КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

DOI 10.28925/2663-4023.2023.21.162176
UDC 004.056:004.738.5

Nataliia Zviertseva
Graduate Student
Department of Software Engineering and Management Intelligent Technologies
National Technical University "Kharkiv polytechnic institute"
ORCID ID: 0000-0001-6279-7586
nataliezviertseva@gmail.com

SYNERGIC APPROACH BASED ASSESSMENT OF BUSINESS-PROCESSES CONTINUITY

Abstract. Informational threats can manifest themselves in different forms, which is due to the features of the global network. The article is devoted to one of the ways of solving the contradiction, which is that, despite the large number of publications, the task of ensuring the continuity of business processes in the conditions of the growing number and variety of cyber attacks on critical infrastructure objects remains unresolved. This is due to the constant modification and increase in the number of cyber attacks, as well as methods and technologies for implementing business processes. Therefore, the development and improvement of methods for assessing the continuity of business processes is an urgent scientific task. The article examines the problem of ensuring the continuity of business processes in the conditions of the growth of cyber threats. The means and methods of committing cybercrimes against critical infrastructure facilities were analyzed. The main strategies and business continuity assessment indicators are defined. The influence of selected strategies and solutions for ensuring business continuity on the value of business process continuity indicators is analyzed. The main trends in the development of cyber security in the context of improving the means and methods of carrying out terrorist information attacks on critical infrastructures are analyzed. Preventive measures to reduce the risk of cyberattacks at the national and international levels have been identified.
The main tasks of ensuring the continuity of business processes based on the PDCA risk management model, indicators for assessing business continuity are considered. The influence of the selected strategies and solutions on ensuring the continuity of business processes is analyzed.

Key words: cyberterrorism, cyberattack, critical infrastructure, business-processes continuity.

INTRODUCTION

The development of society at the beginning of the 21st century is characterized by the following main features [1-4]:

1. the transition from the information society to the high-tech society, which ensures the oversaturation of the latest information and communication technologies, the further development of globalization processes in the modern economy, the dynamics of informatization of such areas of society as the field of communications, energy, transport, oil and gas production and storage systems, financial and banking systems, defense and national security, structures to ensure the stable operation of ministries and departments, widespread transition to electronic management and document management methods;

2. bringing to the fore the most important task of ensuring the security of information, due to information processes occurring throughout the world. This is due to the special importance for the development of the state of its information resources, the growing cost of information in the market, its high vulnerability and often significant damage as a result of its unauthorized use;

3. the formation of a global information space, leading to the emergence of new threats and new forms of international conflicts, including information wars, network confrontations,

hacker attacks, etc., due to the rapid development of the Internet and other information and communication technologies.

The development of computer technologies and information and telecommunication networks give great opportunities to society, at the same time they also give rise to a new type of crime - cybercrime.

Formulation of the problem. The main contradiction underlying the scientific research is that, despite the large number of publications, the task of ensuring the continuity of business processes in the face of the growing number and variety of cyber attacks on critical infrastructure objects remains unresolved. This is due to the constant modification and increase in the number of cyber attacks, as well as the methods and techniques of implementing business processes. Therefore, the development and improvement of business process continuity assessment methods is an urgent scientific task.

Analysis of recent research of the methods of committing crimes of a criminal nature at critical infrastructure facilities and publications.

Information threats can manifest themselves in different forms, due to the characteristics of the global network. The features of the global network, which attracts both individual attackers and their groups, include the following [5-6]:

- Efficiency, cost-effectiveness and availability;

- Weak censorship or its complete absence, and in some cases, the lack of control by the state;

- the presence of a huge potential audience of users scattered around the world;

- fast and relatively cheap distribution of specially selected information, the complexity of its presentation and perception (sending e-mails, organizing news groups, creating sites for exchanging opinions, posting information on separate pages or in electronic versions of periodicals and network broadcasting, etc.);

– confidentiality and anonymity of user work, which are provided by most communication servers;

- availability of the possibility of using special robots (bots) to reduce the time and cost of destructive activities of intruders;

- high efficiency of consequences, which can be both local and global;

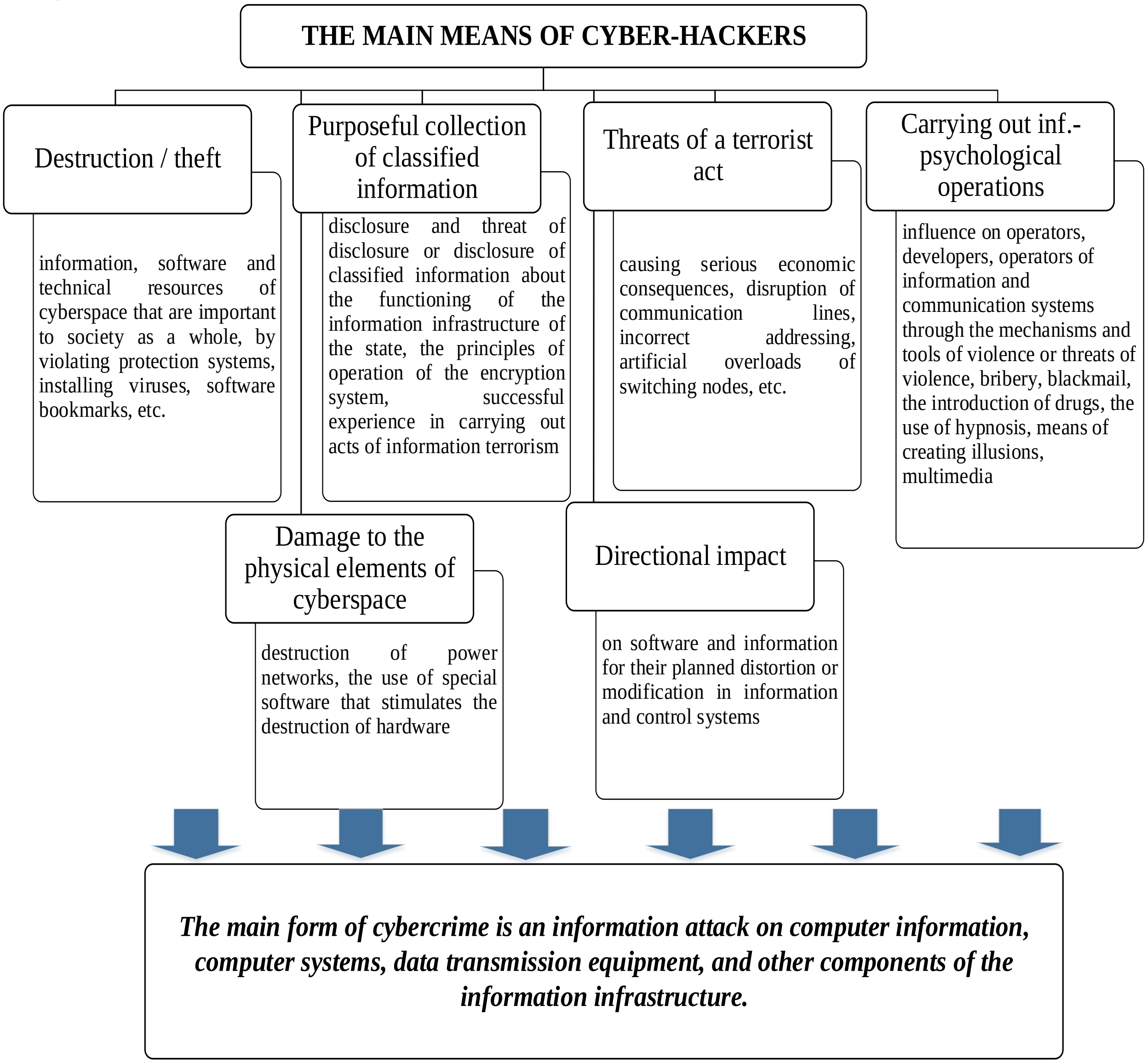
– the difficulty of tracking cybercrime and collecting evidence;

