UDC 351.865

Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences

Yevhen Zhyvylo[1], Vladyslav Kuz[1]

[1]*Kruty Heroes Military Institute of Telecommunications and Information Technologies,*
Street of Knyaz Ostrozki 45/1, Kyiv, 01011, Ukraine

Abstract

Today, interaction between people and objects, including industrial ones, has become an integral part of our everyday life. Access to communications, finance, and all forms of information management and permission to use them can be obtained from almost anywhere using compact devices.

For example, operators can remotely control individual sectors and control operations in several areas at the same time, surgeons can operate on patients thousands of miles away, and car manufacturers can detect when one of their vehicles has been in an accident within a few seconds after the accident.

As a result of the spread of the Internet and wireless data networks, the interconnection of so much data, technology and network equipment and devices has quickly become the basis of modern society. At present, we have become a knowledge-based society that often relies on technology to execute or support almost all tasks and functions of human life. Undoubtedly, this has greatly expanded the range of tasks to be solved, but at the same time, the society became much more vulnerable to threats in information and communication systems.

The vulnerability is explained by the fact that at some point most of the production of different directions and industries is supported by the introduction, storage and search of data/information in a interconnected network of hard disks and data servers, locally or remotely located. And at each of these stages there is an opportunity to steal data, bypass protection, manipulate or replace information. But the risks associated with unintentional accidents caused by human errors, system failures, incompatibility or other unexpected problems, as well as “natural disasters,” must also be taken into account.

Therefore, the security of computer or cyber systems is a matter of national security. Actually, cyber-threats are so great that more and more security experts are pointing out that protection of cyber systems and data is more of a problem than terrorism. Given the scale of the threat (in terms of cyberattacks) and the actual damage it can be argued, certain systems and structures are at risk [1, 2]. It is proved that hackers can break into government and business websites, steal personal data, change the traffic light scheme, accelerate and slow down travel, and much more.

As an example, the implementation of a specially created malware program - Stuxnet. The effects of its use were the self-destruction in 2010 of dozens of centrifuges, which supported Iran’s nuclear program [3, 4]. Some experts think that Stuxnet was created not by independent attackers and possibly with the support of the government. Thus, as a conclusion, it can be confirmed that hackers operate from anywhere in the world, and the links and boundaries between cyberspace and physical systems are sufficiently leveled. Thus, as a conclusion, it can be confirmed that intruders operate from anywhere in the world, and the links and borders between cyberspace and physical systems are sufficiently leveled.

Society is increasingly faced with the fact that a group or even a person armed with a complex computer virus or knowledge about the vulnerability of software or hardware can cause a lot of physical damage to people’s lives or physical destruction, impose significant social or economic damage, and so on. For example, there are facts published by the Financial times on May 8, 2012 (http://on.ft.com/1wviXHW) that an unknown group for many years is trying to penetrate into the systems of managing the networks of gas pipelines of the USA. At the end of 2014, the National Oceanic and Atmospheric Administration of the United States announced that hackers from China successfully broke and destroyed American satellite networks, causing loss of services related to the prediction of various natural cataclysms, air flight corridors, navigation and other industries within a few days (http://wapo.st/1u7N9dJ).

As a rule, the critical infrastructure includes power and transport main networks, oil and gas pipelines, sea ports, high-speed and governmental communication channels, systems of life support (water and heat supply) of mega-cities, waste management, emergency services and emergency response services, high-tech enterprises and enterprises of military-industrial complex, as well as central authorities.

The government critical information infrastructure is only one of many important systems and networks that create our modern society. Therefore, the state and society are fully dependent on the functioning of different objects and subjects of critical information infrastructure, and the loss of integrity of any of them can lead to various kinds of failures (termination of production and transfer of electricity, temporary and long-term interruptions, improper access to medical care, and much more). Each state is a separate critical information infrastructure, but cooperation between states takes place within the framework of global critical information infrastructure. At the same time, large investments in each sector of critical information infrastructure have led to an increase in economic development rates and improvement in the quality of life.

Keywords: critical infrastructure, critical information infrastructure, risks, risk assessment, information technologies, communication systems.

The general problem formulation

Given the limited resources, the objective inability to provide absolute protection and security for all infrastructure systems, the concept of critical infrastructure (CI) is being implemented in many countries around the world, which allows to concentrate attention on systems, networks and separate objects, destruction or violation of which will have the most serious negative consequences for national security.

The critical information infrastructure (CII) concerns physical and information objects, assets and networks that, if damaged, may have a significant influence on the well-being of citizens, the proper functioning of states and industries, or other adverse consequences. Power supply and communication systems can be considered as important objects of the CII, since the work of other objects of the CI depends on their functioning. The constant development of electronic communications, information technologies (IT), information protection and cyber protection led to greater automation of the management of the CI.

The growth of the role of information and the availability of electronic means for its gathering, analysis and modification have made information and information systems (IS) at the same time invaluable asset and profitable goal. At present, many states pay attention to methods and means of detection, systematization and security of a large number of objects of the CI. The loss or disruption of the normal functioning of these objects may lead to significant or even irreversible negative consequences for the security of the state. The destructive influence of attackers on individual of objects of the CII is directed not only at these objects, but also at the CI as a whole. For prompt response and counteraction to cyber attacks and cyber incidents is important to determine the level of importance of objects and subjects of the CI.

