Revista Colombiana de Computación
Vol. 24, No. 2. July – December 2023, pp. 29-38
e-ISSN: 2539-2115, https://doi.org/10.29375/25392115.4707

REVISTA COLOMBIANA
DE COMPUTACIÓN

Assessment of the actual security of the information system by studying the equivalence of the applied technologies

Evaluación de la seguridad real del sistema de información mediante el estudio de la equivalencia de las tecnologías aplicadas

Aslan A. Tatarkanov[1], Rasul M. Glashev[1], Ekaterina S. Nazarova[1]

[1]IDTI RAS, Moscow, Russian Federation.
as.tatarkanov@yandex.ru, rasul.glashev@mail.ru, nazarova_kat@bk.ru

(Received: 29 May 2023; accepted: 13 December 2023; Published online: 31 December 2023)

Abstract. This research is devoted to one of the urgent problems in the field of security provision, implemented in various areas of human activity related to information systems. It is associated with a typical situation of discrepancy between the costs of improving security methods and the level of security achieved in this case. It is shown that one of the most promising methodological approaches aimed at finding a solution to this problem is related to the study of the prospects for adapting existing solutions with integration into the computing environment that implement the new technology. In accordance with this concept, the equivalent transition between information technologies should be implemented while maintaining the level of overall information security. The main research goal was determined – it concerns the development of an analytical model for controlling the equivalence of information technologies in information security systems. The current state in the field of information security was analyzed. It was revealed that the tools and mechanisms existing today and presented on the relevant market that prevent risks and threats to the functioning of information systems associated with data theft and distortion are “narrow”, that is, adapted to solving local problems facing attackers.

Keywords: Applied Technologies, Information Security Systems, Information Security, System Model.

Resumen. Esta investigación está dedicada a uno de los problemas urgentes en el ámbito de la provisión de seguridad, aplicado en diversas áreas de la actividad humana relacionadas con los sistemas de información. Se asocia a una situación típica de discrepancia entre los costes de mejora de los métodos de seguridad y el nivel de seguridad alcanzado en este caso. Se demuestra que uno de los enfoques metodológicos más prometedores para encontrar una solución a este problema está relacionado con el estudio de las perspectivas de adaptación de las soluciones existentes con integración en el entorno informático que implementan la nueva tecnología. De acuerdo con este concepto, la transición equivalente entre las tecnologías de la información debe llevarse a cabo manteniendo el nivel de seguridad general de la información. Se determinó el objetivo principal de la investigación, que se refiere al desarrollo de un modelo analítico para controlar la equivalencia de las tecnologías de la información en los sistemas de seguridad de la información. Se analizó el estado actual en el campo de la seguridad de la información. Se puso de manifiesto que las herramientas y mecanismos existentes hoy en día y presentados en el mercado pertinente que previenen los riesgos y amenazas para el funcionamiento de los sistemas de información asociados al robo y la distorsión de datos son "estrechos", es decir, adaptados para resolver los problemas locales a los que se enfrentan los atacantes.

Palabras clave: Tecnologías aplicadas, Sistemas de seguridad de la información, Seguridad de la información, Modelo de sistema.

Paper type: Research paper.

1 Introduction

Improving means and methods for ensuring the security of such objects of the information environment as computing tools, and communication data and channels that provide the receipt and processing (in terms of presentation, storage or transmission) of the necessary information is a natural process of information technology development in various spheres of human activity (Kaur and Ramkumar 2022). The emergence

©2023 Universidad Autonoma de Bucaramanga. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA 4.0) license (https://creativecommons.org/licenses/by-nc-sa/4.0/).

of new risks regarding information security is associated with the emergence of new information technologies, with an increase in the volume of transmitted information and media data, including data in the field of medicine and telemedicine (Tatarkanov et al., 2022a) (Tatarkanov et al., 2022b). But at the same time, as a rule, the results of increasing the degree of information security do not reflect the significant time and financial costs that are requested to conduct research for this purpose (Syed et al. 2022).

Thus, noteworthy approaches are available within the framework of many applied studies aimed at providing increased security of information systems and technologies that contribute to the creation and subsequent processing of data. However, many of them are superficial, and based on obsolete principles. This is not always expedient in the context of the specifics of a particular problem that needs to be solved. Such an approach, when almost always a separate information object of any developing information system complies with a strictly defined single technology for its development, is associated with an increase in costs due to duplication of technical solutions (including in terms of procurement, implementation and maintenance of computing facilities), their inconsistency, contradiction to each other, etc.

