Architecture of the system with a subsystem of providing fault tolerance, survivability and information protection of specialized information technology

Vasyl Stetsyuk [1*, †], Mykola Stetsyuk [1, †], Yuriy Stetsyuk [1, †], Oleksandr Kozelskiy [1, †], and Piotr Gaj [2, †].

[1] *Khmelnitsky National University, Khmelnitsky, Instytutska street 11, 29016, Ukraine*
[2] *Silesian University of Technology, ul. Akademicka 2A, 44-100 Gliwice, Poland*

Abstract

The construction of a model of a typical architecture of information technology for the construction of specialized information systems intended for the automation of information processing processes, management processes and decision-making processes based on a spatially distributed multi-machine system that provides a high level of fault tolerance, survivability and information protection is considered. The classification and structure of the information system, which has a multi-level organization of interacting hardware and software tools, as well as the features of such an organization when building a subsystem to ensure fault tolerance, survivability and protection of information in a distributed information system of specialized application, are given. Methods of implementation of mechanisms for ensuring fault resistance, survivability and protection of information are considered and classified, with their presentation in a general model of a specialized information system. It is shown that the most urgent problem of the construction of the considered systems is the creation of a method that is a general approach to the construction of highly adaptive systems with increased fault tolerance, survivability and protection of the information processed in them. A key aspect, according to the generalized method, is the creation of a system architecture that can adapt to the requirements of a specific specialized IS. The IS architecture development process itself will include the implementation of two stages. This approach to the development of IS made it possible to ensure the implementation of such general requirements for the construction of systems as systematicity, openness, compatibility, unification and efficiency. As a result, an IS architecture was obtained in which a rational ratio between costs and target effects was achieved.

Keywords

IS architecture, information technology, fault-tolerant system, survivability of systems, information protection, information system.

ICyberPhyS-2024: 1st International Workshop on Intelligent & CyberPhysical Systems, June 28, 2024, Khmelnytskyi, Ukraine

[*] Corresponding author.
[†] These authors contributed equally.

swmua@khmnu.edu.ua (V. Stetsyuk); mykola.stetsiuk@khmnu.edu.ua (M. Stetsyuk); yuriy.stetsuk@khmnu.edu.ua (Y. Stetsyuk); oleksandr.kozelskiy@khmnu.edu.ua (O. Kozelskiy); piotr.gaj@polsl.pl (P. Gaj)

0000-0001-9880-2666 (V. Stetsyuk); 0000-0003-3875-0416 (M. Stetsyuk); 0000-0003-0312-2276 (Y. Stetsyuk); 0009-0002-7157-6499 (O. Kozelskiy); 0000-0001-5647-9979 (P. Gaj)

1. Introduction

The modern level of development of computing facilities and their wide implementation in all areas of human activity increasingly require the creation of computing facilities with a high level of fault tolerance, survivability and information protection. A high level of resistance to destabilizing factors is, in principle, desirable for all types of computing devices, but this requires significant additional technical, software, and financial costs. In this regard, computing devices with high levels of fault tolerance and survivability are used mainly in critical areas where the failure of computing devices leads to severe consequences. Basically, these areas are limited by the following factors:

- creating a threat to people's lives;
- entails severe economic consequences;
- violation of the functioning of complex autonomous technical objects.

The revolution in the field of information technologies has led to the fact that many aspects of the activities of human society have become critically dependent on various means, such as electronic devices in general and computer systems, in particular, data storage (including cloud), various hardware and mathematical support for the functioning of artificial intelligence etc. Their successful work requires such qualities as fault tolerance, reliability, availability and information security. The survivability of mission-critical information systems involves the ability to maintain uninterrupted operation in the face of severe failures, to fail smoothly when critical conditions are reached, and to maintain the ability to restore normal service after failures are resolved.

Not only information technologies, but also malicious software are in constant development. This, in turn, leads to increased demands from users for fault-tolerant functioning, survivability of systems and ensuring information protection. In a society where information gradually acquires the quality of the main value, its loss or distortions are unacceptable.

The analysis of the situation that has developed directs the course of events to the creation of countermeasures, namely the development of a comprehensive system that was able to simultaneously address the problems of fault tolerance, survivability and protection of information at all levels of the information system, but in such a way that the information systems themselves would remain financially affordable. The task of building a functionally stable architecture, which is a complex system that actively interacts with the external environment and functions under the influence of random factors, the presence of adverse effects of various nature and the high cost of the consequences of malfunctions, cannot be solved by simply improving the indicators of reliability, fault tolerance or security.

2. Analysis of known solutions

Durability is an important, albeit non-functional property of the life cycle of specialized information systems [1]. Their survivability elements include the ability of systems to recognize attacks on them and other situations critical to their functioning with the ability to resist them, adapt to avoid them, and change their behavior to reduce the consequences of similar events in the future.

Thus, the vulnerability of using a combination of username and password to access network resources is noted due to a possible coincidence of circumstances, when the repeated use of the password when accessing the services of a dubious provider is combined, which can lead to the theft of corporate and personal data. Therefore, given the fact that more and more public services carry out their activities using the Internet [2, 3], more and more developers, given the importance of the issue, offer a number of their alternative approaches, such as two-factor authentication with detailed biometric verification, individual certificates users, a single sign-on system (known as SSO) and the application of credentials based on privacy-enhancing attributes (P-ABC technology) [4, 5].

Solutions based on P-ABC are reliably protected, provide privacy, but are cumbersome to use; while SSO provides a more convenient solution, but in turn requires a guaranteed trusted identity provider, as it examines all online user activities. To some extent, this can be facilitated by the use of a distributed identity management system within the OLYMPUS system, which will avoid the need for a single trusted party.

Symmetric searchable encryption (SSE), which is widely used in encrypted databases for keyword queries, has been reported to suffer from information leakage. Most existing forward and reverse SSE schemes only consider a single data source model, which is not practical in scenarios where data is distributed across multiple devices. An efficient forward and reverse private SSE scheme for multiple data sources (FBSSE-MDS) is proposed in [6]. It is the first efficient SSE scheme that supports both forward privacy and BP-II reverse privacy (the second level of reverse privacy) in the case of multiple data sources.

In [7, 8] it is proposed to use matrix numerical methods for symmetric cryptography, known as Gauss-Jacques and Gauss-Jordan methods with explicit modularization. Both of them can be used to process private keys, which is vital from the point of view of information security and protection, which provide lower computational cost and complexity.

The use of deliberate error attacks on electronic devices while they are executing a cryptographic algorithm, resulting in a crash, is becoming widespread. The attacker repeatedly repeats them in order to obtain valuable information. A new countermeasure is presented in [9] that applies to cryptographic primitives that use permutation with nearly shift-invariant circular functions during multiple executions of the same algorithm.

Firewalls are designed to identify and block potentially malicious incoming traffic based on a predefined set of rules. But with the development of attack tactics, it becomes more difficult to distinguish between anomalous traffic and normal traffic. The application of the hybrid metaheuristic method [10] for intrusion detection systems (IDS), implemented as a metaheuristic Bat algorithm, which ensures the selection of sixteen features, did not give the desired result due to high time consumption.

Cybersecurity issues have also been on the rise over the years, the most prominent of which is phishing attacks, where malicious websites impersonate legitimate websites in order to obtain the data of gullible users needed for unauthorized access. Current countermeasures, such as anti-phishing software and machine learning (ML) techniques, have proven ineffective in detecting phishing activities on one hand. On the other hand, hackers are developing new ways to bypass these countermeasures. Given the dynamism of phishing attempts, it is necessary to look for innovative and effective solutions to detect website phishing. New research [11] proposes a tree-based logistic model based on rotated forest (RF-LMT) to detect sophisticated website phishing. LMT is a technology that combines logistic regression and a generalized model tree. LMT is a technique that combines logistic regression and single model tree inference. Three datasets with different instance distributions, both balanced and unbalanced, are used to investigate the RF-LMT model. From the results, it is found that LMT performs better than the selected base classifiers.

