Analytical model for calculating the effectiveness of the modified access control subsystem of the information security system against unauthorized access in automated systems

A V Batskih¹, O M Bulgakov², I G Drovnikova¹ and A V Krisilov³

¹Voronezh Institute of the Ministry of internal Affairs of the Russian Federation, 53, Patriots Ave., Voronezh, 394065, Russia
²Krasnodar University Ministry of Internal Affairs of the Russian Federation, 128, Yaroslavskaya str., Krasnodar, 350005, Russia
³Zhukovsky-Gagarin Air Force Academy, 54A, Starykh Bolshevikov st, Voronezh, 394064, Russia

E-mail: svatikova96@mail.ru, ombfrier@yandex.ru, idrovnikova@mail.ru, alexph@mail.ru

Abstract. The paper considers an analytical model for calculating the performance indicator of the access control subsystem of the information protection system against unauthorized access in an automated system, the use of which allows to significantly simplify the calculation and increase its accuracy. The dynamics of subsystem functioning is described using a stochastic Petri net using the Laplace transform. Using the example of the standard information protection system against unauthorized access “Strazh NT 4.0”, the results of calculations of probabilistic and temporal characteristics of the model “Starting the PC and identifying the user” are presented, which describes the functioning of the access control subsystem when it is modified by implementing additional authentication based on the regular user keyboard handwriting recognition. Obtaining analytical dependencies of transition probabilities between the states of a modified subsystem allows optimizing its operation and verifying compliance with the requirements for the probability of performing functional tasks in a given time, while increasing the overall level of security of the automated system.

1. Introduction
In the age of informatization, automated systems (AS) are becoming more and more vulnerable to new types of threats to information security and, first of all, to threats related to unauthorized access (UA) to their information resources. Therefore, the development of a reliable access control subsystem in the information security system (ISS) against UA threats is an urgent task for modern automated systems [1]. Improving the authentication to increase the reliability of the specified subsystem and ensure information security of AS operated in a protected version at various informatization facilities procedure performed by the access control subsystem based on the use of new information and telecommunications technologies, in particular, biometric systems [2]. To increase the real security of the automated system, it is proposed to modify the access control subsystem of the ISS from the UA by implementing two-factor authentication based on recognizing the keyboard handwriting of a regular user when typing a passphrase [3].

An important step in the process of building such a subsystem is to evaluate the effectiveness of its functioning, which means a significant performance indicator that allows us to solve the problems of
operating both the access control subsystem and the ISS from the UA as a whole, taking into account the time characteristics [4, 5]. As an indicator of the performance of the access control subsystem ISS from the UA in the AC, operated in a protected version, it is advisable to use a directly time-dependent dynamic indicator of time efficiency $V_{TEACS}$, which according to [6] is understood as the ability of the program to perform specified actions in a time interval that meets the specified requirements.

In connection with the complexity of the structure and nature of interaction between the elements of the modified subsystem access control ISS from UA conducting assessment of efficiency of its functioning leads to the necessity of solving a number of tasks related to the creation of math (mainly analytic) models of the dynamics of subsystems, the definition and analysis of causal relationships between objects to the development process [7]. To study the processes of information protection from UA in the automated control system and solve these problems, it is advisable to use the mathematical apparatus of Petri nets used for modeling complex systems [8, 9], whose undoubted advantages include: the ability to simulate parallel processes, ease in presenting the graphical model and studying the dynamics of the simulated object, the ability to program the simulated processes.

In accordance with the stated above, for evaluating the performance of the modified subsystem access control ISS from UA in as there is a need to develop an analytical model describing the dynamics of transitions between states of the subsystems and average time of its stay in each of these states. It is made on the basis of use of mathematical apparatus of Petri networks in software environment MATLAB.

2. Materials and methods

The process of functioning of the ISS access control subsystem from the UA to the AC can be represented as a Markov process with a finite number of states, in which an exponential distribution law approximates the time spent by the subsystem in each of the states. For the purpose of constructing probabilistic-temporal characteristics (PTC) of the specified subsystem, a graph model is used, in which the access control subsystem access corresponds to the input of the final Markov process (FMP) in the initial state, and the completion of the subsystem's performance of its functionality for this request – the input of the MP in the final absorbing state. The description of the dynamics of the access control subsystem functioning from the UA is carried out on the basis of the stochastic Petri net model [7] and the probabilistic approach described in [10, 11].