Thus, it is possible to say about an obvious contradiction between the two aspects:

- the need to improve the functionality of information systems that process data flows from different sources to ensure their security;
- opportunities in terms of rationalization and optimization of costs regarding the solution of the repeatedly noted urgent problem.

The approach associated with a multidimensional analysis of the problems and prospects for adapting solutions already used in practice for implementation in new information security tools being developed seems to be most promising and at the same time rational (Ling et al. 2023). Simultaneously, it is necessary to ensure the identity of computing tasks when assessing the security of information system components. Thus, a transition between equivalent information technologies must be ensured to avoid damaging information security. Despite the apparent complexity of this approach, it is the most general and flexible technique in relation to any conditional information system. In this case, the stage of analyzing the possibility of implementing an equivalent transition becomes paramount, which should minimize all other possible costs with other modernization strategies.

Eliminating the difficulties and contradictions described above is not as difficult as it seems. It is sufficient to strive to develop and improve the existing tools and means that contribute to the mathematical justification of the actual security of individual stages and operations of data formation and processing in the process of using information technologies (Bashendy et al., 2023). In this context, the equivalence of methods for creating, for example, messages that include data that is important from the viewpoint of information interaction is the connecting link of a specific object and a conditional set of technological solutions.

The implementation of research work within the framework of solving the identified problem involves obtaining the necessary and useful information in terms of developing a fundamentally new model for controlling the actual equivalence of information technologies within information security systems. All these tasks constitute the aim of this study.

The primary task aimed at achieving the designated goal is research aimed at substantiating the main conceptual provisions of the model for analyzing the degree of information technology security based on the concept of their equivalence.

The complexity of the raised problem is caused by the features of modern information technologies indicated below allow to form a constraint on the calculus of variations in the framework of the establishing equivalence:

- partitioning into related sets of attributes with respect to the given admissible transformations;
- linearity of formation and existence of conditional equivalence;
- formation probability of cyclic structure of the graph of the set of admissible transformations.

2 Literature Review

Assuring the security of a wide range of information systems used in practical and scientific activities is a complex problem, the results of which are closely related to successful protection against viruses, and to the task of establishing high-quality control over the actions of users of information systems, aimed at preventing accidental or purposeful disclosure of confidential information (Kirilchuk et al., 2022) (Shukla, et al., 2022).

Within the framework of searching for effective solutions to the problems of the first group, studies are underway to create and improve antimalware consisting of subroutines (Zelinka et al. 2018). The purpose of the latter is to detect and prevent the spread of viruses and other potentially malicious programs, and to remove them (Meridji et al., 2019)

The developed and implemented software and hardware tools are oriented at achieving this goal, to a greater or lesser extent; these tools are based on a number of methods and technologies for detecting viruses that have certain disadvantages, primarily such as the method for matching the definition of a virus in a dictionary (Levy and Shalom, 2020), the method for generating and distributing signatures (i.e., the attack or virus signatures used to detect them) (Al-Asli and Ghaleb, 2019), the method for detecting suspicious (abnormal) program behavior (Seo and Lee, 2018), the emulation-based method for computer virus detection (Bist, 2013), the method for analyzing the sandbox environment (Madan et al., 2022), the white list technology, the heuristic analysis technologies (Rehman et al., 2018), and others.

In the set of methods for matching the detection of a virus threat in the dictionary, a special software (antivirus) refers to a conditional library or database. Determining the criteria for matching a piece of code to a known signature triggers a software action upon request. An antivirus can disinfect a particular file or delete it (Shukla et al., 2022).

Approaches to the creation and distribution of known codes make it possible to identify which type a virus program attack can potentially become. False calls are unlikely. However, numerous current approaches are characterized by a number of gaps, such as the inability to detect new types of attacks (information about which is not available in the antivirus database) (Aboaoja et al., 2022). Among other things, the lack of resistance to polymorphic threats and modified versions of various known viruses, which is typical for a number of programs, is considered a disadvantage (Dhanasekar et al., 2018). Some solutions even require regular updates.

The antivirus software based on the principle of using a special method to detect the so-called anomalous behavior of programs is worth noting (Zhai et al., 2015). However, this type of antivirus has a drawback: the ability to identify unknown risks and threats is unlikely. Everything is compensated by a function that literally monitors atypical operations, and can respond to potentially malicious operations and events. It should be noted that the suspicious behavior method provides protection even against new viruses, information about which is not available in a particular antivirus software database (Yang et al., 2022). However, the method of detecting viruses by identifying anomalous program behavior has one subjective disadvantage, which is an increased likelihood of false positives or warnings. This is typical for solutions based on the principle of emulation. This method assumes that an executable file is run in an artificial controlled environment for assessment.

