russia
³Voronezh State Technical University, 14, Moscow Avenue, Voronezh, 394026, Russia
⁴Ltd Impulse-Service, 42, Lyublinskaya Street, Moscow, 109387, Russia

E-mail: o.i.bokova@gmail.com, aizhana_kadnova@mail.ru, csit@bk.ru, tmeshcheriakova4@mai.ru, maks@oxrana.org

Abstract. The article is concerned with solving of the practical and theoretical issues of usability characteristics assessment of systems of information protection from unauthorized access digital educational environment. A comparative analysis of innovative technologies of usability characteristics assessment used to assess the quality characteristics of software user interfaces is carried out. The considered methods can be applied to assess the functional quality of systems of information protection in terms of ease of use for users of various categories. Apart from that, the security administrator applies special requirements to the systems of information protection interface. A qualitative and quantitative assessment of usability characteristics for this category of users is required in connection with the significant influence exerted by the administrator on the information security processes and the dependence of his work efficiency on the systems of information protection usability characteristics.

1. Introduction

The tasks of providing security of the information circulating in digital educational environment (DEE) are performed by the information security system (ISS), which is an independent software or hardware and software installed as a part of the protected DEE at the stage of its technical implementation [1,2].

The ISS quality and functional effectiveness depend on its ergonomic management [3]. One of the ways to obtain the maximum possible coordination between the ISS technical component and the features of the operator is to develop a user-friendly program interface [4,5]. An analysis of the software documentation of various ISS [6,7] and of the experience in operating the protected AS indicated that the main operator (user) that interacts with the ISS through an interface is the security administrator. Thus, the aim of this article is to analyze the basic innovative technologies of ergonomic assessment of the ISS user interfaces from the point of view of ease of use for security administrators and of their features during a design of the protected DEE.
2. Materials and methods

Innovative technologies of assessment of the ergonomic indicator «usability» of user interfaces can be divided into the following 4 categories [8]:

- The interview method is a method of collecting information by way of interviewing or questioning the system operators. This method allows to give a correct assessment of the user’s attitude to the system interface in general, or to its components, as well as to identify the problems that are encountered by operators during the product operation.

- Expert methods. Usability experts, together with professional user interface designers, test the product, identify, according to their opinion, any errors, weak points and problems and make recommendations. This is one of the most economical methods, but it requires confidence in the professional competence of experts. Heuristic evaluation can be applied at various points of the system’s life cycle, since during the analysis process the experts do not use this system as such (they don’t perform the operations and actions that the operator is supposed to perform during the system operation).

- Analytical methods are methods that allow to obtain a quantitative assessment of the «usability» indicator of user interfaces. The most common analytical methods are those based on the Hick’s law and Fitts’s law, as well as the GOMS model and its modifications.

Hick’s law is used to obtain the quantitative assessment of the time required by the system operator to make a decision related to the choice of one of a number of options (the more options, the more time required for choice). The latent period of the operator’ intellectual activity when he performs any operation of the set of possible options on the object starts with the moment when he chooses this object or this action.

In accordance with Hick’s law, while choosing from n options, the time required to choose the necessary one is proportional to the logarithm to base 2 of the number of options plus 1. In this case, the condition of equal probability of all options must be fulfilled.

Fitts’s law states that the time required to reach the element is directly proportional to the distance to the element and inversely proportional to the size of the element [9].

Thus, the total time of operation executed by the operator can be calculated by means of the combined application of the Hick’s and Fitts’s laws.

One of the common approaches to the quantitative analysis of user interfaces is the use of the GOMS innovative technology (Goals, Operators, Methods and Selections rules). The most common innovative technology from the GOMS family is the Keystroke-Level Model [10], which is a fast and efficient way to estimate the time an operator takes to perform an operation. As a result of laboratory studies, it was found that despite the fact that for each operator of the «man-machine» system the execution time of a given elementary action can be individual, the measuring for each individual operator can be replaced using standard values of time intervals for each elementary action. In accordance with this innovative technology, any operation performed by the operator consists of six elementary actions. Table 1 shows the indicated elementary actions, their description and standard values of their execution time.

Thus, the execution time of an operation is the sum of the values of time spent on performing elementary actions:

\[ T_{\text{Total}} = T_K + T_P + T_H + T_a + T_R + T_D \]

(1)

Using the above-discussed Keystroke-Level Model innovative technology, we will carry out a quantitative analysis of the «Create New User» operation performed by the security administrator of the «Guardian of NT 3.0» information security system. The «User manager» program interface of «Guardian of NT 3.0» ISS, whereby the security administrator performs the «Create user» operation, is illustrated in figure 1.

The «Create New User» operation consists of the following elementary actions:
• Hand movement to the input device (to the mouse).
• Cursor movement to the «New User» object of the «User Manager» tool interface.

