DOI: 10.30525/978-9934-588-61-7-23

Dubnytskyi V. I.
Doctor of Economic Sciences, Professor at the Department of Entrepreneurship, Organization of Production and Theoretical and Applied Economics
Ukrainian State University of Chemical Technology

Pysarkova V. R.
Postgraduate Student, Assistant Lecturer at the Department of Entrepreneurship, Organization of Production and Theoretical and Applied Economics
Ukrainian State University of Chemical Technology

PROBLEMS OF ENSURING COMPETITIVE IMMUNITY OF THE REGION BY METHODS OF INFORMATION AND PSYCHOLOGICAL SECURITY

Summary

The article identifies, classifies and considers the main risks and threats to information and psychological security. The phenomenon of competitive immunity of the region using the methods of information and psychological security is considered. The characteristic of the information security of the region and the competitive immunity of the region is given. The work proposed the authors' understanding of general competitive immunity of the region, its differences from competitiveness. In a methodological interpretation, the problem posed in the work is structurally considered in the following sequence: national, regional, public and personal security. The relationship of competitive immunity of the regional economic system with the level of economic and information and psychological security is considered. The objectives and key parameters of information security for the regional level are considered.

Introduction

At the global, regional and national levels today, a large place is occupied by the problems of ensuring information security. In the era of globalization, we can talk about the global configuration of forces that must comply with global cultural codes and a special management model [1], in modern military-political conflicts, leading world powers to the active use of the

Internet [2], transforming and modifying the functional capabilities of military management of the bodies with its help, making them more flexible [3].

Information and psychological security appears as an incomplete system of interactions and mutual influences of heterogeneous factors with numerous feedbacks, which as a result can give unexpected effects in the information and psychological and any other sphere [4].

Nowadays, the informational impact on people and society comes to the fore, on the basis of which, the influence of informational-psychological security on the socio-economic development and competitiveness of the regions of Ukraine is observed. Thus, the impact of information and communication technologies (ICT) and psychological spheres of socio-economic development of the regions is evident. However, in order to enhance the positive effects of the use of information resources, it is necessary to narrow the gap between regions in the level of their penetration. In the context of digitalization and information on macro-, meso- and micro levels, the use and operation of information technologies form the attitudes, values and moral principles of the learning mechanism, which is confirmed in a pandemic COVID-19.

Given the above, the study of this problem involves the study, creation and use of methodological apparatus and tools that can take into account the uncertainty and heterogeneity of the source information, giving reasonable estimates of the threats under consideration.

Effective counteraction to threats will be possible upon receipt of their assessment, but it is possible that, solving information and psychological problems, one will have to look for their solution in the technosphere, and, conversely, technical or other issues that are far from the humanitarian sphere will find their solution in it. At the same time, one should not forget and have a methodological opportunity to take into account the fact that any measures to counter threats can be of a dual nature in the sense of their application is capable of simultaneously causing the desired result with respect to some factors, negative consequences relative to others [5].

Part 1. Tasks and threats to information and psychological security

Competitive immunity as a competitive advantage, and security, being in constant interaction, are the key characteristics of the national economic complex. Competitive immunity is an indicator of competition and confrontation with the potential risks of the national economic complex, and security is an essential condition for its existence. The more developed the factors that determine competitive advantages, the more stable the national economic complex will be in front of emerging external and internal threats. Accordingly, most indicators characterizing competitiveness are also indicators characterizing safety.

The relevance of considering the provisions in the context of maintaining and strengthening the competitive immunity of the region is also due to the fact that in the current conditions of the economic space with existing non-standard situations, cyberattacks, crises, the leaders of countries, regions and

cities can no longer think about reducing the vulnerability of their territories, which leads to a decision questions about the security of the territory and its resilience. Higher competitive positions are achieved by those territories that have competitive immunity. Otherwise, even cardinal decisions such as mergers and acquisitions of territories are not ruled out.

The low level and consistent decrease in competitive immunity poses a threat to the security of the economy, when security is a necessary condition for ensuring and enhancing the competitive immunity of the territory. The system «competitiveness – security» is a complex system, the behavior of which depends on a large number of factors of various nature.

A number of scientists were involved in assessing the impact of informatization on competitiveness: D. Sikel, K. Shtirokh, D. Rodrik, F. Trebbi, S. Rosotto, K. Kimura, etc. Their works examined the impact of informatization on the economy as a whole, while the impact of information and psychological security on the competitiveness of the region remains a rather poorly studied topic.

Research in the field of economic security is dedicated to the work of scientists: V.A. Onishchenko, O.I. Stadnichenko, N.Yu. Naumenko, I.Yu. Drevitskaya, E.V. Kolomiets, V.I. Dubnytskyi, R.A. Koval, V.I. Zakharchenko, K.Y. Holovko and others.