– uncertainty of the place, time and process of preparation for the implementation of cyber attacks;

- the possibility of organizing cyber attacks simultaneously on various objects or subjects from various directions without the need to violate any boundaries;

- the possibility of unauthorized connection to computer networks for managing strategic facilities, including military ones;

– spatial and temporal distance from the object or subject of a cyberattack. All cybernetic influences are carried out in cyberspace and directly through cyberspace. The main means of cybercrime are shown in fig. 1.



THE MAIN MEANS OF CYBER-HACKERS

Destruction / theft

information, software and technical resources of cyberspace that are important to society as a whole, by violating protection systems, installing viruses, software bookmarks, etc.

Purposeful collection of classified information

disclosure and threat of disclosure or disclosure of classified information about the functioning of the information infrastructure of the state, the principles of operation of the encryption system, successful experience in carrying out acts of information terrorism

Threats of a terrorist act

causing serious economic consequences, disruption of communication lines, incorrect addressing, artificial overloads of switching nodes, etc.

Carrying out inf.-psychological operations

influence on operators, developers, operators of information and communication systems through the mechanisms and tools of violence or threats of violence, bribery, blackmail, the introduction of drugs, the use of hypnosis, means of creating illusions, multimedia

Damage to the physical elements of cyberspace

destruction of power networks, the use of special software that stimulates the destruction of hardware

Directional impact

on software and information for their planned distortion or modification in information and control systems

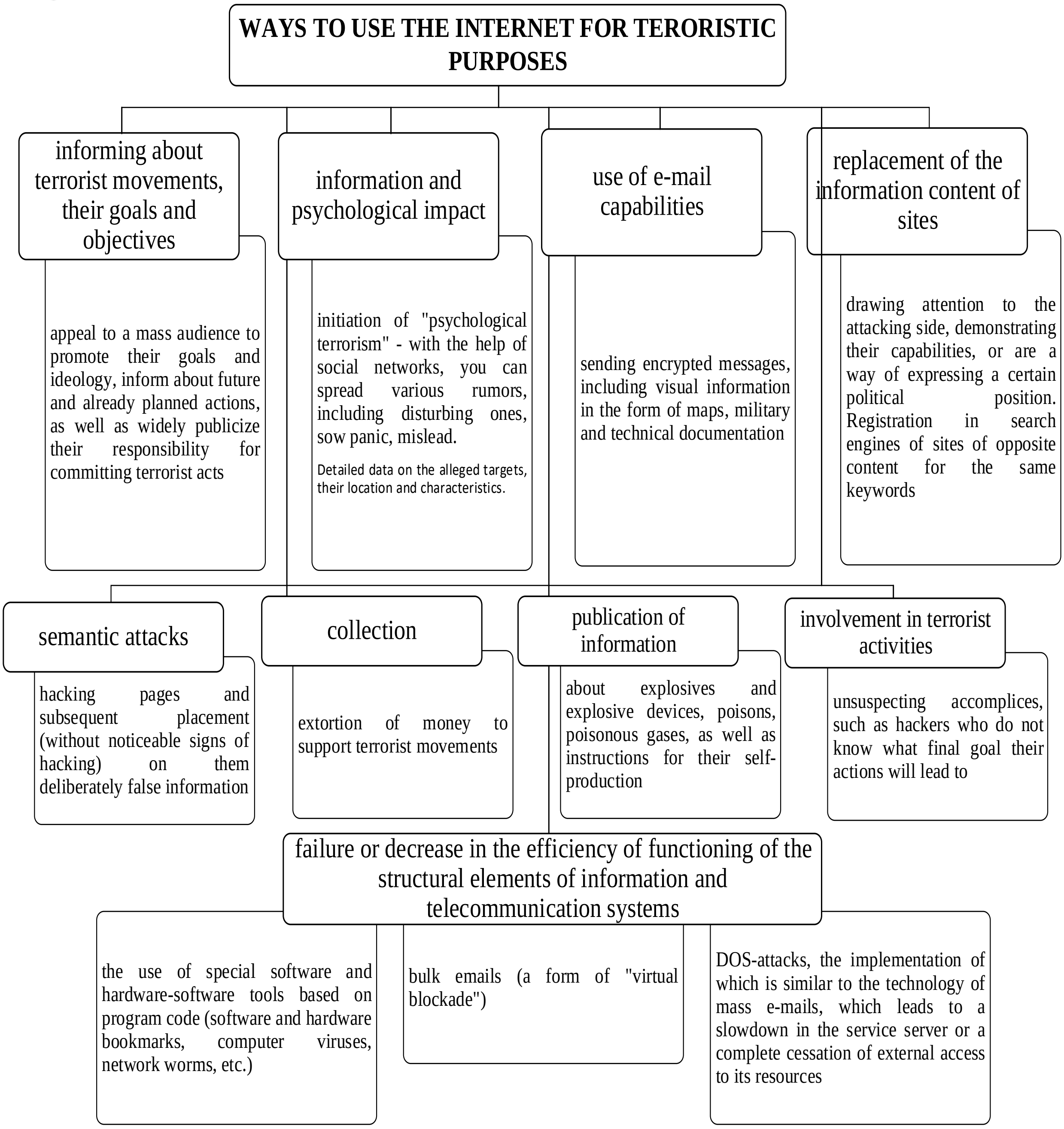
The main form of cybercrime is an information attack on computer information, computer systems, data transmission equipment, and other components of the information infrastructure.

Fig. 1. The main means of cyber attackers

Analysis of fig. 1 shows that criminal activity on the Internet is increasingly becoming a special type of information technology, increasingly using the capabilities of modern information and telecommunication systems for communication and information collection, most criminal acts are designed not only to cause material damage and threaten people's life and health, but also to information and psychological shock, the impact of which on large masses of people creates a favorable environment for the attackers to achieve their goals.

