UDC 004.056.2-5:681.5.09

Modern methods for protecting and storing data in computer systems to ensure their fault tolerance

Alina Yanko, Oleksii Mychailichenko and Alina Hlushko

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, 36011, Ukraine

Abstract

The study's relevance stems from the fact that, in today's world, where digital technologies permeate all areas of life and cyber threats continuously adapt, traditional methods of identifying critical vulnerabilities that rely on internal data often lag behind the evolution of these threats, leaving computer systems critically vulnerable. Ensuring the fault tolerance of computer systems is essential for stability and protection against such threats.

The research methodology includes analyzing modern approaches to ensuring fault tolerance in relation to both hardware and software, utilizing cybersecurity models, redundancy, and data integrity at both the routing and system levels. Reliability was evaluated through theoretical analysis and application of existing technologies, as well as analysis of available system failure statistics based on open data sources.

The main goal of the research was to develop recommendations and practical solutions to enhance the fault tolerance of computer systems through the integration of software and hardware protection methods based on an analysis of existing solutions. The task was to ensure system resilience to hardware-software failures before, during, and after their occurrence, thereby minimizing downtime of the hardware-software complex and data loss.

The research demonstrated that a comprehensive approach provides the best protection, with the ability to identify issues before they arise. This includes component redundancy of both software and hardware types and the implementation of diagnostic and predictive failure systems. Systems equipped with modern anomaly detection methods can respond much faster to potential threats and minimize losses, while hardware systems with active monitoring and automatic switchover to backup components ensure continuity of processes in the event of critical technical failure.

Future technologies, such as using artificial intelligence to analyze system state and predict potential failures, will significantly increase the efficiency and protection of hardware-software systems. However, they currently face compatibility challenges when combined with both legacy and new equipment, limiting their widespread adoption. The results of the research show that systems utilizing a hybrid monitoring approach, combining software and hardware protection, better adapt to changing operating conditions and demonstrate higher fault tolerance.

Keywords: fault tolerance, hardware and software systems, positional number systems.

Introduction

The high demand for timeliness, reliability, and confidentiality in information processing across all sectors of modern society, coupled with the expanding capabilities of computer technologies, has led to the development and implementation of distributed data processing methods through network access to computer systems.

Despite the diversity of critical systems, they share a crucial commonality: the severe damages caused by information security breaches. The value of data stored and processed within computer systems and networks has driven the advancement and refinement of methods, tools, and protocols for information protection [1].

The progress in the development and refinement of modern computers and computer systems is driven, firstly, by the need to reorganize them to address tasks requiring real-time processing of large volumes of interconnected heterogeneous information [2],

and secondly, by the advancement and broad application of nanotechnologies.

Maintaining a high level of parallelism in processing large volumes of information in various forms and representations (such as visual, auditory, television information, biological signals, etc.) is essential for solving critical tasks like recognition, identification, meaning comprehension, construction of logical sequences, environmental modeling, hypothesis generation, and strategy development.

While the intensive application of neurotechnologies in practice, particularly when combined with elements of fuzzy sets to form hybrid neural systems, is considered promising in the near future, the wide variety of applications installed on computers creates opportunities for attackers to exploit vulnerabilities sufficient for system intrusion [3, 4]. Artificial neural networks (ANNs) have attained the status of a foundational architectural principle for the development of sixth-generation computers, which are referred to as adaptive evolutionary computers [3].

Statistics show that the number of malware attacks has been declining since 2018. At that time, 10,5 billion attacks were recorded; by 2022, this number had halved to 5,5 billion. China (47%), Turkey (42%), and Taiwan (39%) have the highest number of infected computers and the highest system infection rates.

Taking into account DDoS attacks (disruptions to normal network functions by overwhelming it with large volumes of internet traffic), the number of major attacks increased by 4,6 million between 2020 and 2023, nearly doubling compared to 2018, reaching 7,5 million (Fig. 1) [4].

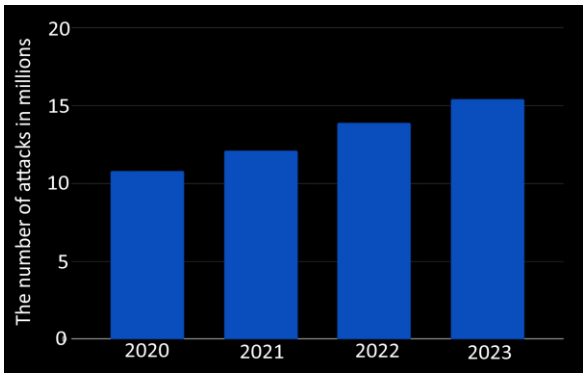

Figure 1: The number of DDoS attacks for the period 2020-2023

The sectoral structure of DDoS attacks is presented in Figure 2. In 2023, the highest number of these attacks was observed in the information and communication technology sector. This indicates that industries with a high degree of integration with digital technologies remain the most vulnerable to such cyber threats.

