DOI: 10.5281/zenodo.2570060
UDC Classification: 368:330.131.7:004
JEL Classification: D81, G22, G32, M15, N20

CYBER INSURANCE AS A TOOL TO MINIMIZE INFORMATION RISKS OF ENTERPRISES IN THE CONTEXT OF GLOBAL ECONOMIC DEVELOPMENT AND INFORMATIZATION OF SOCIETY

КІБЕРСТРАХУВАННЯ ЯК ІНСТРУМЕНТ МІНІМІЗАЦІЇ ІНФОРМАЦІЙНИХ РИЗИКІВ ПІДПРИЄМСТВ В УМОВАХ ГЛОБАЛЬНОГО ЕКОНОМІЧНОГО РОЗВИТКУ ТА ІНФОРМАТИЗАЦІЇ СУСПІЛЬСТВА

Marina A. Demyanchuk, PhD in Economics, Associate Professor
Odessa Mechnikov National University, Odessa, Ukraine
Scopus Author ID: 56607296900
ORCID: 0000-0002-3907-3464
Email: ma-demyanchuk@ukr.net

Natalia D. Maslii, PhD in Economics, Associate Professor
Odessa Mechnikov National University, Odessa, Ukraine
Scopus Author ID: 57201065209
ORCID: 0000-0002-3472-5646
Email: masliy.natalia@gmail.com

Valentyna V. Stankova
Odessa Mechnikov National University, Odessa, Ukraine
ORCID: 0000-0003-0358-2651
Email: vstankova95@gmail.com
Recieved 06.10.2018

Дем'янчук М.А., Маслій Н.Д., Станкова В.В. Кіберстрахування як інструмент мінімізації інформаційних ризиків підприємств в умовах глобального економічного розвитку та інформатизації суспільства. Оглядова стаття.

Основним ресурсом сучасних підприємств є інформація, порушення основних властивостей якої може стати серйозною небезпекою для підприємств в умовах інформатизації суспільства та зростаючого числа загроз (кіберзлочинність). Наслідками кіберзлочинності є втрата корпоративних даних, інтелектуальної власності, даних клієнтів тощо. Тому питання забезпечення захисту інформаційних ризиків та кібербезпеки підприємств від несанкціонованого доступу до внутрішньої інформації компанії є надзвичайно важливими, вирішенню яких сприятимуть продукти страхового ринку, а саме кіберстрахування.

Ключові слова: глобалізація, інформаційне суспільство, інформаційні ризики, підприємство, кіберризики, кібербезпека, кіберстрахування

Demyanchuk M.A., Maslii M.D., Stankova V.V. Cyber-insurance as a tool for minimizing the informational risks of the enterprise in the conditions of global economic development and society informatization. Review article.

The main resource of modern enterprises is information, the breach of the basic properties of which could become a significant danger for these enterprises in the conditions of society informatization and the increasing number of threats (cybercrime). The cybercrime consequences are the loss of corporate and customers' data, the loss of intellectual properties etc. Therefore, ensuring the informational risks protection and enterprise`s cybersecurity from unauthorized access to company's internal information are extremely important issues, the solution of which will be contributed by the products of the insurance market, namely, of the cyber-insurance market.

Keywords: globalization, informational society, informational risks, enterprise, cyber-risks, cyber-security, cyber-insurance

One of the most noticeable phenomena of our time, which increasingly attract the attention of researchers, is society globalization and informatization. Under these conditions international trade is increasing, the capital movements' scale and its pace, information exchanges etc. are also growing. All this is happening around the clock in real time on the world financial markets due to modern technologies and the Internet, which would allow overcoming the distance, borders and time for the assets, ideas and scientific innovations exchange. The main resource of modern enterprises is information, which as well as material resources has quality and quantity, has cost and price. Violations of the basic properties of information can be a serious danger to the enterprises in the circumstances of the growing number of threats and vulnerabilities from both external and internal enterprises` environment. These threats include cybercrime, which is reveals itself in the form of hacker attacks (cyberattacks), which greatly affects the loss of corporate data, intellectual property or customer data, or the loss of all aforesaid. These threats consequences range from regulatory fines and penalties and reputational losses to total business loss. Therefore ensuring the protection of enterprises` informational risks and cybersecurity from unauthorized access to company`s internal information are extremely important issues, the solution of which will be contributed to the insurance market products.