In the context of increasing globalization processes in the world and the formation of an information society, cyberterrorism has become an independent factor that can threaten the state integrity of countries and destabilize the international situation. Terrorist groups are increasingly using the capabilities of the latest information technologies and the Internet to spread propaganda and exchange information, attract new mercenaries, raise funds in their support, plan terrorist attacks, and also to control their implementation [7-10].

The main directions of using the latest information technologies and the Internet for terrorist purposes are shown in fig. 2.



WAYS TO USE THE INTERNET FOR TERORISTIC PURPOSES

informing about terrorist movements, their goals and objectives

appeal to a mass audience to promote their goals and ideology, inform about future and already planned actions, as well as widely publicize their responsibility for committing terrorist acts

information and psychological impact

initiation of "psychological terrorism" - with the help of social networks, you can spread various rumors, including disturbing ones, sow panic, mislead.

Detailed data on the alleged targets, their location and characteristics.

use of e-mail capabilities

sending encrypted messages, including visual information in the form of maps, military and technical documentation

replacement of the information content of sites

drawing attention to the attacking side, demonstrating their capabilities, or are a way of expressing a certain political position. Registration in search engines of sites of opposite content for the same keywords

semantic attacks

hacking pages and subsequent placement (without noticeable signs of hacking) on them deliberately false information

collection

extortion of money to support terrorist movements

publication of information

about explosives and explosive devices, poisons, poisonous gases, as well as instructions for their self-production

involvement in terrorist activities

unsuspecting accomplices, such as hackers who do not know what final goal their actions will lead to

failure or decrease in the efficiency of functioning of the structural elements of information and telecommunication systems

the use of special software and hardware-software tools based on program code (software and hardware bookmarks, computer viruses, network worms, etc.)

bulk emails (a form of "virtual blockade")

DOS-attacks, the implementation of which is similar to the technology of mass e-mails, which leads to a slowdown in the service server or a complete cessation of external access to its resources

Fig. 2. Basic ways to use the Internet

The performed analysis of Fig. 2 showed that social networks are actively used to promote the demonstration of the supposedly comfortable life of militants, the military lifestyle and heroism of militants, the call to fight for their ideals with weapons in their hands, broadcasting scenes of successful military operations and acts of intimidation. Photo and video reports are accompanied by jihadist songs, which occupy an important place in the emerging cultural matrix of the global terrorist community. They have their own mobile app and online store where you can buy a t-shirt or hoodie with the terrorist logo. All these products dangerous for consciousness are distributed in many languages of the world.

Thus, unlike traditional terrorism, which did not threaten society as such and did not affect the foundations of its life, modern high-tech terrorism is capable of producing a systemic crisis in any state with a highly developed information infrastructure. The development of social networks is accompanied by an ever wider use of their capabilities for carrying out information confrontation, an increase in coordination, scale and complexity of the actions of its participants, which most often are both states and separate organized groups, including terrorist ones. The object of cyberattacks is increasingly becoming information resources, disruption or "difficulty" in functioning, which can cause significant economic damage to the opposing side or cause a great public outcry [11].

The aim of the paper is to consider the problem of ensuring the continuity of business processes in organizations of critical infrastructure in the face of increasing cyber threats, based on an analysis of the methods of committing crimes of a criminal nature against critical infrastructure facilities.

RESEARCH RESULTS

Critical information infrastructures.

The use by terrorists of the latest developments in the field of information and communication technologies makes it possible to radically change the methods of terrorist activity, to form flexible and effective network organizational structures that unite individual groups into transnational terrorist groups that are very difficult to detect before committing a terrorist act. Information attacks are usually divided into two categories [12]: disabling an information resource and destructive attacks. Destructive attacks are information (hacker) operations against objects that are capable of destroying an information resource, communication lines, or causing physical destruction of structures that include information systems. If the systems operate in critical infrastructures, then in the worst case scenario, network information attacks can have large-scale consequences with human casualties, just like traditional terrorist attacks.

Critical infrastructure is of key importance for public order, economic stability and national security of states, its protection affects national security issues, and therefore falls within the competence of the state. However, most of the infrastructure is owned by private business, so the state and business are forced to jointly bear responsibility for the security and stable functioning of these systems.

Today, states independently determine what to classify as critical infrastructures, depending on the economic condition of the state, political leadership, geographical and historical features. The Patriot Act of the United States gives the following definition - "critical infrastructures are systems and resources, physical or virtual, so significant to the United States that their destruction or disruption of normal operation can undermine the military-political security of the state, economic stability, health citizens and public order, or entail several of the above factors in any combination" [13]. In Ukraine, at the legislative and regulatory level, there are no definitions of critically important objects and key information infrastructure systems. Both domestic and foreign experts offer generalized definitions of critical objects (CO) and critical information infrastructure of Ukraine (CII) [14-18].

A critically important facility is an facility whose disruption (or cessation) of functioning leads to loss of control, destruction of infrastructure, irreversible negative change (or destruction) of the economy of a country or an administrative-territorial unit, or a significant deterioration in the life safety of the population living in these territories for a long time. .

The key information infrastructure system is an information management or information and telecommunication system that meets one of the requirements:

– manages the CO (process);

– provides information support for the management of the CO (process);

- provides information to citizens about emergency situations.

Thus, the main characteristic of critical infrastructure is its key importance for the security of society and the state. Critical infrastructures can be dual-purpose, both military and civil. In table. 1 shows the ratio of critical infrastructures of the states of Ukraine and the USA.

Table 1

Critical infrastructures of the states of Ukraine and the USA

CO of Ukraine	CO of the USA	purpose
healthcare	public health	civilian facilities
agriculture	food and agriculture	dual-use objects
water supply	water	
public administration	public administration	
information and telecommunication networks	information and telecommunication networks	
energy systems	energy systems	
banking and financial systems	banking and financial systems	
chemical industry	chemical industry and explosive materials	
heat supply	-	
transport system	land and water transport	
industrial industry	critical production	
military-industrial complex	military-industrial complex	military facility
civil defense	emergency response services	dual-use objects

Thus, the analysis of the table. 1. shows that OBS belong to the CO, and ABS provide automation and continuity of business processes, processing, storage and transfer of large volumes of BIN necessary for the activities of the OBS, therefore, the continuity of business processes directly depends on the reliability and security of the functioning of the ABS information infrastructure, availability and integrity of BIN data, and hence the activities of the OBS as a whole.

The analysis and generalization of the existing experience of antiterrorist activities made it possible to formulate the tasks of protecting critical infrastructure from cyberterrorism and the main measures aimed at their solution are presented in Table. 2 [1, 5, 6, 9, 12]. A comprehensive solution of these tasks will make it possible to take the necessary countermeasures in a centralized manner to counter cyberterrorism, significantly reduce the likelihood of its threats to critical infrastructure and ensure the protection of their national interests.

