ЕКОНОМІКА ТА УПРАВЛІННЯ ПІДПРИЄМСТВАМИ (ЕКОНОМІКА ЗВ'ЯЗКУ)

УДК 330.131.7

FEATURES AND CONSEQUENCES OF MANIFESTATION OF INFORMATION RISKS AT THE GLOBAL LEVEL IN MODERN CONDITIONS

Granaturov V. M., Korablinova I.A.

O.S. Popov Odessa National Academy of Telecommunications,
1 Kuznechna St., 65029, Ukraine, Odesa.
vmgrant39@gmail.com, korablinova.irin@gmail.com

ОСОБЛИВОСТІ ТА НАСЛІДКИ ПРОЯВУ ІНФОРМАЦІЙНИХ РИЗИКІВ НА ГЛОБАЛЬНОМУ РІВНІ У СУЧАСНИХ УМОВАХ

Гранатуров В.М., Кораблінова І.А.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
vmgrant39@gmail.com, korablinova.irin@gmail.com

ОСОБЕННОСТИ И ПОСЛЕДСТВИЯ ПРОЯВЛЕНИЯ ИНФОРМАЦИОННЫХ РИСКОВ НА ГЛОБАЛЬНОМ УРОВНЕ В СОВРЕМЕННЫХ УСЛОВИЯХ

Гранатуров В.М., Кораблинова И.А.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
vmgrant39@gmail.com, korablinova.irin@gmail.com

Abstract. The article is devoted to the risk analysis associated with the use of information and information technologies. Activation and deployment of "digital transformation programs" are accompanied by the emergence of new or unfamiliar challenges and threats; they have a significant negative impact on all aspects of society and are called as "information risks". It has been shown that any modern entity with social and economic relations provides a wide range of information risks. The purpose of the research is to identify and substantiate the existing problems of qualitative analysis of the emergence and consequences of global information risks, as well as to develop recommendations for their solution. The analysis of different views according to the problems of global risks has been given. The analysis gives an opportunity to offer a separate group of "global information risks" from a part of global risks. It is shown that this can be determined by: causes and peculiarities of their occurrence and emergence; specific activities in order to reduce the likelihood of their occurrence; exclusion, or mitigation of negative effects of their occurrence; specific requirements for the category, staff and competency of managers who should deal with global information risk management. Recommendations have been offered in order to supplement the existing global risks with a separate group – global information risks and to the list of risks such as "massive fraud and data theft", "large-scale cyber attacks", "destruction of critical information infrastructure and networks". It is necessary to add "global content risks", "risk of privacy loss (for state and private sectors)", as well as "risk of confidence loss in the media (sources of information)". Features of these risks emergence have been considered.

Key words: information, analysis, security, cybersecurity, global information risks, content risks.

Анотація. Статтю присвячено аналізу ризиків, які пов'язані з використанням інформації та інформаційних технологій. Активізація та розгортання програм з «цифрової трансформації» супроводжуються появою нових, дотепер незнайомих викликів та загроз, які чинять суттєвий

негативний вплив на усі сторони життя суспільства, та отримали назву «інформаційні ризики». Показано, що діяльність будь-якого сучасного суб'єкта соціально-економічних відносин передбачає наявність широкого кола інформаційних ризиків. Метою дослідження є визначення та обґрунтування існуючих проблем якісного аналізу особливостей прояву та наслідків інформаційного ризику на глобальному рівні, а також розробка пропозицій щодо їх вирішення. Надано аналіз різних точок зору на проблеми глобальних ризиків, що виникають. Виконаний аналіз дає підставу надати пропозицію щодо доцільності та обґрунтованості виділення у складі глобальних ризиків окремої групи «глобальні інформаційні ризики». Показано, що це визначається: причинами та особливостями їх виникнення та прояву; специфічністю заходів щодо зменшення ймовірності їх наступу, виключення, або пом'якшення негативних наслідків їх наступу; специфічними вимогами до категорії, складу та компетенції менеджерів, які повинні займатися питаннями управління глобальними інформаційними ризиками. Надано пропозиції щодо доповнення існуючого складу глобальних ризиків окремою групою – глобальні інформаційні ризики, до складу якої поряд із ризиками «масових випадків шахрайства та крадіжки даних», «широкомасштабних кібератак» та «руйнування критичної інформаційної інфраструктури та мереж», слід додати «глобальні контентні ризики», «ризик втрати конфіденційності (для державного та приватного секторів)», а також «ризик втрати довіри до ЗМІ (джерел інформації)». Розглянуто особливості прояву кожного з цих ризиків.

Ключові слова: інформація, аналіз, захист, кібербезпека, глобальні інформаційні ризики, контентні ризики.

