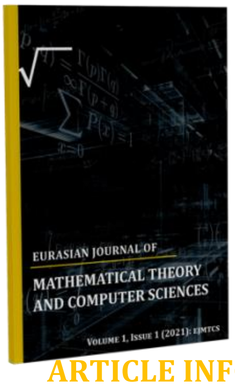
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
IF = 7.906
www.in-academy.uz


EURASIAN JOURNAL OF
MATHEMATICAL THEORY AND COMPUTER SCIENCES
VOLUME 1, ISSUE 1 (2021): EJMTCS

RESEARCH ON THE RELIABILITY OF THE INFORMATION SECURITY SYSTEM

Inomjon Yarashov[1,2]
Mirabbos Akbarov[1]
[1]Diplomat university
-The University of World Economy and Diplomacy
e-mail: iyarashov@uwed.uz

https://doi.org/10.5281/zenodo.15400913

ARTICLE INFO
Received: 08th May 2025
Accepted: 12th May 2025
Online: 13rd May 2025
KEYWORDS
Unauthorized access, information security, theory graph, theory of reliability, semi-Markov process, probability matrix.

ABSTRACT

The advancement and growing efficiency of computing technologies necessitate operation under increasingly noisy environments. These conditions may result in imbalanced heat dissipation, reduced signal strength, and, consequently, system malfunctions and errors in output data. This study focuses on the issue of unauthorized information leakage. The core of the problem is analyzed through graphical models, which are subsequently transformed into a matrix representation. The findings of this research can be utilized for evaluating and enhancing information security measures.

Introduction

Information technologies encompass the methods and systems used for managing and processing data, typically involving computer-based solutions. In this domain [1–6], significant efforts are directed toward tasks such as the collection, storage, protection, processing, and transmission of various types of data via electronic content management (ECM) systems and computer networks [7–12]. A notable challenge arises in data retrieval from high-density hard disk drives, where excessive noise and signal distortion impede accurate reading. In such cases, rather than directly decoding the signal, it is compared against a predefined set of patterns; the most probable match is selected, allowing for a machine word to be inferred. This has renewed attention on evaluating how hardware faults and malfunctions affect the performance of information systems, particularly concerning the protection of sensitive information [13–18] from unauthorized access.

To address these concerns, domestic developers have introduced hardware-based security solutions certified by international standardization bodies, such as the International Electrotechnical Commission. Examples include "Secret Net" and "Dallas Lock," which implement information protection through dedicated hardware modules. These systems are designed to physically isolate components handling sensitive data from those enforcing access control mechanisms. Furthermore, protection software is deployed within a microprocessor based on the Harvard architecture, which separates data and instruction memory. This architectural separation provides additional resilience against malware, preventing unauthorized code execution and tampering with system memory. In contrast, the "Dallas Lock" and "Secret Net" solutions rely more heavily on conventional motherboard elements and external storage for executing their security functions. A comparative analysis of these approaches illustrates differing methodologies in safeguarding data against unauthorized access, highlighting both hardware-based and software-driven strategies [19–27].

The methodology presented in [3] enables the evaluation of information security implementation principles through efficiency indicators—specifically, the protection of information against malicious analysis. Of particular significance is the analysis of the following aspects:

- The impact of the reliability of technical tools used for protecting information from unauthorized access (UA) on the overall security functionality;
- Existing architectures of information protection systems viewed through the lens of reliability theory;
- The role of monitoring the operational status of security components in maintaining effective protection against UA;
- The derivation of requirements for the design and operation of components responsible for monitoring the performance of information security systems.

Addressing these issues requires the use of appropriate mathematical tools and robust evaluation methods. This paper introduces both a mathematical framework and a methodological approach for assessing the influence of reliability in technical information security tools on the effectiveness of information protection functions. It also supports informed decision-making within this scope of analysis. A case study is provided to compare the performance and reliability of information protection systems such as ACKORD, Secret Net, and Dallas Lock, focusing on how effectively these systems implement technical mechanisms to safeguard data from unauthorized access.