Table 2

Main activities aimed at preventing cybercrime

at the national level	*on the international level*
organization of monitoring and forecasting the needs of economic and other structures in various types of information exchange via the Internet	organization of interstate cooperation in the work of international organizations, public committees and commissions in projects for the development of world information networks
coordination of measures of state and non-state departments to prevent threats to information security in open networks. Development of a unified policy	active participation in the development of international legislation and regulatory support for the operation of global networks of open infrastructure

providing for the protection of network equipment on the territory of the country from the penetration of hidden elements of information weapons into it	
development of a state program for improving information technologies that ensure the connection of national and corporate networks to open networks while observing the requirements for the security of information resources	creation of a common anti-terrorist space of the allied countries
improvement of technologies for timely detection and neutralization of unauthorized access to information, creation and use of advanced technologies	development of scientific and methodological support for the suppression of transnational (cross-border) terrorist attacks using global networks, the development of a single conceptual apparatus, a scale for assessing cyber threats and their consequences
development of national legislation regarding the rules for handling information resources, the regulation of the rights, duties and responsibilities of users of open infrastructure networks	development of mechanisms for mutual information about large-scale computer attacks and major incidents in cyberspace, as well as ways to jointly respond to threats of cyberterrorism
establishing a list of information that is not subject to transmission over open networks, and ensuring control over compliance with the established status of information	unification of national legislation in the field of protection of critical infrastructure from cyberterrorism

Strategies and indicators for ensuring business-process continuity.

In any social sphere, security incidents, interruptions (disruptive events) and accidents (disasters) are inevitable. However, their impact on the company's operations must be minimized: data must be preserved, technical means are in working order, reputation is saved, people are not at risk. Solutions to these tasks can be implemented within the framework of business continuity management (Business Continuity Management) - a holistic management process, within which potential threats to the organization's activities are identified, possible impacts on business operations are assessed if these threats materialize, and a system of prescriptions is created to ensure the ability to organizations to recover and respond effectively to incidents in order to ensure that the interests of stakeholders are served, to ensure the protection of reputation, brand and value-creating operations.

There are two main tools for business continuity [13 – 16]:

– business continuity plan (Business Continuity Planning, BCP) – a set of preventive measures, detailed instructions for actions in acute (critical) situations; what they reflect, what their format is, how they should be interpreted, etc. The maximum “age” of data, the loss of which is acceptable (Recovery Point Objective, RPO), is determined;

– Disaster Recovery Planning (DRP) – preparation of the organization for the speedy full recovery of its activities in the event of an accident, emergency, disaster, crisis, etc.

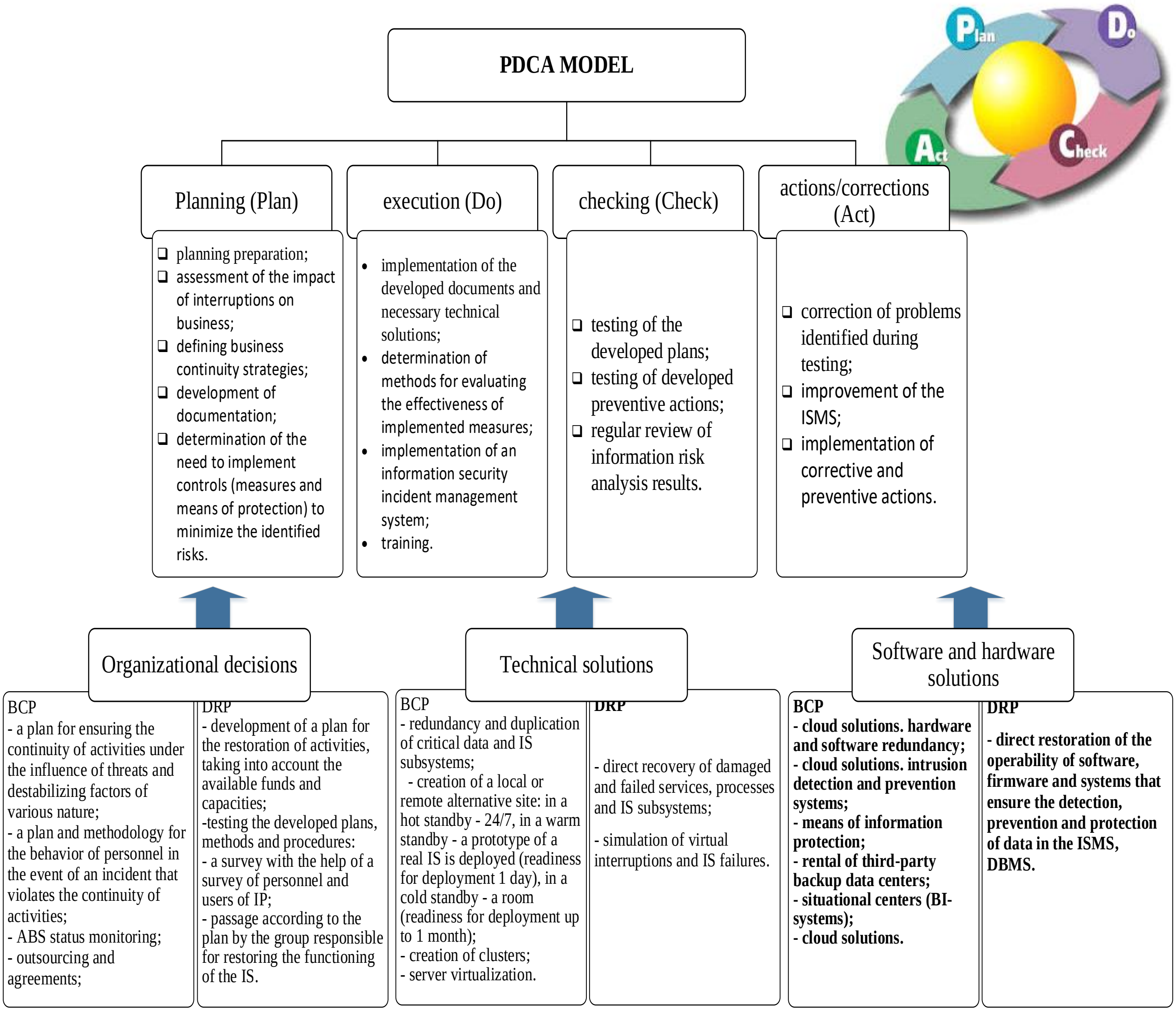
Despite the difference, BCP and DRP are integral parts of business continuity management and overlap procedurally. In this regard, it is convenient to consider them using the PDCA (Plan-Do-Check-Act) management model [13, 17, 18], the main tasks at the stages of the PDCA management model are presented in Fig. 3.

