Optimization of the digital educational environment for training administrators of the information security software system

O M Bulgakov¹, A M Kadnova², E A Rogozin², A V Krisilov³, R V Belyaev³ and A M Nuzhnyy⁴

¹Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, 128, Yaroslavskaya str., Krasnodar, 350005, Russian Federation
²Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 53, Patriots ave., Voronezh, 394065, Russian Federation
³Air Force Academy named after Professor N.E. Zhukovsky and Yu. A. Gagarin, 53 a, Starykh Bolshevikov str., Voronezh, 394064, Russian Federation
⁴Voronezh State Technical University, 84, XX-letiya Oktyabrya str., Voronezh, 394006, Russian Federation

E-mail: aizhana_kadnova@mail.ru

Abstract. This paper is dedicated to the analysis of the effectiveness of the training of security administrators concerning the work with information security systems. Assessment of the effectiveness was carried out by measuring the time taken by the administrator to perform typical operations. According to the results obtained, the reduction of time expenditures differs significantly for different types of operations and depends on the initial level of administrator’s skills. Measuring the operation execution time allows to build an optimal training strategy – to pay maximum attention to master skills in the operations, for which the time savings are maximum when moving to the next skill level. The proposed strategy of specialist training will make it possible to improve the efficiency of the digital educational environment with the use of innovative technologies.

1. Introduction

Information technologies create conditions for digital education development with the use of remote forms of learning, personalization and adaptive educational technologies. The acceleration of the development of digital technologies and their penetration into all spheres of life necessitate the creation of a flexible digital educational environment [1, 2]. To create a digital educational environment, the object rule of constructing educational materials is used. Objects are educational materials in the form of text, graphic, multimedia components and academic performance rating components. To automate the functioning of the digital educational environment, each object is compared with a set of parameters, on the basis of which a decision on its use is made [3]. Optimization of educational resources can be performed both according to the average study time (for a given probability of its acquisition), and the probability of course materials acquisition (for a given time of its study). When constructing the optimal learning strategies and optimizing the structure of educational material, the graph models are used.
Graph models include semantic networks, cognitive maps, Petri nets and Markov chains [4]. The development of the digital educational environment is based on the application of modern information and communication technologies and on the active interaction of all participants of the educational process [3]. Therefore, the actuality of the development of methods for assessing the effectiveness of human interaction with the digital environment is growing. Increase of effectiveness of human interaction with computer tools and the digital environment is one of the key tasks both in the software development and modernization and in the training of users.

2. Materials and methods
To make an experimental assessment of the effectiveness of information security systems interfaces and to optimize the security administrators training process, 83 fifth-year students were involved, that are trained in the specialty 08.01.01. Economic security at the Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation and are taking a course «Information security of an organization» in accordance with the plan of study. In the course of studying this discipline, the laboratory practical’s on information security systems «Strazh NT 3.0», «Dallas Lock», «Pantsir» are provided. When preparing the experiment, during preliminary interviews, all participants were divided into three groups differing in the degree of familiarity with the ISS «Strazh NT 3.0» and with the problem of information security in general. The first group included users who did not classify themselves as advanced computer users, but who attended a lecture course in the discipline «Information Security of an Organization» (entry-level users). The second group included users who did not use the ISS directly, but who had experience with computer equipment and who were advanced users of the Windows OS, text and table editors (middle-level users). The third group included users who had previously worked with different information security systems (advanced users).

During the experiment, all users performed the same set of operations, which allows to analyze the interaction with the software product under realistic conditions, and to assess the operations execution time for users of different training level. The choice of the list of typical operations is based on the typical actions of the ISS administrator, regularly performed in his daily workings (the context of use of the program is described in [5, 6]).

Mouse-tracking is an effective method for assessing the time a person performs different computer operations. The mouse-tracking software tools capture all mouse movements and clicks performed by the security administrator. The use of the mouse-tracking method allows to build a click map showing the elements of the ISS interface that were prevalently clicked on, and experimentally determine the time characteristics of the ISS (execution time of the entire operation, the hold time of the cursor staying on the ISS element). The trajectory of the cursor movement and the time of its fixation on the «Strazh NT 3.0» ISS interface elements during typical operations performing by the security administrator was recorded using the IOGraph V1.0.1 program [7].

3. Results and its discussion
The results of assessment of the typical operations execution time for security administrators with different training levels are presented in Table 1. The execution time for the «entry-level users» user group, the «middle-level users» user group, and the “advanced users” user group is designated as T(1), T(2), T(3) respectively.

Upgrading of skills of security administrators in general leads to the reduction of the time spent on performing typical operations, but the reduction of time expenditures for different operations varies significantly. With the skills improvement from the 1-st («entry-level users») to the 2-nd («mid-level users») level, the largest increase of the execution speed is observed for the most long-running operations “editing information media properties” and «editing permissions», and is up to 75-80 seconds. For the least time-consuming operations, the reduction of time expenditures is ~ 5 seconds. Skills improvement from the 2nd («intermediate users») to the 3rd («advanced users») level gives a much smaller effect, the reduction of time expenditures for most operations is 5-10 seconds, for some operations there is no longer a reduction of time («Classification mark assignment», «Start mode
setting», etc.).