Analysis of recent researches and publications

Nowadays, scientific or practical works in which the problems inherent to cyber-insurance were systematically studied published in small amounts. However, there are domestic and foreign authors which discussed certain aspects of the insurance industry, of the impact of information and communication technologies on the economy, of definitions of cyber-risks and cyber-insurance. Some of them are considered below.

A significant contribution to the study of the insurance market and its trends have made such domestic researchers as V.D. Bazilevich, N.M. Vnukov, S.S. Osadets, G. Picus, And N.V. Pricasyuk, studying the existing examples of new systems on the Ukrainian market and studying foreign examples of similar systems in order to compare them.

In the scientific works of P. P. Vorobienko and V. M. Granaturov, E. Iscan (Iscan, 2012), R. Katz (Katz, 2012), D. Souter (Souter, 2005) and his co-authors, R. Heeks (Heeks, 2010), R. Entner (Entner, 2005) and D. Lewin (Lewin, 2005) the impact of informational and communicational technologies on the economy and the country's economic growth and the problems of using patterns of this influence were revealed.

The analysis of threats and possibilities of insurance protection against cybercrime has been carried out in foreign countries during the last 10-15 years. Works of foreign authors like Y.V. Borodakiy, A.Y. Dobrodeev and I.V. Butusov, S.V. Brenner (Brenner, 2012) and M.D. Goodman (Goodman, 2012) are aimed at risk analysis and insurance protection from cyber threats. Such domestic authors as V.P. Prokhorenko, O.V. Sergienkov, A. Ustenko in their works consider the issues of cybercrime, legal and technical protection against cyber threats.

S. Patel (Patel, 2015) identifies in his works such risks of modern enterprise development as virtual risk, risk of business disruption, macro environmental risks, reputation risk and talent risk. He also provides examples and methods of reducing any of them, also notes that the insurance companies should be actively involved in the insurance of such risks.

Cyber-insurance is one of the tools to counter cyber-risks. The problems of formation and prospects of cyber-insurance market development, innovation in the insurance industry were studied in scientific works of many domestic and foreign researchers. According to V.P. Bratiuk [1], cyber-insurance in Ukraine should become a new kind of insurance against criminal cyber-risks and threats of interference in the activities of automated systems, as the country stays in the process of informatization, and actively implements new information technologies in all spheres of public practice.

To promote the role of cyber-insurance in reducing cyber-risks and in the improvement of cyber-persistence S. Wang (Wang, 2017) [2] suggests to transfer risks from insurance companies as well as to soften the requirements of the insurance supervision authorities of cyber-insurance products, to develop a mutually beneficial partnership between insurance companies and information technology security firms in the direction of providing integrated services to reduce the risk of insurance protection, which is based on the income distribution agreements in the areas of providing consulting services on the risk insurance, investigation of cases and consideration of claims, compensation of losses.

J. Kesan (Kesan, 2017) and K. Hayes (Hayes, 2017) [3] focus on the difficulties associated with determining the amount of financial consequences of data loss that are unpredictable, making the risk difficult for insurance. Insurers have a lack of comprehensive actuarial data that informs about other types of damage, covered by insurance. Some insurance companies respond to this uncertainty by charging a higher premium, creating exceptions and limiting coverage, but these approaches may limit the market for cyber-insurance.

Establishing the interdependence of the models of cyber-risk and cyber-insurance from the models of financial risk, I. Malhotra (Malhotra, 2015) [4] proposes to consider their components in the following aspects: – cyber-risk and cyberattacks are economic games that affect the economic value of a particular object on this unit of the analysis, such as a nation, firm or individual; – the interaction of cyber and the financial sphere should be based on trust; – the economic costs of the onset of cyber-crises and cyberattacks should receive a financial (economic) assessment.

S. Shackelford (Shackelford, 2012) [5] indicates the need of using cyber-insurance as an element of an active strategy to mitigate the risk associated with cyber threats not only for their own competitive well-being, but also to provide critical national infrastructure. According to his works, cyber-insurance could help to quantify the risk and help to protect companies from cyberattacks. At the same time, insurance companies should look for the most vulnerable to cyberattacks companies, for example, telecommunications, high-tech companies, and the media and offer them loss compensation, an individual approach to the conclusion of insurance transactions.

Unsolved aspects of the problem

Taking into account the existing theoretical approaches to the formation of the cyber-insurance market in domestic and foreign practice and legally uncertain essence of the basic concepts of its structure necessitate researches on the analysis of cybercrime, systematization of cyber-security and justification of the feasibility of cyber-insurance development in Ukraine.