Interregional competition has become associated with a fundamentally new quality of competitive processes in the context of the development of informatization, while the format of competition in the world market is changing significantly. If in former realities countries were participants in the world market, then the extremely intensive development and implementation of information technologies, which were the catalyst for globalization, made it possible for individual regions of countries to participate in world competition. The competitiveness of the region in the context of globalization is characterized by a willingness to respond to the challenges of the world market, and the ability to adapt. The innovative potential of the region largely determines the level of competitiveness, and in particular, the level of competitive immunity of the region. The concept of «competitive immunity» was introduced for general use by scientists and a group of scientists: S.G. Vazhenin, I.S. Vazhenina, A.I. Tatarkin, D.A. Kopantsev. Competitive immunity is becoming a new, modern category of competitive advantage analysis.

In the view of I.S. Vazhenina and S.G Vazhenin, as a category competitive analysis, «competitive immunity» is the ability of the subject to not only successfully compete, but also to deal with the potential risks of internal and external shocks, as well as dynamically recover from the destructive phenomena due to the presence of internal, sometimes not yet demanded and not involved resources and assets [6]. Moreover, according to the authors, competitive immunity involves the construction of an effective system to ensure economic security and protect the interests of the territory.

Among the methods and assessments of the region's competitiveness, we note that the most common is the approach of experts from the World

Economic Forum (WEF). They view regional competitiveness as «a set of institutions, policies and factors that determine the level of productivity of a region».

The problem of studying the impact of the development of information technology on the economy of the region seems very relevant, but at the same time quite complex. The American researchers D. Sikel, S. Oliner, K. Shtirokh, exploring the impact of the development of information technology on socio-economic indicators, came to the conclusion that stimulating this sector of the economy provides a powerful multiplier effect [7].

In a methodological interpretation, the problem of the influence of information and psychological security on the competitive immunity of a regional socio-economic system under the conditions of economic and information asymmetry in the development of a region should be structurally considered in the following sequence: national, regional, public and personal security.

Today it is customary to single out international global security, international regional security and national (state and country). The latter, in turn, is divided into national, national-state, social and individual [8].

According to the definition of the researcher A.A. Sergunin, «National security is a state, in which a country's national interests are protected in a broad sense, including political, social, economic, military, environmental aspects, risks associated with foreign economic activity, and the proliferation of weapons of mass destruction, as well as the prevention of threats to the spiritual and intellectual values of the people» [8]. From here we can distinguish and establish various types of security: national, political, economic, informational, technological, military, environmental, social, legal, cultural, intellectual, regional, demographic, genetic, psychological, external, internal, public and personal.

To identify the relationship of competitive immunity and safety it is important to the whole complex design primarily categories of competitiveness, emerging at three main levels – micro, meso-, and macro level. If one wonders what the competitiveness of a country is specifically expressed, then the most likely answer will be the competitiveness of its products. However, the competitiveness of goods is only part of the country's competitiveness. Market conditions are very dynamic, especially in modern conditions of rapid change of generations of equipment and technologies. This requires high competitiveness of firms and enterprises that produce products and provide services. Enterprises, in turn, depend on the general business and investment climate emerging in the country, on the legal support of their activities on the part of state bodies regulating national economic relations.

At each level, competition solves certain problems, therefore, when analyzing competitiveness, it is important to understand what the main goals are pursued in the competition between entities carrying competitive advantages. It is clear that the goals of enterprises and countries will be different, therefore, competitiveness will also vary significantly. These goals

in accordance with the levels of formation of competitive advantages usually vary in scale and time horizons: short-term goals are at the micro level, medium and long-term levels are at the mesoscale and ultra-long goals are at the macro level.

Public safety is a socio-legal category, which is a kind of national security. In a philosophical and philological sense, this type of security contains two components: society and security, as a set of established forms of joint activity of people, in other words, a set of social relations taking shape in the state. This view, in the end, predetermined the conclusion that public safety is a state of public relations that prevents the threat of harm and thereby ensures their normal functioning. This is the safety of all the main components of an individual or collective, which are a kind of cumulative value, protected by moral and legal norms.

Personal safety plays an important role in the process of influencing competitive immunity. An important indicator of personal security is self-esteem of security, a sense of security, which is the basis of the activities of individuals to identify, prevent, mitigate, eliminate and reflect dangers and threats that can destroy them, deprive of fundamental material and spiritual values, cause unacceptable damage, close the path to survival and development. The perception of threats on an individual-personal level is determined by the subjective feeling of the degree of one's own security and vulnerability. An important criterion for an objective assessment of personal and social security is the risk reflection indicator, which develops into several parameters: threat assessment at the public, social group and individual personality levels, an integral indicator of personal security, a subjective assessment of one's own risk, integral indicators of the degree of risk and risk reproduction, as well as assessing the acceptability of risks in public life [9].

Furthermore, the information security of an individual is presented as a system, the elements of which are the information and legal, information and psychological security, as well as the information and analytical, information and technical security. Given the current geopolitical situation, it is especially important to provide protection from the information and psychological impact of various destructive programs, but, unfortunately, the legal support of information and psychological security is imperfect. There is excessive generalization, appraisal and lack of a unified approach to the definition of concepts; there is no existing legal system for determining a meaningful assessment of information products; there is no complex nature of the organizational and legal system of protection against malicious information, which requires not only a combination of material and procedural legal norms, but also a system of organizational and technical measures. Ensuring information and psychological security is an important condition for ensuring national security and stable development of society as a whole, therefore, it is necessary to pay special attention to this problem.