**Table 1.** Typical operations execution time for groups of security administrators of different skill level.

| No | Operations performed by the «Strazh NT .0» ISS administrator | $T^{(1)}$, sec | $T^{(2)}$, sec | $T^{(3)}$, sec |
|----|---------------------------------------------------------------|----------------|----------------|----------------|
| 1  | Editing properties for information media groups               | 120            | 75             | 70             |
| 2  | Adding and deleting registered information media              | 95             | 60             | 55             |
| 3  | Editing information media properties                          | 180            | 105            | 95             |
| 4  | Exporting settings                                           | 70             | 55             | 50             |
| 5  | Creating, deleting and renaming users                         | 100            | 60             | 60             |
| 6  | Viewing password and list of user IDs                         | 55             | 35             | 40             |
| 7  | Changing user password                                        | 80             | 65             | 60             |
| 8  | Viewing and editing user properties                            | 65             | 60             | 50             |
| 9  | Formation of personal identifiers                              | 70             | 55             | 50             |
| 10 | Reading and clearing identifiers                               | 70             | 45             | 40             |
| 11 | Editing permissions                                           | 200            | 120            | 110            |
| 12 | Changing the owner                                            | 45             | 35             | 30             |
| 13 | Editing system audit parameters                                | 70             | 40             | 35             |
| 14 | Classification mark assignment                                 | 60             | 35             | 35             |
| 15 | Setting Start mode and tolerance                              | 50             | 45             | 45             |
| 16 | Editing parameters of additional audit                         | 60             | 50             | 40             |
| 17 | Setting parameters                                            | 55             | 45             | 45             |

The description of the process of security administrators training is further performed by using the following values that determine the effectiveness of skill improvement during the subsequent execution of individual operations:

$$
\Delta t_{12} = T^{(1)} - T^{(2)}, \quad \Delta t_{23} = T^{(2)} - T^{(3)}
$$

To optimize the process of security administrators training, a list of operations was formed in decreasing order of $\Delta t_{12}$, $\Delta t_{23}$ and the cumulative sums were formed that demonstrate the reduction of time expenditures with upgrading of skills of performing $n$ operations, for which this gives the maximum reduction of execution time:

$$
\Delta T_{12}(n) = \sum_{i=1}^{n} \Delta t_{12}(i), \quad \Delta T_{23}(n) = \sum_{i=1}^{n} \Delta t_{23}(i)
$$

The dependences of the cumulative sums on the $n$ number of operations, which are included in the program of administrator skills upgrading, are shown in figure 1. According to the data obtained, the time saving for a set of typical operations $\Delta T$ due to skill improvement from the 1st to the 2nd level is 460 sec., with skill improvement from the 2nd to the 3rd level the corresponding time saving is 6 times less – 80 sec. The rate of increase of cumulative sums decreases with an increase of the $n$ number of operations, and the dependences $\Delta T_{12}(n)$ and $\Delta T_{23}(n)$ attain the saturation. In case of improvement of administrators’ skills in performing 50% of operations it gives the greatest time savings and provides the 80% reduction of time expenditures. This regularity is observed for skill improvement from 1st to 2nd level, as well as for skill improvement from 2nd to 3rd level (figure 1).

**4. Summary**

The use of the proposed indicators of the effectiveness of user interaction with the system allows to make a quantitative assessment of the effects of ISS modernization as well as of the effect of user skills.
upgrading. Apart from that, the analysis of the states for which the user skills upgrading gives the greatest time savings (from entry-level to mid-level and from mid-level to advanced level) allows to optimize user training. The optimal training strategy is to pay maximum attention to the study of system conditions, for which the time savings are maximum when moving to the next level of training. The results can be used, for example, when designing software for the big data analytics for information security risk estimation for cloud infrastructure [8].

![Graph showing time expenditure for performing operations by a security administrator](image)

**Figure 1.** Reducing time expenditure for performing operations by a security administrator due to skill upgrading from the 1st to the 2nd and from the 2nd to the 3rd level.

**References**

[1] Dzhandzhugazova E A, Blinova E A, Orlova L N, Romanova M M and Davydovich A R 2018 Innovations in science and industry-specific education *Modern Journal of Language Teaching Methods* 8(3) 10-21

[2] Konoplyannik T M 2018 Additional education as a prerequisite for the development of society *Trends in the development of education: teacher, educational organization, society: Proc. of the All-Russian scientific and practical conference* (Cheboksary: ChuvashRepublic Institute of education) 342-3

[3] Danchenok L A, Zaitseva A S and Komleva N V 2019 Transformation of the model of additional education in the digital economy *Open education* 23(1) 34-45

[4] Kondratenko E V 2014 Results of development of adaptive educational resource *System analysis and applied informatics* 4 72-6

[5] Information security system “Strazh NT 3.0” Administrator’s guide
http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf

[6] Information security system “Strazh NT 3.0” Description of the application
http://www.rubinteh.ru/public/opis30.pdf

[7] IOGraph https://iographica.com

[8] Tsaregorodtsev A V, Kravets O Ja, 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