Also important the CII [5, 6], including IS, telecommunication and communication networks, automated systems of control of subjects of the CII etc., allows to carry out remote management and management of services, thus increasing efficiency. Unfortunately, at first cyber security (CS) was not considered a top priority for the CII. At that time, CS was defined as an activity, process, ability or state in which information and communication systems (ICS) and information contained in them are protected from damage, unauthorized use or modification, or exploitation.

However, at the same time, it is necessary to predict the practical side of CS in terms of secondary, tertiary and even more remote systems, equipment and processes that are protected. For example, a valve on an oil pipeline is often not considered part of the ICS, but with the appropriate tools and knowledge, an attacker can manipulate the control mechanisms of some valves and regulators, causing a leak in the pipeline that remains unobserved, leading to an ecological catastrophe. Thus, a deep understanding of the complexity and volume of the CII and the mechanisms for its control and management is required. Cyber infrastructure includes all information and communication systems and services, hardware components and software systems that manipulate, store and transmit this information, and also various combinations of these components that are located in such a way as to perform one or more tasks, or to provide one or more services. The complexity of construction and hierarchy of network and system combined with increased functional load makes CII particularly vulnerable to natural disaster, human errors and technical problems, as well as new forms of cyber crime, i.e. the CII becomes especially vulnerable to the action of destructive elements. The main tools used to influence the CII are malware programs (computer viruses, worms, Trojan) that modify and/or destroy information or block computer systems.

Traffic analysis tools for information exchange in computer networks, and tools for changing for sustainable work of the computer network’s and blocking access to its services, are also widely used for destructive purposes. These automated tools allow the intrusion of remote systems, and can be run in seconds, this makes it easier to launch Internet attacks and makes it more difficult to find them. Underestimation of skills, knowledge and experience of cybercriminals (attackers) can become fatal for objects of the CI. The exchange of information and data may get minor changes and have a permanent character. These changes mean that we will have to rethink issues such as privacy, data protection, security, and adapt official activity to the new cyber reality. The dynamics of technological changes in the network environment of institutions, enterprises and organizations means that the management of these institutions should determine the order, develop requirements and measures for cyber-defense and information security, in order to ensure the normal functioning of their electronic information resources (IR) and systems.

In today’s online world, information can be sent, shared and stored in different forms, both digital and physical. Therefore, information security includes protection of such information and technical methods of transmission, exchange and storage. In most information security cases, the focus is mainly on the triads: confidentiality, integrity and availability (CIA) of information. Confidentiality refers to a situation where information is only reviewed by properly authorized parties. Integrity means that the data is protected from erroneous modifications or damage during transmission and storage. Availability is a guarantee that users have the appropriate authority to use the IR at any time they need it, that is, without disruption to services or unnecessary downtime (delay in message transmission).

Modern cyber defense centers focus on security of data and information system, which are involved in data processing. The operation of state cyber defense and cyber threat centers is aimed at deployment and technical support of the cyber defense organizational and technical model, which uses various technical means, approaches, principles and concepts of management of risk to protect information and systems, which are based on information and communication technologies.

This prevents the creation of prerequisites for the application of the wide diversity of digital and physical losses, and consequently, and the financial costs of changes in information that are aimed at the continued operation of the relevant systems, networks and equipment.

This is shown in the following CS definitions, which are most commonly quoted in the literature:

– ISO/IEC 27032:2012 [7] defines “cyber security” (or “cyberspace security”) as “preservation of confidentiality, integrity and availability of information in the cyberspace”, where “cyberspace” is defined as “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”;

– NISTIR 7298 rev. 2 [8] defines “cyber security” as “preventing damage, protecting and restoring computers, electronic communication systems, electronic communication services and wired communications, including information contained therein, ensuring accessibility, integrity, authentication, privacy, and denial of access.”

Therefore, confidentiality, integrity, and availability of information are the main requirements for CS.

Analysis of recent research and publications

Today, the need to assess the risks of strategic management of telecommunication companies and forecast of changes is felt by both the management of telecommunication companies and their contractors, investors and other interested users of telecommunication services. As a result, the identification of unfavorable trends of the enterprise development, differentiation of factors of influence, choice of the method of their estimation, carrying out of the evaluation with further interpretation of the results becomes paramount due to the threat of loss of control of the enterprise management.

That is why to receive objective information about the state of strategic management of telecommunication enterprises it is necessary to use models of different authors. The research analysis of risk in this field is considered in the works of such scientists as H. Androshchuk, D. Bloom, E. Brainerd, T. Vasyltsiv, V. Vitlinskyi, H. Velykoivanenko, M. Dmytriev,L. Donets, M. Ziegler, O. Zorina, I. Ivchenko, A. Kaminskyi, D. Canning, S. Koshechkin, L. Makhanets, L. Rishchuk, V. Smoliak, I. Fedulova, M. Khvesyk, A. Shtangret and others. A group of domestic scientists, such as I. Voronenko, I. Zelisko, N. Klymenko, L. Lazorenko, O. Nahorna, O. Sosnovska also considered this problem in detail in their scientific works.