Thus, general regional security is not only a state of protection of regional interests, but also the ability of regional authorities to create effective mechanisms to ensure competitive immunity of the region, socio-economic

stability and sustainable development of the territory as a relatively independent structure, organically integrated into the country's economy. Thus, the competitive immunity of a region is considered only as a factor of economic security of the region and the country as a whole.

The regions of Ukraine at this stage of economic development, being the subjects of management, directly implement the goals and objectives set for society. Therefore, one can call competitive the region that is capable of realizing the main target: sustainable social and economic development with a high quality of life for its population.

First of all, the competitive advantages of the regions are determined by the success of firms and organizations in the competition against the existing socio-economic conditions. The formation of conditions for the development of competitive relations within the region and the country as a whole is one of the main regional and national priorities of any country, the most important function of state regulation of the economy.

The competitiveness of the region primarily reflects the ability of local producers to be most productive, that is with a sufficiently high productivity, use the available economic potential of the region. It is important, in our opinion, to understand that the region does not need to have rich natural and economic resources in order to be competitive.

The competitiveness of the region can be considered as a system consisting of such elements as the competitive potential of the region, factors and conditions for the formation of a competitive environment, resource efficiency, competitive advantages, competitive immunity, competitive strategies of business entities, state and market mechanisms for managing the economic potential of the region for a more complete satisfaction of human needs [10].

The report of the World Economic Forum in Davos, 2020 [11], published the main risks that countries may face this year, and which show that there is a change in the perception of global risks. Currently, climate deterioration is highlighted, but in addition to processes related to climate change, respondents highlighted and drew attention to other, major and important threats, which include: a slowing economy and social tensions, problems with cybersecurity. An increase in cyberattacks aimed at intercepting and stealing data, information and money leads to the need to analyze and manage information security risks to create an integrated methodology and information security system for an organization, region, country, to ensure the necessary and sufficient measures and means of information protection.

Given that some industries are at greater risk than others, there is no guarantee for any industry that they will not be susceptible to hacker attacks. According to the IBM X-Force Threat Intelligence Index 2020 report, the five most vulnerable sectors in 2019 included the financial services sector, retail, transportation, the media and professional services, the latter, in turn, suggest companies that provide specialized consulting services such as law, accounting and architectural firms.

Comparing the target from the races for three years, from 2017 to 2019, attackers usually follow the money, which shows the financial services sector, which takes first place for three years.

Table 1

Most attacked industries from 2017 to 2019

	Year		
	2017	**2018**	**2019**
Attacked Industries	1. Finance and insurance	1. Finance and insurance	1. Finance and insurance
	2. Information and communication technology	2. Transport	2. Retail
	3. Production	3. Professional services	3. Transport
	4. Retail	4. Retail	4. The media
	5. Professional services	5. Production	5. Professional services

Created on the basis of the IBM X-Force Threat Intelligence Index 2018, the IBM X-Force Threat Intelligence Index 2019, the IBM X – Force Threat Intelligence Index 2020 [12, 13, 14]

It can be seen from Table 1 that information and communication technologies over the past few years have reduced their positions in the ranking of mass hacker attacks after stable maintenance by 2-3 positions in 2013-2017 according to the IBM X-Force Threat Intelligence Index. A change in interest and goals for attacks can lead to the unpreparedness of subjects for these attacks, as a result of concentration on other industries.

However, regardless of industry, each organization may be attacked. Security strategies and tactics must be holistic in their approach and must constantly evolve and adapt to keep threats at bay in an ever-changing threat environment.

If an organization uses the best technical products to ensure security, it should still be prepared for potential attacks, hackers can use either their proximity or psychology and sociology skills to circumvent technology and use insiders to carry out their attacks.

A solid cybersecurity position can be achieved through a combination of multi-level and integrated security solutions, end-user training and awareness, supported by processes, security best practices, management and a safety culture as a shared responsibility [15].

Consideration of priorities in the context of national security and their transfer from the interests of the state, to the interests of the person himself or herself, led science and practice to develop a new look at this problem, which was the information and psychological security.

Information and psychological security suggests that, acting as objects to be protected, individual citizens, society, regions, and the state are considered as social entities.

Currently in Ukraine the main document containing a set of official views of the principles, priorities and guidelines for ensuring cyber security of Ukraine, determining the strategy of cybersecurity of Ukraine is the Presidential Decree on the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 «On the Doctrine of Information Security of Ukraine» [16]. However, this Decree deals mainly with issues related to information technology security. The aspects of information and psychological security in the Decree are touched upon in general terms, as influences and risks, protection from which is one of the national interests of the country.

In the context of informatization and digitalization of various aspects of life, the information and psychological sphere has become an important part of public life, which largely determines the direction of socio-political and economic development of not only the country as a whole, but also individual regions.

Information technology greatly affects the social sphere. In recent years, under the influence of informatization, the model of education has begun to change. E-mail, websites, social networks, educational resources, platforms for learning online, allowed to produce, transmit and consume information at a speed and in volumes inaccessible to humanity before. In addition, a number of countries have launched special programs to informatize the education sector.

