Information systems. Computer sciences. Issues of information security

Информационные системы. Информатика. Проблемы информационной безопасности

UDC 519.95:621.3
https://doi.org/10.32362/2500-316X-2025-13-1-28-37
EDN BUGTUV

RESEARCH ARTICLE

Probabilistic characteristics analysis of virus attack effect on digital substations

Alexander S. Leontyev,
Dmitry V. Zhmatov @

MIREA – Russian Technological University, Moscow, 119454 Russia
@ *Corresponding author, e-mail: zhmatov@mirea.ru*

Abstract

Objectives. This study aims to create analytical methods for evaluating the probabilistic safety characteristics of information and software elements in digital substations in order to ensure security in different virus scenarios.

Methods. The methods of reliability theory, random process theory, and recovery theory were used.

Results. The derived integral ratios were further used to estimate the probability characteristics of information processing security when performing functional tasks in various scenarios of attacks on digital substations, as well as multiple technologies used for protection against such threats. Numerical studies of safe information processing probability of different intensities of attacks and times of their activation were conducted, in order to consider the frequency of diagnostics of the system by the service personnel and customer requirements for the safe operation of the system in a certain period. We performed calculations for various protection technologies against similar attacks on digital substations. A protection technology with system diagnostic deterministic frequency can support customer requirements in the event of accidental and relatively rare virus attacks. Security technologies consider different maintenance personnel operation modes to ensure customer fulfillment requirements for safe information processing probability and the case of deliberate attacks on digital substations in each period.

Conclusions. The technologies considered herein for information protection from attacks on digital substations can provide the necessary level of information security system operation for all types of threats. These technologies can be applied when the system diagnostics frequency increases from twice an hour to at least once every 25 minutes. Our findings underline the importance of timely monitoring of ever-changing attack environments for digital substations.

Keywords: digital substations, flow characteristic, viruses, safe operation probability, information, and computer systems

• **Submitted:** 12.04.2024 • **Revised:** 12.09.2024 • **Accepted:** 21.11.2024

For citation: Leontyev A.S., Zhmatov D.V. Probabilistic characteristics analysis of virus attack effect on digital substations. *Russian Technological Journal.* 2025;13(1):28–37. https://doi.org/10.32362/2500-316X-2025-13-1-28-37, https://elibrary.ru/BUGTUV

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Анализ вероятностных характеристик воздействия вирусных атак на цифровые подстанции

А.С. Леонтьев,
Д.В. Жматов [@]

МИРЭА – Российский технологический университет, Москва, 119454 Россия
[@] *Автор для переписки, e-mail: zhmatov@mirea.ru*

Резюме

Цели. Цель данного исследования заключается в создании аналитических методов для оценки вероятностных характеристик безопасности информационных и программных элементов цифровых подстанций. Эти методы направлены на обеспечение кибербезопасности в условиях различных сценариев воздействия вирусов.

Методы. Использованы методы, базирующиеся на теории надежности, теории случайных процессов и теории восстановления.

Результаты. Выведены интегральные соотношения, которые позволяют оценить вероятностные характеристики безопасности обработки информации при выполнении функциональных задач в различных сценариях атак на цифровые подстанции, а также при использовании различных технологий защиты от подобных угроз. Проведены численные исследования вероятности безопасной обработки информации при различной интенсивности атак и времени их активации с учетом частоты проведения диагностики системы обслуживающим персоналом и требований заказчика к безопасному функционированию системы в определенный период времени. Расчеты выполнены для различных технологий защиты от подобных атак на цифровые подстанции. Показано, что технология защиты с детерминированной частотой диагностики системы может обеспечить требования заказчика к безопасности только при случайных и относительно редких вирусных атаках. Технологии защиты, учитывающие различные режимы работы обслуживающего персонала, могут обеспечить выполнение требований заказчика по вероятности безопасной обработки информации в заданный период времени и при преднамеренных атаках на цифровые подстанции.

Выводы. Рассмотренные технологии защиты информации от атак на цифровые подстанции могут обеспечить необходимый уровень безопасности функционирования информационной системы для всех видов угроз при условии увеличения частоты диагностики системы с 2 раз в 1 ч до не реже 1 раза в 25 мин. Это подчеркивает важность активной мониторинговой политики в условиях постоянно меняющейся среды атак для цифровых подстанций.