Therefore, despite the large number of different models risk assessment of strategic management, modern science does not have a single formal approach, also, the methods of risk assessment for telecommunications systems and networks are not described. Each model is based on its group of indicators and regulatory values.

Allocation of previously unsolved parts of the general problem

Research and analysis of the current state and methods of providing qualitative processing, storage and delivery of information in modern communication networks showed that the perspective direction of problem solution is the necessity of providing the owner or the manager of the object of the CII to carry out organizational and technical measures on cyber defense at the object of the CII.

At the same time, it is necessary to understand that constant risk analysis is one of the elements of the risk management system, since in the process of risk analysis we receive the information necessary for making the right decisions on the risk management strategy, effective choice of risk reduction measures, assessment of the possibility of transfer, perception or avoidance of risk.

However, despite the considerable number of scientific works devoted to this topic, the problems of assessment of risks of strategic management of the objects of the CII state in the context of digital transformation of communication systems and telecommunication networks continue to be are ambiguous and unresolved.

Formulation of the aims of the article

The purpose of the article is to research, define and provide proposals on the methodology of risk assessment of CS of objects of the CII of the state on the example of methods and used technologies in the energy sector of the state, which implements the algorithm of application of the proposed variants of methods by modern scientists using the developed intellectual system.

The main material of the research

The risk management process is a constant process that should take the form of an orderly sequence of events, actions and decisions leading to the CS of the CII. Identifying potential risks is a key challenge in CS. For effective risk analysis, it is extremely important to identify objects of the CII, threats, vulnerabilities and understand the nature of cyber attacks, having defined its causes, scope, limitations and type of potential threats, which may affect the achievement of objectives and objectives of influence on the objects of the CII.

The relationship between the various attackers, threats, the exposed places and their influence on the information with further consequences is shown in Fig. 1.

Currently, the catalog of cyber threats [9] contains at least: malware software, Internet attacks, web attacks, phishing, denial of service, spam, botnets, data and information leakage, insider threats, physical manipulation, damage/theft/loss of information and personal data, crypto theft, demand, cyber espionage, backorders, exploit sets.

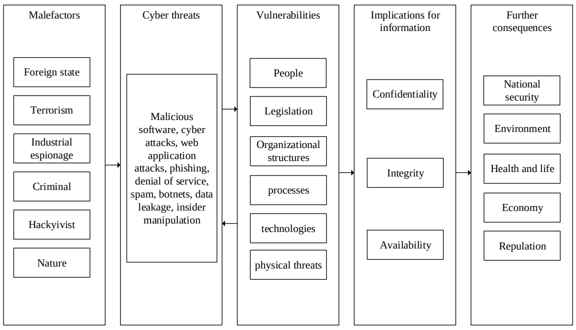

Figure 1: The influence of cyber threats and vulnerabilities on cyber security

As shown in Fig. 2, the risk management process associated with the safety of the CII facility may be an iterative process. An iterative approach to the risk assessment process may take the form of an increase in the level of detail of each iteration or process stop. After each phase/stage there are points of decision making (continuation, completion, return). The iterative approach provides a favorable balance between reducing time, efforts required for certain controls, and confidence in the correct risk assessment.

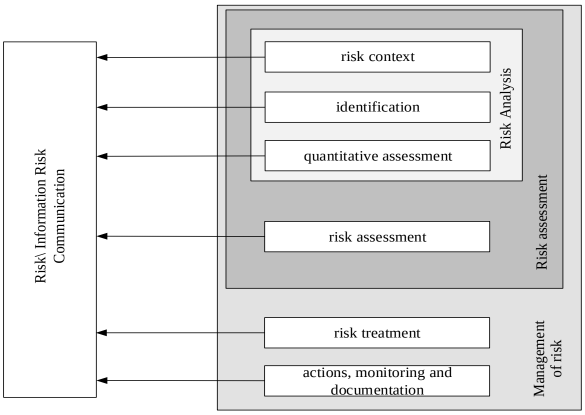

Figure 2: Model risk management process

Because of the rapid development of technology, the growth of digitalization, preventive progressive operations and destructive actions in cyberspace, the objects of the CII can be exposed to increased CS risks, which can adversely affect the goals of the organization responsible for information infrastructure centers. Therefore, organizations must effectively manage risks of the CS. CS risk assessment is an integral part of the organization’s risk management process.

During the assessment of CS risk of the organization, it is necessary to:

- determine what processes can go wrong, and what events, often the result of the actions of the subjects of threats, can make undesirable results for the CII object;
- determine the risk levels to which they relate (understand the risk levels well, which in turn will allow the allocation of adequate actions and resources to manage the highest priorities).