Аннотация. Статья посвящена анализу рисков, связанных с использованием информации и информационных технологий. Активизация и развертывания программ по «цифровой трансформации» сопровождаются появлением новых, до сих пор неизвестных вызовов и угроз, которые оказывают существенное негативное влияние на все стороны жизни общества, и получили название «информационные риски». Показано, что деятельность любого современного субъекта социально-экономических отношений предполагает наличие широкого круга информационных рисков. Целью исследования является определение и обоснование существующих проблем анализа особенностей проявления и последствий информационного риска на глобальном уровне, а также разработка предложений по их решению. Приведен анализ различных точек зрения на проблемы глобальных рисков, которые возникают. Выполненный анализ дает основание выдвинуть предложение о целесообразности и обоснованности выделения в составе глобальных рисков отдельной группы «глобальные информационные риски». Показано, что это определяется: причинами и особенностями их возникновения и проявления; специфичностью мероприятий по уменьшению вероятности их наступления, исключения или смягчения негативных последствий их наступления; специфическими требованиями к категории, составу и компетенции менеджеров, которые должны заниматься вопросами управления глобальными информационными рисками. Даны предложения по дополнению существующего состава глобальных рисков отдельной группой – глобальные информационные риски, в состав которой наряду с рисками «массовых случаев мошенничества и кражи данных», «широкомасштабных кибератак» и «разрушения критической информационной инфраструктуры и сетей», следует добавить «глобальные контентные риски», «риск потери конфиденциальности (для государственного и частного секторов)», а также «риск утраты доверия к СМИ (источников информации)». Рассмотрены особенности проявления каждого из этих рисков.

Ключевые слова: информация, анализ, защита, кибербезопасность, глобальные информационные риски, контентные риски.

A problem statement. Social and economic transformations are taking place in society because of the rapid development and introduction of the latest technologies, particularly information and communication technologies, characterized by the emergence of fundamentally new solutions and unprecedented opportunities in all spheres of human livelihood. One form of global transformation processes emergence, which increases dependence of modern society development on information, is the activation and deployment of programs from "digital transformation" that have spread in the business world in the last few years and involve digital technologies in all sectors of the economy.

At the same time these transformations are being accompanied by the emergence of new and unfamiliar challenges and threats that have a significant negative impact on the world

economy, politics, as well as on society and an individual. Among the urgent problems in the process of the implementation of these programs, which have to be solved, is a widespread impact on almost all spheres of social livelihood risks which are connected with the use of information and information technologies. Therefore, the term "information risks" is increasingly used in the scientific and business communities. The spread and impact of these risks are constantly increasing.

In recent years the urgency of the problem has led to the emergence and growth of scientific works with various aspects of the study of information risks. The analysis shows that only certain issues of this problem have been considered in the literature and have created a certain mosaic. They cannot be considered as a theory that allows structuring existing research and using them effectively in practice. This state is determined by the scale and complexity of the problem, its novelty, as well as the constant emergence of new or unknown sources of this risk.

It is known that information risks appear at different levels of society, the state, the economy as a whole, separate regions, corporations, enterprises, organizations, projects, as well as at the level of an individual. In our opinion, a generalized theory of information risk should be based on the study and generalization of the features of these risks emergence at each level.

This determines the relevance of the research according to the analysis of characteristics and implications of information risks at the global level.

Analysis of recent research and publications. Historically, at first, the problem of information risk began to be considered relative to its emergence at the enterprise level. At the same time, diversity of production, distribution, exchange, consumption of information and use of information technologies led to the fact that in most cases representatives of different activities considered the problem based on the characteristics and capabilities of their activities. Thus, the condition of the problem was characterized by absence of scientists' and practitioners' consensus concerning the majority of current problems of the information risks theory: definition of the concept "information risk"; determination of its composition, relationship with other risks of the object, a place in the system of their classification and so on.

Detailed analysis of the information risk problem of the enterprise has been considered in the works [1, 2], where the existing disadvantages have been defined and proved, as well as recommendations have been provided that may certainly address some of these shortcomings.

However, observations show that today attention has shifted to the emergence of this risk at the global level that affects all aspects of society in one way or another. At the same time, the globality of this risk should be considered as both a territorial coverage and the depth and weight of its emergence.

The problem of global risks arose at the end of the twentieth century as a response to challenges faced by the society as a result of systemic transformations of social and economic relations that occurred as a result of globalization, as well as rapid development and introduction of the latest technologies. The significant impact of these risks on all aspects of society determined the relevance of the problem. As a result, a significant number of publications appeared where the authors tried to present their views of global risks, as well as possible ways for their solutions [3 - 13]. Particularly it is necessary to focus public attention on global risk problems at the World Economic Forum (WEF). For the first time this problem was provided to the general public in 1995 after the President's work publication of the WEF, Klaus Schwab, where ten key problems in the modern changing world were cited [14]. As life shows, most of these problems remain relevant even today. It is considered in the work that the author published 20 years later [15]. Since 2006, the results of WEF specialists' research according to the analysis of global risks that threaten humanity, have been published in the WEF annual reports (The Global Risks Report), the latest one is in [16].

However, the study of publications about the global risk analysis shows that today there is a set of issues that should be discussed in order to achieve a consensus about these issues. One of them is to define the place, role, and significance of information risks, as well as consequences of their occurrence on a global scale. Among promising directions of the research of the problem there is consideration of the information risk's nature from fundamental positions of social and behavioral sciences, as well as in the applied aspect there is development of strategies and programs regarding prevention, or reduction of negative consequences of the information risks occurrence.

Problem definition. The purpose of this research is to identify and substantiate the existing problems of qualitative analysis of emergence and consequences of information risk at the global level, as well as to develop recommendations for their solution.

Presentation of the main material of the research. Today, in the whole world there is a growing interest to information as to "a factor of production", "a factor of economic growth", "a factor of social development", "a factor of influence on behavior of economic entities", "a factor of ensuring the viability of modern organizations", and so on.