Thus, the proposed solutions have their own cost, compatibility, complexity of implementation, deployment time and efficiency, and can be applied both individually and as a set of measures implemented before, during and / or after an incident that caused a disruption in the continuity of the business-processes.

Business Impact Analysis (BIA) is a key business continuity topic and consists of a functional analysis of how interruptions will affect the organization's operations.

The tasks of the BIA include [13 – 16]:

determining the value of each business process;
identification and ranking of interruptions of each business process;
prioritization of business processes;
assessment of resources to ensure the continuity of business processes.
The final result of BIA is the selection of business continuity management strategies.



PDCA MODEL

Planning (Plan)

- ❑ planning preparation;
- ❑ assessment of the impact of interruptions on business;
- ❑ defining business continuity strategies;
- ❑ development of documentation;
- ❑ determination of the need to implement controls (measures and means of protection) to minimize the identified risks.

execution (Do)

- implementation of the developed documents and necessary technical solutions;
- determination of methods for evaluating the effectiveness of implemented measures;
- implementation of an information security incident management system;
- training.

checking (Check)

- ❑ testing of the developed plans;
- ❑ testing of developed preventive actions;
- ❑ regular review of information risk analysis results.

actions/corrections (Act)

- ❑ correction of problems identified during testing;
- ❑ improvement of the ISMS;
- ❑ implementation of corrective and preventive actions.

Organizational decisions

BCP
- a plan for ensuring the continuity of activities under the influence of threats and destabilizing factors of various nature;
- a plan and methodology for the behavior of personnel in the event of an incident that violates the continuity of activities;
- ABS status monitoring;
- outsourcing and agreements;

DRP
- development of a plan for the restoration of activities, taking into account the available funds and capacities;
-testing the developed plans, methods and procedures:
- a survey with the help of a survey of personnel and users of IP;
- passage according to the plan by the group responsible for restoring the functioning of the IS.

Technical solutions

BCP
- redundancy and duplication of critical data and IS subsystems;
- creation of a local or remote alternative site: in a hot standby - 24/7, in a warm standby - a prototype of a real IS is deployed (readiness for deployment 1 day), in a cold standby - a room (readiness for deployment up to 1 month);
- creation of clusters;
- server virtualization.

DRP

- direct recovery of damaged and failed services, processes and IS subsystems;

- simulation of virtual interruptions and IS failures.

Software and hardware solutions

BCP
- cloud solutions. hardware and software redundancy;
- cloud solutions. intrusion detection and prevention systems;
- means of information protection;
- rental of third-party backup data centers;
- situational centers (BI-systems);
- cloud solutions.

DRP

- direct restoration of the operability of software, firmware and systems that ensure the detection, prevention and protection of data in the ISMS, DBMS.

Fig. 3. The main tasks and solutions for ensuring continuity at the stages of the PDCA management model

When determining the value of business processes for information systems (ABS), the values of a number of technical indicators [13 - 16] can be fixed, the relationship between which is shown in Fig. 4.

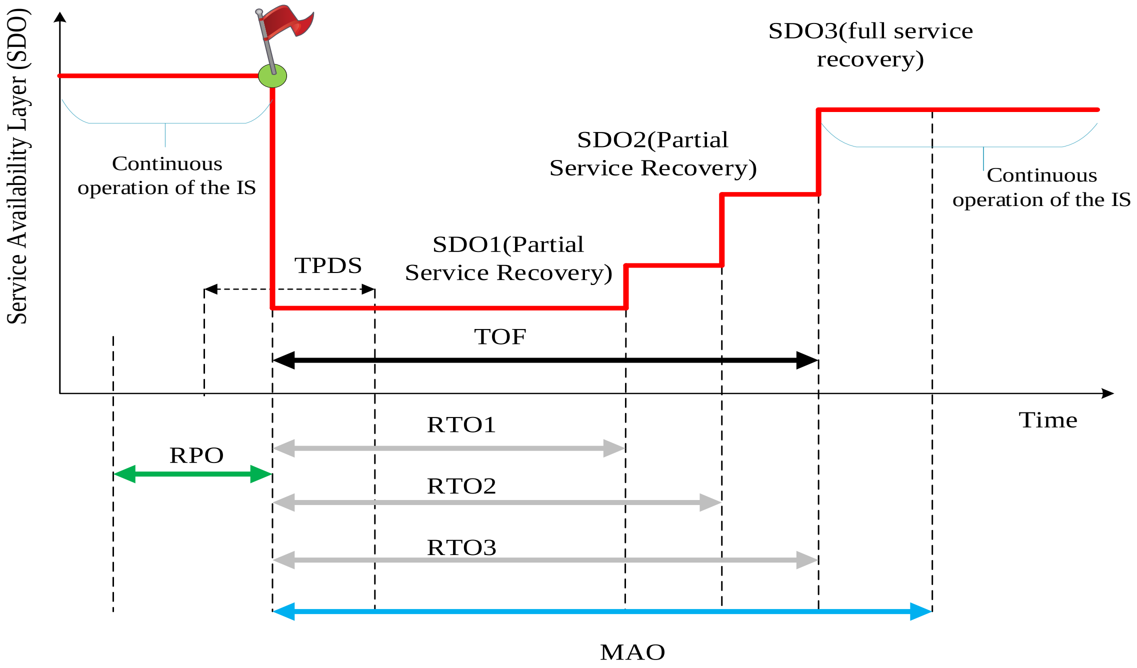

Service Availability Layer (SDO)
Continuous operation of the IS
TPDS
SDO1(Partial Service Recovery)
SDO2(Partial Service Recovery)
SDO3(full service recovery)
Continuous operation of the IS
TOF
Time
RPO
RTO1
RTO2
RTO3
MAO

Fig. 4. Definition of business continuity indicators

MTPD (Maximum Tolerable Period of Disruption, the maximum acceptable period of business interruption) is the period of time after which the adverse consequences resulting from a business interruption become unacceptable.

The starting point of the MTPD interval is assessed as the point at which the impact on the organization is considered unacceptably large, as shown in Figure 5 below.

The definition of MTPD assumes that there is a point beyond which irreparable damage occurs, and before that point there is no irreparable damage. If we talk about the continuity of the organization's business processes, then it is necessary to make the following clarification[17 - 21]. The longer a failure continues and the greater its impact, the more likely it is that the viability of the organization will be threatened, and the more unacceptable the failure becomes. There is no single point beyond which irreparable damage occurs; instead, there is an impact curve, and at some point along that curve, the impact becomes unacceptably large.