The following risks can be identified when assessing the risk:

- incorrect formulation of risk scenarios;
- risk scenarios that describe events “what can go wrong”, which often have non-specific and general character and do not contain specific threats, vulnerabilities, assets and consequences. As a result, it is difficult to understand the level of risks and to associate them with the organizational context or to identify targeted measures for their elimination;
- identifying risks using a compliance-oriented approach is identifying risks from the point of view of assessing safety measures (or their absence), similar to conducting a compliance audit or analysis of non-compliance based on regulatory acts. The approach to compliance risk assessment determines the behavior of the checklist, creating a false sense of security that the CII facility is not subject to any risk if it meets all relevant requirements;
- recognize the absence of risk tolerance factors. Often CS risk management plans institutions of the CII are not included in the organization’s risk management program. As a result, CS risk tolerance at the organizational level is often ignored, and it is difficult for the institution’s management to determine the appropriate level of risk to achieve its business goals;
- determine risk probability based on historical or foreseeable events;
- inaccuracy of the definite approach. This may be due to simultaneous recording of **n** number of cases. Under such conditions, it is possible to assume that the event occurred earlier, especially in the absence of information about the past CS event. In the security context, the probability of an event of the CS does not depend on the frequency of past events;
- handling risks with the help of easy control of measures. When using the general approach to developing measures to control potential risks, many organizations often mitigate the algorithm of detecting CS risks. In turn, this leads to the introduction of controls that do not completely eliminate the root cause. This problem is often related to poor understanding or formulation of risk scenarios.

Under these conditions, the importance of the risk context is an important prerequisite for further risk assessment. This step guarantees that the internal and external stakeholders involved in the risk assessment process have a general understanding of how the risk is formed, the risk acceptance and the risk owner's responsibility.

Assume that the risk of the CS **(R)** is defined as a function:

- probability **(P)** that this threat affects the vulnerability of the asset;
- resuleing influence **(V)** of the occurrence of a threat.

$$R(t)=F\left(P,V\right) \tag{1}$$

It is proposed to define each risk factor separately.

A threat is in any event in which an attacker, using the vector of a threat, acts against an asset in a way that he could potentially harm him. In the context of CS threats can be characterized by tactics, methods and procedures used by attackers.

Vulnerability is a defect in the development, implementation and operation of the asset, or in the internal control of the process.

Probability is the possibility that this threat can use this vulnerability (or a combination of vulnerabilities). The probability can be determined by factors such as detection, suitability for use, and playback.

Influence is the amount of damage caused by the threat that uses the vulnerability (or a combination of vulnerabilities). Under such conditions, the extent of harm can be assessed from the point of view of the state, organization or individual.

Risk tolerance is defined as the level of risk acceptance acceptable to achieve a specific business goal. Defining risk tolerance allows you to clearly define what risk your organization is willing to take. Table 1 provides an example of risk tolerance that can be adapted to the context of each organization.

Table 1
Example of risk tolerance

Risk level	Description of risk tolerance
Very high	The level of risk cannot be accepted, as its adoption will result in such serious consequences, which will have to be immediately stopped. As an option, mitigation strategies should be adopted immediately.
High	The risk level cannot be accepted. Strategies to reduce risk should be developed and implemented over the next month.
Above average	The risk level cannot be accepted. Strategies to reduce risk should be developed and implemented over the next six months.
Average	The risk level can be taken without strategies that can be easily and economically implemented, This risk must be constantly monitored to ensure that any changes are detected and the appropriate decision is made.
Low	The risk level can be taken without strategies that can be easily and economically implemented. This risk should be periodically monitored to ensure that any changes are identified and appropriate decisions are made.

Therefore, risk assessment consists of identifying environmental risks and determining the level of risks identified. The main stages of risk assessment are risk identification, quantitative risk assessment (which are elements of risk analysis) and qualitative risk assessment (Fig. 3).

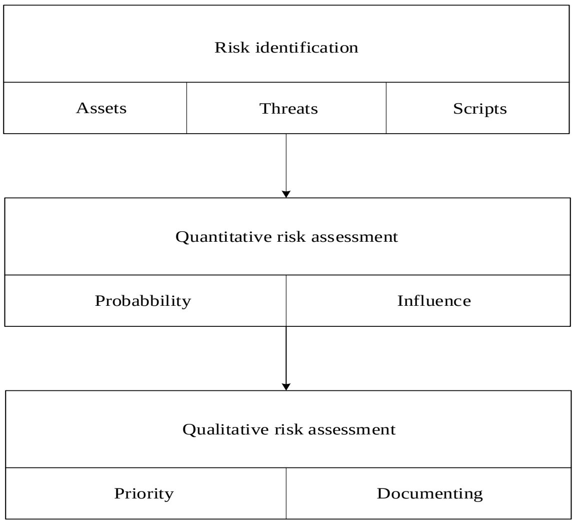

Figure 3: Process of risk assessment

The risk identification task includes the following components:

a) identification of assets (identification and description of all assets that make up the system related to this risk). When identifying assets, it is important to determine which assets are the primary assets, as well as the resources that the attackers can take control to reach the primary asset. For example, in a distributed power management system, the PLC (programmable logic controller), which controls the turbine, is likely to be considered as the main asset, since it directly affects electricity generation. At the same time, the target of the attacker is likely to be manipulation of logic of PLC, namely, termination of electricity generation;

b) identify threats based on inventory and network architecture to identify threats [10, 11] which can use sensitive locations for each asset separately;

c) building a risk scenario is the task of creating scenarios that provide a realistic and comparable view of risk based on business context, system environment, and associated threats. The risk scenario should consist of the following key elements: Assets, threats, vulnerabilities (the above elements can be identified through audits and/or penetration tests, and they can be associated with different physical spaces, the environment through the use of certain technologies, the result of which is a direct result of the threats.