More information is accumulating and processing the data using modern information and communication technologies, and their number and speed of updating is constantly increasing. So, according to Internet World Stats, at the end of 2019 – the beginning of 2020 the number of Internet users in the world was 4,574,150,134, and the entire population of the planet was 7,796,615,710 people [17]. The Internet Live Stats database [18], which can be seen in a dynamic format at the appropriate time, indicates the continuous growth in the number of new Internet users, the number of sites, blogs, sent e-mails and the variety of users' actions on the Internet that generate numerous data streams. According to IDC [19], in 2025 the total volume of data will have increased to 163 zetabytes (for comparison, in 2016 there were about 16 zetabytes, in 2018 – 33 zetabytes). By the end of 2020 the volume of data will have increased to 40 zetabytes.

In turn, increasing the amount of data, which modern organizations are working with, determines the acceleration of cloud computing development and deployment. Due to their help and influence of the programs activation of "digital transformation", 95% of corporations are running their business using these technologies today. The more activity depends on data management technologies in cyberspace, the greater problem of data security, which has a number of threats in economic, social and other aspects both to individuals and organizations and to society as a whole.

It is known when specific tasks are solved, intelligently processed data become as information for decision-making. But complex tasks and the accelerated pace for updating the external environment in the digital age require the interactive interaction of many participants from different parts of the world, that reinforces the tendency for hyper-connection, both at the technical and social levels, as well as increasing and mixing of information flows among themselves.

It becomes apparent that the activity of any modern entity with social and economic relations engenders a wide range of information risks.

The idea of the information risk nature and its possible forms of emergence are shown in Fig. 1. Each of the presented types of losses in different spheres of human activity can be specified both from the viewpoint of a certain analysis level of socio-economic relations research (for example, at mini-, micro-, meso-, macro-, mega-levels), and of each particular entity, its individual directions of work, during a certain project, in a certain period of time, and so on.

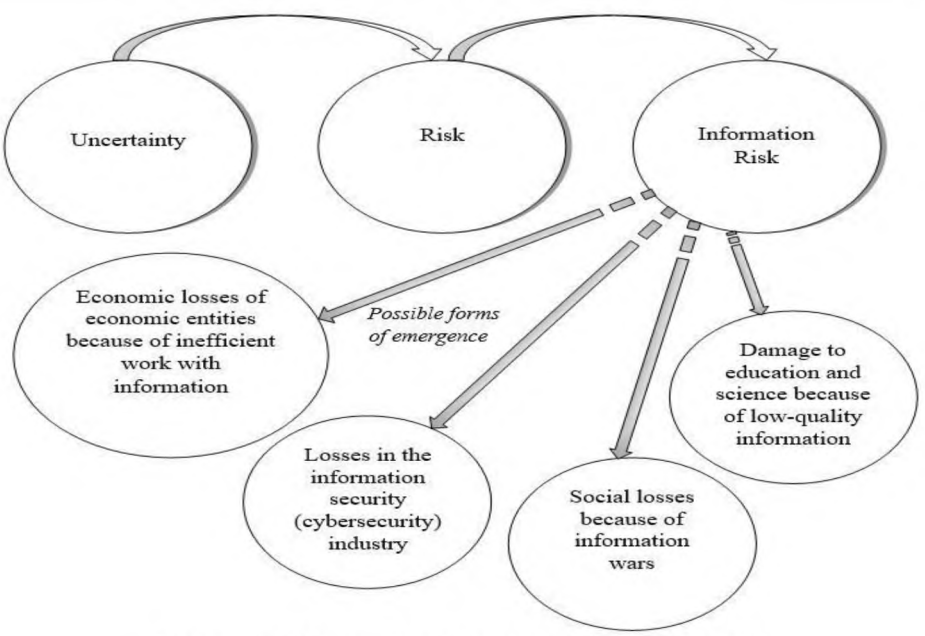

Figure 1 – Nature and forms of information risk

Since the object of our research is to analyze the emergence of information risks at the global level, it is necessary to note that information risks with this name are not directly present in the annual WEF reports. At the same time, it should be noted that as a result of the growing impact of information and information technology risks in recent years, some components of information risks have emerged in a group of global risks.

So, according to the WEF Reports, in 2014, among the 5 top risks, in terms of probability, that a global risk appeared and was labeled as "large-scale cyber-attacks". In the reports of 2018 and 2019, two risks were identified to the top 5 of global risks, related to the use of information and information technologies – "Massive incident of data fraud/theft" and "large-scale cyber-attacks", as well as they were included in the global technological risk group [16].

It should be noted that as a result of expected catastrophic consequences for the environment and human security, associated with climate changes, for the first time in all these years all the 5 top risks were included to the group of environmental risks in the WEF Report in 2020.

However, in the WEF Report in 2020, such risks as "massive cases of data fraud and theft" and "large-scale cyber-attacks" are ranked sixth and seventh in the top risks, outpacing geopolitical, economic, and social global risks. In addition, a risk called "Breakdown of critical information infrastructure and networks" (Critical information infrastructure breakdown) took the sixth place including possible consequences.

Despite a slight decrease in the ranking of presented risks among global risks, more than 75% of specialists who participated in the preparation for the Report noted that the risks of cyber attacks and data loss in 2020 will increase in comparison with 2019. Almost 70% of them spoke about increased risks of confidentiality loss (for the state and private sectors), as well as a confidence loss in the media (sources of information).

The emergence of these risks in recent years in the group of the top global risks has been caused by the existing and possible consequences with their occurrence.

Data theft and use for financial enrichment have become common in recent years. As it is noted in [20], in 2017 hackers stole 172 billion dollars from 978 million users in 20 countries. In 2018, losses from hacker attacks amounted to more than 3 trillion dollars. According to Cybersecurity Ventures cyber-attacks occurred every 14 seconds around the world in 2019 [20].