Threats to the information space are divided into two groups:

– natural threats (threats arising from events and phenomena that are not dependent on society);

– artificial threats (accidental and intentional, caused by society).

The key threats to the information space: information leakage, fraud, cyber attacks, cyber warfare, data loss and/or destruction, unwanted information (content).

Unwanted information (content) is a dangerous and harmful application, newsletter, web pages prohibited by law and materials that do not meet the age limit.

Information leakage is grouped into intentional and accidental, the latter being accomplished due to various malfunctions in the hardware and software equipment or staff deficiencies.

The loss (destruction) of data is rightfully considered an important aspect of the threats to the security of the information space. Violation of the integrity of the infobases is likely to be triggered by equipment malfunctions or malicious events from users, whether they are enterprise workers or pests.

A threat to information security is also fraud. For information fraud include malicious operations with bank cards, hacking online banking.

The threats of terrorist organizations are increasing every year and appear in the virtual world. Wars around the world change their character to information wars, in which the main weapon is the important information [8].

The assessment of the above threats to the information space should be approached carefully, considering many factors. There are a number of protective software shells, the databases of which must be updated daily: protection against inappropriate content, data encryption, backup, fault tolerance systems, etc.

In the field of ensuring information security of the regions of Ukraine, it is necessary to analyze and solve the following tasks:

– determination of the main directions of state policy in the field of ensuring information security at the regional level, as well as ways to implement this policy;

– development of regional special programs to ensure information security of the regions;

– improvement of the regulatory framework for ensuring information security in the subjects of the country;

– adjustment of the parameters of administrative and legal responsibility of officials of the state authorities, local self-government bodies, legal entities and citizens for the improper compliance with the prescribed information security requirements;

– ensuring technological independence in the most important areas of informatization, telecommunications and communications that determine its security;

– development of modern methods and means of information protection, information technology at the regional level.

In the process of forming the concept of economic support for the information security of the region [17], it is advisable to distinguish the following functions of the regional system:

– strategic function contributes to the development of a strategy for the development of a regional information security system acceptable to all participants in this process;

– limiting function makes it possible to take into account the potential of all participants in the solution of current and future tasks of the development of a regional information security system;

– communication function makes it possible to navigate in the external environment and build intra- and inter-regional ties;

– scientific advisory function allows participants in the development of a regional information security system to make managerial decisions, avoiding conflict situations or minimizing their number;

– control function allows you to compare the management decisions made and the possible consequences of their adoption, taking into account the long-term interests of the development of the regional information security system.

Consideration of information and psychological security involves determining the main tasks of ensuring information and psychological security (Figure 1).