The quantitative risk assessment consists of an analysis of elements that include each risk scenario separately to determine the probability of occurrence of a risk scenario and the influence (i.e. the extent of the damage) of the risk scenario.

A purposeful or unexpected event is traditionally used as a metric to measure risk probability. However, the use of such a metric to measure the probability of CS risk may not be appropriate because of the dynamic character of CS threats. If the normal operation of the system has not been broken before, it does not mean that it will not be broken in the future. The probability of CS risks should be assessed in terms of threats and vulnerabilities of the system. The following factors must be taken into account to determine the probability of a CS system risk:

- The phenomenon is "concentration of efforts of attackers on search of vulnerabilities of assets (management systems) of the network". This factor depends on the availability of information about the vulnerability of the system and the influence of the vulnerable assets on the system's functioning;
- The possibility of using is "Development of strategy, tactics and basic algorithm of realization of the shortest ways of vulnerability of system assets". This factor depends on the access rights, the complexity of the tools and the technical skills required to perform the attack;
- The redevelopment is "the increase of preventive action on the assets of the system (network)". This factor depends on the complexity of building the architecture of its organizational and technical model of cyber defense, mechanisms of timely identification of threats and tools of detecting cyber attacks.

A risk scenario can break confidentiality, integrity, and/or asset availability (e.g., information, equipment, operations). Any compromise of assets will lead to negative consequences at such levels:

- state (influence can be considered as a damage to state security and economy);
- organizational (influence can be considered as business activity destruction, reputation destruction and loss of finance);
- individual (influence can be seen as loss of life and injury).

A qualitative risk assessment consists of identifying and understanding the significance of the risk level and includes such tasks:

- identify and prioritize risk (risk matrix is being built);
- documentary execution of risks (risk introduction to the register with the identification of the detected scenario, date, measure, residual risk, etc.).

At the same time, the complexity of cyberphysical relations in the functioning of the CII facilities is in unknown systemic dependencies. Accurate risk assessment requires the development of models that provide the basis for risk analysis and quantitative risk assessment. The relationship between the characteristics of the CII objects facilitates the risk analysis process and the mitigation of their consequences.

Thus, the approach to risk assessment of CS can be applied in the information and analytical system "Security management system" [12], which provides vulnerability detection and risk assessment (risk potential) and simplifies the development of management solutions to prevent CS events.

In accordance with the provisions of the methods considered and the factors outlined above, the identification of real and potential cyber threats is carried out by means of establishing, on the basis of empirical experience, correspondence between such sources and their characteristics. The result is a set of **{ak}**, **k** = 1, 2, ..., {ak} , elements of which are signs of sources of threats, and indices are their numbers.

For objects of the CII, there is a threat of computer attacks:

k = 1 are foreign intelligence services;

k = 2 are criminal structures;

k = 3 are competing organizations;

k = 4 is the staff of the object;

k = 5 are manufacturers of equipment, enterprises which carry out repair and maintenance of means of computing equipment and peripheral equipment of objects of the CI;;

a1 is presence of interest of foreign intelligence services to object of the IR;

a2 is presence of interest of criminal structures to object of the IR;

a3 is presence of interest of representatives of the financial, economic and industrial environment (infrastructure) who have a competitive interest and use the IR of a common object;

a4 is independent technical support and provision of it infrastructure by the officials of the object;

a5 is using of non-certified (non-licensed) software at maintenance and repair works on the object.

In the conditions of increasing risk level of use of phishing attacks, botnets, malware software, ransomware etc., the specific approach is the detection of the IR vulnerabilities of objects of the CII. By reducing the risks of possible computer attacks, it is necessary to use the calculation methods to determine the fact of a potential threat.

When determining the object's IR vulnerabilities, an expert analysis of the object's information environment is carried out to implement the threats of computer attacks. The result is a set of **{bl}**, **l** = 1, 2, ..., L, the elements of which define the vulnerability. At the same time, indices correspond to the numbers of vulnerabilities from their list.

If you assess the level of the threat of a computer attack on an object of the IR, there is a threat for this type of attack are:

b1 are input drivers of information;

b2 are display drivers of information;

b3 are drivers of information processing tools;

b4 are BIOS chip drivers;

b5 is software of servers with open physical access;

b6 is software of communication equipment of the object;

b7 is TCP/IP protocol stack;

b8 is gateway to the Internet;

b9 are application level inter-network interaction protocols;

b10 are undocumented points of inter-network interaction;

b11 are open shared network resources;

b12 are non-certified software components;

b13 is e-mail;

b14 is web-browser;

b15 are cables of equipment of the object on areas where physical access to them is available.

For quantitative assessment of the vulnerability through which a computer attack on objects of the IR of the CII is possible, it is determined by the probability of presence of appropriate favorable conditions. This probability is estimated by experts in the field of the CS. The results of the evaluation are presented by linguistic values: “yes”, “probably”, “possibly”, “unlikely” and “no”, which describe the possibility of using **k** source as a threat to the computer attack of **l** vulnerability.