The indicator of the time efficiency of the access control subsystem functioning from the UA is determined by the probability of transition of the FMP from its initial state to the final one in a time not exceeding $\tau_{max}$. The value of the time efficiency indicator is equal to the probability of the subsystem performing its functions for a time, not exceeding a given threshold:

$$V_{TEACS} = P(\tau \leq \tau_{max}),$$  \hspace{1cm} (1)

where: $\tau$ is the time of implementation of functions by the subsystem; $\tau_{max}$ is the maximum time allocated for performing these functions.

Markov model is used for calculation $V_{TEACS}$, in which transitions between subsystem states are described by a graph of a FMP. A system of equations describing the time delays and probabilities of transitions between all possible states of a FMP simulating the functioning of the access control subsystem is constructed on the basis of the graph of transitions between states:

$$Q_i(\tau) = p_{ii}G_i(\tau) + \sum_{j \neq i}^{n-1} p_{ij} \int_0^\tau g_j(t)Q_j(\tau - t)dt, \hspace{1cm} i = 1..n-1,$$

where: $Q_i(\tau)$ is the probability of Markov process being in the $i$ state reaching the end state $n$ in a time not exceeding $\tau$; $G_i(\tau)$ is the distribution function, equal to the probability of transition from $i$-th state to another in a time not exceeding $\tau$; $g_j(t)$ is the probability density for a random variable $t$ (the time of the system's stay in $i$-th state), $p_{ij}$ is the probability of transitions from $i$-th state to the
The system of equations (2) takes into account the probability of direct transition under the system of \( i \)-th state to the final state \( n \) (the first term) and the probability of its transition from the \( i \)-th state in the \( j \)-th state during the \( t \) subsequent transition from the \( j \)-th state to the final state \( n \) for the remaining time \( (\tau - t) \). Since the time delay of transition to the intermediate state can take any value in the range from 0 to \( \tau \), the second term uses the convolution integral.

To reduce the system of integral equations (2) to a system of linear algebraic equations, the Laplace transform over a variable \( \tau \) is used, so that the image functions will depend on the variable \( \nu \):

\[
q_i(\nu) = p_{ii}G_i(\nu) + \sum_{j=1}^{n-1} p_{ij}g_j(\nu)q_j(\nu), \quad i = 1..n-1,
\]

where: \( q_i(\nu) \) is the Laplace transform of a function \( Q_i(\tau); G_i(\nu), g_i(\nu) \) is the Laplace transform of functions \( G_i(\tau), g_i(t) \).

Further calculations use the exponential distribution of probability and probability density:

\[
G_i(\tau) = \int_0^\tau g_i(t)dt = 1 - e^{-\tau/l_i}, \quad g_i(t) = e^{-t/l_i}/l_i,
\]

where \( l_i \) is the average value of the subsystem's stay time in \( i \)-th state.

The Laplace transform of functions \( G_i(\tau), g_i(t) \) has the following form:

\[
G_i(\nu) = \frac{1}{\nu \cdot (\nu \cdot l_i + 1)}, \quad g_i(\nu) = \frac{1}{\nu \cdot l_i + 1}.
\]

For the convenience of writing, we use the following notation

\[
k_j = p_{ij} \cdot g_i(\nu), \quad m_i = p_{ii} \cdot G_i(\nu), \quad q_i = q_i(\nu), \quad q_j = q_j(\nu).
\]

Then the system of equations (3) will take the following form:

\[
q_i = m_i + \sum_{j=1}^{n-1} k_j q_j, \quad i = 1..n-1.
\]

An analytical solution from the systems of equations (7) with respect \( q_i(\nu) \) to, followed by obtaining \( Q_i(\tau) \) the inverse Laplace transform by analytical execution, allows us to define PTC of access control subsystems, and therefore, an indicator of the time efficiency of its functioning in the ISS from the UA:

\[
V_{TEACS} = L^{-1}[q_i(\nu)(\tau)|_{\tau=r_{max}} = Q_i(\tau)|_{\tau=r_{max}}.
\]

where \( q_i(\nu) \) is the Laplace transform for a function \( Q_i(\tau) \).

The algorithm for calculating the indicator \( V_{TEACS} \) of the typical ISS from the UA, developed using the numerical Givens method (method of rotations), is presented in [8].

The described method of constructing an analytical model for calculating the performance indicator of the access control subsystem ISS from the UA is implemented in the form of an algorithm using the MATLAB software package on the example of the model “Starting a personal computer (PC) and identifying the user” standard widely used in modern ISS systems from UA “Strazh NT 4.0”. The choice of the MATLAB software environment is determined by its advantages: a high level of visualization, the ability to modify models for analyzing other systems of this type, and the availability of integration tools with other software products.