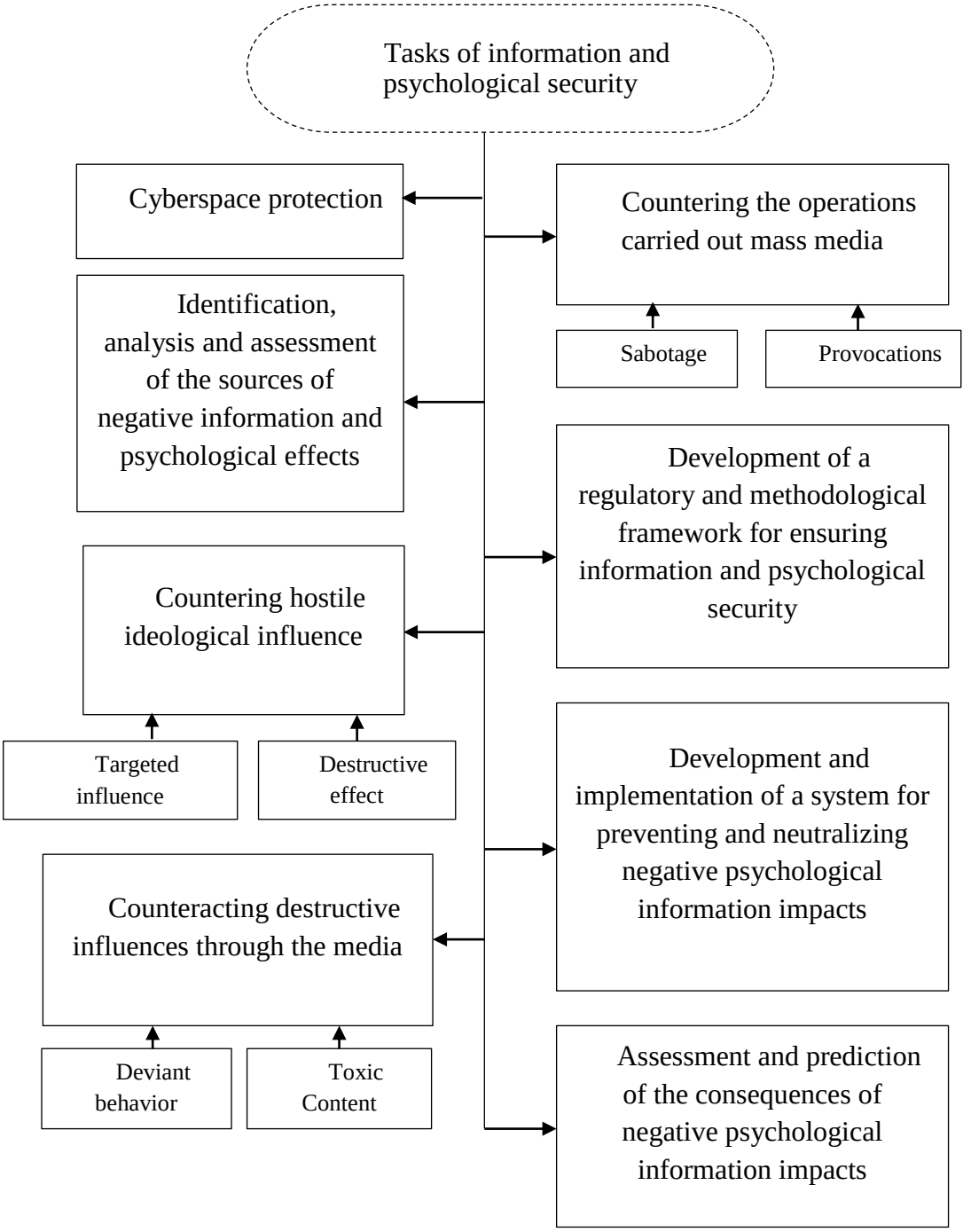

Figure 1. Tasks of information and psychological security

Part 2. Methodical guidelines for monitoring of competitive immunity methods of information and psychological security

In the framework of the concept of competitiveness of a territory, the state of things at a certain point in time is fixed; the competitiveness of the territory largely depends on what is produced in this territory, by whom it is produced and how it is produced, reflects the opportunities realized and the results obtained and grows as a result of the territory's self-development, the creation

of new industries, and the involvement of new raw materials in economic turnover.

When considering the competitive immunity of the territory, attention is focused on the analysis of competitive positions in dynamics with extrapolation to the future and the ability of the territory to participate in the competition, level potential threats and get out of extreme situations with minimal losses; competitive immunity of the territory characterizes the available reserves and potential opportunities; it is strengthened due to the self-realization of the territory through the capitalization of existing and emerging competitive advantages, the aggressive promotion of the economic interests of the territory and its positioning in the economic space [18]. The key to maintaining and strengthening the competitive immunity of the territory is the possession of sustainable competitive advantages, their reproduction, protection and constant addition of new ones.

According to the specifics of the region's economy, the authors understand the «immunity of the territory» as a unique combination of «innate» and «acquired» factors and natural conditions and factors of the economic and environmental environment, including active and passive factor-produced results and products of the functioning of the regions for implementation in the framework of artificial nature, the vital activity of their economic agents, which impede their complete disappearance.

In the category «general immunity of the region» proposed by the authors, an understanding of the unique combination of «innate» and «acquired» factors and natural conditions, and the specifics of the formation of the economic complex and infrastructure of the region, as well as active and passive factor-producing, and conditionally producing «results», «environment» is offered, «products» of the functioning of the region's territories for the implementation of the economic security of the region, the creation of conditions for economic growth and the implementation of economic cycles for the development of regional economic dynamics.

The competitive immunity of the territory reflects a number of new characteristics of modern territorial competition in the context of globalization, which essentially distinguishes it from the concept of economic security.

Competitive immunity of the territory:

– focuses on the analysis of the competitive position of the territory in a globalizing economy in dynamics and with extrapolation to the future;

– testifies to the ability of the territory to successfully compete with other regions and municipalities, to activate opportunities, on the one hand, and level potential threats, on the other, get out of extreme situations with minimal losses;

– not only captures the current state, but mainly characterizes the available reserves and potential opportunities;

– strengthens due to the self-realization of the territory through the capitalization of existing and emerging competitive advantages, the active promotion of the economic interests of the territory and its adequate positioning in the economic space.

Attention should be paid both to the consideration of assistive devices and the barriers to the introduction and effective use of technology. Thus, in order to achieve a high level of regional competitiveness, a full understanding of the factors (cultural, social, economic, and technological), which affect information and psychological security, is necessary. According to Thomas Friedman, the study of the elements that influence the business environment in a digitized and global environment should be an incentive for individuals, organizations and governments to develop effective plans and policies that allow them to seize opportunities, solve problems and be competitive.

In [4], two directions were identified for creating an apparatus for identifying and confronting threats in the context of information and psychological security, associated with identifying risks and modeling continuous processes over time. The direction associated with identifying the risk profile implies the possibility of determining and assessing the level of threats located both in the information and psychological sphere and outside it, with the aim of developing effective ways to counter threats. The direction of modeling continuous processes in time is aimed at identifying trends or patterns, checking scenarios with varying initial conditions, etc. These directions are united by the fact that the object of the study is poorly structured, difficult to formalize systems with heterogeneous elements and poorly measured indicators. The unifying concept for these approaches can also be the concept of «Holistic security» used in the English literature, that is, an approach focused on the integration of all elements designed to protect the organization, considering them as complex and interconnected systems [4].