Table 1. Elementary actions of the «man-machine» system operator: designation, description and execution time.

| No | Designation of elementary action | Description                                                                 | Execution time, sec |
|----|---------------------------------|-----------------------------------------------------------------------------|---------------------|
| 1  | K                               | Pressing a key or a button. This parameter depends on the motor skills of the operator. | 0.2                 |
| 2  | P                               | The time required to move the mouse pointer to an interface element. This parameter depends on the distance to the element and its size in accordance with the Fitts’s law. | 1.1                 |
| 3  | H                               | The time required to move the operator’s hand to the data input device.      | 0.4                 |
| 4  | M                               | The operator time required to decide to perform an elementary action.        | 1.35                |
| 5  | R                               | System response time. This parameter is taken into consideration only when the operator has to wait for system’s response. |                     |
| 6  | D                               | The time taken to draw (manually) $n_D$ straight line segment with total length of $l_D$. | $0.9n_D + 0.16l_D$  |

Figure 1. The interface of «User Manager» tool of «Guardian of NT 3.0» ISS.

• Clicking on the given object. The «New User» dialog box will appear on the screen.
• Cursor movement to the «User name» object.
• Clicking on the given object.
• Hands movement to the keyboard.
• Entering the «a», «b», «u», «k», «o», «v» characters in the «User name» field.
• Hands movement to the input device (mouse).
• Cursor movement to the object «Create a user profile on this computer».
• Clicking on the given object (a checkmark will appear).
• Cursor movement to the «Full name» field.
• Clicking on the given object.
• Hands movement to the keyboard.
• Pressing the «Caps lock» key, entering the “B” character, pressing the «Caps lock» key, entering the «a», «b», «u», «k», «o», «v» characters, pressing the space bar, pressing the “Caps lock” key, entering the «A» character, pressing the «Caps lock» key, entering the «d», «e», «x», «a», «n», «d», «a» characters.
• Hand movement to the input device (mouse).
• Cursor movement to the «Description» field.
• Clicking on the given object.
• Hands movement to the keyboard.
• Pressing the «Caps lock» key, entering the «C» character, pressing the «Caps lock» key, entering the «b», «i», «e», «f» characters.
• Hand movement to the input device (mouse).
• Cursor movement to the «Access authorization» object.
• Clicking on the given object.
• Cursor movement to the «Confidential» element.
• Clicking on the given item.
• Cursor movement to the “Password” field.
• Clicking on a given object.
• Moving hands to the keyboard.
• Entering the «b», «i», «e», «f», «2», «0», «2», «0» characters in the «Password» field.
• Hand movement to the input device (mouse).
• Cursor movement to the «Confirm» field.
• Clicking on the given object.
• Moving hands to the keyboard.
• Entering the «b», «i», «e», «f», «2», «0», «2», «0» characters in the «Confirmation» field.
• Hand movement to the input device (mouse).
• Cursor movement to the «Create» object.
• Clicking on the «Create» object.

Figure 2 shows the interface of the «New User» dialog box of the «User Manager» tool of the «Guardian of NT 3.0» ISS at the instant of performing the elementary action «Clicking on the «Create» Object».

The record of the Keystroke-Level Model with respect to the elementary action M policy, will look like this:

```
H M P K M P K H M K K K K K H M P K M P K H M K K K K K K K K K K K K K K K M P K M P K M P K M H M P K M H M K K K K K K K K K K K K K K K H M P K K K K K K K K K H M P K
```
In accordance with expression (1), we obtain the time during which the security administrator of the «Guardian of NT 3.0» ISS performs the «Create New User» operation:

\[ T_{Total} = 14 \times 1.35 + 10 \times 0.4 + 10 \times 1.1 + 58 \times 0.2 = 45.5 \text{ sec} \]

Thus, this innovative technology allows you to calculate the time that the same security administrator needs to perform a given operation in different ISS, and in accordance with the obtained results to select ISS for the designed protected AS.

4. Experimental methods. The experiment, namely the execution by the operator of the tasks of operating the product through its interface, is carried out in laboratories, including the virtual ones or under normal operating conditions. In this regard, the experts have the opportunity to obtain more accurate qualitative and quantitative evaluation of user interfaces, particularly from the point of view of the «usability» parameter. This innovative technology ensure good results in the phases of technical implementation and operational testing of user interfaces. Similar experiments were carried out in [10, 11], however, an analysis of open reference sources has demonstrated the lack of attempts to carry out experimental assessments of the ISS user interfaces.

3. Results and arguments

All the above-mentioned innovative technologies of user interface assessment can be used to obtain qualitative and quantitative evaluation of the ISS user interfaces from the point of view of usability for security administrators while designing the protected DEE. However, there are several limitations and disadvantages of using these methods.