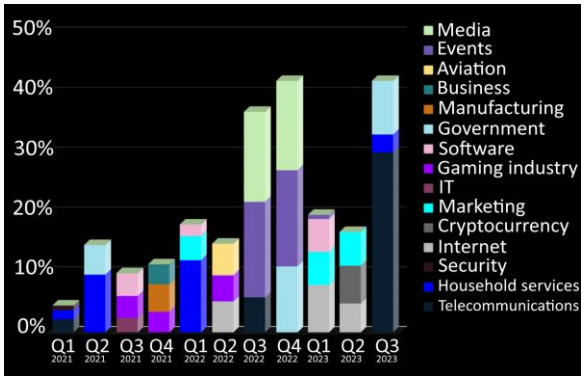

Figure 2: Sectors attacked by DDoS in 2021-2023

Modern software and hardware systems (SHS) are becoming increasingly complex and essential for the seamless operation of electronic and telecommunications technologies, as their reliability depends on the interaction between hardware and software components.

Assessing the reliability of such systems is complicated by the fact that the reliability metric considers both the readiness of the hardware and the probability of correct functioning of the software component over a specified period [5].

Failures in SHS can be caused by defects in the hardware, software errors, or the influence of external factors (such as temperature or radiation), leading to serious risks to material assets and human safety. Thus, the growing demands for accountability and complexity of SHS pose a challenge for developing methods to assess their reliability, requiring the integration of mathematical statistics, software engineering, and reliability theory to create new, more accurate models [6].

1. Presentation of the material

According to the technical description, fault tolerance is the ability of a computer system to continue functioning without human intervention, ensuring business continuity, data integrity, and recovery of functionality for a specified period after a hardware or software failure [7].

The object of information protection is a computer system or an automated information processing system (AIPS). Information security

in an automated information processing system refers to protection against accidental or intentional interference with its normal functional processes, as well as attempts to steal, modify, or destroy its components [8]. The nature of the impact on automated information systems is very diverse, ranging from natural disasters to human errors.

Information can be defined as something intangible but stored and transmitted via a material carrier, where the physical object contains data about itself or another object and has the following characteristics.

1. Value of information – the value of information depends on its usefulness to its owner.

2. Confidentiality of information – this condition indicates the necessity of imposing restrictions on the variety of subjects who may access this information.

3. Integrity of information – a property that ensures the semantic content remains unchanged, even under accidental or intentional distortive or destructive influences during system operation.

4. Availability – the property of being accessible to authorized subjects.

5. Accuracy – defined by the required precision for reflecting external objects and processes at a given time and place.

6. Timeliness – the correspondence of value and accuracy to a specific time period.

This property is expressed by a ratio:

$$C(t) = C_0 e^{\frac{-2.3t}{T}}, \quad (1)$$

where C_0 – the value of information at the time of its occurrence, t – time from the moment the information is generated to the time it is evaluated, T – time from the moment of information generation to its obsolescence [9].

Fault tolerance, from the system's perspective, is the ability to maintain the availability of network services when individual technical components fail. In other words, when a system component fails, its functions are taken over by another component. Therefore, to ensure fault tolerance, it is important to have additional resources, such as backup equipment or excess capacity in the existing hardware [10].

It is important to note that when a component fails, the transfer of its functionality to a replacement must occur quickly to avoid disrupting the service's availability. If this is not possible and the service availability is lost during the transfer of functionality to the replacement component, the system cannot be considered fault-tolerant, as it will lead to the loss of technical resources and the inability to restore functionality.

$$p_{user} = p_{ser} \times p_{net}, \quad (2)$$

where p_{user} – the overall probability of service availability for the user, p_{ser} – the overall probability of service source functionality, p_{net} – the overall probability of network functionality.

A schematic representation of the network as a destructive factor of reliability is shown in Figure 3.

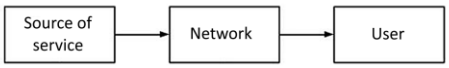

Figure 3: The network as a factor of reduced reliability

An important characteristic of fault-tolerant systems is the absence of a single point of failure. This means that there are no non-redundant components that immediately lose functionality when a failure occurs. A defining feature of fault-tolerant systems is the level of fault tolerance, which determines the number of such component failures in the system that do not lead to the loss of service availability [11].

A fault-tolerant automated system (AS) should minimize downtime and allow for minimal information loss during operation. The structural diagram of the reliability of such a fault-tolerant AS is shown in Figure 4.