In [12], the technique of dynamic detection of malicious software based on signatures when tracing API calls is given.

An ever-increasing problem is the use of DDoS attacks by attackers [13, 14]. Using a huge number of distributed, but coordinated in their actions, botnets have become one of the most complex cyber threats. Existing botnet detection approaches cannot detect unknown botnet threats and are time-consuming [15].

New blocking approaches are proposed that are used to detect and effectively prevent the propagation of botnets in software-defined networks. Its content is determined by connections in the botnet network and its intellectual blocking. A cheat system is also proposed, based on two goals: to reduce the botnet's infection rate and to waste the attacker's time.

There are more and more questions about security against internal threats [16]. Traditional approaches to detecting anomalies in systems based on sets of rules generate a large number of messages that are difficult to adapt to specific situations. The introduction of MUEBA's multi-model system for spatio-temporal analysis, which combines individual historical user analysis and group analysis to detect insider threats, improved the situation, but did not eliminate it.

In [17], a system architecture is proposed, which uses virtual machines, which can be used in the implementation of software fault-tolerant systems. The top level in its hierarchy details the recovery actions implemented by the various policies such as N-modularity, transparent coordination of developer efforts, robust procedures, and optimistic recovery that such a framework enables.

In [18], neural architectures are proposed for increasing fault tolerance. First, according to real deployment scenarios, the computation errors and weight errors are formalized, which are modeled by Multiply-Accumulate (MAC)-independent and identically distributed Bit-Bias (MiBB) model and Stuck-at-Fault (SAF) model in accordance. In the following, a multi-objective NAS framework is established based on failure models to identify high-performance and fault-tolerant replicable architectures. In addition, fault-tolerant training (FTT) is incorporated into the search process to further improve the fault-tolerance of iterative architectures.

The field of the Internet of Things (IoT), as noted in [19, 20, 21], has grown exponentially, and today it is a new field of application of specialized information systems. The IoT architecture includes a variety of sensors, actuators, radio frequency and wired network channels [23]. A failure in IoT can occur at any level of its architecture. The application of fault-tolerant data distribution plays an important role for IoT-enabled systems in ensuring quality of service (QoS). This will reduce latency, reduce power consumption, and maximize throughput. For this purpose, a systematic review of data aggregations, data dissemination and independent mechanisms is used. Data distribution becomes efficient when data aggregation, error detection, and fault tolerance are performed at the same communication layer. Many developers have theoretical framework discussions aiming to find efficient and fault-tolerant data distribution using group formation framework for IoT-enabled system and various fault-tolerant methods including benchmarking approach.

The analysis of the state of ensuring fault tolerance, survivability and protection of information in the currently existing information technologies covered almost all levels of the systems built on their basis - from their hardware platform to the application software of automated client workplaces and computer networks on which they are based. As a conclusion, we have to agree with the conclusion that today a large number of quite effective methods of ensuring fault resistance, survivability and protection of information in distributed specialized information systems have been developed. But their weaknesses, which restrain their application, are low availability, due to large financial costs, increasing complexity and limitations of the integrated application of all means at all levels of the information systems architecture.

3. Formulation of the problem

The continuous development of computer information technologies has led to the need to use similar technologies in an increasingly wide range of applications in the construction of specialized information systems. This, in turn, requires a new approach in their construction. They must provide their functionality with simultaneously high levels of fault tolerance, survivability and protection of the information processed in them. And since we are talking about specialized information systems of wide application, they should also be financially affordable.

At present, the issues of fault tolerance and survivability of computer equipment due to the use of their reliability, redundancy, methods and means of technical and diagnostic maintenance, their reconfiguration, maintenance and repair are quite well studied. However, providing these tools separately from each other does not lead to a significant increase in the reliability and fault tolerance of complex systems, which are modern computer systems.

The task is to find such a model of the architecture of information technology, which would integrate both the means of ensuring fault tolerance and the means of survivability and protection of information, so that it could become the basis for the construction of specialized information systems. In this way, the scientific problem solved can be described as relevant and as one that has wide practical application.

4. Main part

4.1. Using the convergence of methods to increase the survivability of the system

Ensuring fault tolerance, survivability and protection of information in specialized information technologies, which function under the constant threat of the effects of destructive software and computer attacks using developed methods, makes it possible to improve their resistance to the negative manifestations of various destructions in each individual case. But part of the steps of three different developed methods [25, 26] are convergent, so it is advisable to combine them into one method according to common steps and states of the system in which it will be implemented.

Then a subsystem will be presented in the information system, which will implement the provision of fault tolerance, survivability and information protection of specialized information technologies, which will combine all three developed methods [23].

At the heart of solving the task of building a specialized information system with increased means of ensuring fault tolerance, survivability and protection of information, an architectural approach based on the use of the presented abstract model is obviously quite important. The application of the generalized method [23] of providing fault tolerance, survivability and information protection allows to simplify the technology of implementation of protection subsystems, allowed the joint use of the same resources, which contributed to increasing the efficiency of subsystems ensuring fault tolerance, survivability and information protection. His idea is shown in the form of a graph model in figure 1.

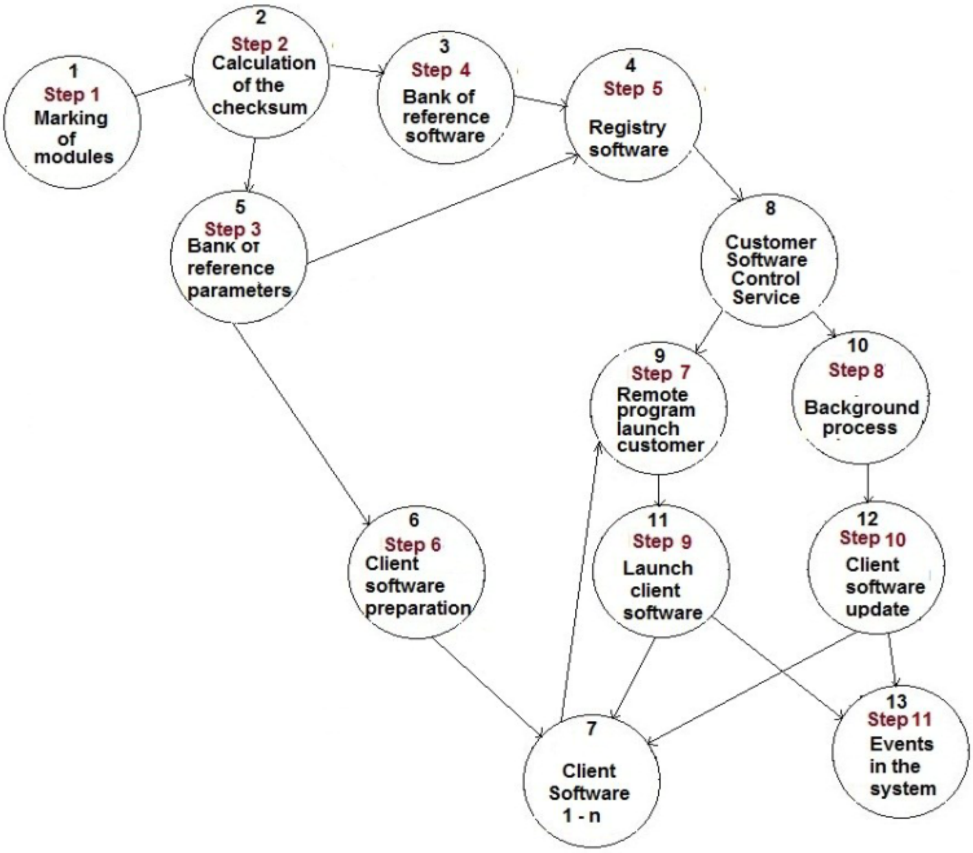


Figure 1: The integrated model of the combination of methods of ensuring survivability and protection of information in the information system is presented in the form of a graph.