3. Result and discussion
Graph models “Starting the PC and identifying the user”, describing the functioning of the access...
control subsystems of the ISS from the UA “Strazh NT 4.0” in secure automated systems (the user's login mechanism through identification and authentication) before and after its modification, figures 1-a and 1-b, respectively, represent the functions performed, and the probabilities of FMP transitions from various states to a finite state (absorbing state) the state and average time spent subsystem in each state of the subsystem under consideration are shown in table 1 [12].

![Diagram](image1.png)

**Figure 1.** Graph models of the process of functioning of subsystems “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” before and after its modification.

The time characteristics of the subsystem were recorded using a stopwatch.

Figure 1 shows that in case of three wrong password input (states 1.4 and 1.5), as well as discrepancies the keyboard of the user's handwriting (state 1.6) that protects your PC from brute force, with the subsequent registration of the fact of violation of working with ISS from UA and writing errors identify the user in the event log. When the conditions for correct password entry and matching keyboard handwriting are met, the user is authenticated (state 1.8, figure 1-b) (transition to the next subsystem of the ISS from the UA).

For further calculations, the following values of transition probabilities $p_{ij}$ between subsystem states were used “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” before and after its modification.

Value $p_{ij}$ before the modification:  

- $P[1,1,1.1] = 1$;  
- $P[1,1.1,1.2] = 0.01; P[1,1.1,1.3] = 0.99$;  
- $P[1.2,1.1] = 0.1$;  
- $P[1.3,1.4] = 1$;  
- $P[1.4,1.5] = 0.01; P[1.4,1.7] = 0.99$;  
- $P[1.5,1.4] = 0.99; P[1.5,1.6] = 0.01$;  
- $P[1.7,1.8] = 1$.

Values $p_{ij}$ after modification:  

- $P[0,1.1] = 1$;  
- $P[1.1,1.2] = 0.01; P[1.1,1.3] = 0.99$;  
- $P[1.2,1.1] = 0.1$;  
- $P[1.3,1.4] = 1$;  
- $P[1.4,1.5] = 0.01; P[1.4,1.7] = 0.99$;  
- $P[1.5,1.4] = 0.99; P[1.5,1.6] = 0.01$;  
- $P[1.7,1.8] = 0.99; P[1.7,1.6] = 0.01$;  
- $P[1.8,1.9] = 1$.

Calculation results $Q_i(r)$ for the subsystem “Starting the PC and identifying the user” of the ISS from the UA in protected areas AS during its transition from states 0-1.7 to the final absorbing state 1.8 (before modification) are shown in figures 2-a, 2-b, and from states 0-1.8 to the final absorbing state 1.9 (after modification) – in figures 2-c, 2-d.
Table 1. The reaction subsystem “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” for destructive impact and time spent in the specified states.

| № state | The probability of transition FMP from various states to the final (absorbing) state | Functions performed by the subsystem | Time, sec | № state | The probability of transition FMP from various states to the final (absorbing) state | Functions performed by the subsystem | Time, sec |
|---------|---------------------------------------------------------------------------------|--------------------------------------|----------|---------|---------------------------------------------------------------------------------|--------------------------------------|----------|
| 0       | \( Q_1 \)                                                                         | Getting started with the subsystem (when the subsystem stops performing functions) | 10       | 0       | \( Q_1 \)                                                                         | Getting started with the subsystem (when the subsystem stops performing functions) | 10       |
| 1.1     | \( Q_2 \)                                                                         | Presenting an ID                     | 1        | 1.1     | \( Q_2 \)                                                                         | Presenting an ID                     | 1        |
| 1.2     | \( Q_3 \)                                                                         | The ID stops working (if you try again, you must enter it again)                  | 6        | 1.2     | \( Q_3 \)                                                                         | The ID stops working (if you try again, you must enter it again)                  | 6        |
| 1.3     | \( Q_4 \)                                                                         | Access to password entry             | 1        | 1.3     | \( Q_4 \)                                                                         | Access to enter a password           | 1        |
| 1.4     | \( Q_5 \)                                                                         | Entering a password                  | 5        | 1.4     | \( Q_5 \)                                                                         | Entering a password                  | 5        |
| 1.5     | \( Q_6 \)                                                                         | Re-entering the password             | 5        | 1.5     | \( Q_6 \)                                                                         | Re-entering the password             | 5        |
| 1.6     | \( Q_7 \)                                                                         | Blocking the login when entering the password three times incorrectly            | 1        | 1.6     | \( Q_7 \)                                                                         | Blocking the login when entering the password three times incorrectly (if the keyboard handwriting does not match) | 1        |
| 1.7     | \( Q_8 \)                                                                         | User authentication                  | 1        | 1.7     | \( Q_8 \)                                                                         | Research of the user's keyboard handwriting | 1        |
| 1.8     | \( Q_9 \)                                                                         | Login                                | 5        | 1.8     | \( Q_9 \)                                                                         | User authentication                  | 1        |
|         |                                                                                   |                                      | 1.9     |         | \( Q_{10} \)                                                                       | Login                                | 5        |