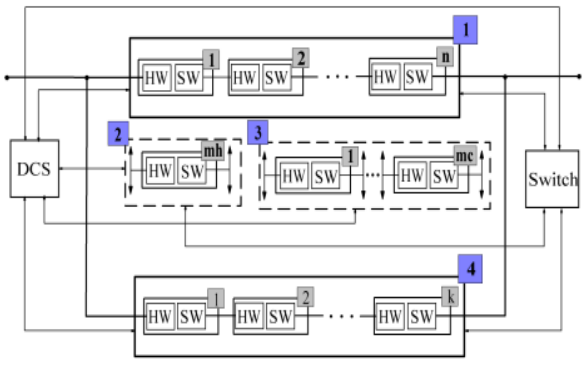

Figure 4: The structural diagram of the reliability of SHS

where 1 – the main SHS, 2 – modules that are in hot standby, 3 – modules that are in cold standby, 4 – backup SHS [6].

The impact of system updates in SHS is demonstrated in the article [6], where the following states are presented: S1, S4, and S7 – states in which the system is operational; S2, S5 – states in which the system is functional but not operational due to software version replacement (downtime state); S3, S6, S8 – states in which the system is non-operational due to a software failure caused by hardware faults, but a software reboot is in progress; S9, S10 – states in which the system is non-operational due to a software failure (downtime states) (Fig. 5).

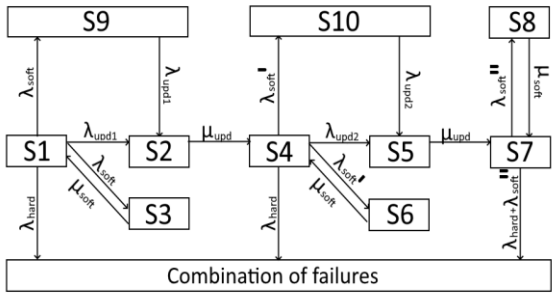

Figure 5: The behavior model of a software-hardware system with dual software updates and software reboot after failures caused by hardware malfunctions

The results (Figure 6) show that the service life duration of SHS with software updates, where the probability of failure-free operation $P_f \geq 0{,}99$, obtained using the model without considering the software update (relation 1), is lower than the service life duration for the SHS with dual software updates (relations 2 and 3).

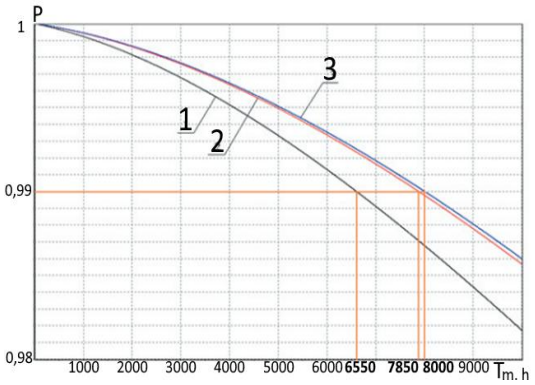

Figure 6: The dependence of the probability of failure-free operation of a fault-tolerant system on its service life duration

The conducted study of the dependence of the availability function of SHS at various values of software failure rates is presented in Table 1.

Table 1

The sensitivity of traffic from different applications to the values of QoS indicators.

Software failure rate, hours	Goel-Okumoto model	S-shaped model	Complexity index model
First version	$3{,}516\times10^{-6}$	$1{,}744\times10^{-9}$	$1{,}221\times10^{-3}$
Second version	$2{,}143\times10^{-9}$	$3{,}64\times10^{-14}$	$7{,}286\times10^{-8}$

The calculation of the steady-state availability coefficient yields a value of C_a=0,977 for the model with the complexity index, and C_a=0,981 for the two other software reliability models (Fig. 7).

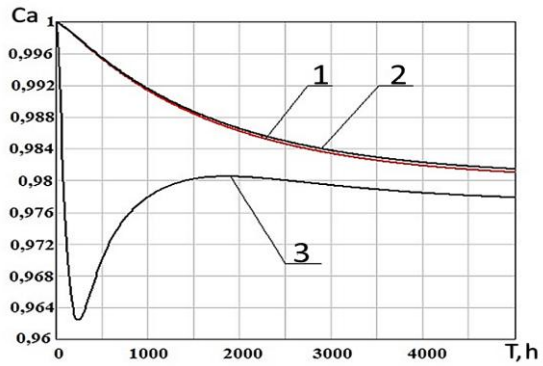

Figure 7: The dependencies of the availability function C_a on time T for different values of the software failure rates, obtained based on various models (1 – Goel-Okumoto model, 2 – S-shaped model, 3 – complexity index model)

The study showed that the use of traditional software reliability models leads to inflated reliability estimates for SHS, including the availability coefficient, which makes it difficult to accurately assess the risks associated with the operation of such systems [6].