The aim of the article is to study cyber-insurance as a tool to minimize information risks of the enterprises in the conditions of global economic development and society informatization.

The main part

One of the main types of economic crime is illegal activity in the global cyberspace, second only to the

misappropriation of assets. Cybercrime accounts for 38% of economic crime in the financial services sector. Cybercrime knows no geographical or national boundaries [6].

According to the European Commission [7], more than 1 million people worldwide are attacked by cybercriminals every day. According to the analytical center of the Zecurion company [8], in the year of 2011, 819 cases of data leakage were registered in the world, the total damage from which amounted to $ 20 billion. These researches indicate that cases of the disclosure of information about customers from online stores have become more frequent. The threats associated with information risk, as dangerous as the threat of physical assets of the company.

With such a variety and complexity of attacks in the business world, where everything is interconnected and has become global, cumulative cyber-risks are a major issue nowadays.

Data leakage incidents tend to trigger a chain reaction and cause significant reputational and financial damage. Thus, information protection becomes a priority for companies, especially in connection with the current trend of development of the regulatory framework in the direction of strengthening the responsibility of companies for confidentiality and data protection [6].

The global trend towards the growth of cybercrime has not spared the CIS countries. Thus, in the last few years, the number of cyberattacks on Ukrainian organizations has increased significantly. The purpose of hackers are not only state institutions and enterprises, but also the private sector, hitting on which attackers expect to undermine the financial system of the country or get a monetary benefit. Thus, an example of such an incident was the attack on the Ukrainian Bank through the SWIFT system [9], as a result of which the Bank lost $ 10 million. In addition, in its report about information security in 2016, Cisco [10] reports that more than half of the surveyed Ukrainian companies were subjected to cyberattacks.

By the number of incidents related to data leakage in 2017-2018, medical institutions (17.4%), public authorities (15.2%) and organizations in the trade industry (12.2%) are leading. By the number of compromised records – it companies (33.9%), trade enterprises (20.2%) and government agencies (15.8%). The number of cases of leakage of payment information has increased dramatically - 26.8% of the total. The most popular payment data leakage scenarios are cloud storage leaks (45.3%) and email leaks (44.1%). In 2017, 600 million crimes were committed in the world, the damage from their business amounted to $ 400 billion. Seven out of every ten attacks of cybercriminals are carried out on commercial organizations.

The issue of cybersecurity is global, therefore, of particular interest to this issue is the international telecommunication Union, whose Recommendations given the following definition [11]: cybersecurity is the collection of tools, policies, security guidelines, security safeguards, guidelines, risk management approaches, actions, training, practical experience, insurance, and technology that can be used to protect cyber-environment, organization and user resources.

Specialized state organizations fight against cybercrime, uniting in this fight with other organizations and even entire States. The study showed that first place in the Global Cybersecurity Index (GCI) (tab. 1) ranked Singapore, then the United States, Malaysia and Oman. Among the countries of Europe are leading Estonia, France and Norway. Last place was occupied by Equatorial Guinea. Concerning the CIS countries in the GIC of 2017: Georgia – 8th place (0.819), Russia – 10th place (0.788), Belarus – 39th place (0.592), Azerbaijan – 48th place (0.559), Ukraine – 58th place (0.501). It should be noted that all countries of the world are divided into three groups: presenter, admission and initiation. Ukraine according to the GIC rating refers to states where the cybersecurity sector is in the process of being added [11].

Table 1. The top 10 countries in the ranking of GCI (normalized score)

Country	GCI rating	Juridical	Technical	Organizational	Capacity-building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States of America	0.91	1.00	0.96	0.92	1.00	0.73
Malaysia	0.89	0.87	0.96	0.77	1.00	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1.00	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Source: compiled by the authors on the materials [11]

As the GIC shows, there is a gap in cybersecurity preparedness around the world between all regions of the world. Cybersecurity obligations are often shared among countries that work well in some circles and less well in others. Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation must be harmonious in order to be most effective. In addition, cybersecurity is not

just a concern of every government, but also requires the commitment of the private sector and consumers [11]. Thus, it is important to develop a culture of cybersecurity where citizens are aware of the trade-off between risk and monitoring when using electronic networks.

The most problematic for Ukraine are the following indicators: lack of industry centers of cybersecurity; standards of cybersecurity organizations and professional standards in the industry; Internet security of children; practical implementation of activities in this area; mechanisms to stimulate the industry [12].