Ключевые слова: цифровые подстанции, характеристика потоков, вирусы, вероятность безопасного функционирования, информационно-вычислительные системы

• **Поступила:** 12.04.2024 • **Доработана:** 12.09.2024 • **Принята к опубликованию:** 21.11.2024

Для цитирования: Леонтьев А.С., Жматов Д.В. Анализ вероятностных характеристик воздействия вирусных атак на цифровые подстанции. *Russian Technological Journal.* 2025;13(1):28–37. https://doi.org/10.32362/2500-316X-2025-13-1-28-37, https://elibrary.ru/BUGTUV

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

Modern information computer systems (ICS) are part of the control loop of socioeconomic and sociopolitical processes. They enable the main stages of analysis of the current situation to be automated, the emergence and development of crisis situations to be identified, and recommendations for their elimination and prevention to be formed. ICSs also provide analytically processed and summarized information for supporting the decision-making process [1]. Therefore, such systems are subject to increased requirements for timeliness and reliability of the information processed.

The software and hardware tools of an ICS should provide support for document preparation processes, taking into account possible interferences, including the impact of viruses, failures, malfunctions, and information distortion [2]. The integrated use of analytical methods to study virus threats and modeling on their basis the processes of virus impact on the information system with the help of the *KOK* tool-modeling software complex was considered for the first time in the work of A.I. Kostogryzov and G.A. Reznikov [3]. In order to facilitate the joint use of the original multilevel network analytical models of TDF research taking into account distortions in the input information [2] and analytical models that take into account information distortion by viruses, it seems reasonable to extend the class of models considered in [3] using recovery theory methods, as demonstrated in [4].

The studies [2, 5, 6] consider issues of evaluating the probabilistic-temporal characteristics of information processing taking into account failures, malfunctions, and distortions of input information under the limitations on the service time set by the customer. These studies also evaluate the reliability characteristics of ICS hardware, software and networks, which are the source of information for situation centers. At present, insufficient attention is paid to assessing the impact of viruses on the probabilistic-temporal characteristics of information processing, taking into account customer requirements for the security of system operation and the range of information protection technologies used by service personnel. Therefore, the analytical evaluation of probabilistic characteristics of information and software resources security under various scenarios of virus impact and information protection technologies appears a relevant research task.

The works [7–11] address computer viruses and their impact on data security, the main ways of virus penetration into the system, as well as a comparative analysis of antivirus programs. The articles [12–15] propose analytical models for an accurate determination of the intensity of virus attacks. The results obtained can be used as initial data for the development of a higher-level information security model, considered in the present article.

Data security is acquiring particular significance in the modern digital world, where information technology plays a key role in managing various systems, including energy networks. One of the main challenges in this context is the protection of digital substations from malicious impacts such as viruses.

For effective protection against viruses in digital substations, evaluation models that can predict the probabilistic characteristics of the possible impact of viruses on computer systems are needed. Such models can be useful in developing protection strategies and making decisions about the security of the information infrastructure.

One of the key elements of evaluation models is to consider the probability of viruses affecting digital substations. This requires an analysis of various attack scenarios and evaluation of the probability of their occurrence. In addition, it is important to consider the probability of detection and removal of viruses, as well as their potential impact on system operation.

Another important aspect to consider is the temporal aspect of attacks. Viruses may be active at specific time intervals or may be continuous. In order to properly assess risks and develop appropriate countermeasures, evaluation must take into account such temporal parameters. The various defense technologies which can be applied to prevent and detect virus attacks on digital substations must also be considered. Evaluation models should employ the effectiveness of these technologies and their ability to secure the system.

1. MAJOR CYBERATTACKS ON DIGITAL POWER SUBSTATIONS

Digital substations are a critical part of modern infrastructure, providing reliable transmission and distribution of electricity. However, as technology advances, digital substations are becoming more vulnerable to cyberattacks.

Table 1 presents the names of the main virus attacks on digital power substations.

The type of virus attack can impact various aspects of a digital power substation, including:

- *System functionality*. Virus attacks can disrupt the normal functioning of control, monitoring, and protection systems, thus leading to system failure or malfunction.
- *Data security*. Some types of viruses can be directed to steal or destroy data stored in a digital substation, thus leading to leaks of sensitive information or loss of important data.
- *System integrity*. Virus attacks can damage hardware or software components of a substation, thus resulting in loss of or damage to equipment and interruption of operations.