Mathematical model of functioning of the system of protection against unauthorized access to information based on the theory of reliability

Information protection systems designed to counter unauthorized access are required to execute a specific set of critical tasks (functions) that ensure a high level of security within an automated system (AS), as identified in [2]. These core functions include:

T1. Implementation of identification and authentication mechanisms resistant to destructive software threats.

T2. Monitoring and verification of the integrity of the AS's hardware and software components.

T3. Control over access to actual (non-test) data.

T4. Regulation of access to all objects within the file system.

T5. Control over the execution of user-defined and system-level tasks.

T6. Maintenance of a secure and isolated software execution environment.

The activation rate of these protection functions is directly influenced by the frequency at which users initiate tasks. Undetected faults or malfunctions in individual components of the technical Information Protection System (IPS) can significantly degrade the overall reliability and effectiveness of the system's defensive capabilities.

Given the critical nature of these security tasks, it becomes imperative to incorporate a dedicated subsystem within the IPS architecture that continuously monitors the operational status of protection functions.

In a general model, the functioning of an information system protected against unauthorized access can be described as an interaction among the following components:

- The data subject to protection;
- The suite of security functions (T1–T6);
- Potential failures or malfunctions in the technical elements of the IPS;
- Monitoring systems tasked with ensuring the operability of security mechanisms;
- Subsystems responsible for restoring functionality in the event of failure.

A careful consideration of their interaction allows us to identify a process characterized by a finite set of possible states that uniquely determine the state of the system under study at each moment of time

$$S = \{ S_1, S_2, \ldots\ldots, S_r \}. \tag{1}$$

The operational behavior of the system under investigation can be interpreted as a sequence of transitions between discrete states, representing the various phases of system functionality. The likelihood that the system will transition from a given state S_i to another state S_j at the subsequent time step is generally influenced not only by the current state but also by the entire trajectory of preceding states.

However, the most extensively studied models in this context are those adhering to the Markov property, where the future state of the system depends solely on its present state, regardless of the historical path taken to reach it. In such Markov chains, the probability of transitioning from S_i to S_j is governed only by the current state S_i.

To model the behavior of the information security system accurately, several reasonable assumptions are made:

- The probability of simultaneous state changes in multiple system components (e.g., a hardware failure coinciding with the termination of a specific information protection function) is considered negligible;
- The transition probabilities between states are assumed to be time-invariant, ensuring a stationary process;
- Within an infinitesimally small time interval, it is practically impossible for the system to make a transition to a neighboring state and return from it immediately.

Given the stochastic and unpredictable nature of failures and system behavior, it is justified to model the system's evolution using an ergodic semi-Markov process. In this framework, transitions between states are described by a transition probability matrix characteristic of an ergodic Markov chain, enabling the analysis of long-term behavior and steady-state distributions.

$$P = \begin{matrix} P_{11} & P_{12} & \cdots & P_{1r} \\ P_{21} & P_{22} & \cdots & P_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ P_{r1} & P_{r2} & \cdots & P_{rr} \end{matrix}$$

(2)

with $S = \{S1, S2, .., Sr\}$ –the set of return states of the semi-Markov process and the average residence time in each of the return states $m_i, S_i \in S$.

Obtaining a mathematical expression for assessing the reliability of the implementation of information protection functions of the system under research

The construction of a mathematical model aimed at assessing the efficiency and reliability of the implementation of information protection functions against unauthorized access (UA) is based on the methodology outlined in [6]. In this context, errors in the performance of security functions are primarily attributed to undetected failures in the technical components responsible for implementing these functions. It is assumed that the software components responsible for information protection are error-free.

Since undetected failures can lead to incorrect or incomplete execution of protection tasks—thereby compromising data integrity—their effect is modeled equivalently to that of outright failures. Thus, in the reliability calculations, both undetected and detected failures are categorized uniformly as "failures."

System Configuration and Parameters

The model considers the interaction between the following components:

- Protected Information;
- Security Functions (T1–T6);
- Failures in Technical Means;
- Monitoring System for operability;
- Recovery System for restoring failed components.