Each vertex of the given graph model corresponds to the steps of the integrated method, which are conditionally divided into four groups of method steps: preparatory, ensuring fault tolerance and survivability, ensuring information protection, and steps of documenting events in IS. And each edge can transition between steps.

To assess the level of fluidity of information technology, you can use the generalized minimax criterion [24], which is presented in the following form:

$$K = \min_{y \in Y} \max_{x \in X} F(x, y), \qquad (1)$$

where:

$$X = (x_1, x_2,,,.x_n),\ Y = (y_1, y_2,,,.y_n)$$

Here, x_1, x_2,...,.x_n are the parameters of resistance:
x1 – workplace productivity;
x2 – reliability of information system elements;
x3 - fault tolerance of subsystems;
x_4 - number and type of performed functions;
x_5 - calculation accuracy;
x6 - bandwidth of network channels;
x7 - RAM capacity;
...
xn are other parameters affecting fault tolerance.
y1, y2,...,.yn - parameters of survivability and information protection parameters:
y1 - number and type of performed functions;
y2 - control over information processing by the operator;
y3 - operator activity control;
y4 - control of the relevance of the software of automated workplaces;
y5 - availability of a backup system;
y6 - control over computer network channels;
y7 - encryption of network traffic;
y8 - division of the computer network into virtual segments-subnets;
...
yn - and so on.

4.2 Solving the task of obtaining a specialized IT architecture

The key aspect, according to the generalized method, the graph model of which is shown in figure 1, is the creation of a system architecture that can adapt to the requirements of a specific specialized IS. The IS architecture development process itself will include the implementation of two stages.

The first is the development of the constructive part of the system, the second is its adaptation to the specific functionality of the system due to the iterative nature of the process itself. This approach to the development of IS made it possible to ensure the implementation of such general requirements for the construction of systems as systematicity, openness, compatibility, unification and efficiency.

As a result, an IS architecture was obtained in which a rational ratio between costs and target effects was achieved. For the convenience of presenting the architecture of a specialized IS, we will present it with a generalized macro-level model (Figure 2).

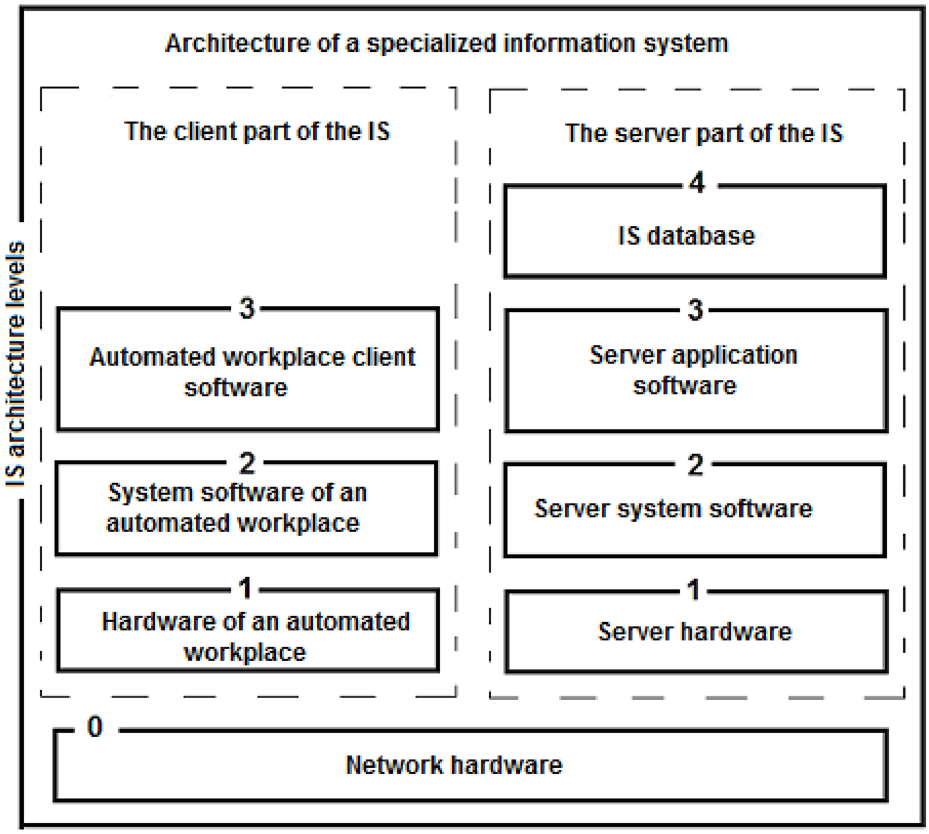

Architecture of a specialized information system
IS architecture levels
The client part of the IS
The server part of the IS
4
IS database
3
Automated workplace client software
3
Server application software
2
System software of an automated workplace
2
Server system software
1
Hardware of an automated workplace
1
Server hardware
0
Network hardware

Figure 2: Generalized macro-level model of the architecture of specialized IS.

It includes client and server parts, each of which is implemented by several levels of its components. Its feature is the inclusion in the components of all levels of the architecture of means that are responsible for fault tolerance, survivability and information protection, taking into account the overall efficiency of IS.

Another, zero level of the IS macro-architecture shown in Figure 2, includes network hardware that serves to combine the client and server parts into a single system.

To solve the problem of obtaining an information system architecture with an increased level of fault tolerance, survivability and information protection, it is proposed to implement a method that includes three groups of steps:

- steps of the method for the server part of the IS;
- method steps for client workplaces;
- steps of the method for the network part of the IS.

4.3 A model for ensuring fault tolerance, survivability and information protection for the server part of the IS

The architecture of the hardware platform of the server part (Figure 2) has a much more complex component structure compared to the architecture of the client ARM - it is not only the center around which the entire specialized IS is built, but also the location of the information processed in the system. Therefore, ensuring increased survivability, fault tolerance and information protection of the server part of specialized IS is the main task that needs to be solved when building any information system.

We formulate the main requirements for the architecture of the server part, in the form of steps of the method of ensuring fault tolerance, survivability and information protection:

1. Inclusion in the server part of two servers - the main server and the backup server, which must be territorially distributed;
2. Inclusion in the IS architecture of the crypto-protection server;
3. Introduction to the server part of the backup service;
4. Introduction of software update control service.
5. Each of the servers must:

- powered by intelligent power supply units, which guarantees the integrity and consistency of data, non-damage of database structures;
- include disk subsystems organized according to the scheme of the RAID-array type 1, which will increase the protection of information;
- provide background quality control of the surfaces of disk drives, which will allow early response to possible problems.

The implementation of all steps of the method is shown in the form of a model of the architecture of the server part of the IS in Figure 3, where its main component composition is given. As can be seen from the model (Figure 3), the architecture of the server part of the IS includes main and backup, territorially separated database servers (step 1). They are connected by the backup service, which is based on its own information channel, which allows you to maintain the relevance of backup copies at a high level (step 3).

If the main IS server fails, the system will automatically switch, with a slight time delay, to the backup server, where an up-to-date copy of the database is always present. This organization of IS architecture ensures its high fault tolerance and survivability.

The crypto-protection server serves to encrypt the network traffic of uncontrolled information transmission channels (step 2), which makes network intelligence impossible to a large extent.

Another important aspect of the proposed architecture of the server part of the IS is the inclusion in its composition of the component that is responsible for the relevance of the client software of the ARM (step 4). It includes a repository of client software that allows you to update and restore damaged software of client ARMs in automatic mode, which contributes to increasing fault tolerance and survivability of client ARMs, constant availability of IS functions. The same service provides the client software, upon its request, with parameters to run if the request is found to be legitimate. Such an algorithm excludes access to database information of illegal copies of software, which increases information security.