Each of the five linguistic values is related to the probability of **pkl** using **k** source of **l** vulnerability. On the basis of this probability, the probability **Pl** of using the **l** vulnerability (**l** = 1, 2, ..., 15) by possible five sources of threats is determined:

$$P_l = l - \left(\gamma l_1 \left(1 - pl_1\right) \cdot \gamma l_2 \left(1 - pl_2\right) \cdot \gamma l_3 \left(1 - pl_3\right) \cdot \gamma l_4 \left(1 - pl_4\right) \cdot \gamma l_5 \left(1 - pl_5\right)\right) \quad (2)$$

where **ɣlk** is the coefficient of compliance equal to 1 if **l** vulnerability obeys to **k** source and equal to 0 if not.

This allows to form a set of **{um}**, **m** = 1, 2, ..., M, computer attack threat [11]:

u1 is the download harmful software with the features of an alternate operating system with extended authority;

u2 is unauthorized copying of information;

u3 is unauthorized modification of information;

u4 is implementation of a false authorized object;

u5 is replacement of system software;

u6 is network traffic redirection;

u7 is manipulation of data in remote mode;

u8 is hacking of e-mail box;

u9 is blocking of e-mail box;

u10 is replacement of Web browsers;

u11 is use errors in application software algorithms;

u12 is blocking the user's host;

u13 is blocking the router;

u14 is firewall bypass.

The quantitative characteristic of the level of the **m** threat of a computer attack, where **m** = 1, 2, ..., 14, on the IR of objects of the CII is the probability:

$$P_m^{(y)} = 1 - \Pi\left(1 - \alpha\text{lm} \cdot \text{Pl}\right) \qquad (3)$$

where Pl – matches the expression (2);

αlm –the factor of urgency of vulnerability of object information for initiation of threats of computer attacks is equal to 1, if **l** vulnerability is actual for initiation of **m** threat and 0, if not actual.

The value of the relevance of the vulnerabilities of object of the CII information for the initiation of computer attack threats is shown in Table 2.

Table 2
Value of the factor of urgency of information vulnerabilities of objects of the II for initiation of threats of computer attacks

Computer attack threats	Vulnerability of information resources of objects of the CII to realization of threats of computer attacks														
	b1	*b2*	*b3*	*b4*	*b5*	*b6*	*b7*	*b8*	*b9*	*b10*	*b11*	*b12*	*b13*	*b14*	*b15*
u1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
u2	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1
u3	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1
u4	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
u5	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
u6	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
u7	1	1	1	0	0	0	1	0	0	0	0	0	1	0	0
u8	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u9	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u10	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1
u11	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0
u12	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0
u13	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0
u14	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0

Taking into account the threat of computer attacks, the values of the coefficient of destruction of threats of computer attacks on the information resources of objects of the CII are given in Table 3.

Table 3
Value of the coefficient of destruction of threats of computer attacks on information resources of objects of the CII

Destruction	Threats of computer attacks													
	u1	*u2*	*u3*	*u4*	*u5*	*u6*	*u7*	*u8*	*u9*	*u10*	*u11*	*u12*	*u13*	*u14*
НК	1	1	0	1	0	0	1	1	0	1	0	0	0	1
НМ	1	0	1	1	1	1	1	0	0	1	1	0	0	1
БД	1	0	0	1	0	0	1	0	1	1	1	1	1	1

From the foregoing, it follows that the merit of the existing methods of assessing current threats to information security is the simplicity of the assessment procedures. The disadvantages, which essentially limit their use for an adequate assessment of measures to ensure the cyber-stability of objects of the CII, should be borne in mind the lack of a possibility to account for the dynamics of counteraction to such attempts of threats and low statistical reliability, which is characteristic of expert assessments.

Implements the algorithm of the application of the shown methods for the analysis of cyber threats and risk assessment of the CS break of the CI the technology consists of four main stages:

1) Analysis of cyber threats:

- setting the context;
- security audit;
- formation of scenario concepts;

2) Modeling of scenarios:

- decomposition of threats;
- scenario formation;
- setting criteria;
- setting estimates of probability values of concepts (variables);
- network construction and architecture;
- formation of a private model of threats;
- scenario analysis;

3) Risk assessment;

4) Classification of objects.

The proposed technology is designed for the following groups of users:

– security engineer, i.e. specialist in the field of information security of the company, or, in the absence of such, administrator of the local computing network;

– engineer with knowledge in energy (expert): depending on the level of detail, the study can be both an energy security expert and an operator/power engineer at the facility; in the field of safety: security engineer;

– an analyst who can act as a knowledge engineer.

The interrelation of the stages of technology, methods and blocks of the intellectual system is presented in Table 4.

Table 4

Stages of technology, methods and tools

Stages	Groups of users	Methodology	Tools
Analysis of cyber threats	Security engineer	Methodology for analyzing cyber threats of energy infrastructure	Expert system
Modeling of scenarios	Security engineer, knowledge engineer (industry security expert)	The method of creating scenarios of extreme situations in energy	Block of Bayesian trust networks
Risk assessment	Knowledge engineer (expert), analyst	Methodology of risk assessment of the CS break of energy infrastructure	Risk assessment block
Ranking of objects	Analyst		

Functionally, the CS assessment system is presented in Fig. 4.