Let us define the following elements for the queueing model of the system:

- β: Arrival rate of elementary tasks (requests) into the system (Poisson flow);
- P_1: Probability of immediate failure detection by real-time monitoring mechanisms during task execution;
- P_2: Probability of post-task failure detection via logical analysis after task completion;
- γ: Parameter of the exponential distribution for task execution time (both in operable and inoperable states);
- θ: Parameter of the exponential distribution for the time required to execute a test task when no protection function is being executed;
- P_3: Probability of instantaneous failure detection during test task execution;
- P_4: Probability of post-check failure detection after a fully executed test task.

Operational Assumptions

1. The technical means responsible for executing security functions are subject to random failures and require both real-time and post-process diagnostics.
2. The test task serves as a diagnostic function and is executed only when no active protection task is in progress.
3. Upon arrival of a new protection task, any ongoing test task is immediately terminated to prioritize real-time security.
4. Failure detection during protection or test task execution is probabilistic, with detection events governed by P_1, P_2, P_3, and P_4.
5. The execution durations are modeled as exponentially distributed random variables, ensuring memorylessness and simplifying Markovian analysis.

It is assumed that all values are $0 \leq P_i \leq 1$. In all cases of detection of a failure (calculation errors), technical means of protecting information from unauthorized access are sent for restoration, after which the solution of the problem is repeated on request or work continues according to the test program. The flows of failures and restorations are assumed to be the simplest ones with parameters λ and μ, respectively. As a result of monitoring the operational status of technical tools responsible for safeguarding information from unauthorized access (UA), potential malfunctions can be identified prior to the initiation of protection functions. This early detection mechanism enhances the module's preparedness to execute its intended role, thereby improving the overall dependability of the information security functions.

The operational modes of the information protection hardware vary based on two main conditions: whether a service request has been issued for the protection function or whether the module has encountered a malfunction. These operational scenarios are categorized into the following states:

S1: No active request exists; the information protection module is fully functional and engaged in executing a diagnostic task.

S2: There is no incoming request; however, the system has failed and is currently under recovery.

S3: No request is present; the module is malfunctioning but continues executing a test routine, with the fault remaining undetected.

S4: A request has been received and is being processed by a functioning information protection unit.

S5: A request is being handled by a faulty module where the malfunction has not yet been recognized.

S6: Although a protection request exists, the module is in a recovery state due to a detected failure.

A state transition diagram illustrating these interactions is provided in Figure 1.

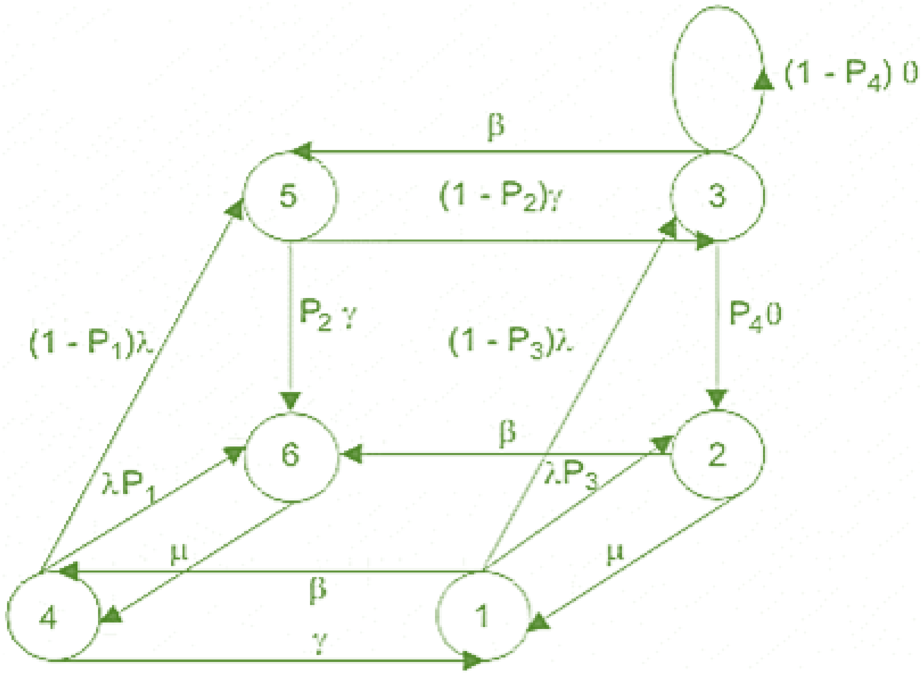


Figure 1. Graph of transitions of the studied technical means of protecting information from unauthorized access