- *System availability*. Some virus attacks may cause denial of service or overload network resources, thus resulting in temporary system unavailability to process requests to operators.
- *Personnel safety*. Virus attacks can create dangerous situations for personnel working at the substation, for example by changing system parameters without their knowledge or possibly causing physical damage to equipment.
- *Financial losses*. A successful virus attack can cause significant financial losses associated with system restoration, lost revenue due to equipment downtime, and consumer reimbursements.

Threats from internal users, such as employees of energy companies, also pose a serious risk to the security of digital substations. Unauthorized access to systems, loss of confidential information or malicious actions within the company can have disastrous consequences.

Measures for preventing potential consequences of virus attacks include:

- regular updates of software and protection systems;
- introduction of multi-level authentication for access to substation control systems;
- training personnel on the basics of cybersecurity and identification of phishing attacks;
- monitoring network activity in order to detect suspicious behavior;
- implementation of clear security policies and access control to critical systems.

Table 1. Virus attacks on digital power substation

Name of attack	Description	Potential consequences
SQL-injection	Introduction of malicious SQL code into an application or database through incorrect processing of the user input	Gaining unauthorized access to data, changing or deleting information in the database
Malicious software	Installing malicious software on substation computers or devices for the purpose of stealing the data, interrupting operations, or controlling the system	Substation disruption, loss of data confidentiality, interruption of power supply
Phishing	Sending fake emails to deceive substation personnel, to gain access to systems or confidential information	Unauthorized access to systems, leakage of confidential data
DDos-attack[1]	Overloading the network or substation servers by sending a large number of requests, in order to disrupt operations	Failure of service, temporary or prolonged interruption of substation operation
GOOSE-messages[2] spoofing	Gaining unauthorized access to substation systems through the use of stolen credentials	Potential change of system operation parameters, disruption of system operation, threat to power supply security
Ransomware	Infection of the system with malicious program code, blocking access to data, demanding a ransom in order to restore access	Data loss, substation interruption, financial losses
Man-in-the-Middle	Intercept and alter communications between substation devices such that an attacker can manipulate data	Possibility of data manipulation and distortion, interruption of information exchange
Zero-Day Exploit	Exploitation of a vulnerability in software that has not yet been discovered and fixed by the developers	Unauthorized access, malware introduction, potential threat to system security
Spoofing (falsification)	Forging addresses or identities to create a false perception of authenticity or authorization	Breach of authentication, possible misleading of the control system
Attack on the hardware	Attempting to affect substation hardware, such as power transformers or circuit breakers	Potential damage to equipment, interruption of power supply

[1] Distributed denial of service.
[2] Generic object-oriented substation event is a protocol designed for communication between relay protection devices by transmitting data digitally over Ethernet.

Cyberattacks on digital power substations pose a serious threat to the energy infrastructure. Understanding the main types of attacks and taking appropriate measures for their prevention is an important task in ensuring the safety and reliability of substations in the face of ever-increasing cyber threats.

2. FORMULATION AND SOLUTION OF THE PROBLEM OF EVALUATING PROBABILISTIC SAFETY CHARACTERISTICS FOR DIGITAL SUBSTATIONS

Preventive diagnostic tools are assumed to be able to detect all infiltrated viruses and traces of their impact. Recovery tools are assumed to be able to fully restore the violated integrity of information and program resources of the *i*th type. As a result of diagnostics, viruses are eliminated. The integrity of information and program resources is then restored if distortions are detected, and interrupted requests can be processed again after restoration of system integrity. Evaluation using analytical approaches is based on the application of random process recovery theory methods [4].

In order to perform the necessary analytical transformations, it is required to set the following parameters:

$V_{imp}(t)$, distribution function (DF) of time between virus impacts on the system;

$V_{act}(t)$, DF of the virus activation time after it has entered the system;

$F_{diag}(t)$, DF of time between diagnostics;

$G_i(t)$, the DF of information processing time of the *i*th type, including waiting time in the queue and processing time itself.

The distribution functions used are approximated in analytical models by two-parameter Erlangian or hyperexponential DFs within the framework of second-order theory on mathematical expectations and variance [4].

DF moments $G_i(t)$ (mathematical expectation and variance) are estimated using multilevel models which describe information processing processes in the digital substation system. These models are formalized with the multilevel analytical nested models (mass service networks), using technological processing operations, emerging hardware and software failures [2]. This approach is original in terms of the temporal characteristics of request processing in nested hardware-level network models. Such an approach is relatively independent of the type of DFs which characterize the flows of requests at this level and the type of flows in the network model of the software level. This allows the flows at the hardware level to be approximated by Poisson flows. The approach enables not only the hardware-level network model to be decomposed, but also the multilevel model into network models of different levels. These can then be investigated by analytical methods. In particular, the hardware-level model is analyzed using the analytical methods of intermediate mass service theory. The software-level network model, which uses the approximation of real distributions by Erlang for the first two points, and hyperexponential distributions using the Erlang stage method, is reduced to an equivalent Markovian model. This is then assessed using well-known analytical methods.