When we apply the interview method to obtain a ISS user interface evaluation, it is necessary to pay attention to the fact that, until now, there are no valid, reliable and well-structured questionnaires used within the framework of this method for secure administrators of the protected DEE of ISS. As a result, using this method during test of the «ISS – Security Administrator» system, the analysis managers and experts on their own develop the questionnaires for security administrators that would allow to obtain an evaluation of the ISS interface. The process of developing such questionnaires demands much effort and does not give any guarantees that this effort results in a high-quality and reliable questionnaire.

The application of the expert method during assessment of the ISS user interface does not allow to identify the serious interface structural problems regarding the configuration of the entire ISS, but only minor local problems in a limited number [12]. And considering that this method does not assume an analysis of the security administrator’s behavior, testing, mathematical calculations etc., the results obtained by the information protection expert may seem rather subjective and baseless.

The disadvantage of analytical methods application within the framework of evaluation of ISS interfaces is the approximate and averaged nature of the calculations. Despite the fact that the above-considered laws demonstrate a rather high degree of compliance with practical data, Hick’s law is applicable only to simple and quick decisions in the appropriate context, and Fitts’s law in certain circumstances reproduces incorrectly the time spent on movements by certain categories of users. The Keystroke-Level Model, in its turn, does not take into account errors made by security administrators during ISS operation, their mental workload or tiredness[9].

Considering that the experimental methods mean testing the «ISS – Security Administrator» system under conditions most closely resembling the real ones, it becomes possible to obtain the most accurate qualitative and quantitative assessments of the analysed ISS interface in regard to the ease of use for the security administrator. However, the technical equipment by which the analysis of the ISS interface is carried out is expensive and requires highly qualified staff performing the configuration.

When performing the assessment of ISS user interfaces, as a rule, the problem of choice arises regarding the most suitable innovative technology of assessment of the «usability» parameter of ISS performance. The right choice will significantly increase the efficiency of the process of evaluating the «usability» ISS DEE parameter. At present time, there are no comprehensive innovative technology that would ensure a systematic approach to the assessment of ISS user interfaces, therefore, the solution to the problem is a combination of the considered innovative technologies.
4. Conclusion
Thus, the article examines the expert, analytical and experimental innovative technologies of user interface assessment, as well as an interview technology, the use of which in combined form during designing the protected DEE will make it possible to choose between the proposed ISSs in terms of ease of use for a security administrator or to increase the «usability» parameter of the already implemented ISS at different stages of its life cycle.

The balanced application of the considered innovative technologies will allow to implement a professionally designed ISS, to increase the functional effectiveness of the «ISS-Security Administrator» system. This will allow the security administrator to avoid a large number of errors during the ISS operation and to reduce the time required to carry out the security operations regarding the protected DEE. The results can be used, for example, when designing software for the following tasks: data flows in an IP-based networks [13], information security risk estimation for cloud infrastructure [14].

References
[1] 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 87-96
[2] Kadnova A M, Makarov O Yu, Mishin S A and Rogozin E A 2019 Algorithm of the creation of the protected automated systems Information technology security 26 93-100
[3] Shlaen P Ya and Lvov V M Ergonomics for engineers: Ergonomic support to development of human-machine systems: problems, methodology, technology (Tver: TSU) p 214
[4] State Standard 28195-89 Software quality assessment General considerations http://a-podkidyshhev.ru/GOST/28195-89.pdf
[5] Kadnova Á 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 32-9
[6] The system of information protection from unauthorized access «Dallas Lock 8.0» Operation manual https://www.dallaslock.ru/products/szi-dallas-lock
[7] The system of information security «Guardian of NT 3.0» Administrator’s Guide https://www.guardnt.ru/doc
[8] Cooper A, Reiman R and Cronin D 2009 Alan Cooper about Interface. The Essentials of Interaction Design (St. Petersburg: Symbol Plus) p 688
[9] Stuart C, Moran T and Newell A 1983 The Psychology of Human Computer Interaction (USA: Lawrence Erlbaum Associates) p 312
[10] Soukoreff R W 2004 Towards a standard for pointing device evaluation, perspectives on 27 years of Fitts’ law research Int. J. of Human–Computer Stud 61 751-89
[11] Oksanich I N 2010 A model of decomposition of mental operators in a problem-oriented user interface and its experimental study Mathematical machines and systems 105-12
[12] Golovach V In 2005 Usability testing a bon march www.usethics.ru/lib/testing_by_the_cheap.html
[13] Nedyalkov I, Stefanov A and Georgiev G 2019 Studying and Characterization of the Data Flows in an IP-Based Network International Journal on Information Technologies and Security 1(11) 3-12
[14] Tsaregorodtsev A V, Kravets O J, Choporov O N and Zelenina A N 2018 Information Security Risk Estimation for Cloud Infrastructure International Journal on Information Technologies and Security 4(10) 67-76