The risks of data fraud and theft are largely related to the risks of widespread cyber-attacks. So, according to [21], in the fourth quarter of 2018, almost 48% of cyber-attacks were in order to obtain data, most of them were for further selling of the received information. The second group of perpetrators of data theft incidents includes persons who, as a result of their authority, had access to the data (present or former employees, consultants, counterparties, and so on).

An example is the cyber-attack on the American bank Capital One and it happened on July 30, 2019. Experts believe that this computer hack is one of the largest in history [22]. Criminals gained access to 100 million applications for credit cards, 140,000 social security numbers and 77,000 bank accounts.

However, consequences of cyber-attacks are not limited to data theft. In the most severe cases, their aim is to damage critical infrastructure – transport, electricity, banking, industrial and other vital sectors. According to experts' forecasts [23], losses from cyber-attacks will have exceeded 6 trillion dollars by 2021. Moreover, experts estimate that a complete Internet disconnection will reduce daily GDP for 1.9% in countries with high levels of connectivity and for 0.4% in countries with low levels of connectivity [24].

It should also be noted that, in addition to economic losses, results of cyber-attacks can cause devastating physical consequences that threaten the environment and even human life. It is no coincidence that today it is thought that cyber-attacks are more dangerous than nuclear weapons [25].

Studying the Allianz Risk Barometer [26], it is also possible to see the anxiety of business communities because of increasing cyber incidents in recent years. At the same time, according to the survey of business representatives in 2019, the problem of cyber incidents was considered at the threat level of economic activities termination (Figure 2). Today cyber incidents (39% of responses) ranks as the most important business risk globally in the report Allianz Risk Barometer 2020 (Fig. 3).

Taking into account the severe losses of society as a result of the presented risks, the international community is taking measures to reduce their occurrence, as well as to mitigate dangerous consequences of this attack to some extent.

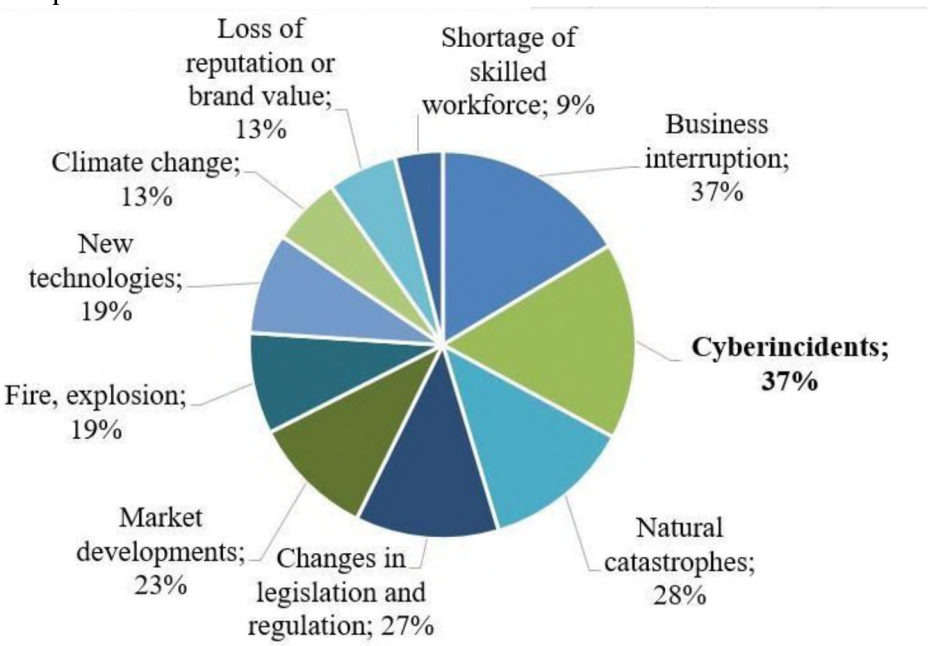

Figure 2 – Distribution of answers of business representatives in order to determine the main dangers in 2019*

*It was built according to the report of Allianz Risk Barometer [26]

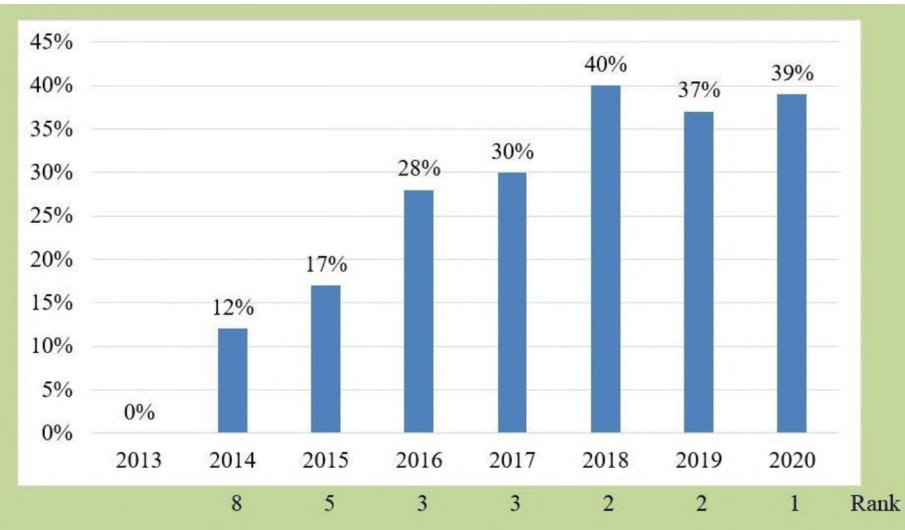

Figure 3 – Dynamics of distribution of respondents' answers about the importance of cyber incidents for their business

*It was built according to the reports of Allianz Risk Barometer (2013 – 2020)

So, Directive 95/46/EC was adopted in 1995 [27]. It included legislative measures for the personal data protection. However, development of information technologies, digital development of society and catastrophic increase in data theft caused the necessity to revise the requirements for personal data protection. Therefore, new EU requirements for personal data protection – General Data Protection Regulation (GDPR) – have been introduced since May 2018 [28].