Virus detection methods using so-called “sandboxing” methods involve simulating an operating system (often on a virtual machine) and running an executable file in this simulated system (Sharma et al., 2022). The efficiency of software implementing these methods is much higher than of all others, but the cost of running them is also much higher (Chakkaravarthy et al., 2019).

A whitelisting technique is interesting (Barbosa et al., 2013). It is characterized by the fact that instead of searching for known potentially dangerous programs, it excludes the very fact of executing operations in addition to those previously set by the administrator, i.e., marked as safe (Huh et al., 2011). This is an advantage because restrictions on code updating for a particular virus are eliminated. At the same time, applications outside the conditional list compiled by the administrator are not executed (Wang et al., 2020).

Heuristic analysis techniques are also noteworthy (Bo et al., 2017). They can be based on the methods for:

- (heuristic) scanning. It is supposed to check the emulated software with a special analyzer;
- decompiling. In this case, the code of suspicious software is “decompiled”, and analyzed in parts.

In the case of scanning, the analyzer emulates a virus acting within a certain instruction (Vouvoutsis et al., 2022). A checksum is then determined. If at least a partial match to a known signature is detected, the antivirus offers treatment, deletion or quarantine measures.

In the case of decompiling, a suspicious file in code form is checked against known signatures and virus activity patterns (Wang et al., 2023). The object is recognized as suspicious according to the same principle as before: at least minimal compliance with the criteria of known risks and threats is required.

In certain cases, applying heuristic analysis techniques is quite successful (Gopinath and Sethuraman, 2023; Shaukat et al., 2022). The disadvantages of this technology include, for example, the existence of easy ways to fool the heuristic analyzer, and its “excessive suspiciousness”, which causes the possible “false triggering”. Noteworthy, numerous tests have been conducted on the components of heuristic analysis. Their results suggest that the efficiency of scanning is unsatisfactory in practice in 50% of cases. Treatment

with heuristic analysis methods is not always possible. In such situations, it is necessary to update databases to obtain information on new virus codes and treatment sequences. On the whole, despite a number of drawbacks, this technological solution has prospects for development.

Various methods have been proposed as part of the search for effective solutions to the second group of tasks to ensure reliable control over the actions of users of information systems to prevent accidental or deliberate disclosure of confidential information. The essence of the procedures designed to ensure the solution of this problem consists in analyzing the activities of information system users, aimed at the possibility of identifying admissible or inadmissible actions stipulated by the information security requirements for the system. This is a very labor-intensive task. For this reason, its solution is logical and expedient by means of a special approach, in the framework of which it is supposed to abandon the description of a conditional set of permissible or undesirable actions. Forming patterns of individual cases, indicating a probable violation of the state of security becomes a priority. At the same time, it is necessary to analyze the relevant criteria.

Therefore, one can say that the solution of the noted problem is possible by applying a model approach, where some basic data about technologies will be templates. In this case, individual options can be represented as objects of the "highest" class with specified parameters and functions contributing to elimination of potential risks and threats to a particular information system.

However, it is usually problematic to implement the described protection methodology in scientific and industrial organizations, for which the goal of protecting information is secondary to the main type of their activity, due to the lack of the possibility of conducting such a correct analysis without using a wide range of cutting-edge personal user and computer cryptographic information protection tools. developed on personal sites with their own computing resources and security (Uchendu et al., 2021; Moreira et al., 2016).

The survey and analysis performed make it possible to state that many advanced tools and mechanisms that prevent the implementation of threats such as information theft or substitution solve "narrow", limited tasks. This is a drawback, because it excludes the provision of such a level of security that could be compared to the costs of organizing and maintaining the functioning of information security systems. The reasons are the imperfection of the developed solutions, their inconsistency with the level of development of information access and processing equipment, the inability of antiviruses to detect fundamentally new potentially dangerous signatures. The following drawback was also identified: many current systems and protection tools are built into information systems without preliminary analytical measures, which is undesirable in the context of integration, when one or another protected environment is comprehensive and complicated.