The data presented in Pashorin's book show an increase in computer failures related to external intrusions into systems, which encourages the development of systems for the timely detection of such intrusions. It also proposes an approach to protecting computer networks based on intrusion detection systems, which is a widely adopted solution when neural network systems are not used [12].

In the article [13], Borysenko develops a methodology for the early detection of potential attack paths in computer systems. The system architecture includes one or more instances of different types of agents to address the problem of identifying potential damage paths. In the

adopted architecture, there is no distinct "central control" – everything is managed by a family of agents. Depending on the situation, any agent can become the main agent, initiating and/or performing functions of collaboration and management [13].

According to the research published in the Scientific Bulletin of UNFU, a method for regulating the movement of monitoring data, dialogue, and dialogical data within the structure of distributed cyber-physical systems has been developed. The main idea of the proposed method lies in the systematization of the structure and classes of information resources that make up monitoring and dialogue data. The method for calculating the external appearance of classified structures for the following types of control computer systems (CCS) is proposed: user-based, automatic control, single-channel monitoring systems, time-division systems, and multiprocessor data processing systems [14].

Fault tolerance is the primary means of ensuring service availability in the event of unplanned disruptions in the availability of certain technical measures. The presence of redundancy for the purpose of implementing fault tolerance can also be used to carry out planned activities related to the interruption of system component functionality without affecting service availability [11].

$$p_{user} = (1 - \prod_{N} p_{ser}) \times p_{net}, \quad (3)$$

where p_{user} – the overall probability of service availability for the user, p_{ser} – the overall probability of service source functionality, p_{net} – the overall probability of network functionality.

The network as a means of implementing fault tolerance is schematically presented in Figure 8.

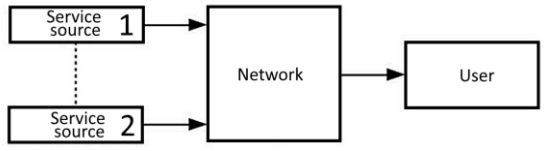

Figure 8: The network as a means of implementing fault tolerance

Considering a computer system as part of a network, the impact of routing on data collection and processing has been identified. Therefore, according to the ITU-T Y.1540 recommendation, Table 2 presents the maximum permissible values of key QoS indicators defined for networks, depending on the type of network application used.

Table 2

The sensitivity of traffic from various applications to QoS indicators

Application	Reliability	Average delay	Jitter	Bandwidth
Email	High	Low	Low	Low
File transfer	High	Low	Low	Average
Web access	High	Average	Low	Average
Audio on demand	Low	Low	Low	Average
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Video conference	Low	High	High	High

It is worth noting that these QoS requirements form the basis for creating eight classes of network quality of service. In particular, class 5 does not have a threshold value, which indicates that it can be dynamically created according to current requirements [15].

The study showed that a promising direction for the development of routing solutions is fault tolerance. This is due to the fact that modern routing protocols can respond to changes in network conditions within tens of seconds, and the timers for recalculating routing tables are within this range. However, since gigabit and even terabit data transfer speeds are used in the core of the network, when a network element fails or becomes overloaded, recalculating the route for the failed element leads to a significant packet loss [16].

Thus, fault-tolerant routing ensures the use of redundant resources, where the backup route(s) are calculated simultaneously with the primary route(s). Researchers have derived a number of requirements that are inherently contradictory, as there is currently no single universal routing protocol that fully satisfies these requirements.

Based on the analysis of the main approaches to mathematical modeling of routing tasks, a generalized structure of the routing flow model has been defined.

The selection of optimal criteria for decision-making in routing is a crucial aspect in completing the formulation of models for both unicast and multicast routing. Linear criteria can

be used as an example for calculating the optimal route.

$$\sum_{k\in K^0\cup K^б}\sum_{E_{i,j}\in E} c_{i,j}^k, x_{i,j}^k \Rightarrow \min, \quad (4)$$

where $c_{i,j}^k$ – routing metric, which characterizes the structural and functional parameters of the communication channel (CC) $E_{i,j}\in E$ quantitatively reflects the conditional cost of using the given CC. The higher the numerical value of the specified metric, the lower the probability of including this channel in the desired unicast and/or multicast route.

Taking into account other studies, quadratic optimality criteria are proposed in work [17], which have the following form:

$$\sum_{k\in K^0\cup K^б}\sum_{E_{i,j}\in E} x_{i,j}^k, c_{i,j}^k, x_{i,j}^k \Rightarrow \min, \quad (5)$$

Its use, as opposed to the linear analog, contributes to a more balanced utilization of network communication channels, but somewhat increases the computational complexity of the routing algorithm implementation.