The first EU legislation for cybersecurity, Network and Information Security Directive (2016/1148/EC Directive), appeared much later than the measures for personal data protection [29]. Its purpose is to improve the security of networks and information systems by introducing activities at the national level and enhancing cooperation in the EU for risk management.

However, as it was noted in [16], international and national policies on these issues do not keep pace with technological progress. At the same time, there is a tendency to increase efforts combination of criminal organizations in order to confront these measures [30]. As a consequence, today the probability of their detection and prosecution, even in the United States, is estimated at 0,05% [3].

The legislation provided the personal data protection and networks and information systems security mainly due to organizational and technical measures. It was consistent with the concept that these risks were included in technological risks among the group of global risks.

We stated our opinion in [32] about the validity of these risks location in the global risk system, directly in a group of the global technological risk. However, the problem of studying the nature and emergence of risks associated with the use of information and information technologies is not limited with the list and location of some of them in the current set of global risks. In our opinion, today there are other significant risks in this area that have not been discussed by the scientific community yet, as well as there is a list of other issues which have to be further addressed.

It is necessary to answer the first question in the process of studying these risks about the definition and justification of sources of their occurrence. It should be noted that all of them include the known sources of any risks – spontaneity of natural processes and phenomena, natural disasters; accidents; existence of conflicting tendencies, conflicts of conflicting interests; scientific and technological progress and so on [33]. However, the number of these sources and importance of their emergence differ significantly at each level.

Analysis of the information risks sources at the global level indicates that, in most cases, they are related to conflicting trends and conflicting interests. As a result, they have criminal and

legal roots. In turn, it determines the peculiarities of social measures in order to prevent or reduce the negative consequences of these risks.

Since the main and almost single source of information risks at the global level is the existence of conflicting trends, conflicts of conflicting interests, it raises doubts about the validity of their relation to global technological risks.

The specific sources, emergence, and implications of information risks at the global level create an opportunity to recommend a separate "global information risk" group for a part of global risks. In our opinion, the content of this group is not limited to the risks of "massive data fraud and theft" and "large-scale cyber-attacks", as well as "destruction of critical information infrastructure and networks".

One significant threat that has a negative impact on almost all countries and society as a whole is the false information dissemination in separate countries, as well as information dissemination with aggressive relations towards them. Because of consequences of untrue (false, or deliberately distorted) so-called fake information there are wars (such as the beginning of war in Iraq because of developing chemical weapons of mass destruction), stock exchange panics, global economic crises, and so on. Another threat is the information dissemination that attacks public danger and morality, as well as incitement of national, racial, and religious enmity.

Information wars appeared because of this risk emergence, which may manipulate (use and manage) information in order to create a negative impact in society on the image of the object, damaging it and acquiring a competitive advantage over it. There are information war consequences, such as forms of confrontation between entities (states, blocs, parties and so on); undermining the international authority of a contender, his cooperation with other countries; losses among vital political, economic, defense and other interests; creating political tension and chaos, and in the worst cases, civil violence, or wars between countries.

When it comes to any undesirable information content of certain countries, or regions, realization of corresponding threats leads to so-called "global content risks". An example of content risks emergence is the accusation of the United States about interference in their presidential election by the Russian Federation, because of information distribution that negatively affected the image of the Democratic Party of the United States and, according to its representatives, influenced the elections results.

Subsequently, there was a significant deterioration in inter-state relations between the United States and the Russian Federation, which to some extent affects the state of the world security, as well as adopting (strengthening) the USA sanctions against the Russian Federation, which involve the interests of many countries of the world and affect the world economy.

It should be noted that the information influence on the object, which involves information wars, is happening because of the media. In order to increase the efficiency of this influence, it is necessary to use computer networks, in a complex with cyber-attacks and so on. Therefore, sometimes information wars are identified with cyber wars (wars for dominance in cyberspace), or with network wars (wars using network technologies). However, in our opinion, the global content risk should be treated separately from those mentioned above, according to the measures which can help to mitigate its impact.

In addition to this, the important social impact of content risk was given in [16], while open cyberspace has made it possible to democratize certain processes and increase access to information and data, in addition it provides growing opportunities for spreading lies (accidentally and intentionally) that have led to a gradual erosion of confidence in the media, social networks and even in governments.

One of the current emergence of global content risk as a form of global information risk should be considered the damage caused during the so-called infodemia – "the term that has begun to be widely used to denote the fake flow of information, pseudo-scientific news and false advice regarding to COVID-19" [34]. Therefore, today there are initiatives against disinformation all over the world. Among them there is an initiative of researchers from the

University in Washington, "who study how social media can spread untrue and half-true information, as well as false advice about COVID-19, and how users of social networks should orient in the information space during infodemia" [34].