Thus, one can speak about an increased relevance of research in terms of the cumulative functioning of various kinds of information systems with reference to the work of the means used to protect them. At the same time, system analysis is important, because the nature and aspects of data presentation at different levels of operations from storage and transmission to the synthesis of a certain kind of messages are not always constant. Analytical activities should literally contribute to the description of undesirable processes, obtaining information about the behavior of viruses that provoke risks and threats. The protection of a specific information technology is most appropriate to consider as an opportunity to establish a real sequence of operations, methods and means in relation to a variety of information resources that contribute to the assurance of actual security. Protection must guarantee the immutability and stability of the marked sequence, and the possibility of determining legitimacy within a particular system. Thus, integrity is important, it can be ensured only by formalizing information protection aspects that are different in essence and content in the context of the tasks being solved. In this case, protection should be considered as a process, and information security – as a technology. This approach does not contradict the principles of ensuring the equivalence of information means and tools of a number of reference solutions.

3 Theory

The requirement to protect the technology of storage, processing and presentation of an information object is understood as the possibility of forming rules that can be applied to a message in the IS, and the possibility of determining their legitimacy. The condition for using exclusively permitted operations in a specific sequence is the initial conceptual provision for constructing the appearance of the model for analyzing the degree of information technology security.

As noted previously, the equivalence of the tools and methods of forming different local and large-scale arrays, including information that is important from the viewpoint of the interaction of the software environment elements as computer communications progress can be the linking element in the context of a particular information object and within various technologies.

The equivalence of the sequence of attributes $a_1^1 \dots a_n^1$ and $a_1^2 \dots a_n^2$, characterizing these information technologies, is understood as the equivalence of two different information technologies IT_1 and IT_2 of creating a certain information object containing data on a single information fact. As shown by conducted studies, the information technology represented by a large number of abstract attributes $a \in A$ $(a_1, a_2, \dots, a_n)$ can be transformed into a sequence $t_1, t_2, \dots, t_n$,, which is a word in some abstract alphabet T, In this case, two different information technologies IT_1 and IT_2 will be equivalent if the sequences $t_1^1 \dots t_n^1$ and $t_1^2 \dots t_n^2$ are equivalent, provided that there is a mapping: $\varsigma: a \to t$, $t \in T$.

At the same time, it should be noted that the existence of an object of a specific technology that can be represented in the required form is possible within the framework of an information system, provided that there is a bijection represented like this: $\varsigma: o \to a$

The presented bijection literally determines the correspondence to a specific action, or a specific operation (out of the set of allowed $\boldsymbol{O}$) $o \in O$ and attribute $a \in A$.

Note that equivalence, and isomorphism for two sets $\boldsymbol{A}$ and $\boldsymbol{B}$, must meet the following conditions (hereinafter in the text, the "tilde" sign $\llcorner\!\lrcorner$ denotes an equivalence relation):

– always$A \sim A$;
– if $A \sim B$, then $B \sim A$;
– if $A \sim B$ and $B \sim C$, then $A \sim C$.

As part of the procedures for generating rules that can be applied to a message in an IS, and determining their legitimacy, the purpose of setting security requirements for an abstract system (as compared to an applied one) leads to an excessive set of operations to determine:

– admissible actions of the information system that form messages;

– pairs of operations, the use of which in the process of creating messages is admissible, but only in the context of deviation from the conditional basic process, which is not anomalous.

However, with this approach, it is impossible to operate with the finiteness of establishing equivalence for information technologies: it enables to get a large number of different variations of information technologies, which in the vast majority of practical cases (in the case of non-synthetic data) will not intersect on a set of symbols, even after applying the relations establishing equivalence.

When solving applied problems, the purpose set can be achieved in the process of solving the following problems:

– forming a list of required operations based on a description of a set of applied tasks;

- identifying a conditional sample of technology, provided that any other is reduced to the given one by establishing equivalence as a set of relations.

The formalized system of rules (hereinafter, we denote this system by $\boldsymbol{\Theta}$), which provide the possibility of assessing the equivalence of symbols under the established requirements for the information technology security, is a set of relations of the following type:

$$c_1^1 \dots c_t^1 \sim d_1^1 \dots d_s^1$$
$$\dots$$
$$c_1^v \dots c_t^v \sim d_1^v \dots d_s^v$$

where $c_j^i, d_k^i \in T,\ 1 \le i \le v,\ 1 \le j \le t,\ 1 \le k \le s$ are sequences of symbols characterizing the equivalence of applying sequences of operations $c_1^1 \dots c_t^1$ and $d_1^1 \dots d_s^1$.