We consider a regeneration process in which the regeneration points correspond to the start time of the next antivirus diagnosis of digital substations.

Let $\{t_n\}_{n=1}^{\infty}$ be the recovery process, moments t_n of which correspond to the time of the next antivirus diagnostics of the system.

If the intervals between diagnostics τ are the same, then the following formula is valid:

$$\xi_i(t) = \int_0^{t_{n+1}-t} V_{imp}(t - t_n - \theta) V_{act}(\theta) dG_i(\theta), \quad (1)$$

wherein $\xi_i(t)$ is the probability that during the processing of the *i*th type of request the processed information will be infected with viruses on the time interval $t_n \le t \le t_{n+1}$, $n \ge 1$.

In accordance with the basic properties of recovery processes and the limit theorem of recovery theory, the probability of information distortion by viruses $P_{vir(i)}$ is defined by relation (2), and the probability that information is not distorted is estimated by formula (3):

$$P_{vir(i)} = \frac{1}{F_{diag}^{(1)}} \int_0^{\infty} \left\{ \left[1 - F_{diag}(t) \right] \int_0^{\tau - t} V_{imp}(t - \theta) V_{act}(\theta) dG_i(\theta) \right\} dt, \quad (2)$$

$$P_{imp(i)} = 1 - P_{vir(i)}. \quad (3)$$

Over a given period of time T_{giv} from the moment of the last prophylaxis under the condition $T_{giv} < F_{diag}^{(1)}$, the probability of the hazardous impact absence is defined by the ratio:

$$P_{imp(i)}(T_{giv}) = 1 - \int_0^{T_{giv}} V_{imp}(T_{giv} - \theta) V_{act}(\theta) d\theta. \quad (4)$$

We use formula (4) to estimate the probability of the absence of dangerous effects without any diagnostics. It assumes that by the onset of the period T_{giv}, the integrity of information resources is ensured.

3. TECHNOLOGIES FOR PROTECTING INFORMATION SYSTEMS FROM HAZARDOUS IMPACTS

When implementing information technologies in digital substations, the frequency of routine diagnostics by maintenance personnel depends significantly on the frequency of exposure to threat sources, such as viruses. When making calculations, we will consider different scenarios of threats (viruses) impact on digital substations and different scenarios of routine diagnostics by maintenance personnel. Due to insufficient statistics concerning the impact of viruses on digital substations, we will assume that different digital substations use the same virus protection technologies.

Routine diagnostics and system integrity control of information and software resources are performed at certain intervals during implementation of protection technologies. The system integrity is restored using the methods provided for the purpose of detection of inactivated sources of danger (viruses) or traces of their impact.

We examine the probability of secure information processing at different levels of intensity of viruses and their activation time, different frequency of system diagnostics by maintenance personnel, and given customer requirements for the probability of secure system operation.

The following designations for the initial data are used in the calculations:

j is an index of scenario variant and protection method;

$\sigma_j = \frac{1}{V_{\text{imp}}^{(1)}}$ is the frequency of impact on the system for virus introduction;

$\beta_j = F_{\text{act}}^{(1)}$ is the average activation time of the infiltrating virus in jth scenario;

$T_{\text{int.}j} = F_{\text{diag.}j}^{(1)}$ is the average time interval between the end of the previous diagnosis and the beginning of the next one in jth scenario;

$T_{\text{diag.}j}$ is the duration of diagnostics, including restoration of system integrity (set in advance).

The customer should impose requirements on the following parameters:

$P_{\text{giv.}j}$ is the minimum permissible probability of safe operation of the system (predefined by the customer).

The following indicators are evaluated:

$P_{\text{imp.}j}$ is a probability of absence of hazardous impact during a specified period $T_{\text{giv.}j}$ in jth scenario.

From the user point of view, the system is assumed to be safe for a given time T_{giv} = 1 day, if no hazardous impact occurs during this time or if all sources of danger are detected immediately when they enter the system. Moreover, these models assume that after diagnostics, as well as after integrity restoration, the system remains in a completely safe state.