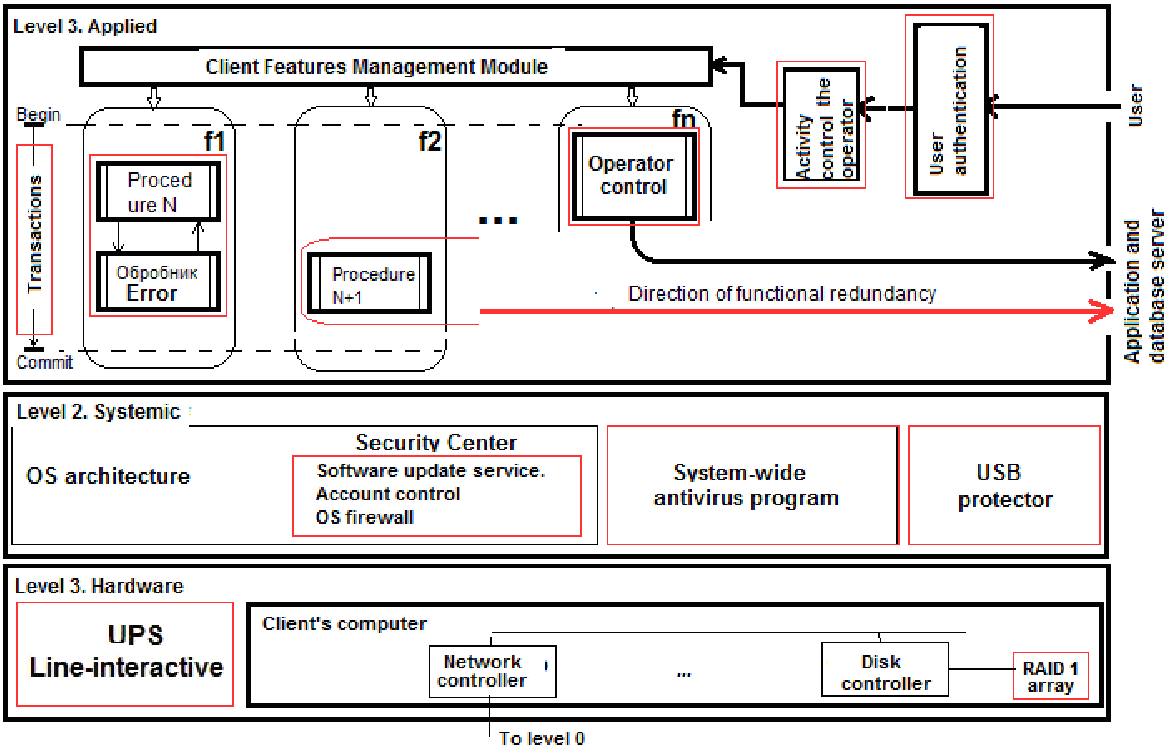


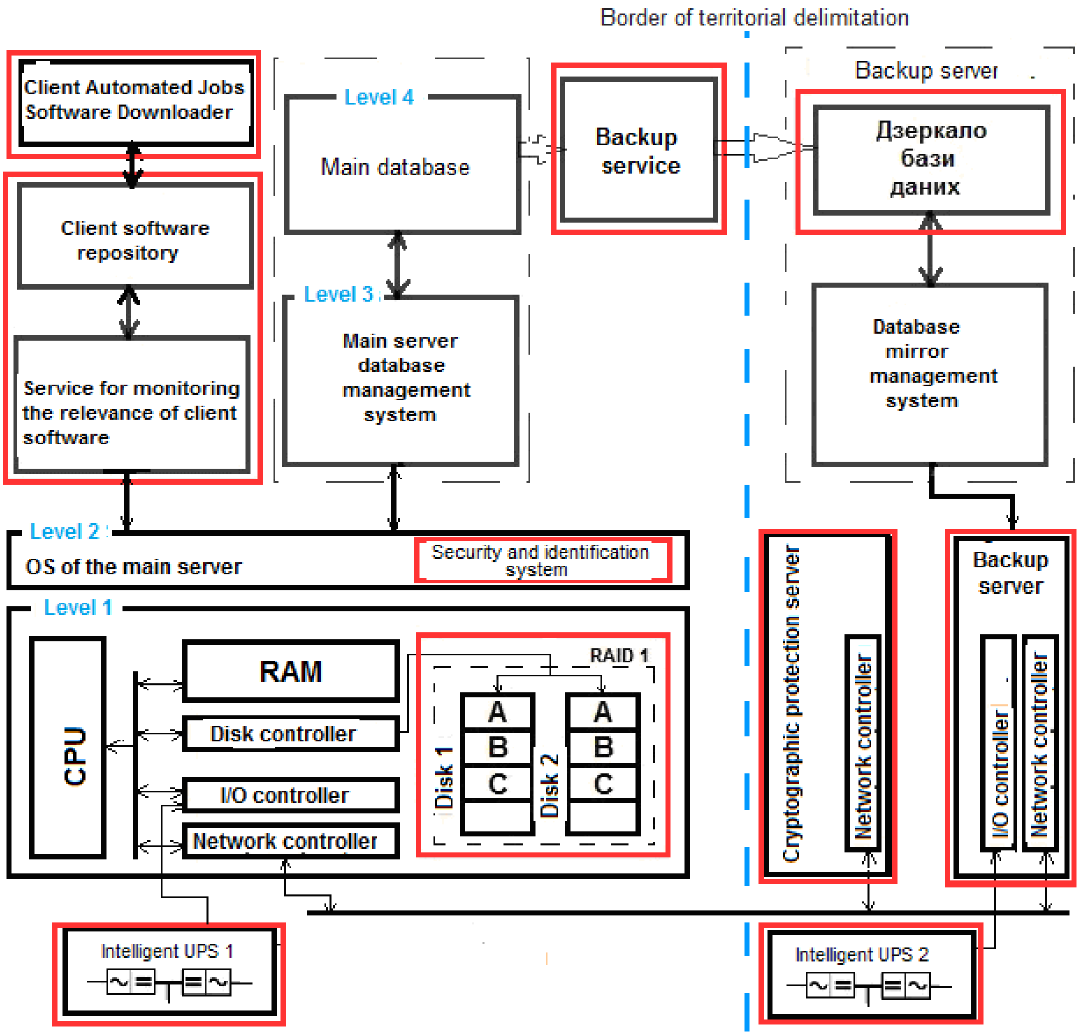
Figure 3: Microarchitecture of the hardware platform of a typical ARM client part of the IS.

4.4 A model for ensuring fault tolerance, survivability and information protection for the client part of the IS using the convergence of methods

In order to ensure fault tolerance, survivability and protection of information, the second group of steps of the generalized method is formulated as follows:

1. Connecting the client workstation to the server involves obtaining launch parameters if the launch request is recognized as legitimate.
2. Mandatory user authentication in the IS.
3. Control over the actions of the workplace operator from the IS side.
4. Monitoring the activity of the workplace operator.
5. All information editing is performed under transaction management.
6. The client computer does not store information, both that which is processed in the IS and that which serves to run the client software.
7. The set of available functions of the client workplace is determined by the parameters stored on the database server.

The implementation of all the steps of the second group of the method made it possible to build a model of the architecture of the client's workplace with the means of ensuring fault tolerance, survivability and information protection implemented in it. As can be seen from Figure 4, it is a three-level structure, where the first level is the hardware platform of the client workplace, the second is the level of system software, and the third level is the level of application software that implements a certain set of IS functions.