Note that strict fixation of the established pair of sets $\boldsymbol{T}$ and $\boldsymbol{\Theta}$ is not just necessary, but is already a sufficient condition for determining the rules of the IT security level. This statement is based on the fact that T determines all possible operations, and the set of values Θ denoted their options in the process of considering the sequence of IT operations under the condition of linearity limitation, fixing the operations applied to a certain message, which is the only restriction on the formation of a sequence of operations that make up information technology. This condition means that no IS operation applied to the message can change the sequence of previously performed operations. This means that when IT is described by a sequence of attributes $a_1 \dots a_{k-1}(t_1 \dots t_{k-1})$, whatever symbol t_k that characterizes the next operation applied to the message is, its writing into a word in the process of creating IT will not change any component of the sequence $t_1 \dots t_{k-1}$.

Within the framework of the model described above, considering the fact that only permitted operations are used in a specific sequence, the task of determining the equivalence of two information technologies leads to the need to create a final procedure that regulates the equivalence of IT attributes by reducing one technology to another using a relation from Θ.

Figure 1 shows an outline flowchart of the procedure for identifying the equivalence of two information technologies (that is, when solving the problem of compliance of the presented information technologies with the general security requirements described by the set (T,Θ)) reflecting the following sequence of actions:

– assessment, or verification of the actual identity of characters of a certain technology ($a_j = b_j$);

– identification of equivalence relationships if the first character is represented as b_1 (for example, $b_1 c_2 \dots c_t^r \sim d_1^r \dots d_s^r$);

– solution of the subproblem of determining equivalence $a_1 \dots a_n$ and $d_1^r \dots d_s^r$ (there may be several of them, that is, branching is possible).

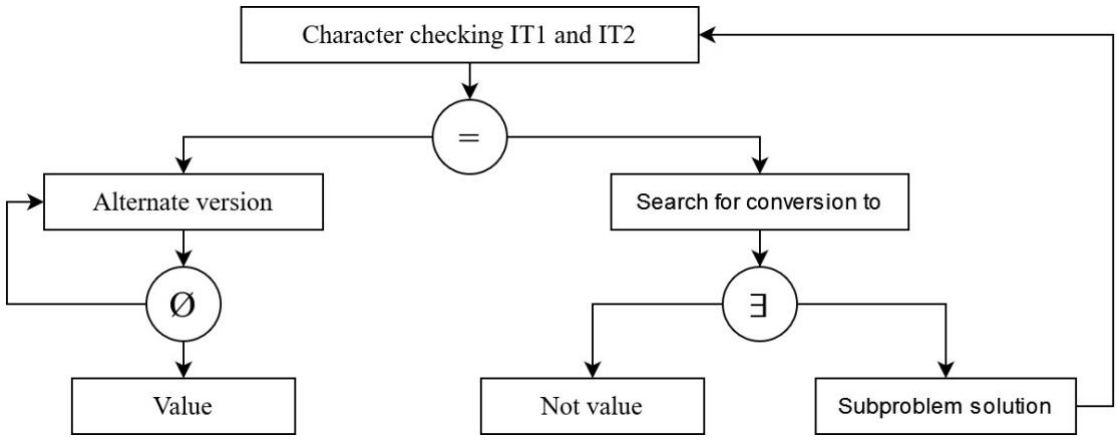

Figure 1. Outline flowchart of the procedure for identifying the equivalence of two information technologies.

Thus, the performed analytical work, based on the principles of variation of variables that describe in one way or another the task of establishing the equivalence of information technologies within a given class, makes it possible to assert that the developed procedure is not final. This can be explained by the fact that a conditional infinite search is possible against the background of the corresponding incessant modifications. The point is that the chain of subtasks can be constantly extended in the process of searching for the required character within the framework of a formalized system of rules. Modifications in this case can provoke the formation of higher-level subtasks at a stage that, in an ideal scenario, would exclude excessive complexity.

Information technology models are easy to describe using graphs based on the sequential attribute assignment algorithm. However, this requires each attribute to strictly correspond to a separate vertex of the graph.