However, despite the importance of countering the content risk emergence, unlike other components of global risk, there is no effective legislation agreed by the international community in order to reduce the emergence and dissemination of fake information.

The relevant legislation, in one form or another, was adopted in Malaysia, Singapore, France, Germany, Russia and others [35]. However, in most cases it has significant shortcomings, reduces its effective application, and is criticized by the opposition and human rights defenders as an attempt to use this legislation to protect authorities, as well as it suppresses freedom of speech and fight with opposition.

An example of an approach according to the international community's fight against false information can be noted by the European Commission as so-called a "soft" plan "Overcoming online disinformation: the European approach" [36].According to the authors of this plan, the problem solution relies almost entirely on online resources – "self-regulation is the most suitable way for online platforms in order to take measures very quickly regarding the solution of the problem". According to the voluntary rules, agreed with the largest Internet companies (Google, Facebook, and Twitter), the latter ones have a commitment to use political advertising, penalize distributors because of advertising fake information on the Internet, develop and implement means to prevent the use of robots which spread fake news and so on. The main idea of this plan is to create a forum in which representatives of Internet platforms, advertisers, mass media and civil society should participate in order to create a certain code of the fight against disinformation or the certain standards permissible in the network, which should operate within the European Union. Such a position, to some extent, prevents the European Commission from possibly being accused by the community of increasing censorship. However, in our view, it is impossible to solve the problem effectively without the active participation of Governments and EU leadership in the Internet regulation, establishment of independent organizations for this purpose.

As with other components of global information risk, protection against content risk involves the mainly technological measures that Internet operators have to perform – detect and eliminate fake information, prevent the use of robots spreading such information.

In our opinion, both for content risk and for other components of global information risk, organizational, managerial, and socio-psychological methods of influence should be used more widely to eliminate or reduce the negative consequences of their occurrence.

Conclusions. The analysis shows the necessity to supplement the existing group of global risks with a separate group – global information risks and to the list of risks such as "massive fraud and data theft", "large-scale cyber attacks", "destruction of critical information infrastructure and networks", it is necessary to add "global content risks", "risk of privacy loss (for state and private sectors)", as well as "risk of confidence loss in the media (sources of information)".

The separation of global information risk as a separate group among global risks is determined by: causes and characteristics of their occurrence and emergence; specificity of the activities for reducing likelihood of their occurrence, exclusion, or reduction of negative effects of their occurrence; specific requirements for the category, staff and competence of managers who should deal with global information risk management. It will contribute to the development of a well-founded, coherent public strategy in order to respond challenges and threats for preventing the occurrence and consequences of risky events.

The specific emergence of these risks with their criminal and legal roots, has to be developed and implemented to manage these risks. For this purpose, a number of social, psychological and educational tools should be provided with technological measures.

One of the issues, that also should be studied and solved, is an in-depth analysis of nature of information risks and their manifestations and consequences at different levels – mini-, micro-, meso-, macro-, mega-levels (at the level of certain enterprises, relations and interaction of economic entities; at the level of industry, region, state, international economy, etc.). Understanding the nature of information risks, as well as their emergence at different levels, will allow managers of structural elements from different levels to respond adequately to their emergences and consequences.

REFERENCES:

1. Granaturov V.M., Korablinova I.A. Informatsiinyi ryzyk pidpryiemstva: shchodo vyrishennja problemy qui pro quo u vyznachenni ponjattja /Innovatsijna ekonomika, 2017, № 5-6 (69), p. 199-206. [in Ukrainian].

2. Granaturov V.M., Korablinova I.A. Suchasnyi etap «tsyfrovoi transformatsii» kompanii: mozhlyvosti, zagrozy ta problemy adaptatsii do novykh umov / Avtorske svidotstvo № 81566 vid 20.09.2018. [in Ukrainian].

3. Beck U. Risk Society: Towards a New Modernity. London: Sage Publications Ltd, 1992. – 298 p.

4. Luhmann N. Die Wirtschaft der Gesellschaft. – Frankfurt/M., 1988. – 269 p.

5. Schwebler Robert. Individualversicherung in Wirtschaft und Gesellschaft // Versicherungswirtschaft. – 1990. – № 1. – P. 12.

6. Heilmann Wolf-Rudiger. Risk management der privaten Haushalte // Versicherungswirtschaft. – 1992. – № 7. – 397 p.

7. Managing International Risk. Essays Commissioned in Honor of the Centenary of the Wharton School, Edited by Herring R.J., University of Pennsylvania. Cambridge University Press, 1986. – 273 p.

8. Hertwig J., Maus S. Global Risks: Constructing World Order through Law, Politics and Economics. Peter Lang, 2010. – 258 p.

9. Lustig H., Roussanov N., Verdelhan A. (2014). Countercyclical currency risk premia. Journal of Financial Economics. 2014. Vol. 111, 527 – 553 pp.

10. Krzakiewicz Kaziemierz. Ryzyko w zarzadzaniu przedsiebiorstwem. – Poznan: TNOiK, 1990.

11. Bekhman G. Sovremennoe obshhestvo: obshhestvo riska, informacionnoe obshhestvo, obshhestvo znanij. Per. c nem. A.YU. Antonovskogo, G.V. Goroxovoj, D.V. Efimenko i dr. – M.: Logos, 2010. – 248 p. [in Russian].