In accordance with the graph shown in figure 1-a, from the state transition 1.7 is possible only in state 1.8, so the amount of intermediate states in the expression (2) becomes zero for \( Q_k(\tau) \) specific values of transition probabilities and sojourn time of the considered subsystem in state 1.7 (see table 1), we can obtain the following simple expression:

\[
Q_k(\tau) = p_{78} G_k(\tau) = Pr[1.7,1.8](1 - e^{\frac{-\tau}{\tau^7}}) = 1 - e^{\frac{-\tau}{\tau^7}}.
\]  

(9)

Reasoning in this way, we can obtain a similar expression for \( Q_n(\tau) \) the graph presented in figure 1-b, since only the transition from state 1.8 to state 1.9 is possible:

\[
Q_n(\tau) = p_{89} G_n(\tau) = Pr[1.8,1.9](1 - e^{\frac{-\tau}{\tau^8}}) = 1 - e^{\frac{-\tau}{\tau^8}}.
\]  

(10)
Figure 2. Transition probabilities of the subsystem “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” from various states to the final absorbing state before and after its modification.

Schedule and $Q_8(\tau)$ (figure 2-b) and $Q_9(\tau)$ (figure 2-g) obtained by analytical solution of the system of equations (3) and performing an inverse Laplace transform for set functions $Q_\tau$, full correspond to expressions (9, 10), which confirms the correctness of the proposed analytical model of the considered subsystem ISS from UA and the developed algorithm of calculation of PTC. The value $Q_\tau$ in figures 2-b and 2-d is zero, since in accordance with the graph models presented in figure 1, the probability of the subsystem transition from the state 1.6 to the final state is zero.

A value $Q_i(\tau)$, that expresses the probability of a subsystem transition “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” from the initial state to the final, is one of the main indicators of the dynamics of its functioning in the protected AU and is equal to the probability of the subsystem performing its functions for a period of time not exceeding $\tau$.

In the case with graphs $Q_i(\tau)$, separately presented in figure 3, the probability of the subsystem performing functions “Starting the PC and identifying the user” increases with the growth of the maximum allowed time $\tau$ and reaches 0.9 at $\tau = 33.2$ C (before modification) and at $\tau = 35.2$ C (after modification). The threshold is probably 0.63 (for exponential distribution function the threshold is...
equal to the probability of stay in state for a time equal to the average time of stay in this state \( \tau = l_i \) ) \( \tau \sim 19,1 \) with a (up to modifications) and \( \tau \sim 20,3 \) with (after modifications) that exceeds the amount of time spent reporting subsystem in the states that form the shortest path from the initial state ("Starting the PC") to the final state ("Login") (see graphs at figures 1-a, 1-b and table 1), equal to 23 before the modification subsystem (0-1.1-1.3-1.4-1.7-1.8) and 24 after modification (0-1.1-1.3-1.4-1.7-1.8-1.9). The obtained results allow us to state that the implementation of two-factor authentication based on recognizing the keyboard handwriting of a regular user when typing a passphrase, does not significantly affect the time indicator of the system software functioning.

**Figure 3.** Transition probabilities of the subsystem “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” from the initial to the final state (the probability of performing functions for no more \( \tau \) than a time ) before and after its modification.

The numerical results obtained with the help of graph models (figures 1-a, 1-b), on the one hand, agree with simple estimates based on the sum of the average residence times under the system “Starting the PC and identifying the user” in certain states. On the other hand, the application of the transition model between its states allows us to calculate the PTC of the subsystem more accurately. An increase in accuracy is provided by taking in to account all possible transitions between the states of the considered sub-system in the integral equations (2).

The graph shown in figure 3 and \( Q_1(\tau) \) allow to estimate the probability of the subsystem performing its functions “Starting the PC and identifying the user” for any specified time. In more detail, the obtained numerical results of probabilities of performance of functions by the considered subsystem before and after its modification are presented in table 2.