In such a situation, the set of required conditions regarding the solvability of equivalence for a particular information technology or a set of tools and methods for solving the corresponding problems is reduced to the statement presented below. To establish the actual equivalence of arbitrary technologies within a conditional class, if there is a given system of relations in a formalized set of rules, it is required to ensure the implementation of the following conditions: the graph G^1 characterizing system Θ must not have closed paths, while the other graph G^2 characterizing the system must not have two connected closed paths. Here and below, G^1 it is a graph whose vertices are marked with the first characters from the left and right parts of the relations from Θ, and the presence of an arc from vertex a to vertex b indicates the presence of the following relation in Θ: $aa_2 \dots a_n \sim bb_2 \dots b_m$. Graph G^2 is a complement of G^1, and the presence of an arc from vertex a to vertex b indicates the presence of the following relation in Θ: $aa_2 \dots a_n \sim bb_2 \dots b_m$ or $aa_2 \dots a_n \sim b_1 \dots b \dots b_m$.

It should be emphasized that information technologies and acceptable relations of establishing actual equivalence within their framework literally break a lot of information systems into subsets within the framework of conditions and security requirements. This yields the division into classes. Any particular of the latter can be represented as a set of information technologies, in relation to which:

- for a given set of operations, the following condition is satisfied: o ∈ O (or $\{t_1 \dots t_n\}$, $t \in T$);
- with the existing set of equivalence relations, the entire set of formalized rules is fulfilled.
- In addition, it is required that:
- each information technology was reduced to an equivalent set of means, tools and methods for solving the appropriate tasks, but within the framework of a formalized system of rules or relations;
- none of the technologies included in a certain class was reduced to a similar one from the same class within the framework of relations and rules in a formalized system.

Thus, a new contribution to the research area lies in the fact that the authors defined the necessary conditions of equivalence solvability of two information technologies for a given set of admissible transformations, which are possible in the absence of closed paths of special kind in the graph structure of the equivalent transformations. Classes of information technologies with a solvable problem of establishing equivalence and rules for reducing abstract classes to classes of this type by methods of studying their admissible transformations are formulated. It is shown that the process of determining the equivalence of information technologies for the given algorithm within the described classes has polynomial complexity. The practical significance of the obtained results consists in the formation of a new tool for information technology security.

Since the security requirement literally defines a set of formalized rules against the background of the need to compare two conditional information technologies within the framework of establishing the equivalence, a standard is necessary. The formation of a reference technology involves the parallel implementation of operations to create the corresponding class. This is inevitable against the background of the description of the latter. It is possible in the context of a practical task only with knowledge and understanding of certain aspects and the essence of the conditional information technology associated with a particular class. Otherwise, the description is impossible.

4 Results and Discussion

The results of this theoretical study represent the development of theoretical approaches to establishing the equivalence of mathematical structures applied to the information technology model. The equivalence of technologies is something like a property of sequence in terms of the implementation of certain operations within the corresponding information environment for receiving information messages, as a result, analysis in this context can open up opportunities for controlling, and ensuring compliance with security requirements relating to given sets of information arrays represented by messages. The model representation makes it possible to assess the security of various related systems.

The practical implementation of this conceptual approach in the form of an analytical “tool” organized in a certain way is possible only when observing the series formulated in the course of the study, including the necessary requirements for the solvability of the equivalence of two information technologies on a finite set of admissible transformations.

The results are the basis for the possible implementation of projects related to the introduction of the mechanisms for controlling the equivalence of information processes used in electronic document management.

The obtained theoretical results gave an opportunity to:

- define specific requirements for the information technology security model. They are aimed at identifying sequences of attributes within individual parts of the message code, determining the authenticity of the processed technology and its belonging to a particular class. Additionally, these requirements provide secure storage for the rules used to establish technology equivalence within a conditional class;
- perform work aimed at the test solution of the corresponding problem. This refers to the analysis of the information technology equivalence.

Thus, the experimental work made it possible to develop an algorithmically consistent approach establishing the information technology equivalence. It is correct in the context of the previously noted set of means and tools for solving the corresponding problem. In addition, reasonable restrictions were defined for certain classes of information technologies. They contribute to the solvability of establishing actual equivalence.

5 Conclusion

Security assurance for a wide range of information systems implemented in practical and scientific activities in various fields of human activity is a complex, integrated, but very urgent problem. The search for its effective solution is closely connected with successful protection against viruses, the establishment of high-quality (aimed at preventing accidental or purposeful disclosure of confidential information) control over the actions of users of information systems, and with the investment of optimal funds to achieve these goals.

5.1 Findings of the study

The research has formed a tool for analyzing the information technology security by controlling their equivalences. This approach is based on a formal mathematical model of information technology considered in the general case within the framework of a set with minimal restrictions associated with the natural features of information technologies as technologies for the formation of a certain product. The essence of the model is reduced to the implementation of an assessment of the actual security of various related information systems, while it is not assumed that changes in operations aimed at processing information are necessary. The addition of the existing functionality of analytical tools is a sufficient condition.