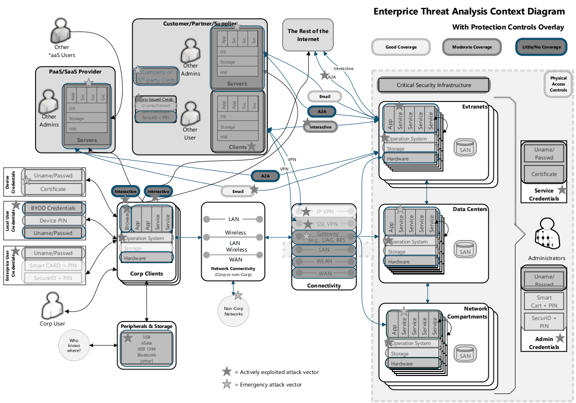

Figure 4: Scheme of Cybersecurity assessment system

Although the algorithm for using these methods to analyze cyber threats and assess risks of violation of the CS of the CI involves different levels, stages and components, but it must be a single document and consist of the following hierarchical stages (levels):

– Stage “Analysis of cyber threats”.

At this stage the context is established, i.e. description of the main characteristics of the given object, its identification and description of the assets of the information and technological system.

However, the audit of security of the institution (enterprise, organization) at the initial stages consists in the identified critical components and identified existing vulnerabilities [13].

Therefore, the analysis of cyber threats in the intellectual system is carried out with the help of technological and program instruments that are part of the production expert system. Lists of critical assets and identified vulnerabilities are formed according to existing/discovered cyber threats, as well as typical attack vectors, which represent a sequence of potential threats and vulnerabilities to target assets. On the basis of the result concepts and connections are formed between them for further development of scenarios. Formally, the output data of the first stage of the technology of cyber threats analysis and risk assessment are presented by the formula (4).

$$P=\left\{V,T,A,R_V\right\} \quad (4)$$

– Stage “Modeling of scenarios”.

This stage is proposed to be built according to “scenario planning” [17] using the tools of Bayesian networks, which consists in calculating the value of trust in the proposed scenarios based on the existing trust options in the network.

Scenarios are evaluated by the integral of each IP address, DNS name, IP address range, subnetwork, and even a text file (by scanning).

Such calculations are considered as a pessimistic scenario - a set of events and relationships between them, which lead to maximum losses and damages as a result of their occurrence and development [18].

Previously, the model of Bayesian networks was used for modeling of risks of critical situations at realization of strategic threats [15], but threats CS at the same time were not considered.

In connection with the inclusion of cyber threats in the number of strategic threats [11], the following structure of a typical scenario of a threshold situation, caused by the realization of cyber threats, is proposed, which is represented by formula (5):

$$S=\left(X^{f},X^{v},X^{t},X^{c}\right) \quad (5)$$

where: **S** is the structure of the scenario of the extreme situation in the energy sector, caused by the implementation of cyber threats; $\mathbf{X^f}$ are variables, according to the factors affecting the emergence of an extreme situation; $\mathbf{X^v}$ are variables for indicating the vulnerabilities of the ICS assets; $\mathbf{X^t}$ are variables to indicate threats; $\mathbf{X^c}$ are variables, consequences associated with the probable occurrence of an extreme situation in energy. Next, the construction of scenarios of the occurrence of extreme situations under certain conditions of the ICS state of the object is carried out, probable threats are determined taking into account information about the distribution of attack vectors. On the basis of the analysis of scenarios management decisions are taken as the order of actions necessary to achieve the desired conditions and situations [14].

– Stage “Risk assessment”.

Risk is considered as a combination of the consequences of some event (incident) and the possibility of its occurrence in accordance with the international standard ISO/IEC 27005: 2011 “Information technologies. Security techniques. Information security risk management”. The risks of implementing a sequence of threats leading to an extreme situation are assessed by both qualitative and quantitative indicators. The description of such risks is based on the qualitative information received from experts (specialists in information and CS, engineering staff with knowledge in the field of energy), which are necessary to define and describe each of the six described types of concept scenarios. Quantitative information related to the peculiarities of the system operation is used further when the values in the concepts are filled in.

The paper considers the interrelation of it risks and risks of accidents and catastrophes of complex technogenic systems [4]. The measurement of the risk level is carried out for all significant scenarios, which are assigned the values of the probability and consequences of the risk [16]. The presence of vulnerabilities at risk assessment allows to define the list of critical assets at the enterprise for further substantiation of financial expenses for security provision. Risk assessment is carried out taking into account the established criteria of the assessment.

– Stage “Classification of objects”.

This stage of the technology consists in the classification of objects according to established criteria and risk levels for each of them. Critically important objects are key objects (or their aggregates) of relevant infrastructures, the influence of which can provoke the most negative effect in the economy, a key resource or lead to the destruction of the entire infrastructure [2].