Considering the first area associated with identifying risks, it is worth noting that there are a number of provisions that must be approved by the highest corporate bodies (board, executive management). Namely:

– the definition of «risk appetite», which is usually corporate rules and policies for risk response strategies, which means that the corporation must define an acceptable level of risk as the level of risk that will not affect the organization’s productivity;

– responsibility for control activities and structure of risk reports;

– creation of units responsible for risk management [19].

To ensure successful protection against potential abuse, methods to control incidents and to identify possible risk assessment must be developed. The risk management plan should include the important steps shown in Figure 2.

In the context of the onset of risk, we further consider the main aspects of information security: accessibility, integrity, confidentiality. By the availability of information we mean the ability of a subject to access data upon request at any time provided by the system’s work schedule. Moreover, access to information makes sense to divide into several stages:

– the ability to send a request for certain data to the information system;

– the generation of a response to a request within a period of time not exceeding the timeout value by the system (depends on the system’s operability, as well as on its workload by processing other requests or other work);

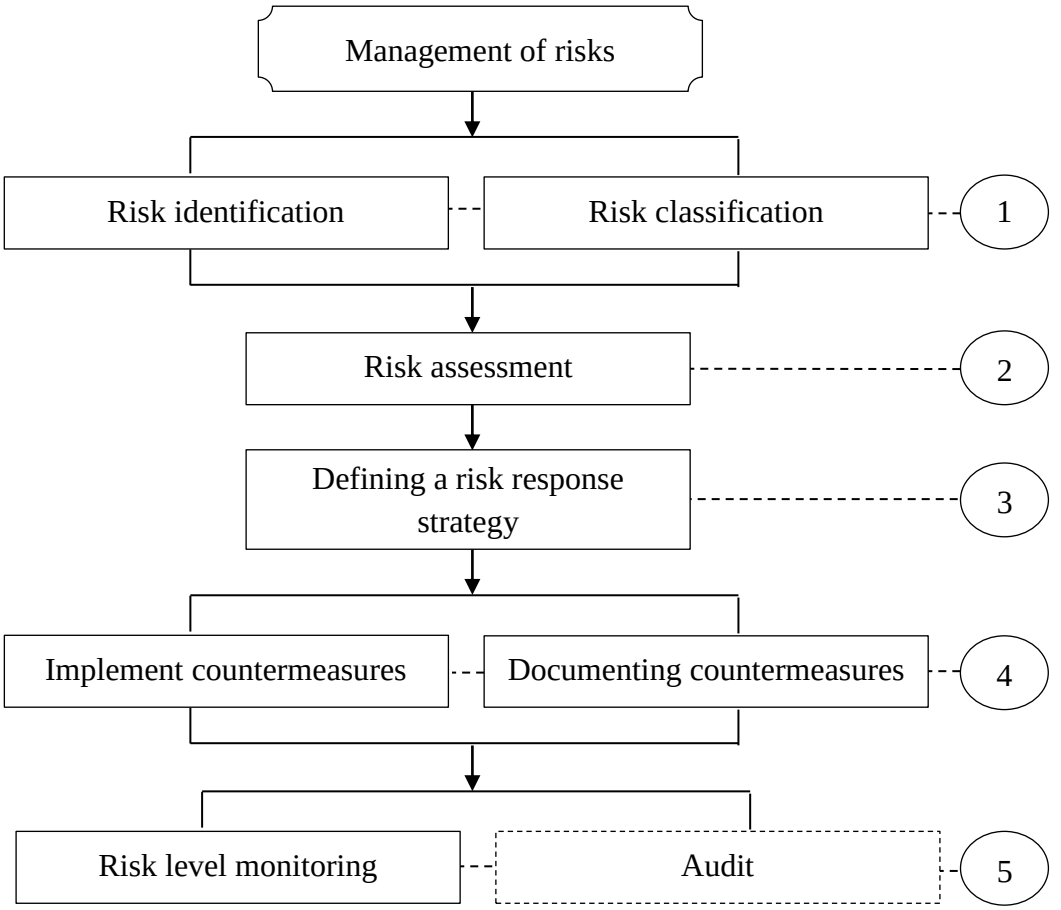

Figure 2. Risk Management Stages

– the ability to deliver the response of the information system to the subject within a time not exceeding the timeout (depends on the operability of the system interface through which it sends responses to requests, as well as on the serviceability and congestion of the communication channel between the subject and the server).

So, the ability to receive data on demand depends on the health and workload of the communication channel between the user and the interface of the information system and on the health and workload of the information system itself.

The technical reasons for the violation of the communication channel between the user and the system interface can be very different: from trivial hardware malfunctions and software failures to successful denial of service attacks.

The risk of a malfunction in the information system containing the information requested by the user depends on the reliability of the combination of hardware and software components that make up the system, as well as on the adequacy of the operator managing their work. Accessibility violations arise due to non-compliance with standards at the design, production or operation of the system.

Integrity. By integrity we mean the relevance and consistency of information, its security from destruction and unauthorized changes or deletions.