This transition graph corresponds to the matrix P of transition probabilities of the nested Markov chain and the vector $||m_i||$ of average residence times of the semi-Markov process in each state $S_i \in S$ ($i \in [1,6]$), defined as:

$$P = \begin{matrix} 0 & \frac{p_3\lambda}{\beta+\lambda} & \frac{(1-p_3)\lambda}{\beta+\lambda} & \frac{\beta}{\beta+\lambda} & 0 & 0 \\ \frac{\mu}{\beta+\mu} & 0 & 0 & 0 & 0 & \frac{\beta}{\beta+\mu} \\ 0 & \frac{p_4\theta}{\beta+\theta} & \frac{(1-p_4)\theta}{\beta+\theta} & 0 & \frac{\beta}{\beta+\theta} & 0 \\ \frac{\gamma}{\lambda+\gamma} & 0 & 0 & 0 & \frac{(1-p_1)\lambda}{\lambda+\gamma} & \frac{p_1\lambda}{\lambda+\gamma} \\ 0 & 0 & 1-p_2 & 0 & 0 & p_2 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}$$

$$\|m_i\| = \frac{1}{\beta+\lambda} \quad \frac{1}{\beta+\mu} \quad \frac{1}{\beta+\theta} \quad \frac{1}{\lambda+\gamma} \quad \frac{1}{\gamma} \quad \frac{1}{\mu}.$$

Derivation of a mathematical expression to estimate the average time of safe operation of the system under research

Evaluating how reliably the functions for protecting information from unauthorized access (UA) are executed provides meaningful insights and enables a comparative analysis of different architectures for constructing information protection systems. Although the numerical differences between alternative designs may appear minimal, their influence on the system's security can be substantial. Hence, it becomes more practical to assess these options based on their performance—specifically, by examining the expected duration of fault-free operation, i.e., the average time between false determinations regarding UA.

Upon detailed examination, it becomes evident that the transition diagram depicted in Figure 1 lacks the capability to compute the time span between successive incorrect UA-related conclusions (i.e., the safe operation duration of the technical component responsible for UA protection). To address this limitation, we propose incorporating an **absorbing state**, designated as **S7**, which represents a scenario where a fault in the UA protection module remains undetected. Introducing this state modifies the transition structure, resulting in an updated model illustrated in Figure 2.

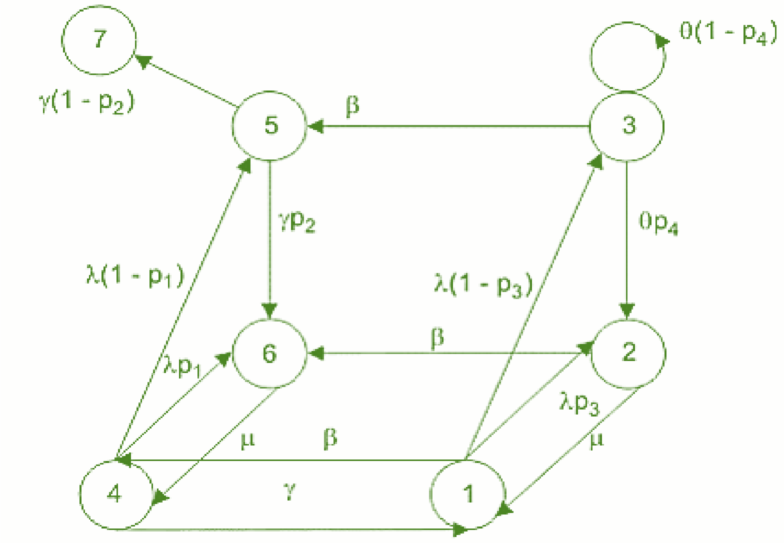


Fig. 2. Graph of transitions of the process under research with an absorbing state