The average time required for a diagnostic procedure, including repair work, is estimated to be 60 s. The initial data for calculations is presented in Table 2.

Given insufficient statistics on the impact of viruses on digital substations, virus exposure scenarios, including virus intensity and activation time, were chosen according to the data presented in [3]. Estimation calculations were performed using exponential distribution functions. In this asymptotic case, the analytical relations obtained using recovery theory methods and the analytical formulas presented in [3] give the same results. Therefore, as in [3], the tool-modeling complex for assessing the quality of functioning of *KOK* information systems was used for the preliminary assessment calculations of the impact of viruses on electric substations. In the future, as in [4], real distributions will be approximated by two-parameter Erlangian or hyperexponential distributions for the first two moments.

Figure 1 presents the calculation results of the safe operation probability of digital substations in a variety of threat impact scenarios, and the routine diagnostics scenarios of the information integrity and program resources by maintenance personnel $(j = \overline{1,10})$ in accordance with the given initial data (Table 2).

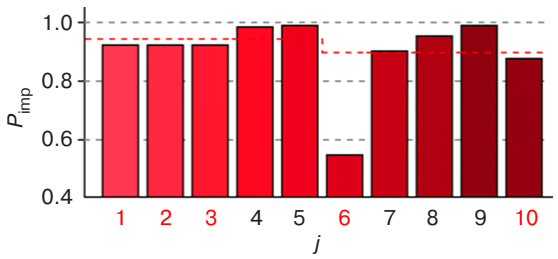

Fig. 1. Probability of safe operation of the information system in different threat scenarios $(j = \overline{1,10})$ for a digital substation

Based on the above preliminary assessment calculation and the data presented in Table 2, the following conclusions can be drawn.

1. Protection of digital substations from deliberate threats with the frequency of impact once a day is provided by diagnostics of information and program resources at least once every 6 h (Fig. 4, j = 7, 8, 9).
2. At the same time, for threats occurring on average once every 1 h, the probability of no dangerous virus exposure during a day would be 0.88 at a diagnostic frequency of once every 30 min, less than the specified 0.9.

We examine the question concerning when diagnostic modes of information and software resources of digital substations can provide the required security of digital substations for the most dangerous scenario of virus attacks. These are when new viruses penetrate the system on average once every 1 h with their activation time of 1 h.

Table 2. Security evaluations of information system operation at a digital substation

Threat characteristics			Characteristics of the substation service device			Customer's requirements
j	σ_j	β_j	$T_{int,j}$	$T_{diag,j}$	$T_{giv,j}$	$P_{giv,j}$
1	1 week^{-1}	6 h	1 week	1 min	1 day	0.95
2	1 week^{-1}	6 h	3 days	1 min	1 day	0.95
3	1 week^{-1}	6 h	1 day	1 min	1 day	0.95
4	1 week^{-1}	6 h	6 h	1 min	1 day	0.95
5	1 week^{-1}	6 h	3 h	1 min	1 day	0.95
6	1 day^{-1}	3 h	1 day	1 min	1 day	0.90
7	1 day^{-1}	3 h	6 h	1 min	1 day	0.90
8	1 day^{-1}	3 h	3 h	1 min	1 day	0.90
9	1 day^{-1}	3 h	1 h	1 min	1 day	0.90
10	1 h^{-1}	1 h	30 min	1 min	1 day	0.90

Figures 2–5 show the dependencies of the probability of the absence of dangerous impacts on information resources of digital substations for the most dangerous scenario of deliberate virus impacts $P_{imp.10}$ ($j = 10$). These are in the event of changes in the intensity of threat impacts, average virus activation time, interval between diagnostics and probabilistic-time requirements of the customer.

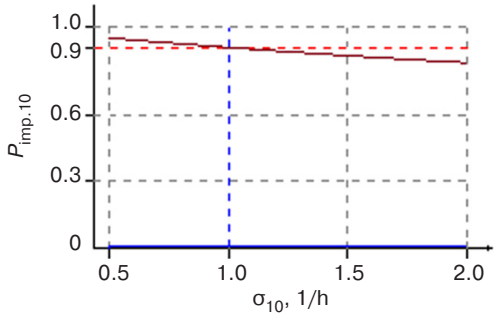

Fig. 2. Dependence of the value of $P_{imp.10}$ on the frequency of exposure to threats