With the proposed technology, objects are classified according to the size of the risks of an extreme situation, which covers some territory and a group of objects in their relationship with other objects of the CI, information about which is embedded in the scenario as concepts of consequences, external threats or factors. The criteria of classification significance are proposed (6):

$$KS=\left\{C,R,O\right\} \tag{6}$$

where: **KS** is criterion of significance; **C** is risk assessment criteria, **R** is integral index of risks of the object, **O** is the object is represented by a combination of basic characteristics.

The result of this stage is a hierarchical list of objects.

Therefore, the proposed technology, in comparison with traditional approaches to ensuring the CS, is aimed at identifying vulnerabilities and cyber threats, the implementation of which can cause disruption of the functioning of an important object to such an extent that the incident can be considered as an extreme situation in the economy, a threat to life or a destructive situation in industries and ecology.

The reliability of the proposed technology at the development stage is confirmed by expert assessments of experts in the field of energy and CS, which will be supported by its further approval.

Conclusions on this research and prospects of further research in this direction

The paper presents the methods of assessing the risks of CS violations of the CII state objects based on an intelligent system, combined in the technology of cyber threat analysis and risk assessment of CS violations of important objects.

In connection with a formally defined regulatory and legal field, which would not be enough to regulate the mentioned branch, and given the considerable number of scientific works devoted to this topic, the technology aimed at defining objects of special importance, the most prone to the risks of CS violation was proposed. Also, the article presents the procedure of determining predicted critical losses and probable consequences of the losses and the algorithm of classification of the list of such objects is formed.

References

[1] Barometr ryskov. Allianz nazval hlobalnые rysky predpryiatyi y fynansovoho sektora na 2019 hod. URL: https://forinsurer.com/news /19/01/16/36513?hl=%EA%E8%E1%E5 %F0% F0%E8%F1%EA%E8.

[2] Global Cyber Insurance Market (2019-2025). URL: https://www.researchandmarkets.com/reports/4871728/global-cyber-insurancemarket-2019-2025.

[3] Forbes [2016], «Cyber Crime Costs Projected To Reach $2 Trillion by 2019». https://www.forbes.com/sites/stevemorgan /2016/01/17/cyber-crime-costsprojected-to-reach-2-trillion-by-2019/#7885d6313a91.

[4] Shaun S. Wang. Integrated Framework for Information Security Investment and Cyber Insurance https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674.

[5] Scott J. Shackelford (2012) Should Your Firm Invest in Cyber Risk Insurance? Business Horizons, http://ssrn.com/abstract=1972307. 699.

[6] Jay P. Kesan & Carol M. Hayes Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment 102 Minn. L. Rev. 191 (2017), University of Illinois College of Law Legal Studies Research Paper No. 1718.

[7] Yogesh Malhotra (2015). Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at- Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era, Post-Doctoral Research Thesis on Finance, Risk, and, Quant Modeling Beyond the Global Financial Crisis, Suni Polytechnic Institute, New York. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547.

[8] Bratiuk V. P. Sutnist kiber-zlochyniv ta strakhovyi zakhyst vid kiberryzykiv v Ukraini / V. P. Bratiuk // Aktualni problemy ekonomiky. - 2015. - № 9. - S. 421-427.

[9] Prykaziuk N. V. Novi mozhlyvosti dlia rozvytku strakhovoi systemy Ukrainy / Nataliia Valentynivna Prykaziuk, Tetiana Petrivna Motashko // Ukrainskyi zhurnal

prykladnoi ekonomiky. - 2016. - Tom 1. - № 4. - S. 177-192.

[10] Kiber-strakhuvannia: novyi instrument ryzyk-menedzhmentu [Elektronnyi resurs]. - Rezhym dostupu: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu.

[11] Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. 2016. V. 253. № 1. P. 1–13.

[12] Jain P., Pasman H. J., Waldram S., Pistikopoulos E. N., Mannan M. S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. Journal of Loss Prevention in the Process Industries. 2018. V. 53. P. 61–73.

[13] Mokhor V., Bakalynskyi O., Bohdanov O., Tsurkan V. Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry. Information technology and security. 2017. V. 5. № 1. P. 71–82.

[14] Bochkovskyi A., Gogunskii V. Development of the method for the optimal management of occupational risks. Eastern-European Journal of Enterprise Technologies. 2018. V. 1, № 3 (97). P. 6–13.

[15] Prokopenko T., Grigor O. Development of the comprehensive method to manage risks in projects related to information technologies. Eastern-European Journal of Enterprise Technologies. 2018. № 2(3) (92). P. 37–43.

[16] Mokhor V. V., Honchar S. F. Ydeia postroenyia alhebrы ryskov na osnove teoryy kompleksnыkh chysel. Эlektronnoe modelyrovanye. 2018. 40. № 4, S. 107–111.

[17] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart. A review of cyber security risk assessment methods for SCADA systems. Computers & Security. V. 56. 2016. P. 1–27.

[18] Martin Eling, Jan Wirfs. What are the actual costs of cyber risk events? European Journal of Operational Research. 2019. V. 272, № 3. P. 1109–1119.

[19] Derek Young, Juan Lopez Jr., Mason Rice, Benjamin Ramsey, Robert McTasney. A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection. V. 14. 2016. P. 43–57.

[20] Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab A. L. Rassan, Md Zakirul Alam Bhuiyan. Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security. V. 74. 2018. P. 323–339.