This graph corresponds to the transition matrix and the vector of the average residence time in each of the marked states:

$$\hat{P} = \begin{array}{ccccccc} 0 & \dfrac{p_3\lambda}{\beta+\lambda} & \dfrac{(1-p_3)\lambda}{\beta+\lambda} & \dfrac{\beta}{\beta+\lambda} & 0 & 0 & 0 \\ \dfrac{\mu}{\beta+\mu} & 0 & 0 & 0 & 0 & \dfrac{\beta}{\beta+\mu} & 0 \\ 0 & \dfrac{p_4\theta}{\beta+\theta} & \dfrac{(1-p_4)\theta}{\beta+\theta} & 0 & \dfrac{\beta}{\beta+\theta} & 0 & 0 \\ \dfrac{\gamma}{\lambda+\gamma} & 0 & 0 & 0 & \dfrac{(1-p_1)\lambda}{\lambda+\gamma} & \dfrac{p_1}{\lambda+\gamma} & 0 \\ 0 & 0 & 0 & 0 & 0 & p_2 & 1-p_2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

$$\|m_i\| = \frac{1}{\beta+\lambda} \quad \frac{1}{\beta+\mu} \quad \frac{1}{\beta+\theta} \quad \frac{1}{\lambda+\gamma} \quad \frac{1}{\gamma} \quad \frac{1}{\mu} \quad \infty .$$

Given that the system under analysis includes an absorbing state denoted as S7, the mean time of proper functioning of the technical means for safeguarding information against unauthorized access can be mathematically represented as the expected time the process remains within the set of transient states (namely, S1 through S6) before it transitions irreversibly into the absorbing state.

Conclusion

The significance of this research stems from the rapid advancement of information technologies and the growing importance of ensuring information security. Within the framework of the study, the problem of unauthorized access to data is approached through the lens of reliability theory, providing both a theoretical foundation and practical applicability. By employing graphical modeling, the internal processes of the analyzed system were effectively visualized, thereby enhancing the precision and clarity of the research outcomes. Furthermore, the methodological framework developed in this study holds potential for adaptation and application across various types of information security systems.

References:

1. A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

2. I. Yarashov, "Algorithmic Formalization Of User Access To The Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-3, doi: 10.1109/ICISCT52966.2021.9670023.

3. A. Kabulov, I. Normatov, I. Kalandarov and I. Yarashov, "Development of An Algorithmic Model And Methods For Managing Production Systems Based On Algebra Over Functioning Tables," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670307.

4. A. Kabulov, I. Saymanov, I. Yarashov and A. Karimov, "Using Algorithmic Modeling to Control User Access Based on Functioning Table," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795850.

5. A. Kabulov, I. Kalandarov and I. Yarashov, "Problems Of Algorithmization Of Control Of Complex Systems Based On Functioning Tables In Dynamic Control Systems," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670017.

6. A. Kabulov and I. Yarashov, "Mathematical model of Information Processing in the Ecological Monitoring Information System," 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021, pp. 1-4, doi: 10.1109/ICISCT52966.2021.9670192.

7. A. Kabulov, I. Yarashov and A. Otakhonov, "Algorithmic Analysis of the System Based on the Functioning Table and Information Security," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746.

8. Kabulov A. V., Yarashov I. K., Jo‘Rayev M. T. Computer viruses and virus protection problems //Science and Education. – 2020. – T. 1. – №. 9. – C. 179-184.

9. Kabulov A. et al. Algorithmic method of security of the Internet of Things based on steganographic coding. 2021 IEEE International IOT //Electronics and Mechatronics Conference, IEMTRONICS. – 2021.

10. Madrahimova D., Yarashov I. Limited in solving problems of computational mathematics the use of elements //Science and Education. – 2020. – T. 1. – №. 6. – C. 7-14.

11. Kabulov A., Yarashov I., Vasiyeva D. SECURITY THREATS AND CHALLENGES IN IOT TECHNOLOGIES //Science and Education. – 2021. – T. 2. – №. 1. – C. 170-178.

12. Kabulov A., Muhammadiyev F., Yarashov I. ANALYSIS OF INFORMATION SYSTEM THREATS //Science and Education. – 2020. – Т. 1. – №. 8. – С. 86-91.

13. Gaynazarov S. M. et al. ALGORITHM OF MOBILE APPLICATION FOR MEDICINE SEARCH //Science and Education. – 2020. – Т. 1. – №. 8. – С. 600-605.