Border of territorial delimitation
Backup server
Client Automated Jobs Software Downloader
Level 4
Main database
Backup service
Дзеркало бази даних
Client software repository
Level 3
Main server database management system
Database mirror management system
Service for monitoring the relevance of client software
Level 2
OS of the main server
Security and identification system
Level 1
CPU
RAM
Disk controller
I/O controller
Network controller
RAID 1
Disk 1
A
B
C
Disk 2
A
B
C
Cryptographic protection server
Network controller
Backup server
I/O controller
Network controller
Intelligent UPS 1
Intelligent UPS 2

Figure 4: The architecture of the server part of the information system is depicted with micro-level detail.

The micro-architecture of the system software of the client's automated workplace (Figure 3, level 2) includes components of the operating system and other system software, which are intended to provide fault tolerance, survivability and information protection. Almost all operating systems include a subsystem with the conventional name "Security Center", which, in turn, includes the following components:

- update service – provides support for OS software in an up-to-date state;
- account control service - provides controlled access to the computer according to authority. Contributes to the protection of information from its acquisition by outsiders;
- the Windows firewall provides control over incoming and outgoing connections. Connections that do not meet security requirements are automatically blocked. With

this, it protects Internet traffic, preventing the penetration of malicious software into the computer, which generally increases the survivability of the IS.

Also, the architecture of this level includes means of general countermeasures against system-level malicious software (antiviruses, protector and USB, etc.).

The architecture of the client part ends with the third level (Figure 4), which is a layer of application software that implements the functions of the user's ARM. A feature of its implementation is the integrated use of means of fault tolerance, survivability and information protection (steps 1 - 6). They are integral parts of almost all components of the APM, which, together with the means of the two lower levels, made it possible to obtain a client APM with increased parameters of resistance, survivability and security of the information processed by it.

Each ARM is a set of functions f1 - fn (Figure 4 level 3), each of which is built using a typical skeletal part, realizing the principle of unification. The skeletal parts include means of fault tolerance and survivability: procedures using two interacting processes, one of which is a non-trivial error handler (f1 Figure 4), functional redundancy, with the possibility of managing the workload of an automated workplace (f2 Figure 4). Maximum attention is paid to the protection of information on the side of the automated workplace.

A number of software components are used. These include non-trivial data editors with data integrity control elements (fn Figure 4), execution of all data manipulations under transaction management, as well as components of user authentication and its activity in IS.

4.5 A model for providing fault tolerance, survivability and information protection of specialized IT in its network architecture

The network part of the information system is built by following the following steps of the generalized method of ensuring fault tolerance and survivability of information technology:

1. The IS network is segmented into virtual segments.
2. The main and backup server are geographically separated and placed in a local segment that is not accessible from the external network.
3. The crypto-protection server ensures the inaccessibility of specialized IS information from the external network and serves as a connecting link between clients and the server part.
4. All information channels of the IS network are divided into open and closed. Access control to open channels is carried out organizationally, and information is transmitted in encrypted form on closed channels.
5. All ARM clients connected to open channels work using the key generated by the crypto server when setting up access.

The architecture of the network component includes a managed switch and data cable lines (Figure 5). This architecture uses two types of information channels. The first type is channels that are under constant control and therefore allow data transmission in an open form, which allows you to achieve maximum work productivity.

The second type is uncontrolled. Through them, data is transmitted in the mode of cryptographic protection. This reduces the performance of the IS, but ensures data security.

As can be seen from Figure 5, the use of a managed switch makes it possible to create virtual local networks with their own security policies.

The use of switches with the possibility of implementing such an architecture in combination with cryptographic protection of network traffic significantly increases the parameters of the survivability of the IS and the protection of information in the IS, reliably preventing the conduct of network intelligence, depriving attackers of the information necessary to launch an attack.

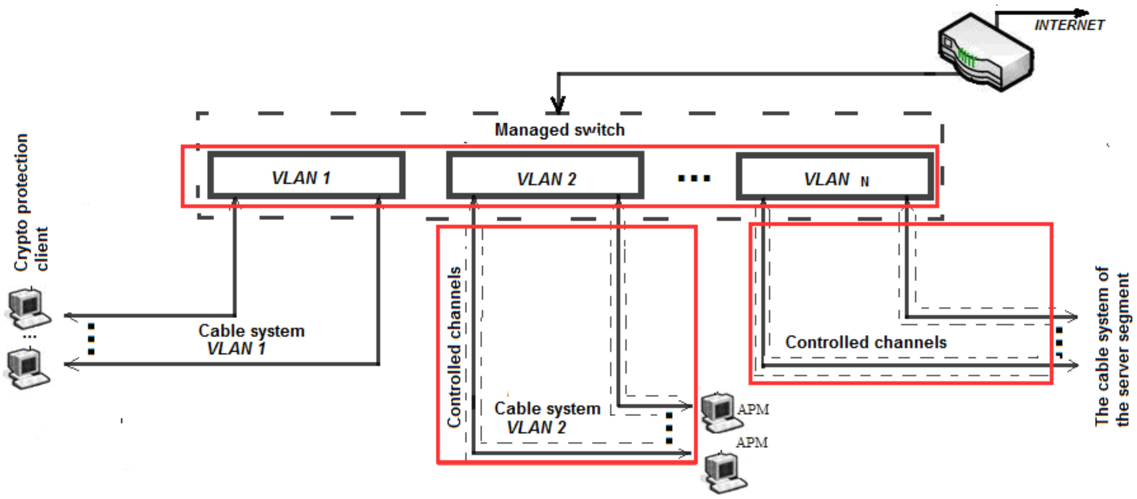


Figure 5: Micro-architecture of the network part of the information system.

As a result, the proposed architecture guarantees the invisibility of the main and backup servers from the external network. All requests of client automated workplaces, in an encrypted form, are sent to the crypto protection server. A simplified diagram of this implementation of the server segment is shown in Figure 6.

Each client of the crypto server is provided with a key generated during its configuration. In this way, the crypto server will be able to decrypt and redirect the request of only the registered client.

Such network organization can be very useful for corporations implementing their own specialized IS. This can be achieved by using managed switches that provide the creation of virtual local networks.

By combining all the steps of the three groups, we will get a generalized method of building a model of a specialized information system with an increased degree of fault tolerance, survivability and information protection.

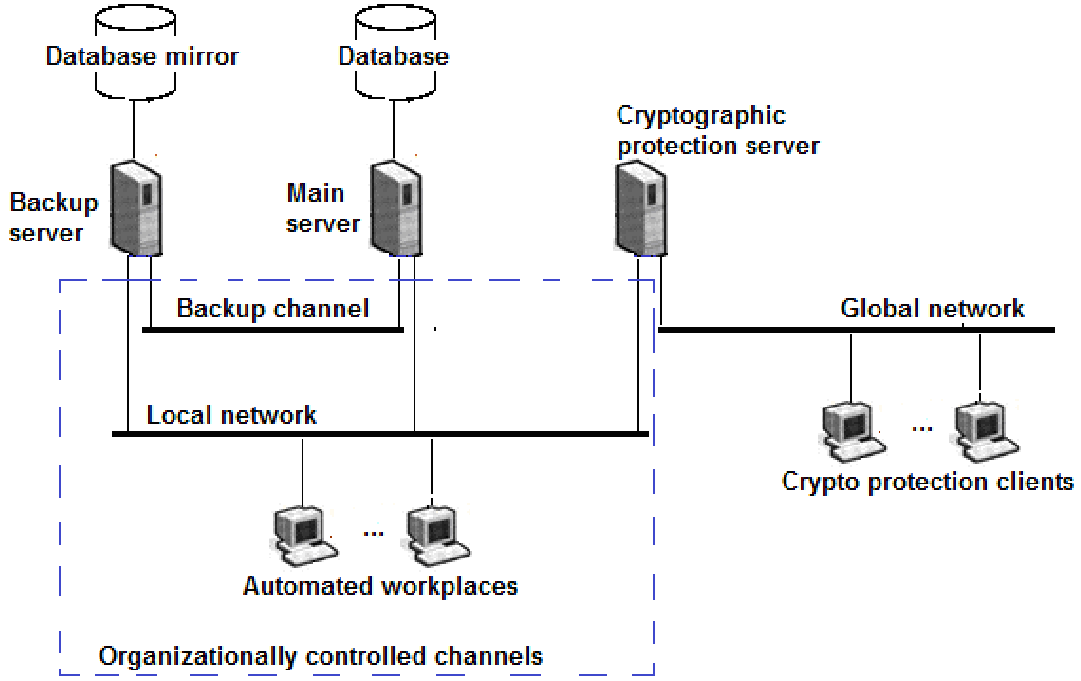
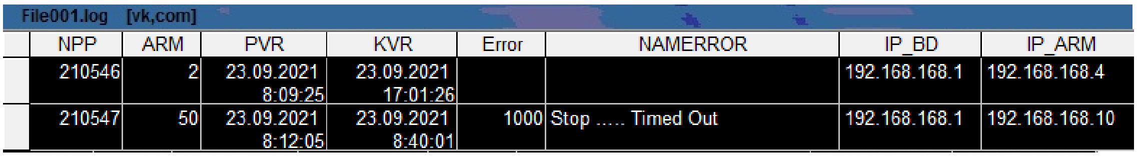