However, to ensure load balancing in accordance with the Traffic Engineering concept requirements, as shown in works [18], it is proposed to modify the form of the overload prevention conditions for communication channels into expressions of the following form:

$$\sum_{k\in K^0}\lambda^k x_{i.j}^k \le \alpha\varphi_{i,j},\ E_{i,j}\in E, \quad (6)$$

where α – additional control variable has been introduced, which characterizes the upper dynamically controlled threshold for the load of communication channels. The relationship of the load threshold is shown in Figure 9.

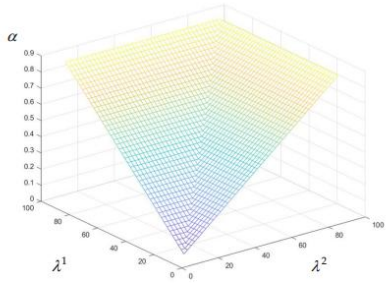

Figure 9: The relationship of the load threshold of network communication channels α with the intensities of two packet flows

An appropriate constraint is imposed on it according to its physical meaning:

$$0 \le \alpha \le 1 \quad (7)$$

To improve the quality of service, this variable must be minimized, thereby determining the type of optimization criterion for routing decisions and load balancing in the network [15].

Considering the possibility of detecting failures before they occur, the article [16] discusses a number of algorithms for justifying the diagnostic model of mutual internal checks. Based on the simulation results (Fig. 10), dependencies of diagnostic reliability and diagnostic time on the number of failures for different systems were obtained.

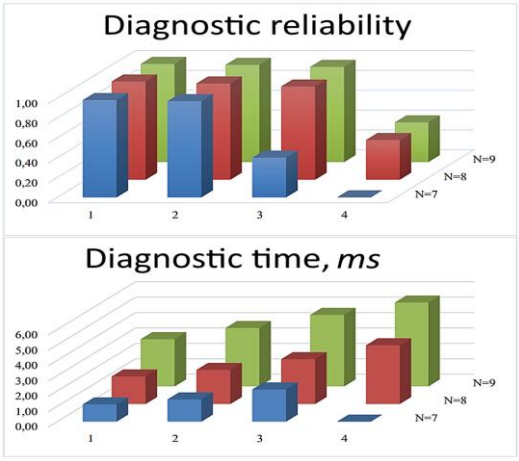

Figure 10: The assessment of the reliability of the mutual internal checking procedure

Mathematical modeling confirms the correctness of the theoretically developed concept of ensuring the fault tolerance of software systems through diagnostics based on mutual informational coordination.

In particular, from the graphs of the dependencies $D = f(t)$, it is evident that the number of failures t does not exceed the allowable limit, and the diagnostic reliability is high D>0,95 (Fig. 11).

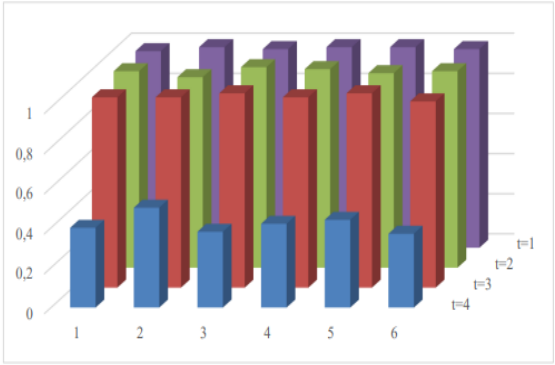

Figure 11: The implementations of D* and the 95% confidence intervals for N=9 modules

The analysis of the obtained confidence intervals shows that as the number of failures t increases, the confidence interval expands, while it narrows as t decreases. This is explained by the greater variability in diagnostic results at higher values of *t*.

Depending on the architectural decisions taken, the entire set of computing systems in positional numeral systems (PNS), usually binary, can be divided into four main groups: for instance, the application of the SISD architecture (Single Instruction Stream, Single Data Stream) dominates in the classical Von Neumann architecture. The formation of non-positional code structure (NPCS) $A = (a_1 \square a_2 \square ... \square a_n)$ in system of residue classes (SRC) is based on the use of parallelism principles and the independence of the formation of remainders a_i.

The use of the properties of the SRC ensures the presence of three types of redundancy in the computing system (CS): structural, informational, and functional. This, in turn, allows for improved fault tolerance of non-positional computing structures in SRC through the application of methods based on passive (constant structural redundancy) and active (structural redundancy through substitution) fault tolerance. It has been identified that the CS and its components in SRC belong to easily controlled and diagnosed computing structures. This feature contributes to the development of methods for efficient data control and diagnosis within SRC. Thus, the use of the properties of SRC makes it possible to create a unique system for error control and correction without interrupting computations, which is especially important for CS operating within complex real-time technical systems [19, 20].