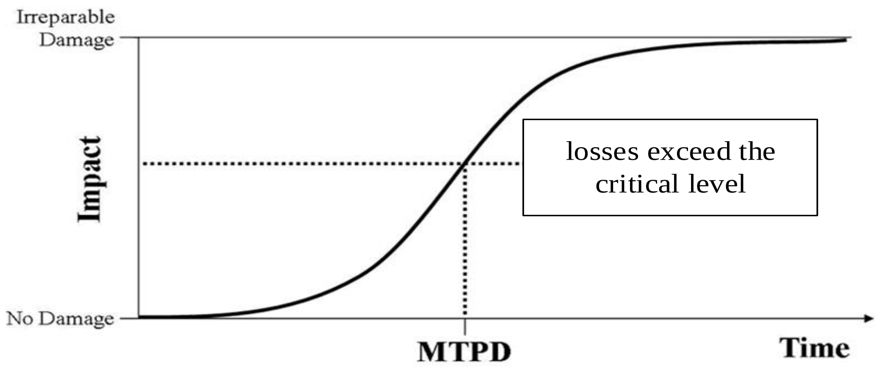


Fig. 5 The point at which the impact on the organization caused by service denials becomes unacceptable

The general equation describing the S-shaped curve is

$$N = \frac{K}{1 + \exp(a - rt)} \tag{1}$$

where *a* is the integration constant, at *t*=0 $a = \ln\left(K - N\right) / N$, *N* is the current value of losses, *K* is the maximum level of losses, *r* is the rate of increase in losses.

It demonstrates that the impact of a failure can be relatively small during the time period immediately following an incident, increasing rapidly as it approaches a situation where irreparable damage occurs. At some point along this curve, the impact becomes unacceptably large.

For other organizations, especially those with penalties for non-delivery of service, the impact curve will not be smooth.

The perception of MTPD can be described as follows. It is not known at what point the organization will be irreparably damaged, but it is known when the impact on the organization becomes too large (N_b). Based on the above dependence, it is possible to determine the MTPD point:

$$t^s_{MTPD} = (a - \ln(K / N_b - 1)) / r \tag{2}$$

SDO (Service Delivery Objective, target service availability) - shows the level of service availability at a certain point in time;

RTO (Recovery Time Objective, target recovery time) - the period of time after the interruption occurred, during which the minimum level of activity of the organization, as well as the systems, applications and functions supporting it, must be restored, is determined by the formula:

$$\begin{gathered} \textit{for consistent recovery of services} \\ T_{RPO} = \sum_{i \in S} RTO_i; \\ \textit{for concurrent service recovery} \\ T_{RPO} = \max_{i \in S} \left\{ RTO_i \right\}, \end{gathered} \tag{3}$$

where *S* is a set of services that are implemented by business processes.

Taking into account the fact that restoration can be of a stepwise nature (i.e., sequential restoration of the operation of disrupted services), we denote the level of service availability (*SDO*) in the i-th restoration period (SDO_i) as L^i_{SDO}, we can obtain the following dependence

$$(i < j) \to (RTO_i < RTO_j) \wedge (L^i_{SDO} < L^j_{SDO}) \tag{4}$$

The resulting dependency demonstrates the fact that during sequential restoration, the level of service availability increases, and indirectly reflects the fact that during restoration, access to restored services is denied. It is also assumed that: *RTO < MTPD.*

RPO (Recovery Point Objective, target recovery point) - the period of time for which data must be restored after a past interruption.

MAO (Maximum Allowable Outage) is a period of time after which there is a risk of permanent termination of the IS activity, if the provision of services, data, business processes and / or services is not resumed. For *MAO*, the relation

$$\max_{i\in I}\left\{RTO_i\right\} \le MAO\,, \qquad (5)$$

where *I* is the number of restored services.

TOF (current downtime) - the period of time during which the activity was interrupted as a result of the failure of the IS or its components, the unavailability of services and data, in the case acceptable to the enterprise, should be less than the maximum allowable downtime. It is assumed that TOF≤MAO;

TPDS is the time to plan and deploy business continuity and recovery solutions, ideally solutions and plans should be developed and implemented prior to a business continuity incident, *TPDS* << *RTO*.

Analysis of fig. 4 showed that in order to reduce TOF, an integrated approach is needed to solve the problems of BCP and DRP. The introduction of preventive measures to protect against cyber threats aimed at disrupting continuity will not only minimize the loss of IR data in the IS, but also reduce the target data recovery time.

A similar effect is achieved due to the fact that plans and means to ensure business continuity are developed and deployed not during a failure, but during the normal operation of the IS before the threat is realized and an avalanche effect occurs, Fig. 6.

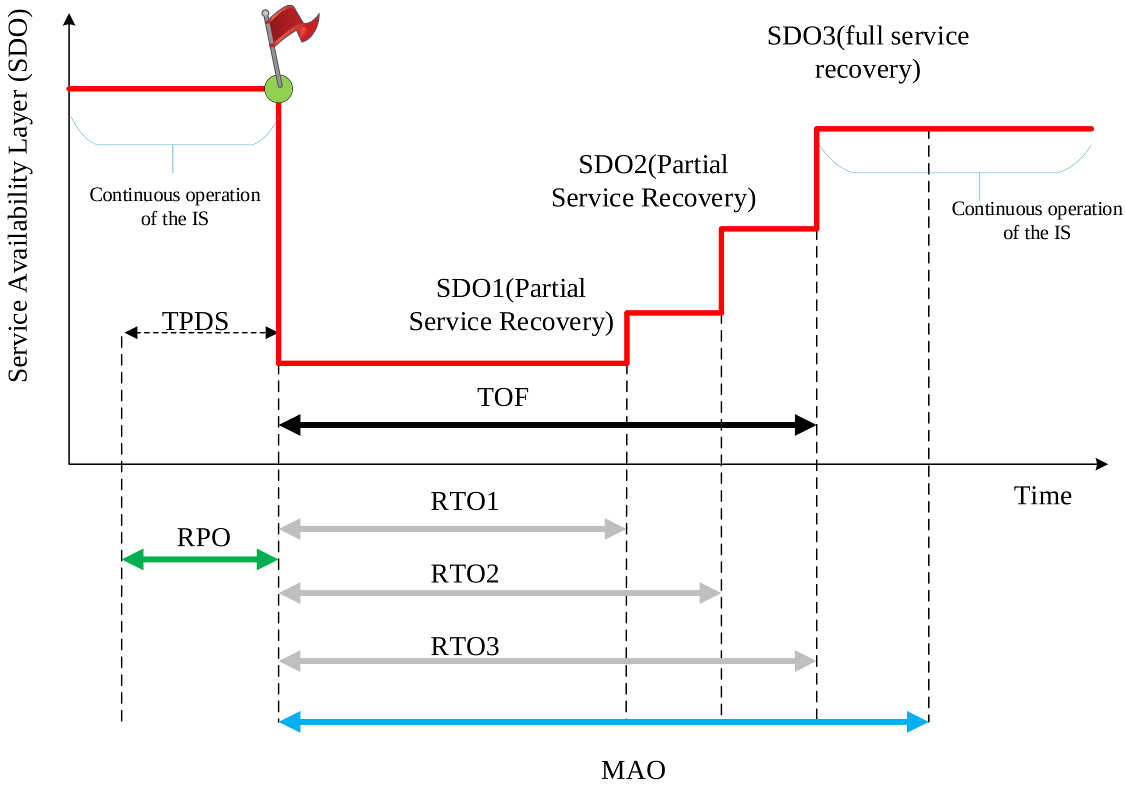

Service Availability Layer (SDO)
SDO3(full service recovery)
SDO2(Partial Service Recovery)
SDO1(Partial Service Recovery)
Continuous operation of the IS
Continuous operation of the IS
TPDS
TOF
Time
RTO1
RPO
RTO2
RTO3
MAO