**Table 2.** Probabilities of subsystem performing functions “Starting the PC and identifying the user” ISS from the UA “Strazh NT 4.0” for a time not exceeding \( \tau_{max} \).

| \( P(\tau \leq \tau_{max}) \) | Time of execution of functions by the subsystem, \( \tau \), with |
|-------------------------------|-----------------------------------|
|                              | Before modification | After modification |
| 0.1                           | 6.6                  | 7.5                  |
| 0.2                           | 8.9                  | 9.9                  |
| 0.3                           | 11.0                 | 12.1                 |
| 0.4                           | 13.2                 | 14.3                 |
| 0.5                           | 15.5                 | 16.7                 |
| 0.6                           | 18.2                 | 19.4                 |
| 0.7                           | 21.5                 | 22.8                 |
| 0.8                           | 25.7                 | 27.4                 |
| 0.9                           | 33.2                 | 35.2                 |
| 0.95                          | 40.5                 | 43.5                 |
| 0.99                          | 56.5                 | 110.5               |
Performing similar calculations for various input parameters ($r_{max}$) makes it possible to optimize the operation of the modified access control subsystem ISS from the UA to the AS and check its compliance with the requirements for the probability of performing functional tasks in a given time while increasing the overall level of security of the system.

4. Conclusion
The paper offers an analytical model for calculating the performance indicator of the access control subsystem of the ISS from the UA in secure automated systems, the use of which allows increasing the accuracy and repeatedly reducing computational costs when calculating its PTC. Model is implemented as an algorithm in the MATLAB software environment. The results of calculations of the probabilistic-temporal characteristics model are provided “Starting the PC and identifying the user” it describes the process of functioning of the modified access control subsystem on the example of a typical one widely used in the ISS system from the UA “Strazh NT 4.0”. The system change was completed by implementing two-factor authentication based on recognizing the keyboard handwriting of a regular user when entering a passphrase.

Obtaining analytical dependencies of transition probabilities between the states model of the modified access control subsystem model expands the possibilities for analysis and allows optimizing the system for performing functional tasks by the subsystem while increasing the overall level of security of the automated control system.

Considered a method of constructing an analytical model of process of functioning of the modified subsystem access control ISS from UA can be used to enhance the as security and the effect of operate as a subsystem of access control and ISS from UA in as a whole.

5. References
[1] Schneier B 2019 We Have Root: Even More Advice from Schneier on Security (Wiley) 304 p
[2] Nikitin V V 2018 Model and method of multimodal authentication of an automated system user (Voronezh: dis. ... to the Andes. Techn. date of birth: 05.13.19) pp 140
[3] Alekseyev V A, Olives D V and Gorelov D Y 2017 Comparative analysis of promising technologies for authentication of users of a personal computer by keyboard handwriting (Kharkiv: Radio engineering: all-Ukrainian interdepartmental scientific and technical collection) 189 pp 195-201
[4] Xin Z 2013 Research on effectiveness evaluation of the mission-critical system (Proceedings of 2013 2nd International Conference on Measurement, Information and Control) pp 869-873
[5] Yun L and others 2015 Effectiveness Evaluation on Cyberspace Security Defense System (International Conference on Network and Information Systems for Computers. IEEE Conference Publications) pp 576-579
[6] GOST 28195-89 Estimation of quality of software facilities. General provisions
[7] Zinoviev P V, Zastrozhnov I I and Rogozin E A 2015 Methods and tools for evaluating the effectiveness of a confidential information resource protection subsystem in its design in electronic document management systems: monograph (Voronezh: Voronezh state technical University) pp 106
[8] Peterson J J 1984 Theory of Petri nets and models of computer systems (Moscow: Mir) pp 264
[9] Linyuan Y and others 2016 Network security analyzing and modeling based on Petri net and Attack tree for SDN (2016 International Conference on Computing, Networking and Communications. ICNC) pp 133-187
[10] Alfyorov V P, Batskikh A V, Krisolov A V, Popov A D and Rogozin E A 2020 Using a numerical-analytical model to assess the effectiveness of the information security system against unauthorized access in the analysis of its probabilistic and temporal characteristics (Bulletin of Dagestan state technical University. Technical Sciences) 47 1 pp 58-71
[11] Travnikova I G, Zinoviev P V and Rogozin E A 2016 Numerical methods for calculating the efficiency index of the auxiliary subsystem in the electronic document management system
[12] Batskikh A V 2020 *Simulation model of the functioning of the modified access control subsystem of the information protection system against unauthorized access in the CPN Tools software environment* (Herald Voronezh Institute of the Ministry of internal Affairs of Russia) 3 pp 96-106