In the article, Dmytrenko analyzes modern backup methods: cold, warm, and hot backups, the common backup address protocol, and the virtual routing backup protocol. She also demonstrates how to activate additional equipment as an appropriate backup method for IoT devices based on redundancy [21].

This article discusses various data structures that can be used for storing system data. Specifically, these include linked lists, extended linked lists, hash tables, B-trees, B+-trees, and binary decision diagrams. The extended lists showed the best results: on average, they used 1,54 times more memory and took 1,68 times longer to generate a session. The reverse extended list showed an average advantage of 1.43 times in generation time [22].

The article develops a reliability mathematical model that takes into account first and second kind errors of the switching device for a hot-standby system. This model is designed to determine the probability of failure-free operation of the system. Based on the state and event model of the system, a homogeneous Markov model was constructed. This model is represented by a system of Kolmogorov-Chapman equations:

$$\frac{d}{dt} p(t) = Ap(t), \; y(t) = Cp(t), \tag{8}$$

where t – time, $p(t)$ – vector containing state probability functions, $y(t)$ – vector containing the investigated probability functions.

It has been shown that as the values of parameters corresponding to errors increase, the probability of fault-free operation of the system decreases within defined limits (Fig. 12, 13).

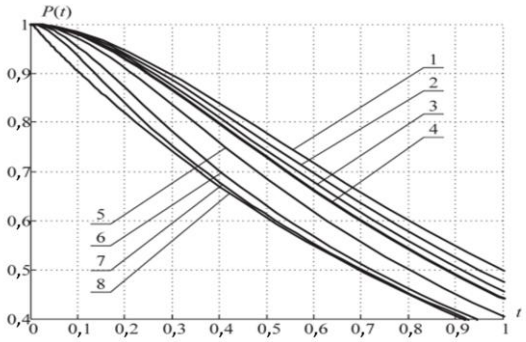

Figure 12: A family of reliability curves showing the impact of first-type switching device errors on the fault-free operation probability of the system

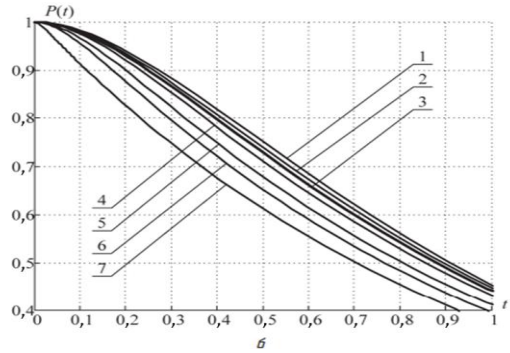

Figure 13: A family of reliability curves showing the impact of second-type switching device errors on the fault-free operation probability of the system [23]

Cybersecurity requirements [24] often lead to the addition of security control mechanisms into the architecture of existing systems rather than

encouraging the development of resilient networks. However, it is often impossible to prevent malicious actors who aim to infiltrate the system [25]. Therefore, data backup technologies and enhancing system resilience in the event of an attack are becoming increasingly important. Distributed file storage systems provide a solution that enables immediate data recovery. This is an attractive and widespread solution for managing large and complex systems [26], such as energy companies, robotics, water networks, wireless sensor networks, and traffic management.

System resilience is ensured through backup, but data loss may occur when reverting to the last known good state of the data. System backups are better than nothing, but they are insufficient. Therefore, the NIST Privacy Framework emphasizes that data protection is more important than protecting devices or training users in device security.

In the development of a secure distributed protected data storage systems (SDPSS) based on redundant SRC, it is proposed to consider detecting and correcting only a single error, since, according to the 2022 Backblaze Storage Cloud report, the failure rate of storage devices (SDs) is only slightly dependent on the size of the device and largely depends on its operational time. Accordingly, for devices that have been operating continuously for more than 8 years, the failure probability does not exceed 3,73% for small drives (up to 10 Tb), while for drives sized 12-16 Tb, the average failure rate is 1,07%.

This confirms the high reliability of modern data storage devices [24].

Conclusions

The latest methods of data protection and fault tolerance analysis have been examined to ensure the security of computer systems. The results show that fault tolerance is a fundamental element for the stable operation of such systems, and that proactive fault prevention plays a crucial role in ensuring the continuity of processes.

A comparison of hardware and software data protection reveals that a unified approach is preferable for enhancing system reliability.

Therefore, the implementation of a comprehensive approach to data protection can ensure high fault tolerance of these systems.