The obtained theoretical results made it possible to formulate requirements for a simplified model of information technology security, and conduct an experimental study in terms of solving the problem of analyzing the equivalence of information technologies.

5.2 Recommendations for future research

It seems significant and appropriate in the context of future research to analyze the applicability of the presented model for solving many practical problems. This is also true, among other things, for assessing unwanted operations performed by users within the framework of medical information systems.

Statement of conflict of interest

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

Selected findings of this work were obtained under the Grant Agreement in the form of subsidies from the federal budget of the Russian Federation for state support for the establishment and development of world-class scientific centers performing R&D on scientific and technological development priorities dated April 20, 2022, No. 075-15-2022-307.

ORCID iD

Aslan A. Tatarkanov https://orcid.org/0000-0001-7334-6318
Rasul M. Glashev https://orcid.org/0000-0002-8649-9740
Ekaterina S. Nazarova https://orcid.org/0009-0008-7938-7995

References

Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware detection issues, challenges, and future directions: A survey. *Applied Sciences, 12*(17), 8482. https://doi.org/10.3390/app12178482

Al-Asli, M., & Ghaleb, T. A. (2019). Review of signature-based techniques in antivirus products. 2019 International Conference on Computer and Information Sciences (ICCIS). https://doi.org/10.1109/iccisci.2019.8716381

Barbosa, R. R. R., Sadre, R., & Pras, A. (2013). Flow whitelisting in SCADA networks. *International Journal of Critical Infrastructure Protection, 6*(3–4), 150–158. https://doi.org/10.1016/j.ijcip.2013.08.003

Bashendy, M., Tantawy, A., & Erradi, A. (2023). Intrusion response systems for cyber-physical systems: A comprehensive survey. *Computers & Security, 124*, 102984. https://doi.org/10.1016/j.cose.2022.102984

Bist, A. S. (2013). Code emulation technique for computer virus detection. *International Journal of Engineering Sciences and Research Technology*, *2*(12), 3479–3481.

Dhanasekar, D., Di Troia, F., Potika, K., & Stamp, M. (2018). *Detecting Encrypted and Polymorphic Malware Using Hidden Markov Models.* Guide to Vulnerability Analysis for Computer Networks and Systems, 281–299. https://doi.org/10.1007/978-3-319-92624-7_12

Gopinath M., & Sethuraman, S. C. (2023). A comprehensive survey on deep learning based malware detection techniques. *Computer Science Review*, *47*, 100529. https://doi.org/10.1016/j.cosrev.2022.100529

Huh, J. H., Lyle, J., Namiluko, C., & Martin, A. (2011). Managing application whitelists in trusted distributed systems. *Future Generation Computer Systems, 27*(2), 211–226. https://doi.org/10.1016/j.future.2010.08.014

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences, 34*(8), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018

Khayrutdinov, M. M., Golik, V. I., Aleksakhin, A. V., Trushina, E. V., Lazareva, N. V., & Aleksakhina, Y. V. (2022). Proposal of an algorithm for choice of a development system for operational and environmental safety in mining. *Resources, 11*(10), 88. https://doi.org/10.3390/resources11100088

Kirilchuk, S., Reutov, V., Nalivaychenko, E., Shevchenko, E., & Yaroshenko, A. (2022). Ensuring the security of an automated information system in a regional innovation cluster. *Transportation Research Procedia, 63*, 607–617. https://doi.org/10.1016/j.trpro.2022.06.054

Levy, A., & Shalom, B. R. (2020). Online parameterized dictionary matching with one gap. *Theoretical Computer Science, 845,* 208–229. https://doi.org/10.1016/j.tcs.2020.09.016

Ling, X., Wu, L., Zhang, J., Qu, Z., Deng, W., Chen, X., Qian, Y., Wu, C., Ji, S., Luo, T., Wu, J., & Wu, Y. (2023). Adversarial attacks against Windows PE malware detection: A survey of the state-of-the-art. *Computers & Security, 128*, 103134. https://doi.org/10.1016/j.cose.2023.103134

Madan, S., Sofat, S., & Bansal, D. (2022). Tools and techniques for collection and analysis of internet-of-things malware: A systematic state-of-art review. *Journal of King Saud University - Computer and Information Sciences, 34*(10), 9867–9888. https://doi.org/10.1016/j.jksuci.2021.12.016