14. Кабулов А. В. Шерзод Туйлибоевич Болтаев, and Гулдофарид Муроджоновна Хабибжонова.«АЛГОРИТМИЧЕСКИЕ АВТОМАТНЫЕ МОДЕЛИ И МЕТОДЫ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ МИКРОПРОЦЕССОРНЫХ СИСТЕМ УПРАВЛЕНИЯ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.» //WORLD SCIENCE: PROBLEMS AND INNOVATIONS. – 2019.

15. Yarashov I., Normatov I., Mamatov A. THE STRUCTURE OF THE ECOLOGICAL INFORMATION PROCESSING DATABASE AND ITS ORGANIZATION //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 114-117.

16. Yarashov I., Normatov I., Mamatov A. ECOLOGICAL INFORMATION PROCESSING TECHNOLOGIES AND INFORMATION SECURITY //International Conference on Multidimensional Research and Innovative Technological Analyses. – 2022. – С. 73-76.

17. Kabulov A., Yarashov I., Mirzataev S. DEVELOPMENT OF THE IMPLEMENTATION OF IOT MONITORING SYSTEM BASED ON NODE-RED TECHNOLOGY //Karakalpak Scientific Journal. – 2022. – Т. 5. – №. 2. – С. 55-64.

18. I. Yarashov, "Development of a reliable method for grouping users in user access control based on a Functioning table," 2022 International Conference on Information Science and Communications Technologies (ICISCT), 2022, pp. 1-5.

19. Normatov I., Yarashov I., Boboqulov B. Development of models for describing the processing of environmental information in security problems of controlling a protection system based on petri nets //Central Asian journal of mathematical theory and computer sciences. – 2022. – Т. 3. – №. 12. – С. 229-239.

20. Kabulov A., Yarashov I., Daniyarov B. Systematic analysis of blockchain data storage and sharing technology //Central Asian journal of mathematical theory and computer sciences. – 2022. – Т. 3. – №. 12. – С. 240-247.

21. Jumaboyeva A., Yarashov I. Maxsus maktabgacha ta’lim tashkilotlarida nutqida nuqsoni boʻlgan bolalarni axborot texnologiyalari asosida pedagogik metodlar orqali tahlil qilish// O'zbekistonda ilmiy - amaliy tadqiqotlar mavzusida Respublika 17-ko'p tarmoqli ilmiy masofaviy onlayn konferentsiya.-2020.-С.249-250.

22. Kabulov A.V., **Yarashov I.K.** Algorithmic model of synthesis and elimination of risks based on Functioning table. Modern problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference. – Fergana. 2021. p.205-206.

23. Kabulov A.V., **Yarashov I.K.** Algorithmic modeling user access control based on Functioning table. Modern problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference. – Fergana. 2021. p.206-207.

24. Kabulov A.V., **Yarashov I.K.,** Kalandarov I.I., Otakhonov A.A. Algorithmic analysis of a system based on a Functioning table and importance for information security. Modern

problems of applied mathematics and information technologies al-Khwarizmi 2021: abstracts of the international scientific conference. – Fergana. 2021. p.207-208.

25. Yarashov I, Normurodov D. "Parol boʻyicha autentifikasiyalashning asosiy tahdidlari va shaxsiy parolning zaiflik". Uzliksiz ma'naviy tarbiya kontsepsiyasini amalga oshirishdagi ommaviy axborot vositalarining roli mavzusida Respublika onlayn ilmiy-amaliy konferentsiya, 2020.pp 492-496.

26. Islambek Saymanov, Inomjon Yarashov. "IoT arxitekturasida funksional darajalari tahlili". Ijtimoiy sohalarni raqamlashtirishda innovasion texnologiyalarning o'rni va ahamiyati Respublika ilmiy-amaliy konferensiya. 2020. Karshi, pp 359-361.

27. Inomjon Yarashov, Normatov Dilmurod. "Kiber fizik tizimlar va Iot tizimlarning qiyosiy tahlili". Axborot-kommunikasiya texnologiyalari va telekommunikasiyalarning zamonaviy muammolari va yechimlari Respublika ilmiy-texnik konferensiya, 2020 . Fergana, pp 338-340.