References

[1] P. Grabusts, "Security Protocols Analysis in Relation to Information Structures Protection," *2019 60th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, Riga, Latvia, 2019, pp. 1–5, doi: 10.1109/ITMS47855.2019.8940767

[2] S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, and V. Skryl, "The Mechanism of Information Security of the National Economy in Cyberspace," in *Proc. 4th Int. Conf. Building Innovations, Cham*, 2023, vol. 299, pp. 791–803. doi: 10.1007/978-3-031-17385-1_67

[3] T. B. Martyniuk, A. V. Kozhemiako, and L. M. Kupershtein, "Analiz tendentsii rozvytku suchasnykh komp'iuternykh system [Analysis of trends in the development of modern computer systems]", *Met. Syst. Optoelectron. Digit. Image Signal Process.*, vol. 4, no. 153, pp. 5–10, 2017.

[4] M. Ohnyvchuk, H-X Technologies (2023, Dec. 14). Cyberattacks 2022-2023: An overview of the largest incidents and what to expect in 2024 [Online]. Available: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua

[5] A. Yanko, V. Krasnobayev, R. Liubchenko, and P. Sabelnikova, "Protsedura zabezpechennya vidmovostiikosti kompiuternoi systemy na osnovi vykorystannia modularnoi arytmetyky [Procedure for ensuring fault tolerance of a computer system based on modular arithmetic]", *Syst. Manag. Navig. Commun. Sci. Proc.*, vol. 4, no. 74, pp. 125–128, Dec. 2023.

[6] V. V. Vyshnivs'kyi, Y. V. Kargapolov, Y. V. Berezovska, M. Yu. Berezivskyi, and R. V. Kosminskyi, "Otsinka pokaznykiv nadijnosti informatsiinykh system pry obmezhenii apriornii informatsii [Evaluation of reliability indicators of information systems with limited a priori information]", *Sciences of Europe*, no. 63-1, pp. 8–14, 2021. doi: 10.24412/3162-2364-2021-63-1-8-14.

[7] Cabinet of Ministers of Ukraine, "Resolution on Approval of the Procedure for State Control over International Transfers of Dual-Use Goods," No. 86,

Kyiv, Jan. 28, 2004. [Online]. Available: https://ips.ligazakon.net/document/TM033560

[8] S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, and A. Cherviak, "Cybersecurity and improvement of the information security system," *J. Balkan Tribol. Assoc.*, vol. 29, no. 5, pp. 818–835, 2023. [Online]. Available: https://scibulcom.net/en/article/L8nV7It2dVTBPX09mzWB

[9] L. Dong *et al*., "Research on Computer Security Protection Technology Based on Information," *2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, Dalian, China, 2020, pp. 459–464, doi: 10.1109/ICISCAE51034.2020.9236872.

[10] V. Krasnobayev, A. Yanko, and A. Hlushko, "Information security of the national economy based on an effective data control method," *J. Int. Commerce, Econ. Policy*, article no. 2350021, 2023. doi: 10.1142/S1793993323500217

[11] D. I. Cherkasov, "Vysoka dostupnist' merezhvykh servysiv: vyznachennia ta osnovni fatory vplyvu [High availability of network services: definition and key influencing factors]", *Naukovi zapysky NaUKMA*, vol. 163, pp. 98–102, 2014.

[12] V. I. Pashorin, P. Yu. Kravchuk, and Y. V. Kraiak, "Zastosuvannia system vyiavlennia vtohrnien' dlia zakhystu kompiuternykh merezh [Application of intrusion detection systems for computer network protection]", *Nauk. Visnyk: zb. nauk. prats Yevropeiskoho univ.*, eds. O. I. Tymoshenko et al., Kyiv: Vyd-vo Yevropeiskoho univ., pp. 89–99, 2024.

[13] B. V. Borysenko, "Metodolohiia rannoho vyiavlennia potentsiinykh kanaliv urazhennia kompiuternykh system [Methodology for early detection of potential attack channels in computer systems]", *Comput. Sci. Appl. Math.*, no. 1, pp. 46–53, May 2024, doi: 10.26661/2786-6254-2024-1-06.

[14] I. R. Pitukh and N. Ya. Vozna, "Sposoby orhanizatsii rukhy monitorynhovykh, intehratyvnykh i dialohovykh danykh u strukturakh rozpodilenykh kompiuternykh system [Methods of organizing the movement of monitoring, interactive, and dialog data in distributed computer system structures]", *Sci. Bull. UNFU*, vol. 31, no. 3, pp. 101–108, Apr. 2021. doi: 10.36930/40310316.

[15] A. Asaduzzaman, P. Kamalakannan and F. N. Sibai, "The Eight Class of Service Model - An Improvement over the Five Classes of Service," *2021 8th International Conference on Electrical and Electronics Engineering (ICEEE)*, Antalya, Turkey, 2021, pp. 287–291, doi: 10.1109/ICEEE52452.2021.9415966.