Fig. 6 Reducing the time to restore the functioning of the business system (TOF) through the application of preventive plans and protection measures

This allows immediately after the onset of an incident to coordinate the actions of personnel and start recovery or completely avoid downtime and losses due to prompt switching to a backup site.

Thus, in order to ensure an integrated approach to the continuity of business processes of the OBS, it is proposed to use ABS duplication based on the concept of alternative sites (hot standby site (Hot Site), warm standby site (Warm Site), cold standby site (Cold Side) using strategies for updating data - copying backup data (electronic vaulting, off-site data protection, periodic transfer of database copies to alternative media, usually in batch mode), remote journaling (remote journaling, periodic transfer of a log of completed transactions from the main site to an alternative one), remote mirroring (full duplication in real time), which will provide the required indicators of the value of business processes.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

As a result of the research:

1. The main trends in the development of cybersecurity are analyzed in the context of the perfection of means and methods for conducting terrorist information attacks on critical infrastructures. Preventive measures have been identified to reduce the risk of cyber attacks at the national and international levels.

2. The main tasks of ensuring the continuity of business processes based on the PDCA management risk model, indicators for assessing business continuity are considered. The impact of the chosen strategies and solutions to ensure the continuity of business processes is analyzed.

The direction of further research is the development or improvement of methods and algorithms for evaluating and ensuring the continuity of business processes of critical infrastructure objects.

REFERENCES

1 Hryschuk, R.V., Danyk, Yu.G. (2016). *Fundamentals of cyber security: Monograph*. ZhNAEU.

2 Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al. (2021). *Synergy of building cybersecurity systems*. PC TECHNOLOGY CENTER. http://doi.org/10.15587/978-617-7319-31-2

3 Sokol, Y., Trush, O., Yevseiev, S., & Milov, O. (2023). Implementation of Information and Communication Technologies in the Educational Process. У *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE. https://doi.org/10.1109/hora58378.2023.10156664.

4 Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al. (2022). Modeling of security systems for critical infrastructure facilities. PC TECHNOLOGY CENTER. http://doi.org/10.15587/978-617-7319-57-2

5 Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O., Salii, A., Timochko, O., Tiurin, V., & Yarovyi A. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. *Eastern-European Journal of Enterprise Technologies*, *4*(9 (100), 6–19. https://doi.org/10.15587/1729-4061.2019.175978

6 Milov, O., Voitko, A., Husarova, I., Domaskin, O., Ivanchenko, Y., Ivanchenko, I., Korol, O., Kots, H., Opirskyy, I., & Fraze-Frazenko, O. (2019). Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. *Eastern-European Journal of Enterprise Technologies*, *2*(9 (98), 56–66. https://doi.org/10.15587/1729-4061.2019.164730

7 Milov, O., Yevseiev, S., Vlasov, A., Herasimov, S., Dmitriiev, O., Kasianenko, M., Pievtsov, H., Peleshok, Y., Tkach, Y., & Faraon, S. (2019). Development of scenario modeling of conflict tools in a security system based on formal grammars. *Eastern-European Journal of Enterprise Technologies*, *6*(9 (102), 53–64. https://doi.org/10.15587/1729-4061.2019.184274

8 Milov, O., Yevseiev, S., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V., Ivanchenko, Y., Pavlenko, M., Salii, A., & Yarovyy, S. (2019). Development of the interacting agents behavior scenario in the cyber

security system. *Eastern-European Journal of Enterprise Technologies*, *5*(9 (101), 46–57. https://doi.org/10.15587/1729-4061.2019.181047

9 Ivanchenko, E.V., Khoroshko, V.A. (2014). Trends in the development of cyberterrorism. In *MNPK "Modern Information and Electronic Technologies"* (p. 105 – 106).

10 Some aspects of cyberterrorism. http://nk.org.ua/geopolitika/nekotoryie-aspektyi-kiberterrorizma-16846.

11 Yevseiev, S., Ryabukha, Y. ., Milov, O., Milevskyi, S., Pohasii, S., Melenti, Y., Ivanchenko, Y., Ivanchenko, I., Opirskyy, I., & Pasko, I. (2021). Development of a method for assessing forecast of social impact in regional communities. *Eastern-European Journal of Enterprise Technologies*, *6*(2 (114), 30–43. https://doi.org/10.15587/1729-4061.2021.249313

12 Zvertseva, N.V., Evseev, S.P., Rzaev, H.N., Mamedova, T.A., Samedov, F.G. (2018). Classifier of cyber threats of information resources of automated banking systems. *Cyber security: education, science, technology*, *2*(2), 48-67.

13 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.

14 Leonenko, H., & Yudin, O. (2013). Problems of ensuring information security of ukraine critical information infrastructure systems. Collection "Information technology and security", 2(1), 44–48. https://doi.org/10.20535/2411-1031.2013.2.1.58384.

15 Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A. ., Mykus, S., Milov, O. ., Prokopenko, O., Sievierinov O., & Chopenko, D. (2021). Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, *3*(9(111), 63–83. https://doi.org/10.15587/1729-4061.2021.233533

16 Yevseiev, S., Milov, O., Zviertseva, N., Lezik, O., Komisarenko, O., Nalyvaiko, A., Pogorelov, V., Katsalap, V., Pribyliev, Y., & Husarova, I. (2023). Development of the concept for determining the level of critical business processes security. *Eastern-European Journal of Enterprise Technologies*, *1*(9 (121), 21–40. https://doi.org/10.15587/1729-4061.2023.274301

17 _ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity. http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.

18 ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

19 Laptiev, O., Sobchuk, V., Subach, I., Barabash, A., Salanda, I. (2022). The Method of Detecting Radio Signals Using the Approximation of Spectral Function. In *CEUR Workshop Proceedings, 3384,* (p. 52–61). Scopus.

20 Sobchuk, V., Zelenska, I., Laptiev, O. (2023). Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. *Bulletin of the Polish Academy of Sciences Technical Sciences*, *71*(3). https://doi.org/10.24425/bpasts.2023.145682

21 Laptiev, O., and al. (2023). *Methodology for confirming the feasibility of exploiting detected vulnerabilities in a corporate network using polynomial transformations of bernstein. Challenges and threats to critical infrastructure*. Collective monograph. NGO Institute for Cyberspace Research.