Given the growing number and seriousness of cybercrime, the risk management of organizations is forced to enter into its list of another danger to business and the state, which previously did not pay attention: hacker attacks, which have become a reality today. It is necessary to work with these risks and look for ways to optimize them.

IT and cyber-risks mean any risk that leads to financial loss, destruction or deterioration of the reputation of the Bank as a result of the failure of it systems, information security systems. This risk can materialize in the following ways [13]:

— deliberate and unauthorized breach of security to gain access to information systems for the purpose of espionage, extortion or damage to reputation;
— unintentional or accidental security breach, which, however, can still lead to certain material and non-material losses;
— operating IT-risks due to low system integrity, or other factors.

Cyber risks have their own characteristics, certain types of events and possible losses (tab. 2 and tab. 3) and unlike traditional risks can catch up with business anywhere in the world and in almost every business process.

Table 2. Types of events and characteristics of cyber risks

Event type		Event characteristics
1. Non-targeted attacks	Fishing (farming, click ford etc.)	type of internet fraud, the purpose of which is to gain access to confidential user data-logins and passwords.
	carding	a type of fraud, in which an operation using a bank card, which is not innovative or confirmed by its holder, or its details.
	SMS-fraud	a type of fraud in which the bank's client receives an SMS messages and/or a call from an unknown number in order to obtain confidential information on the payment card.
2. Targeted attacks	Financial fraud	criminological phenomenon, which is a criminal activity and is expressed in a system of criminal and legal acts, which are committed by deception or abuse of trust in the process of formation, distribution and use of funds for material gain.
	Data bases robbery	it is characterized by illegal trafficking in another's data set, organized according to the concept, which describes the characteristics of these data and the relationship between their elements, in their own selfish interests or for selfish interests of another person.
	Industrial	a kind of economic espionage, which is characterized by a narrowing of the scale of the tasks of obtaining information of interest from the state-to the scale of one or more firms-competitors
	DDoS attacks	an attack on a computer system with the intention of making computer resources inaccessible to users for whom the computer system was intended
	Cyber-extortion (crypto-lockers)	a virus attack that involves the use of malicious software (malware), the files in which are encrypted and makes them unusable, until the ransom is paid
3. Attacks from the inside	Intentional damage and information robbery	unauthorized copying of information, failure of its infrastructure, loss of portable devices, sending "wrong" data, distribution of conference information via social networks, provision of low-quality outsourcing services (cloud services, data centers, call centers)
	Information destroying	the sequence of operations designed for software or hardware to permanently delete data, including residual information
	Targeted attack assistant	support for attacks of "custom" nature, specifically aimed at one site or a group of them, United by one feature (sites of one company, belong to a certain field of activity, or combined by a number of features)

Source: compiled by the authors on the materials [14-22]

Table 3. Features and potential losses from cyber-risks

Cyber-risks features	Possible losses from cyber-risks
1. Specificity of risks and losses. 2. Information asymmetry and interdependence of security (possible information secrecy information on the part of the policyholder). 3. Specific properties of response plans in the case of cyber-risks. 4. Most events are caused by deliberate actions – the prospect of subrogation. 5. The evolution of information systems and cyberattacks, which can lead to a change in the nature of cyber-risks. 6. Involvement of professional consultants at the stage of policy conclusion and loss settlement. 7. The availability of statistical data and the complexity of damage assessment. 8. Difficulty in determining coverage, exclusions, limitations, liability and time for claims.	1. Direct losses (theft of funds, loss of information, software damage, equipment failure, etc.). 2. Losses from business interruption. 3. Liability to third parties (for damage, disclosure of information). 4. Damage resulting from industrial espionage and theft of intellectual property. 5. Loss or damage to the company's reputation. 6. Additional costs (anti-crisis PR, legal services, etc.).

Source: compiled by the authors on the materials [14-22]

There are three main areas to minimize or eliminate cyber-risks: security technology solutions, educational work in the sphere of counteraction and prevention of crimes, as well as cyber-insurance.

The concept of cyber insurance today is quite new and little studied. In recent years, this tool has become widespread in the international market. And now it offers more than 60 insurance companies around the world. At this stage the Ukrainian insurance market is significantly lagging behind its Western counterparts in the matter of development and implementation of product cyber-insurance. In recent years, the tool of cyber-insurance has widespreaded in the international market. And now it offers more than 60 insurance companies around the world, unlike the Ukrainian market [13].

The main objective of cyber-insurance is protection against large-scale cyber-attacks. This type of insurance provides a financial mechanism for recovery from large losses, helping enterprises to return to normal operation, maintain stability, solvency and reduce losses as a result of a break in production [23].