The risk of information integrity violation is provided by the following factors:

– the probability of failure of the equipment and software of the information system, since a violation of the relevance and consistency of data can occur as a result of failures in their operation;

– the degree of reasonableness of the algorithms and the reliability of authentication of users of the system who have the right to edit the data stored in it;

– the likelihood of undocumented features in the software;

– non-compliance with the requirements of the standards at the design, production or operation of the system;

– imperfection of the organizational structure of the information system. For example, the need for frequent reconfiguration of the system or its individual parts is fraught with a violation of the integrity of the data stored and processed in it, as well as additional costs;

– the human factor. For example, the likelihood of social engineering in relation to persons who have access to edit the data stored in the system. Insider threats.

Confidentiality. By confidentiality we mean the security of information from unauthorized read access.

The risk of violation of confidentiality of information is provided by the following factors:

– the degree of sophistication of the algorithms and the reliability of user authentication systems with the right to access the data stored in it;

– the likelihood of undocumented features in the software;

– non-compliance with the requirements of the standards at the design, production or operation of the system;

– imperfection of the organizational structure of information system. For example, the need for frequent reconfiguration of the system or its individual parts is fraught with a violation of the confidentiality of the data stored and processed in it, as well as additional costs;

– the human factor. For example, the likelihood of social engineering in relation to persons with access to the system. Insider threats [20].

The previously mentioned holistic security is a strategic guide to help human rights defenders maintain their well-being in action. A holistic approach integrates self-care, prosperity, digital security and information protection into traditional security management practices. In the context of information and psychological security as a lever to ensure the competitive immunity of the region, the holistic approach will take into account not only the technical side of the problem, but also the socially oriented one. The holistic cybersecurity approach takes into account human, cultural and social factors. People and processes are just as important. Information and psychological security focuses on the person. It is necessary to take into

account the aspects that attacks are intended for people, are also performed by humans, human behavior can be the key to closing security gaps [15]. From this we can conclude that people can either be the weakest link in the chain of security, or the key to enhance the overall level of cyber security at the macro-, micro- and meso level.

By taking an integrated approach to cybersecurity, it is more readily possible to prevent, mitigate and eliminate attacks. This approach includes people, processes, and technology. It considers not only technical, but also human, social, cultural and managerial factors that are relevant to the detection, prevention and correction of cybersecurity vulnerabilities.

Conclusions

Economic sabotage may well be inspired by informational provocations, psychological actions aimed at the psychological suppression of power and society, and the morale of the armed forces directly affects defense capability, reducing combat potential even with material and technical superiority. This series of obvious examples can easily be continued. Such phenomena don't have to be considered on a global scale, for example, at the corporate level. This may affect the safety of assets and, accordingly, the economic situation of the organization.

Therefore, in an era marked by intense competition, globalization and the increased importance of knowledge as a driving force in the economy, it is advisable for organizations and governments to understand the dynamic and significant role that ICTs play in ensuring information and psychological security and increasing competitiveness.

The issues of ensuring the competitive immunity of regions through the prism of information and psychological security are not considered and require further research, and in the conditions of intensified territorial competition, providing regions and cities with quality information is becoming increasingly necessary. Today, more than ever, the ability to predict market changes and adapt to them accordingly is required. One can hardly speak about the viability of the territory, its high competitive immunity without accumulating funds and resources to anticipate unexpected situations, to identify internal and external risks and make appropriate management decisions.

Regular monitoring of the territory's competitive immunity is a kind of early warning system for threats that could potentially damage the development of a region or city and reduce economic attractiveness. Monitoring of competitive immunity of the territory can play a key role in advancing competitors in certain tenders for the implementation of large projects, assessing potential risks and favorable opportunities for investments, early warning of the actions of a competitor, etc. Monitoring of competitive immunity of a territory allows you to learn not to survive when there was a need for this, and to live fully, identifying and minimizing risks in a timely manner; understand that the most viable and competitive are those territories that, along with making money, are oriented towards the multiplication of

fundamental values; have the ability not to break in unusual situations and rapidly changing conditions; have an emergency preparedness program and be able to implement it when this situation arises [21].

The current global economic crisis associated with the coronavirus pandemic has urged the possibility of maintaining competitiveness at the macro-, meso- and microeconomic levels in the country. Everything that is happening in the world will undoubtedly affect and will continue to affect people's lives. Coronavirus has a big impact on the economy, and everything that happens can lead to even more catastrophic consequences. Based on the results of the study, we can conclude that the situation in the world economy, under the influence of the «information and psychological» and dynamic effects of the coronavirus, will significantly change the approaches to gaining competitive immunity in most territories and regions of countries. More stringent competition in global markets is expected.