12. Globalnye riski XXI veka: predely regulirovanij [pod red. N.P. Shmelyova i dr. – M.: In-t Evropy RAN, 2013. – 142 p. [in Russian].

13. Ivanov O.B. Globalnye riski i tendencii sovremennogo mira. – ETAP: ekonomicheskaj teorij, analiz, praktika, 2017. – P. 7-20. [in Russian].

14. Schwab Klaus. Overcoming Indifference: 10 Key Challenges in Today's Changing World – NYU press, 1995. – 396 p.

15. Shwab K. Chetvyortaj promyshlennaj revolyucij. – «Eksmo», 2016. – (Top Business Awards). – 138 p. [in Russian].

16. The Global Risks Report 2020. – URL: https://www.weforum.org/reports/the-global-risks-report-2020.

17. World Internet Users and 2019 Population Stats. – URL: https://www.internetworldstats.com/stats.htm.

18. Internet Live Stats. – URL: https://www.internetlivestats.com/.

19. V mire proayalizirovano menee 1% vsej informacii, zashhishheno menee 20%: rezultaty ezhegodnogo issledovanij IDC. – URL: http://bit.samag.ru/uart/more/23.

20. Poteri organizacij ot kiberprestupnosti. – URL: http://www.tadviser.ru/index.php/.

21.Kiberataki. – URL: http://zdrav.expert/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8.

22. Na amerikanskij bank sovershili moshhnuyu kiberataku. – URL: https://delo.ua/business/na-amerikanskij-bank-sovershili-moschnuju-kibera-356170/

23. Walker, I. 2019. “Cybercriminals Have Your Business in Their Crosshairs and Your Employees Are in Cahoots with Them”. Forbes. 31 January 2019. URL: https://www.forbes.com/sites/ivywalker/2019/01/31/cybercrimi-nals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#683a874a1953

24. Deloitte. 2016. The Economic Impact of Disruptions to Internet Connectivity. A Report for Facebook. Deloitte. URL: https://www2.deloitte.com/content/ dam/Deloitte/global/Documents/Technology-Media-Telecommunica-tions/economic-impact-disruptions-to-inter-net-connectivity-deloitte.pdf.

25. Kiberataki strashnee, chem yadernoe oruzhie: kak mirovye SMI otreagirovali na virus Petya. – URL: https://tass.ru/mezhdunarodnaya-panorama/4374732.

26. Allianz Risk Barometer 2019. – URL: https://www.agcs.allianz.com/content/ dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf.

27. Direktiva 95/46/IES Yevropeiskogo Parlamenty i Rady «Pro zakhist fizichnikh osib pri obrobci personalnix danix i pro vilne peremishhennya takix danix. – URL: https://zakon.rada.gov.ua/ laws/show/994_242. [in Ukrainian].

28. General Data Protection Regulation (GDPR) – Final text neatly arranged. – URL: https://gdpr-info.eu/.

29. The Directive on security of network and information systems (NIS Directive). – URL: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

30.Keesem, L. "The Business of Organized Cybercrime: Rising Intergang Collaboration in 2018". SecurityIntelligence. 20 March 2019. – URL: https://securityintelligence.com/the-business-of-organized-cybercrime-ris-ing-intergang-collaboration-in-2018/

31. Eoyang, M., A. Peters, I. Mehta and B. Gaskew. To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors. Third Way. 29 October 2018. – URL: https://www.thirdway.org/report/to-catch-a-hacker-to-ward-a-comprehensive-strategy-to-identi-fy-pursue-and-punish-malicious-cyber-actors.

32.Danchenko A. I., Granaturov V.M., Vorobiyenko P.P. On the risks of a new technological structure – «INDUSTRY 4.0». Innovaciina ekonomika. – 2017. – № 9-10 (71). – P.22 – 27.

33. Granaturov V.M. Ekonomicheskii risk: sushhnost, metody izmereniya, puti snizheniya: uchebnoe posobie. – 4-e izd., pererab. i dop. – M.: Delo i servis, 2016. – 288 s. [in Russian].

34. Borotba z dezinformatsieyu pid chas epidemii COVID-19. – URL: https://csdrs.ukma.edu.ua/index.php/uk/17-holovni-novyny/177-borotba-z-dezinformatsieyu-pid-chas-epidemiji-covid-19. [in Ukrainian].

35. Trepalina YU. Zakony protiv feikovikh novostei stanovyatsya mirovim trendom. – URL: https://nag.ru/articles/article/103823/zakonyi-protiv-feykovyih-novostey-stanovyatsya-mirovyim-trendom.html. [in Russian].

36. Evrokomissiya budet boronsya s nepravdivimi novostyami. – URL: http://mignews.com/news/politic/ 270418_114326_25099.html.

ЛІТЕРАТУРА:

1. Гранатуров В.М., Кораблінова І.А. Інформаційний ризик підприємства: щодо вирішення проблеми qui pro quo у визначенні поняття / Інноваційна економіка, 2017, № 5-6 (69), с. 199 – 206.

2. Гранатуров В.М., Кораблінова І.А. Сучасний етап «цифрової трансформації» компаній: можливості, загрози та проблеми адаптації до нових умов / Авторське свідоцтво № 81566 від 20.09.2018.

3. Beck U. Risk Society: Towards a New Modernity. London: Sage Publications Ltd, 1992. – 298 p.

4. Luhmann N. Die Wirtschaft der Gesellschaft. – Frankfurt/M., 1988. – 269 p.

5. Schwebler Robert. Individualversicherung in Wirtschaft und Gesellschaft // Versicherungswirtschaft. – 1990. – № 1. – P.12.