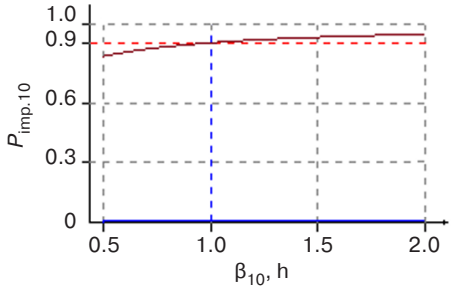

Fig. 3. Dependence of the value of $P_{imp.10}$ on the average time of threat activation

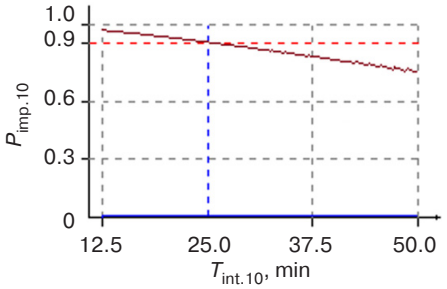

Fig. 4. Dependence of the value of $P_{imp.10}$ on the average interval between diagnostics

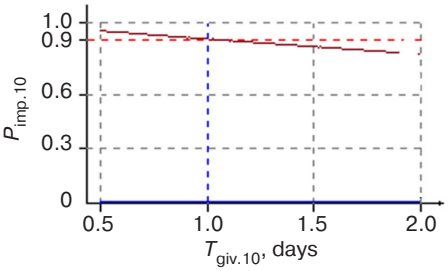

Fig. 5. Dependence of the value of $P_{imp.10}$ on the time set by the customer $T_{giv.10}$

The calculation results presented in Figs. 2–5 show that the system security decreases noticeably with increasing virus intensity. In all the scenarios considered, an increase in the virus activation time leads to an increase in and the system security. When the time of absence of virus influences T_{giv} set by the customer decreases, the system security increases in all threat scenarios and protection methods.

The results obtained indicate that when system diagnostics is implemented every 25 min rather than once every 1 h (shown in Fig. 4), the protection of digital substations from the most dangerous scenarios of virus impact can provide the required security of information resources of digital substations while meeting the specified customer requirements for the probability of safe operation.

These scenarios of virus threats and ways to combat them are general in nature and can be applied to study the security of various digital substations.

CONCLUSIONS

This study provides a review of the main types of cyberattacks on digital power substations, along with their potential consequences and prevention measures.

We established integral relations that allowed us to evaluate the probabilistic characteristics of safe information processing of digital substations under different scenarios of virus exposure, as well as when using different technologies of information protection from dangerous influences. These ratios provide an opportunity to analyze the probability of safe information processing of digital substations in different levels of virus impact intensity, virus activation time, frequency of diagnostics by maintenance personnel and specified customer requirements for the probability of safe operation of the message management system in digital substations.

We conduct calculations for different technologies of the information protection of digital substations from dangerous influences. Particular attention was paid to the most dangerous scenarios of virus impact and to the protection technology which ensures the customer-defined safety of digital substations functioning under all considered threats. An important conclusion is that by implementing this technology and reducing the interval of diagnostics of information resources of digital substations to 25 min, the level of safety of digital substations system operation can be significantly increased.

The results obtained provide practically applicable recommendations to ensure the security of information resources in digital substations using modern technologies of protection against virus attacks. The findings are relevant in the context of the growing complexity of threats and high dynamics of digital technology development, emphasizing the need for effective measures to ensure the security of digital substation information systems.

Authors' contributions

A.S. Leontyev—developed integral equations to assess the probabilistic characteristics of information processing security; conducted numerical studies on the probability of secure information processing under varying attack intensities, activation times, and system diagnostic frequencies; analyzed the impact of a deterministic diagnostic frequency on meeting customer safety requirements under random and infrequent attacks.

D.V. Zhmatov—investigated the effectiveness of various protection technologies against attacks on digital substations; analyzed protection technologies that consider the operating modes of maintenance personnel and their impact on meeting customer requirements; formulated conclusions about the need to increase system diagnostic frequency to ensure security under deliberate attacks; emphasized the importance of an active monitoring policy in the changing threat landscape for digital substations.