Cyber-insurance gained its popularity in developed countries due to the understanding that by implementing the latest solutions in the field of cybersecurity and carrying out constant work with the staff, there is always the 1% risk of compromising the system, which is impossible to predict and evaluate. Cyber-insurance is characterized by a wide range of coatings and, above all, protects the company from financial losses.

Until now, there are no standards in the world fixed by the legislation on the issue of insurance of cyber-risks, however, among the positive indicators of the cybersecurity industry of Ukraine, analysts of the International telecommunication Union [11] noted the legislative base (tab. 4), professional education, state regulation of cybersecurity issues, interdepartmental and international cooperation in the field, the level of public-private partnership.

Table 4. The main regulatory and legal acts that regulate the issues of cybersecurity in Ukraine

Name of regulatory act / date of adoption	Issues that are regulated by the following legislatives
Directive 2002/58 / EU of the European Parliament and the Council "About the privacy and electronic communications" / 12.07.2002	The Directive harmonizes the provisions of states-member necessary to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the right of privacy, with respect to the processing of personal data during the electronic communications sector and to ensure the free movement of such data and equipment for electronic communications and Community services.
Convention about cyber-force / 23.11.2001	The Convention establishes measures to be implemented on the national level and in international cooperation on offences
The Law of Ukraine "About basic principles of cybersecurity of Ukraine" / 05.10.2017	The law defines the legal and organizational basis for ensuring the protection of vital interests of a person or a citizen, society and the state, national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, the powers of state organizations, enterprises, institutions, individuals and citizens in this area, the basic principles of coordination of their activities to ensure cybersecurity.
The Decree of the President of Ukraine Cybersecurity Strategy of Ukraine / 15.03.2016	The aim of the Strategy is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state.
The Law of Ukraine "About information" / 02.10.1992	The law regulates relations on creation, collection, receipt, storage, use, distribution and protection of information.
The Law of Ukraine "About information protection in informational and telecommunication systems" / 05.07.1994	The law regulates relations in the field of information security in information and telecommunication and informational systems
The Law of Ukraine "About copyright and related rights" / 23.12.1993	The law protects the personal non-property rights and property rights of authors and their successors, associated with the creation and use of works of science, literature and art – copyrights, and the rights of performers, producers of phonograms and videos and broadcasting organizations - related rights.
The Law of Ukraine "About distribution of copies of audio-visual works, phonograms, videos, computer programs, databases" / 23.03.2000	The law defines the legal basis for the distribution of copies of audio-visual works, phonograms, videos, computer programs, databases and is aimed at protecting the interests of copyrights, related rights and consumer rights

Source: compiled by the authors on the materials [24-31].

At this stage the Ukrainian insurance market is significantly lagging behind its Western counterparts in the matter of development and implementation of product cyber-insurance [12]. It should be noted that international stockbrokers (brokers and insurance companies) represented in Ukraine, having a ready working policy of protection against cyber-risks, are in no hurry to offer it to Ukrainian business, on the following grounds: 1) against the background of the General economic stagnation, shareholders don`t notice the prospects and volume of the market that could interest them; 2) shareholders consider the Ukrainian portfolio too high-risky.

June 27, 2017 entered the history as a day that showed how vulnerable the country's economy to cyberattacks is. According to the police the attack affected more than 2,000 companies, among large companies in the private sector, the virus affected LLC "Nova Poshta", a chain of DIY stores "Epicenter", industrial-construction group "Kovalska", the major Ukrainian mobile operators: PJSC "Kyivstar", PrJSC "Vodafone" and "Lifecell" and

others.

In July, 2018 employees of the security service of Ukraine (SSU) has fought off a hacker attack on the network equipment LLC "Aulska cloroperelivna stanciya", which is the critical infrastructure of the country.

As found by the employees of the security services, within a few minutes of system control of technological processes and devices for detecting signs of emergency situations of the enterprises were affected by the malware VPN Filter [1]. This cyberattack could potentially lead to disruption of technological processes and a possible accident. The idea of the hackers was to block the sustainable operation of the overflow station, which provides liquid chlorine water and sewage enterprises throughout Ukraine.

After massive hacker attacks on Ukrainian business and the public sector over the past year, domestic entrepreneurs began to think about how to protect themselves from such risks. For the domestic insurance market, this phenomenon is far from mass and in the world volumes (the world market of cyber-insurance is estimated at $ 3-3.5 billion) is still very far away. Ukrainian insurers certify that there is a demand for such a product in the domestic market, noting that, first of all, it may be of interest to companies that have serious databases.