6. Heilmann Wolf-Rudiger. Risk management der privaten Haushalte // Versicherungswirtschaft. 1992. – № 7. – 397 p.

7. Managing International Risk. Essays Commissioned in Honor of the Centenary of the Wharton School, Edited by Herring R.J., University of Pennsylvania. Cambridge University Press, 1986. – 273 p.

8. Hertwig J., Maus S. Global Risks: Constructing World Order through Law, Politics and Economics. Peter Lang, 2010. – 258 p.

9. Lustig H., Roussanov N., Verdelhan A. Countercyclical currency risk premia. Journal of Financial Economics. 2014, Vol. 111, 527 – 553 pp.

10. Krzakiewicz Kaziemierz. Ryzyko w zarzadzaniu przedsiebiorstwem. – Poznan: TNOiK, 1990.

11. Бехманн Г. Современное общество: общество риска, информационное общество, общество знаний. / Г. Бехманн; пер. с нем. А.Ю. Антоновского, Г.В. Гороховой, Д.В. Ефременко та ін. – М.: Логос, 2010. – 248 с.

12. Глобальные риски XXI века: пределы регулирования / [под ред. Н.П. Шмелёва и др.] . – М.: Ин-т Европы РАН, 2013. – 142 с.

Granaturov V. M., Korablinova I.A.

Features and consequences of manifestation of information risks at the global level in modern conditions

13. Иванов О.Б. Глобальные риски и тенденции современного мира // ЭТАП: экономическая теория, анализ, практика, 2017. – С. 7 – 20.
14. Schwab Klaus. Overcoming Indifference: 10 Key Challenges in Today's Changing World – NYU press, 1995. – 396 p.
15. Шваб К. Четвертая промышленная революция. – «Эксмо», 2016. – (Top Business Awards). – 138 с.
16. The Global Risks Report 2020. – URL: https://www.weforum.org/reports/the-global-risks-report-2020.
17. World Internet Users and 2019 Population Stats. – URL: https://www.internetworldstats.com/stats.htm.
18. Internet Live Stats. – URL: https://www.internetlivestats.com/.
19. В мире проанализировано менее 1% всей информации, защищено менее 20%: результаты 6-го ежегодного исследования IDC. – URL: http://bit.samag.ru/uart/more/23.
20. Потери организаций от киберпреступности. – URL: http://www.tadviser.ru/index.php/
21. Кибератаки. – URL: http://zdrav.expert/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8.
22. На американский банк совершили мощную кибератаку. – URL: https://delo.ua/business/na amerikanskij-bank-sovershili-moschnuju-kibera-356170/
23. Walker, I. 2019. “Cybercriminals Have Your Business in Their Crosshairs and Your Employees Are in Cahoots with Them”. Forbes. 31 January 2019. – URL: https://www.forbes.com/sites/ivywalker/2019/01/31/cybercrimi-nals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/#683a874a1953
24. Deloitte. 2016. The Economic Impact of Disruptions to Internet Connectivity. A Report for Facebook. Deloitte. – URL: https://www2.deloitte.com/content/ dam/Deloitte/global/Documents/Technology-Media-Telecommunica-tions/economic-impact-disruptions-to-inter-net-connectivity-deloitte.pdf
25. Кибератаки страшнее, чем ядерное оружие: как мировые СМИ отреагировали на вирус Petya. – URL: https://tass.ru/mezhdunarodnaya-panorama/4374732.
26. Allianz Risk Barometer 2019. – URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf.
27. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних". – URL: https://zakon.rada.gov.ua/ laws/show/994_242.
28. General Data Protection Regulation (GDPR) – Final text neatly arranged. – URL: https://gdpr-info.eu/.
29. The Directive on security of network and information systems (NIS Directive). – URL: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
30. Keesem, L. “The Business of Organized Cybercrime: Rising Intergang Collaboration in 2018”. SecurityIntelligence. 20 March 2019. – URL: https://securityintelligence.com/the-business-of-organized-cybercrime-ris-ing-intergang-collaboration-in-2018/
31. Eoyang, M., A. Peters, I. Mehta and B. Gaskew. To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors. Third Way. 29 October 2018. – URL: https://www.thirdway.org/report/to-catch-a-hacker-to-ward-a-comprehensive-strategy-to-identi-fy-pursue-and-punish-malicious-cyber-actors.
32. Danchenko A. I., Granaturov V.M., Vorobiyenko P.P. On the risks of a new technological structure – «INDUSTRY 4.0». Інноваційна економіка. – 2017. – № 9-10 (71). – С.22 – 27.
33. Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: учебное пособие. – 4-е изд., перераб. и доп. – М.: Дело и сервис, 2016. – 288 с.
34. Боротьба з дезінформацією під час епідемії COVID-19. – URL: https://csdrs.ukma.edu.ua/index.php/uk/17-holovni-novyny/177-borotba-z-dezinformatsieyu-pid-chas-epidemiji-covid-19.
35. Трепалина Ю. Законы против фейковых новостей становятся мировым трендом. – URL: https://nag.ru/articles/article/103823/zakonyi-protiv-feykovyih-novostey-stanovyatsya-mirovyim-trendom.html.
36. Еврокомиссия будет бороться с неправдивыми новостями. – URL: http://mignews.com/news/politic/ 270418_114326_25099.html.
DOI 10.33243/2518-7139-2020-1-1-108-119