REFERENCES

1. Starovoitov A.V., Starikov P.P., Dubitsky K.A., Lukyanov S.E., Pavlov L.P., Simonov V.M., Syedin D.Yu. Computerized complex of federal information systems for supporting decision-making in the field of science and technology. *Informatizatsiya i svyaz' = Informatization and Communication*. 2021;6:7–19 (in Russ.). https://doi.org/10.34219/2078-8320-2021-12-6-7-19
2. Leontyev A.S. Multilevel Analytical and Analytical-Simulation Models for Evaluating the Probabilistic and Temporal Characteristics of Multimachine Computing Complexes with Regard to Reliability. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal = International Research Journal*. 2023;5(131) (in Russ.). https://doi.org/10.23670/IRJ.2023.131.8
3. Kostogryzov A.I., Reznikov G.Y. Modeling of Hazardous Impact Processes on Protected Information System. *Informatsionnye tekhnologii v proektirovanii i proizvodstve = Information Technologies in Design and Production*. 2004;2:17–27 (in Russ.).
4. Gusev K.V., Leontiev A.S. Theoretical Development of Models for the Assessment of Security against Unauthorized Access and Preservation of the Confidentiality of the Information Used. *IT Standard*. 2021;4(29):38–44 (in Russ.).
5. Akimova G.P., Solovyev A.V., Tarkhanov I.A. Modeling the reliability of distributed information systems. *Informatsionnye tekhnologii i vychislitel'nye sistemy = Journal of Information Technologies and Computing Systems*. 2019;3:70–86 (in Russ.). https://doi.org/10.14357/20718632190307
6. Pavsky V.A., Pavsky K.V. Mathematical Model for Calculating Reliability Indicators of Scalable Computer Systems Considering Switching Time. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences*. 2020;2(212): 134–145 (in Russ.). https://doi.org/10.18522/2311-3103-2020-2-134-145

7. Minitaeva A.M., Sokolov A.V. Main Ways of Penetration and Impact of File Viruses on the System. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*. 2023;4–3(79):56–60 (in Russ.). https://doi.org/10.24412/2500-1000-2023-4-3-56-60
8. Litvinov P.V. Simulation modeling of information security issues as a tool for assessing security and cost optimization. *Mir komp'yuternoi avtomatizatsii = Computer Automation World*. 2016;1:43–53 (in Russ.).
9. Blazutskaya E.Y., Sharafutdinov A.G. Next Generation Viruses and Antiviruses. *NovaInfo.ru*. 2015;1(35):92–94 (in Russ.).
10. Popov I.O., Marunko A.S., Petrov O.I., Oleinik A.A. Viruses and Antivirus Programs in Information Security. *Nauchnye zapiski molodykh issledovatelei = Scientific Notes of Young Scientists*. 2020;8(4):74–80 (in Russ.).
11. Sidenko G.A., Redko G.V., Beznos O.S. Comparative Analysis of Antivirus Programs. *StudNet*. 2020;9:676–680 (in Russ.).
12. Zavodtsev I.A., Borisov M.A., Bondarenko M.M., Meleshko V.A. Refined Method of Analytical Modeling of Viral Software Propagation Processes for Assessing Security of Informatization Objects. *Computational Nanotechnology*. 2022;9(1):11–20 (in Russ.).
13. Boyko A.A. Method of Analytical Modeling of Viruses Propagation Process in Computer Networks with Different Topology. *Trudy SPIIRAN = SPIIRAS Proceedings*. 2015;5(42):196–211 (in Russ.). https://doi.org/10.15622/sp.42.4
14. Magazev A.A., Tsyrulnik V.F. Investigation of a Markov Model for Computer System Security Threats. *Aut. Control Comp. Sci.* 2018;52(7):615–624. https://doi.org/10.3103/S0146411618070180
[Original Russian Text: Magazev A.A., Tsyrulnik V.F. Investigation of a Markov Model for Computer System Security Threats. *Modelirovanie i analiz informatsionnykh sistem*. 2017;24(4):445–458 (in Russ.). https://doi.org/10.18255/1818-1015-2017-4-445-458]
15. Kotenko I.V., Vorontsov V.V. Analytical Models of Network Worms Propagation. *Trudy SPIIRAN = SPIIRAS Proceedings.* 2007;4:208–224 (in Russ.). https://doi.org/10.15622/sp.4.15