Figure 6: Topology scheme of the IS computer network with provision of cryptographic protection of information.

5. Experimental studies

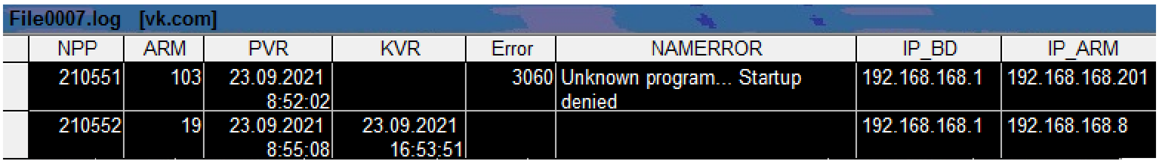
Figure 7 shows the reaction of the system to the lack of activity of the operator of client ATM No. 50. In order to prevent uncontrolled access to IS information through the use of an ATM that may not be controlled by the operator.



File001.log [vk,com]

NPP	ARM	PVR	KVR	Error	NAMERROR	IP_BD	IP_ARM
210546	2	23.09.2021 8:09:25	23.09.2021 17:01:26			192.168.168.1	192.168.168.4
210547	50	23.09.2021 8:12:05	23.09.2021 8:40:01	1000	Stop ..... Timed Out	192.168.168.1	192.168.168.10

Figure 7: IC reaction to the time-out of ARM No. 50.



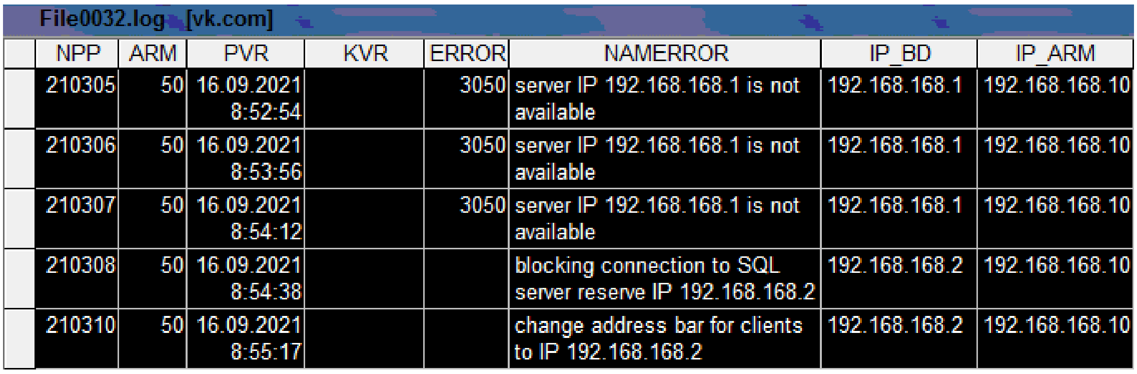
File0007.log [vk.com]

NPP	ARM	PVR	KVR	Error	NAMERROR	IP_BD	IP_ARM
210551	103	23.09.2021 8:52:02		3060	Unknown program... Startup denied	192.168.168.1	192.168.168.201
210552	19	23.09.2021 8:55:08	23.09.2021 16:53:51			192.168.168.1	192.168.168.8

Figure 8: Reaction of the information system to an attempt to launch illegal software.

IS reaction to an attempt to launch the software of a reference software not registered in the bank of the service of monitoring the relevance of the client's software. In Figure 8 shows the event 210551 recorded in the log file. It shows that at the specified time an attempt was made to launch the ARM software No. 103 from the computer station with the IP address 192.168.168.201. Since it conflicts with the connection registry reference parameters, this ARM is not allowed to run.In this way, the IS prevents the possibility of obtaining illegal access to information through the use of illegal copies of software of client workstations, stopping the attack from within the system. An external attack on the server is practically impossible due to classified traffic and network segmentation with clearly defined security policies, which makes it invisible from the external network and does not show up during port scanning.

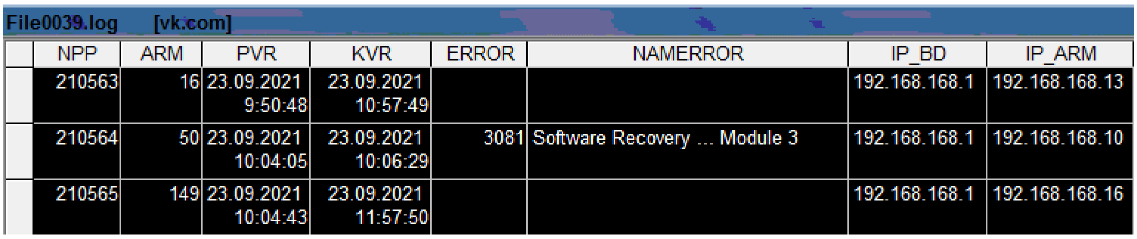
In Figure 9 shows the sequence of events recorded in the IS log file, which illustrate the process of losing access to the main server and switching client ARMs to the backup one. A special procedure that monitors the availability of the main server with a period of one minute switches client ARMs to the backup server after three confirmations of the unavailability of the main server. This is necessary to prevent accidental switching of servers.



File0032.log [vk.com]

NPP	ARM	PVR	KVR	ERROR	NAMERROR	IP_BD	IP_ARM
210305	50	16.09.2021 8:52:54		3050	server IP 192.168.168.1 is not available	192.168.168.1	192.168.168.10
210306	50	16.09.2021 8:53:56		3050	server IP 192.168.168.1 is not available	192.168.168.1	192.168.168.10
210307	50	16.09.2021 8:54:12		3050	server IP 192.168.168.1 is not available	192.168.168.1	192.168.168.10
210308	50	16.09.2021 8:54:38			blocking connection to SQL server reserve IP 192.168.168.2	192.168.168.2	192.168.168.10
210310	50	16.09.2021 8:55:17			change address bar for clients to IP 192.168.168.2	192.168.168.2	192.168.168.10

Figure 9: Reaction of the information system when the main server is unavailable.



File0039.log [vk.com]

NPP	ARM	PVR	KVR	ERROR	NAMERROR	IP_BD	IP_ARM
210563	16	23.09.2021 9:50:48	23.09.2021 10:57:49			192.168.168.1	192.168.168.13
210564	50	23.09.2021 10:04:05	23.09.2021 10:06:29	3081	Software Recovery ... Module 3	192.168.168.1	192.168.168.10
210565	149	23.09.2021 10:04:43	23.09.2021 11:57:50			192.168.168.1	192.168.168.16

Figure 10: Updating the software of the automated workplace due to its non-compliance with the reference parameters.