Звєрцева Наталія
Аспірант
Кафедра програмної інженерії та інтелектуальних технологій управління
Національний технічний університет «Харківський політехнічний інститут»
ORCID ID: 0000-0001-6279-7586
nataliezviertseva@gmail.com

ОЦІНКА БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ НА ОСНОВІ СИНЕРГІЧНОГО ПІДХОДУ

Анотація. Інформаційні загрози можуть проявлятися в різних формах, що зумовлено особливостями глобальної мережі. Стаття присвячена одному із шляхів вирішення протиріччя, яке полягає в тому, що, незважаючи на велику кількість публікацій, завдання забезпечення безперервності бізнес-процесів в умовах зростання кількості та різноманітності кібератак на об’єкти критичної інфраструктури залишається невирішеним. Це пов’язано з постійною модифікацією та збільшенням кількості кібератак, а також методів і технологій реалізації бізнес-процесів. Тому розробка та вдосконалення методів оцінки безперервності бізнес-процесів є актуальним науковим завданням. У статті досліджено проблему забезпечення безперервності бізнес-процесів в умовах зростання кіберзагроз. Проаналізовано засоби та способи вчинення кіберзлочинів проти об’єктів критичної інфраструктури. Визначено основні стратегії та показники оцінки безперервності бізнесу. Проаналізовано вплив обраних стратегій і рішень забезпечення безперервності бізнесу на значення показників безперервності бізнес-процесів. Проаналізовано основні тенденції розвитку кібербезпеки в контексті вдосконалення засобів і методів здійснення терористичних інформаційних атак на об’єкти критичної інфраструктури. Визначено превентивні заходи для зниження ризику кібератак на національному та міжнародному рівнях.
Розглянуто основні завдання забезпечення безперервності бізнес-процесів на основі моделі управління ризиками PDCA, показники оцінки безперервності бізнесу. Проаналізовано вплив обраних стратегій і рішень на забезпечення безперервності бізнес-процесів.

Ключові слова: кібертероризм, кібератака, критична інфраструктура, безперервність бізнес-процесів.

REFERENCES

1 Hryschuk, R.V., Danyk, Yu.G. (2016). Fundamentals of cyber security: Monograph. ZhNAEU.

2 Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al. (2021). Synergy of building cybersecurity systems. PC TECHNOLOGY CENTER. http://doi.org/10.15587/978-617-7319-31-2

3 Sokol, Y., Trush, O., Yevseiev, S., & Milov, O. (2023). Implementation of Information and Communication Technologies in the Educational Process. У 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE. https://doi.org/10.1109/hora58378.2023.10156664.

4 Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al. (2022). Modeling of security systems for critical infrastructure facilities. PC TECHNOLOGY CENTER. http://doi.org/10.15587/978-617-7319-57-2

5 Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O., Salii, A., Timochko, O., Tiurin, V., & Yarovyi A. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4(9 (100), 6–19. https://doi.org/10.15587/1729-4061.2019.175978

6 Milov, O., Voitko, A., Husarova, I., Domaskin, O., Ivanchenko, Y., Ivanchenko, I., Korol, O., Kots, H., Opirskyy, I., & Fraze-Frazenko, O. (2019). Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. Eastern-European Journal of Enterprise Technologies, 2(9 (98), 56–66. https://doi.org/10.15587/1729-4061.2019.164730

7 Milov, O., Yevseiev, S., Vlasov, A., Herasimov, S., Dmitriiev, O., Kasianenko, M., Pievtsov, H., Peleshok, Y., Tkach, Y., & Faraon, S. (2019). Development of scenario modeling of conflict tools in a security system

based on formal grammars. Eastern-European Journal of Enterprise Technologies, 6(9 (102), 53–64. https://doi.org/10.15587/1729-4061.2019.184274

8 Milov, O., Yevseiev, S., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V., Ivanchenko, Y., Pavlenko, M., Salii, A., & Yarovyy, S. (2019). Development of the interacting agents behavior scenario in the cyber security system. Eastern-European Journal of Enterprise Technologies, 5(9 (101), 46–57. https://doi.org/10.15587/1729-4061.2019.181047

9 Ivanchenko, E.V., Khoroshko, V.A. (2014). Trends in the development of cyberterrorism. In MNPK "Modern Information and Electronic Technologies" (p. 105 – 106).

10 Some aspects of cyberterrorism. http://nk.org.ua/geopolitika/nekotoryie-aspektyi-kiberterrorizma-16846.

11 Yevseiev, S., Ryabukha, Y. ., Milov, O., Milevskyi, S., Pohasii, S., Melenti, Y., Ivanchenko, Y., Ivanchenko, I., Opirskyy, I., & Pasko, I. (2021). Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies, 6(2 (114), 30–43. https://doi.org/10.15587/1729-4061.2021.249313

12 Zvertseva, N.V., Evseev, S.P., Rzaev, H.N., Mamedova, T.A., Samedov, F.G. (2018). Classifier of cyber threats of information resources of automated banking systems. Cyber security: education, science, technology, 2(2), 48-67.

13 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.

14 Leonenko, H., & Yudin, O. (2013). Problems of ensuring information security of ukraine critical information infrastructure systems. Collection "Information technology and security", 2(1), 44–48. https://doi.org/10.20535/2411-1031.2013.2.1.58384.

15 Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A. ., Mykus, S., Milov, O. ., Prokopenko, O., Sievierinov O., & Chopenko, D. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3(9(111), 63–83. https://doi.org/10.15587/1729-4061.2021.233533

16 Yevseiev, S., Milov, O., Zviertseva, N., Lezik, O., Komisarenko, O., Nalyvaiko, A., Pogorelov, V., Katsalap, V., Pribyliev, Y., & Husarova, I. (2023). Development of the concept for determining the level of critical business processes security. Eastern-European Journal of Enterprise Technologies, 1(9 (121), 21–40. https://doi.org/10.15587/1729-4061.2023.274301

17 ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity. http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.

18 ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

19 Laptiev, O., Sobchuk, V., Subach, I., Barabash, A., Salanda, I. (2022). The Method of Detecting Radio Signals Using the Approximation of Spectral Function. In CEUR Workshop Proceedings, 3384, (p. 52–61). Scopus.

20 Sobchuk, V., Zelenska, I., Laptiev, O. (2023). Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences, 71(3). https://doi.org/10.24425/bpasts.2023.145682

21 Laptiev, O., and al. (2023). Methodology for confirming the feasibility of exploiting detected vulnerabilities in a corporate network using polynomial transformations of bernstein. Challenges and threats to critical infrastructure. Collective monograph. NGO Institute for Cyberspace Research.