СПИСОК ЛИТЕРАТУРЫ

1. Старовойтов А.В., Стариков П.П., Дубицкий К.А., Лукьянов С.Э., Павлов Л.П., Симонов В.М., Съедин Д.Ю. Комплекс автоматизированных государственных информационных систем поддержки управленческих решений в сфере науки и техники. *Информатизация и связь*. 2021;6:7–19. https://doi.org/10.34219/2078-8320-2021-12-6-7-19
2. Леонтьев А.С. Многоуровневые аналитические и аналитико-имитационные модели оценки вероятностно-временных характеристик многомашинных вычислительных комплексов с учетом надежности. *Международный научно-исследовательский журнал.* 2023;5(131). https://doi.org/10.23670/IRJ.2023.131.8
3. Костогрызов А.И., Резников Г.Я. Моделирование процессов опасного воздействия на защищаемую информационную систему. *Информационные технологии в проектировании и производстве*. 2004;2:17–27.
4. Гусев К.В., Леонтьев А.С. Теоретическое развитие моделей для оценки защищенности от несанкционированного доступа и сохранения конфиденциальности используемой информации. *ИТ Стандарт*. 2021;4(29):38–44.
5. Акимова Г.П., Соловьев А.В., Тарханов И.А. Моделирование надежности распределенных вычислительных систем. *Информационные технологии и вычислительные системы* (*ИТиВС*). 2019;3:70–86. https://doi.org/10.14357/20718632190307
6. Павский В.А., Павский К.В. Математическая модель для расчета показателей надежности масштабируемых вычислительных систем с учетом времени переключения. *Известия ЮФУ. Технические науки*. 2020;2(212):134–145. https://doi.org/10.18522/2311-3103-2020-2-134-145
7. Минитаева А.М., Соколов А.В. Основные способы проникновения и воздействия файловых вирусов на систему. *Международный журнал гуманитарных и естественных наук*. 2023;4–3(79):56–60. https://doi.org/10.24412/2500-1000-2023-4-3-56-60
8. Литвинов П.В. Имитационное моделирование вопросов информационной безопасности как инструмент оценки защищенности и оптимизации затрат. *Мир компьютерной автоматизации.* 2016;1:43–53.
9. Блазуцкая Е.Ю., Шарафутдинов А.Г. Вирусы нового поколения и антивирусы. *NovaInfo.ru*. 2015;1(35):92–94.
10. Попов И.О., Марунько А.С., Петров О.И., Олейник А.А. Вирусы и антивирусные программы в информационной безопасности. *Научные записки молодых исследователей.* 2020;8(4):74–80.
11. Сиденко Г.А., Редько Г.В., Безнос О.С. Сравнительный анализ антивирусных программ. *Научно-образовательный журнал для студентов и преподавателей «StudNet»*. 2020;9:676–680.
12. Заводцев И.А., Борисов М.А., Бондаренко М.М., Мелешко В.А. Уточненный способ аналитического моделирования процессов распространения вирусного программного обеспечения для оценки защищенности объектов информатизации. *Computational nanotechnology*. 2022;9(1):11–20.
13. Бойко А.А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры. *Труды СПИИРАН*. 2015;5(42):196–211. https://doi.org/10.15622/sp.42.4
14. Магазев А.А., Цырульник В.Ф. Исследование одной марковской модели угроз безопасности компьютерных систем. *Моделирование и анализ информационных систем*. 2017;24(4):445–458. https://doi.org/10.18255/1818-1015-2017-4-445-458
15. Котенко И.В., Воронцов В.В. Аналитические модели распространения сетевых червей. *Труды СПИИРАН*. 2007;4:208–224. https://doi.org/10.15622/sp.4.15

About the authors

Alexander S. Leontyev, Cand. Sci. (Eng.), Senior Researcher, Associate Professor, Department of Mathematical Support and Standardization, Institute of Information Technologies MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: leontev@mirea.ru. RSCI SPIN-code 5798-9721, https://orcid.org/0000-0003-3673-2468

Dmitry V. Zhmatov, Cand. Sci. (Eng.), Associate Professor, Department of Mathematical Support and Standardization, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: zhmatov@mirea.ru. Scopus Author ID 56825948100, RSCI SPIN-code 2641-6783, https://orcid.org/0000-0002-7192-2446

Об авторах

Леонтьев Александр Савельевич, к.т.н., старший научный сотрудник, доцент кафедры математического обеспечения и стандартизации информационных технологий, Институт информационных технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: leontev@mirea.ru. SPIN-код РИНЦ 5798-9721, https://orcid.org/0000-0003-3673-2468

Жматов Дмитрий Владимирович, к.т.н., доцент, доцент кафедры математического обеспечения и стандартизации информационных технологий, Институт информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: zhmatov@mirea.ru. Scopus Author ID 56825948100, SPIN-код РИНЦ 2641-6783, https://orcid.org/0000-0002-7192-2446

Translated from Russian into English by Lyudmila O. Bychkova
Edited for English language and spelling by Dr. David Mossop