References:

1. Nemchuk, A. A. (2004). Globalnoe upravlenie v sovremennom mire: politologicheskiy analiz [Global governance in the modern world: political science analysis]. *Extended abstract of candidate's thesis*. (in Russian)

2. Zinoveva, E. S. (2015). Globalnoe upravlenie Internetom: Rossiyskiy podhod i mezhdunarodnaya praktika [Global Internet governance: the Russian approach and international practice]. *Vestnik Moskovskogo gosudarstvennogo instituta mezhdunarodnyih otnosheniy – Bulletin of Moscow state Institute of International Relations*, 4, 111-117. (in Russian)

3. Melnik, G. S., Nikonov, S. B. (2014). Mediynyiy komponent v doktrine informatsionnoy bezopasnosti [Media component in the doctrine of open security]. *Upravlencheskoe konsultirovanie – Management Consulting*, 1, 20. (in Russian)

4. Melnik, G. S., Misonzhnikov, B. Ya., Vinogradova, S. M. (2017). Informatsionno-psihologicheskaya i kognitivnaya bezopasnost [Information-psychological and cognitive safety]. Sankt-Peterburg. (in Russian)

5. Shishkin, V. M. (2015). Dvojstvennost sredstv obespecheniya bezopasnosti i ocenka ih konechnoj rezultativnosti [The duality of security and assessment of their ultimate effectiveness]. *Analiz, modelirovanie, upravlenie, razvitie ekonomicheskih system – Analysis, modeling, management, development of economic systems*: a collection of scientific papers IX International School-Symposium AMUR-2015. Simferopol: TNU im. V. I. Vernadskogo, 416-421. (in Russian)

6. Vazhenina, I.S., Vazhenin, S.G. (2010). Fenomen konkurentnogo immuniteta territorii [The phenomenon of competitive immunity of the territory]. *Obshestvo i ekonomika – Society and Economics*, 136-156. (in Russian)

7. Oliner, S., Sikel, D., Shtirokh, K. (2008). Explaining the productive decade. Materials of the US Federal Reserve Conference. Washington. (in English)

8. Sergunin, A. A. (2007). Nacionalnaya i mezhdunarodnaya bezopasnost: novye podhody i koncepty [National and international security: new approaches and concepts]. Problemy bezopasnosti i voenno-silovoj politiki v mezhdunarodnyh otnosheniyah – *Problems of security and military-power policy in international relations*. SPb.: SPbGU. (in Russian)

9. Maksimova, S. G., Goncharova, N. P., Noyanzina, O. E. (2012). Osobennosti vospriyatiya riska v strukture ocenki lichnoj i socialnoj bezopasnosti [Features of risk perception in assessing personal and social security]. News of Altai State. (in Russian)

10. Mahanko, G. V. (2015). Ekonomicheskaya bezopasnost i konkurentosposobnost regiona kak vazhnejshaya sostavlyayushaya ekonomicheskoj bezopasnosti Rossii

[Economic security and competitiveness of the region as the most important component of the economic security of Russia], 1-16. (in Russian)

11. The World Economic Forum «The Global Risks Report 2020». *www3.weforum.org.* Retrieved from: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (in English)

12. X-Force Threat Intelligence Index Produced by IBM X-Force Incident Response and Intelligence Services (IRIS) 2020. *www.kommersant.ru.* Retrieved from: https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf (in English)

13. X-Force Threat Intelligence Index Produced by IBM X-Force Incident Response and Intelligence Services (IRIS) 2019. *www.securindex.com.* Retrieved from: https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf (in English)

14. X-Force Threat Intelligence Index Produced by IBM X-Force Incident Response and Intelligence Services (IRIS) 2018. *ru.scribd.com.* Retrieved from: https://ru.scribd.com/document/384939824/IBM-Security-X-Force-Threat-Intelligence-Index-2018 (in English)

15. Delta Munoz (2018). A Holistic Approach to Cybersecurity: Because Technology Is Not Enough. *ascensiongt.com*. Retrieved from: https://ascensiongt.com/2018/01/21/ holistic-cybersecurity (in English)

16. Doktrina informacijnoyi bezpeki Ukrayini (2017). [The Doctrine of Information Security of Ukraine]. *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/ show/47/2017 (in Ukrainian)

17. Bejnar, I. A. (2008). Principialnye osnovy ekonomicheskogo obespecheniya informacionnoj bezopasnosti regiona [Fundamentals of economic support of information security of the region]. *Region: sistemy, ekonomika, upravlenie – Region: systems, economics, management,* 1, 29-33. (in Russian)

18. Vazhenin, S. G. Vazhenina, I. S. (2012). Identefikaciya i ocenka territorialnoj konkurencii [Identification and assessment of territorial competition]. *Ekonomika regiona – Regional Economy*, 1, 29-40. (in Russian)

19. Spremić, M. (2012). Corporate IT Risk Management model: A holistic view at managing information system security risks. Proceedings of the ITI 2012 34th International Conference on Information Technology Interfaces, Cavtat, 299-304. (in English)

20. Mazov, N. A., Revnivyh, A. V., Fedotov, A. M. (2011). Klassifikaciya riskov informacionnoj bezopasnosti [Classification of information security risks]. *Informacionnye tehnologii – Information Technology*, 9, 80-89. (in Russian)

21. Vazhenina, I.S., Vazhenin, S.G. (2013). Metodicheskie orientiry monitoringa konkurentnogo immuniteta territorii[Methodological guidelines for monitoring the competitive immunity of the territory]. *Ekonomicheskij analiz: teoriya i praktika – Economic analysis: theory and practice*, 35, 23-31. (in Russian)