In the background, the control service checks the software of client workplaces for relevance. In Figure 10 shows the event 210564 of the log file, which recorded the fact of non-compliance of the parameters of the software modules of ARM No. 3 with the reference ones. The reason for this can be a SWP attack or self-destruction, as a result of which the checksum of the module has changed and it had to be updated from the system SW bank.

According to the given examples of fragments of log files (Figure 7 - 10), it was established that the means of ensuring fault tolerance, survivability and protection of

IS information have a sufficient level of selectivity to the causes of disturbances in the system, providing its personnel with a wide range of information for further analysis.

Graphs (Figure 11) obtained by calculations according to formula (2) for the survivability results of formula (2) are shown:

$$K_e(M_{IT}) = \sum_{j=1}^{m} \sum_{p=0}^{n_p} \sum_{q=0}^{n_q} \left(\alpha_{1,j,p,q} \cdot \frac{T_{f_1(M_i),1}}{T_{f_1(M_i),1} - (T_{f_1(M_i),2} + T_{f_1(M_i),3})} + \alpha_{2,j,p,q} \cdot \frac{T_{f_2(M_i),1} + T_{f_2(M_i),2}}{T_{f_2(M_i),1}} \right), \tag{2}$$

Where $\alpha_{1,j,p,q}$ – is the coefficient for the value that determines fault tolerance in quantitative units;

$\alpha_{2,j,p,q}$ – coefficient for the value that determines survivability in quantitative units; $\alpha_{1,j,p,q} + \alpha_{2,j,p,q} = 1$.

$$\mu = \frac{1}{\sum_{j=1}^{m} \sum_{p=0}^{n_p} \sum_{q=0}^{n_q} \left(\alpha_{1,j,p,q} \cdot \frac{T_{f_1(M_i),1}}{T_{f_1(M_i),1} - (T_{f_1(M_i),2} + T_{f_1(M_i),3})} + \alpha_{2,j,p,q} \cdot \frac{T_{f_2(M_i),1} + T_{f_2(M_i),2}}{T_{f_2(M_i),1}} \right)},$$

The estimated values of fault tolerance and survivability of the given information technology are shown in Figure 12 when implementing the developed generalized method of ensuring its fault tolerance and survivability into a typical information system, calculated according to formula (3) and reflect the appropriate level of resistance to malicious software destruction and various computer attacks in the process of activation of subsystems ensuring system survivability, which is ensured at a level of at least 67% [25].

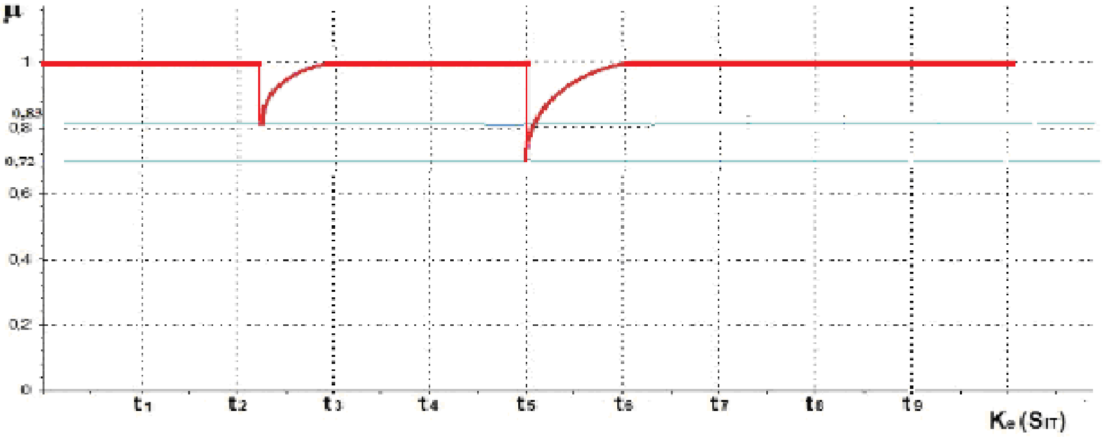


Figure 11: Schedule of manifestations of the vitality of the information system.

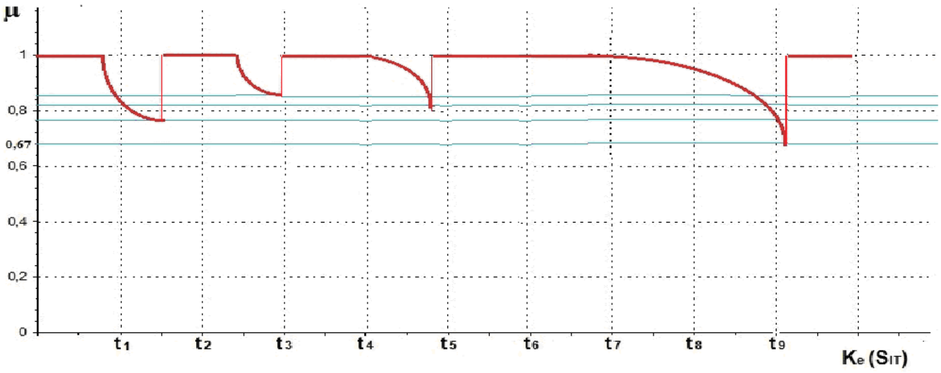


Figure 12: Evaluation of the values of levels of fault tolerance and survivability of IS.

6. Conclusions

Thus, the proposed architecture of the information system implemented in itself the developed method of ensuring fault tolerance, survivability and information protection of information technology, which consists in combining and integrating into information technology mechanisms for ensuring fault tolerance, survivability and protection of information according to their coincidences in states when responding to the destruction of malicious software security and computer attacks, which made it possible to create specialized IS resistant to these influences.

According to the developed method of ensuring fault tolerance, survivability and protection of IT information, the architecture of the means in which it is implemented is proposed, on the basis of which an IS is created for conducting experimental studies on the proposed solution for improving the fault tolerance, survivability and protection of information of specialized IT under the effects of cyberattacks and computer attacks.

As a result of the use of the listed measures, an information system architecture of highly specialized use for various fields of application was obtained, where processes are monitored in unreal or unreal time with improved parameters of fault tolerance, survivability and information protection. The results of the research conducted with the developed IS and the application of the IT performance evaluation methodology confirm the improved level of stability and survivability in corporate computer networks, which is more than 67%, for IT in which the method of ensuring fault tolerance, survivability and protection of IT information is implemented.

References

[1] P. Stavroulakis, M. Kolisnyk, V. Kharchenko, N. Doukas, O. Markovskyi, N. Bardis, Reliability, Fault Tolerance and Other Critical Components for Survivability in Information Warfare. In: M. Obaidat, E. Cabello, (eds) E-Business and Telecommunications. ICETE 2019. Communications in Computer and Information Science, vol 990. Springer. doi: 10.1007/978-3-030-11039-0_17.

[2] T. Frederiksen, J. Hesse, A. Lehmann, R. Torres Moreno, Identity Management: State of the Art, Challenges and Perspectives. In: Friedewald, M. Önen, M. Lievens, E. Krenn, S. Fricker,

(eds) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, 576 (2019). Springer, Cham. doi: 10.1007/978-3-030-42504-3_4.

[3] S. Jarecki, A. Kiayias, H. Krawczyk, Round-optimal password-protected secret sharing and T-PAKE in the password-only model. In: P. Sarkar, T. Iwata, (eds.) ASIACRYPT 2014. LNCS, Springer, Heidelberg 2014 vol. 8874, pp. 233–253. doi: 10.1007/978-3-662-45608-8_13.