Meridji, K., Al-Sarayreh, K. T., Abran, A., & Trudel, S. (2019). System security requirements: A framework for early identification, specification and measurement of related software requirements. *Computer Standards & Interfaces, 66*, 103346. https://doi.org/10.1016/j.csi.2019.04.005

Moreira, N., Molina, E., Lázaro, J., Jacob, E., & Astarloa, A. (2016). Cyber-security in substation automation systems. *Renewable and Sustainable Energy Reviews, 54*, 1552–1562. https://doi.org/10.1016/j.rser.2015.10.124

Rehman, Z.-U., Khan, S. N., Muhammad, K., Lee, J. W., Lv, Z., Baik, S. W., Shah, P. A., Awan, K., & Mehmood, I. (2018). Machine learning-assisted signature and heuristic-based detection of malwares in Android devices. *Computers & Electrical Engineering, 69*, 828–841. https://doi.org/10.1016/j.compeleceng.2017.11.028

Seo, J., & Lee, S. (2018). Abnormal behavior detection to identify infected systems using the APChain algorithm and behavioral profiling. *Security and Communication Networks, 2018*, 1–24. https://doi.org/10.1155/2018/9706706

Sharma, A., Gupta, B. B., Singh, A. K., & Saraswat, V. K. (2022). Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense. *Computers & Security*, *115*, 102627. https://doi.org/10.1016/j.cose.2022.102627

Shaukat, K., Luo, S., & Varadharajan, V. (2022). A novel method for improving the robustness of deep learning-based malware detectors against adversarial attacks. *Engineering Applications of Artificial Intelligence*, *116*, 105461. https://doi.org/10.1016/j.engappai.2022.105461

Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. *Computer Science Review*, *45*, 100496. https://doi.org/10.1016/j.cosrev.2022.100496

Sibi Chakkaravarthy, S., Sangeetha, D., & Vaidehi, V. (2019). A Survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, 1–23. https://doi.org/10.1016/j.cosrev.2019.01.002

Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A Cyber security analysis. *Computers & Security*, *112*, 102536. https://doi.org/10.1016/j.cose.2021.102536

Tatarkanov, A., Lampezhev, A., Polezhaev, D., & Tekeev, R. (2022a). Development of components of a distributed fault tolerant medical data storage system. *International Journal of Engineering Trends and Technology*, *70*(12), 76–89. https://doi.org/10.14445/22315381/ijett-v70i12p209

Tatarkanov, A., Lampezhev, A., Polezhaev, D., & Tekeev, R. (2022b). Suboptimal biomedical diagnostics in the presence of random perturbations in the data. *International Journal of Engineering Trends and Technology*, *70*(11), 129–137. https://doi.org/10.14445/22315381/ijett-v70i11p213

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Vouvoutsis, V., Casino, F., & Patsakis, C. (2022). On the effectiveness of binary emulation in malware classification. *Journal of Information Security and Applications*, *68*, 103258. https://doi.org/10.1016/j.jisa.2022.103258

Wang, G.-Y. (2022). Churn prediction for high-value players in freemium mobile games: Using random under-sampling. *Statistika: Statistics and Economy Journal*, *102*(4), 443–453. https://doi.org/10.54694/stat.2022.18

Wang, Y., Jia, P., Peng, X., Huang, C., & Liu, J. (2023). BinVulDet: Detecting vulnerability in binary program via decompiled pseudo code and BiLSTM-attention. *Computers & Security*, *125*, 103023. https://doi.org/10.1016/j.cose.2022.103023

Wang, Y., Li, Q., Chen, Z., Zhang, P., & Zhang, G. (2020). A survey of exploitation techniques and defenses for program data attacks. *Journal of Network and Computer Applications*, *154*, 102534. https://doi.org/10.1016/j.jnca.2020.102534

Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., & Han, H. (2022). A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security*, *116*, 102675. https://doi.org/10.1016/j.cose.2022.102675

Zelinka, I., Das, S., Sikora, L., & Šenkeřík, R. (2018). Swarm virus - Next-generation virus and antivirus paradigm? *Swarm and Evolutionary Computation*, *43*, 207–224. https://doi.org/10.1016/j.swevo.2018.05.003

Zhai, X., Appiah, K., Ehsan, S., Howells, G., Hu, H., Gu, D., & McDonald-Maier, K. (2015). Exploring ICMetrics to detect abnormal program behaviour on embedded devices. *Journal of Systems Architecture*, *61*(10), 567–575. https://doi.org/10.1016/j.sysarc.2015.07.007