[16] J. Cheng, N. Taylor and P. Hilber, "Impact of Advanced Bushing Diagnostic Techniques on Operation Reliability and Maintenance Strategy," *2022 IEEE International Conference on High Voltage Engineering and Applications (ICHVE)*, Chongqing, China, 2022, pp. 1–5, doi: 10.1109/ICHVE53725.2022.9961703.

[17] D. R. Ramirez and E. F. Camacho, "Characterization of min-max MPC with bounded uncertainties and a quadratic criterion," *Proceedings of the 2002 American Control Conference (IEEE Cat. No.CH37301)*, Anchorage, AK, USA, 2002, pp. 358–363 vol.1, doi: 10.1109/ACC.2002.1024830.

[18] O. Nevzorova, B. Sleiman, A. Mersni, and V. Sukhoteplyj, "Vdoskonalennia potokovoi modeli bahatoadresnoi marshrutyzatsii na pryntsypakh tekhnolohii Traffic Engineering [Improvement of the flow model for multicast routing based on Traffic Engineering technology principles]," *Probl. Telecommun.*, no. 2(25), 2019. doi: 10.30837/pt.2019.2.02.

[19] S. Onyshchenko, A. Yanko, and A. Hlushko, "Improving the efficiency of diagnosing errors in computer devices for processing economic data functioning in the class of residuals," *Eastern-European J. Enterp. Technol.*, vol. 5, no. 4(125), pp. 63–73, 2023, doi: 10.15587/1729-4061.2023.289185

[20] V. Krasnobayev, S. Koshman, V. Kurchanov, and D. Zinevich, "Osnovni vlastyvosti nepozytsiynoi systemy chyslennya u klasi lyshkiv i yikh vplyv na strukturu ta pryntsypy realizatsii aryfmetychnykh operatsii kompiuternoi systemy [Main properties of the non-positional numeral system in the class of residues and their impact on the structure and principles of arithmetic operation implementation in a computer system]", *Syst. Control, Navig. Commun. Sci. Work*,

vol. 2, no. 54, pp. 114–118, Apr. 2019. doi: 10.26906/SUNZ.2019.2.114.

[21] O. Dymentrenko and M. Skulish, "Metody vidmovoistyikosti rezervuvannia prystroiv IoT [Fault tolerance methods for IoT device reservation]", *IKKT*, vol. 2, no. 04, pp. 59–65, Feb. 2023. doi: 10.36994/2788-5518-2022-02-04-06

[22] V. Mikhav, Y. Meleshko, M. Yakymenko, and D. Bashchenko, " Metody zberihannia danykh rekomendatsiinoi systemy na osnovi zviaznykh spyskiv [Methods of data storage in a recommendation system based on linked lists]", *Syst. Control, Navig. Commun. Sci. Works*, vol. 4, no. 66, pp. 59–62, Dec. 2021. doi: 10.26906/SUNZ.2021.4.059

[23] I. I. Moskvina, T. O. Stefanovych, and S. V. Shcherbovskykh, "Vrakhuvannia pomylok pershoho ta druhoho rodu peremykalnoho pryistroiu dlia systemy iz hariachym rezervuvanniam [Considering type I and type II errors of the switching device for a system with hot redundancy]", *Tekhnol. Audit Prod. Reserves*, no. 5/2(25), pp. 22–25, 2015. doi: 10.15587/2312-8372.2015.51357

[24] S. Kulyna, "Systema rozpodilenoho zakhyshchenoho zberihannia danykh [Distributed secure data storage system]", *Bull. Lviv State Univ. Life Saf.*, vol. 27, pp. 48–59, Jun. 2023. doi: 10.32447/20784643.27.2023.06

[25] A. S. Yanko, V. A. Krasnobayev, A. Kuznetsov, and K. Kuznetsova, "The data errors control in the modular number system based on the nullification procedure," in *Proc. 2nd Int. Workshop Cyber Hygiene & Conflict Manage. Glob. Inf. Netw.*, Kyiv, Ukraine, 2020, pp. 580–593.

O. Shefer, O. Laktionov, V. Pents, A. Hlushko, and N. Kuchuk, "Practical principles of integrating artificial intelligence into the technology of regional security predicting," *Adv. Inf. Syst.*, vol. 8, no. 1, pp. 86–93, 2024, doi: 10.20998/2522-9052.2024.1.11.

[26] Y. Zhu, H. Jiang, J. Wang and F. Xian, "HBA: Distributed Metadata Management for Large Cluster-Based Storage Systems," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 6, pp. 750-763, June 2008, doi: 10.1109/TPDS.2007.70788.