[4] T. Frederiksen, Y. Lindell, V. Osheter, B. Pinkas, Fast distributed RSA key generation for semi-honest and malicious adversaries. In: H. Shacham, A. Boldyreva, (eds.) CRYPTO 2018. LNCS, Springer, Cham, 10992 (2018) 331–361. doi: 10.1007/978-3-319-96881-0_12.

[5] F. Wu, S. Tung, J. Huang, A Robust Two Factor Authentication Scheme with Fine Grained Biometrics Verification. In: S. Hsieh, L. Hung, R. Klasing, (eds) New Trends in Computer Technologies and Applications. ICS 2022. Communications in Computer and Information Science, Springer, Singapore, 1723 (2022) 407-418. doi: 10.1007.

[6] L. Mei, C. Xu, L. Li, Efficient Forward and Backward Private Searchable Symmetric Encryption for Multiple Data Sources. In: X. Sun, X. Zhang, Z. Xia, E. Bertino (eds) Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science, 1424 (2021). Springer, Cham. doi: 10.1007/978-3-030-78621-2_10.

[7] Martínez, F. García, A Comparative Study Between Two Numerical Methods for Symmetric Cryptography Uses and Applications. In: Latifi, S. (eds) ITNG 2021 18th International Conference on Information Technology-New Generations. Advances in Intelligent Systems and Computing, 1346 (2021). Springer, Cham. doi: 10.1007/978-3-030-70416-2_16.

[8] S. Vatshayan, R. Haidri, J. Verma, Design of hybrid cryptography system based on vigenère cipher and polybius cipher, in 2020 International Conference on Computational Performance Evaluation (ComP E(IEEE, New York, 2020), pp. 848–852.

[9] K. Miteloudi, L. Batina, J. Daemen, N. Mentens, ROCKY: Rotation Countermeasure for the Protection of Keys and Other Sensitive Data. In: A. Orailoglu, M. Jung, M. Reichenbach, (eds) Embedded Computer Systems: Architectures, Modeling, and Simulation. SAMOS 2021. Lecture Notes in Computer Science, vol 13227. Springer. doi: 10.1007/978-3-031-04580-6_19.

[10] K. Balogun, M. A. Gbolagade, A Hybrid Metaheuristic Algorithm for Features Dimensionality Reduction in Network Intrusion Detection System. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2021. ICCSA 2021. Lecture Notes in Computer Science(), vol 12957. Springer, Cham. doi: 10.1007/978-3-030-87013-3_8.

[11] A. Balogun, N. Akande, F. Usman-Hamza, V. Adeyemo, Rotation Forest-Based Logistic Model Tree for Website Phishing Detection. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2021, 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part IX, pp 154-169. doi: 10.1007/978-3-030-87013-3_12.

[12] O. Savenko, A. Nicheporuk, I. Hurman, S. Lysenko, Dynamic signature-based malware detection technique based on API call tracing, CEUR-WS 2393 (2019) 633-643.

[13] J. Li Zhang, C. Chen, K. Lee, L. Lee, A Practical Botnet Traffic Detection System Using GNN. In: Meng, W., Conti, M. (eds) Cyberspace Safety and Security. CSS 2021. Lecture Notes in Computer Science(), vol 13172. Springer, Cham. doi: 10.1007/978-3-030-94029-4_5.

[14] F. Ja'fari, S. Mostafavi, K. Mizanian, E. Jafari, An intelligent botnet blocking approach in software defined networks using honeypots. J. Ambient Intell. Humanized Comput., 2993–3016 (2020). doi: 10.1007/s12652-020-02461-6.

[15] S. Lysenko, K. Bobrovnikova, O. Savenko, A Botnet Detection Approach Based on The Clonal Selection Algorithm, in: Proceedings of 2018 IEEE 9th International Conference on Dpendable Systems, Services and Technologies, DeSSerT-2018, Ukraine, (2018), pp. 424-428.

[16] J. Liu, J. Zhang, C. Du, D. Wang, A Multi-model System for Insider Threat Detection. In: Y. Xu, H. Yan, H. Teng, (eds) Machine Learning for Cyber Security. ML4CS 2022. Lecture Notes in Computer Science, vol 13655. Springer, (2023). doi: 10.1007/978-3-031-20096-0_23.

[17] M. Ancona, A. Clematis, G. Dodero, E. Fernandez, V. Gianuzzi, System Architecture for Software Fault Tolerance. In: Belli, F., Görke, W. (eds) Fehlertolerierende Rechensysteme / Fault-Tolerant Computing Systems. Informatik-Fachberichte, 147 (2018). Springer, Berlin, Heidelberg. doi: 10.1007/978-3-642-45628-2_24.

[18] K. Hu, D. Ding, S. Tian, R. Gong, L. Luo, FTR-NAS: Fault-Tolerant Recurrent Neural Architecture Search. In: H. Yang, K. Pasupa, A. Leung, J. Kwok, (eds) Neural Information Processing. ICONIP 2020. Communications in Computer and Information Science, 1333 (2020). Springer, Cham. doi: 10.1007/978-3-030-63823-8_67.

[19] V. Prajapati, T. Sharma, L. Awasthi, Theoretical Aspect on Fault-Tolerant Data Dissemination in IoT Enabled Systems. In: V. Balas, G. Sinha, B. Agarwal, (eds) Emerging Technologies in Computer Engineering: Cognitive Computing and Intelligent IoT. ICETCE 2022. Communications in Computer and Information Science, 1591 (2022). Springer, Cham. doi: 10.1007/978-3-031-07012-9_15.

[20] M. Moghaddam, H. Muccini, Fault-Tolerant IoT. In: R. Calinescu, F. Giandomenico, (eds) Software Engineering for Resilient Systems. SERENE 2019. Lecture Notes in Computer Science, 11732 (2019), Springer, Cham. doi: 10.1007/978-3-030-30856-8_5.

[21] Y. Ishikawa, K. Sugiura, D. Takao, Fault Tolerant Data Stream Processing in Cooperation with OLTP Engine. In: A. Mondal, H. Gupta, J. Srivastava, P. Reddy, (eds) Big Data Analytics. BDA 2018. Lecture Notes in Computer Science, 11297 (2018). Springer, Cham. doi: 10.1007/978-3-030-04780-1_1.

[22] M. Fischer, O. Riedel, A. Lechler, Comprehensive Analysis of Software-Based Fault Tolerance with Arithmetic Coding for Performant Encoding of Integer Calculations. In: M. Trapp, F. Saglietti, M. Spisländer, F. Bitsch, (eds) Computer Safety, Reliability, and Security. SAFECOMP 2022. Lecture Notes in Computer Science, 13414 (2022). Springer. doi: 10.1007/978-3-031-14835-4_10.

[23] M. Stetsiuk, A. Kashtalian, The methods of ensuring fault tolerance, survivability and protection of information of specialized information technologies under the influence of malicious software. (Computer Systems And Information Technologies), 2022, №1, pp 36 - 44.

[24] J. Frank, Safety and Security of Cyber-Physical Systems Engineering dependable Software using Principle-based Development. Springer Vieweg Wiesbaden, (2022) 537. doi: 10.1007/978-3-658-37182-1.

[25] M. Stetsyuk, L, Bedratyuk, B. Savenko, V. Stetsyuk, O. Savenko, Providing the Resilience and Survivability of Specialized Information Technology Across Corporate Computer Networks. 1st International Workshop on Intelligent Information Technologies & Systems of Information Security.2020; CEUR-WS. 2623 (2020) 219-238.

[26] M. Patil, T. Abukhalil, S. Patel, T. Sobh, Ub swarm: hardware implementation of heterogeneous swarm robot with fault detection and power management. International Journal of Computing, 15(3), 2016, 162-176. doi:10.47839/ijc.15.3.849.