Cyber-insurance is one of the fastest growing areas in the insurance market. Losses from cybercrime are growing every year. According to experts, the damage from cybercrime in 2019 will exceed 2 trillion dollars, but expenses on cyber-insurance are equal to $ 7.5 billion. Therefore, the market of cyber insurance will enter a large scale until 2020, as experts in the field of IT and cybersecurity are convinced. If in 2015 the market of cyber-defense is $ 75 billion, by 2020 it should have grown to $ 175 billion.

The main trends in cybersecurity in 2018, presented in the framework of Cyber Security Forum [19], are:

1. the emergence of new viruses and the expansion of the Arsenal of cybercriminals through the use of new technologies. Cybercriminals are more likely to attack legitimate software developers than the ultimate target. Large companies with multi-layer cybersecurity are at risk. In such cases, it is much easier to use an intermediary, which can be a manufacturer of popular programs that are used in the corporate segment. Criminals continue to spread the virus-coders. A lot of attacks with their participation focused on the industrial system. Another attractive target for hackers is personal data. They are characterized as "new oil". At the same time, big data will be used in the attacks themselves – for a more targeted appeal to the user. It also increases the complexity of malware detection and removal through the use of DNS, encryption, disembodied, and other technologies;
2. infrastructure cyber threats-attacks on software interfaces, mass hacking of routers and modems, hacking of ATMs and POS-terminals, creation of a centralized network management system, as well as attacks on cloud services;
3. attacks on cryptocurrencies. For these purposes, cybercriminals actively use botnet networks for mining, as well as carry out attacks on exchanges and users;
4. changes in legislation. The priority task of the companies, taking into account the innovations in the legislation, is to increase the cost of cybersecurity;
5. the social aspect. It means the development of the idea of insurance against cyber threats. Companies are beginning to see cyber threats as a key commercial risk. Financial institutions and technology companies should be the first to introduce cyber risk insurance. There has been an increase in the manipulation and hacking of media and social media for the sake of profit from retail fluctuations provoked by information fakes. At the same time, Internet users remain a "weak link" and one of the main tools of cybercriminals. Most viruses enter corporate networks via e-mail and employees open files and links.

So, taking into account the conducted researches the authors define the organizational model of cyber insurance process (fig. 1), which includes the main structural elements of the insurance process with the definition of the features of cyber insurance, the subjects of insurance relations, the purpose and subject of insurance, risk insurance, insurance event and event, damage and insurance payment.

The policyholders of this insurance product can be entities of different spheres of economic activity – from private to public. These are the entities that deal with personal data and are intended to protect the data from the consequences of their leakage or illegal use.

At the underwriting stage, it is necessary to introduce such a tool to determine the risk faced by the analyzed company as pen testing. This tool is very important and necessary in order to have a real understanding of the dangers to which the studied company is exposed, there are certain tools that need to be understood and evaluated. Otherwise, you can't underestimate the security breaches that could endanger the company. So, thanks to pen testing or penetration tests, it is possible to accurately identify such security holes.

According to some foreign insurance companies [18] the agreement with cyber-insurance can compensate:

1. Direct loss – interruption of activities, the cost of data recovery, loss of income as a result of the failure of it networks or web sites.
2. Damage caused to third parties-responsibility for the safety of data, claim costs in connection with the responsibility for hacking the database of confidential information.
3. Additional expenses – expenses for legal support, covering the amount of fines and penalties in connection with violations of confidential information.
4. Additional services related to the settlement of the consequences of the incident (customer notification, forensic examination, expert support).

Also, the insurance indemnity may include expenses for [18]:

— the examination for determining the severity and scope of the breach; the stories of individuals affected by the breach;
— the work of the specialist call-center for the settlement of requests from affected individuals;
— the work of a PR-company to provide professional advice.

It is important that production interruption and loss of profit as a result of the mentioned incidents fall under the coverage of company. In addition, insurance companies offer such additional terms and conditions: reimbursement of cyber-investigation costs, anti-crisis PR to restore the reputation, the costs of defense and IT systems.

Insurance coverage may include the following types [21]:

1. losses associated with data breach-liability for breach of personal data, corporate information (trade secrets, professional information, budgets, customer lists, etc.), computer system security (virus infection, destruction, modification or deletion of information, physical theft or loss of hardware, etc.);

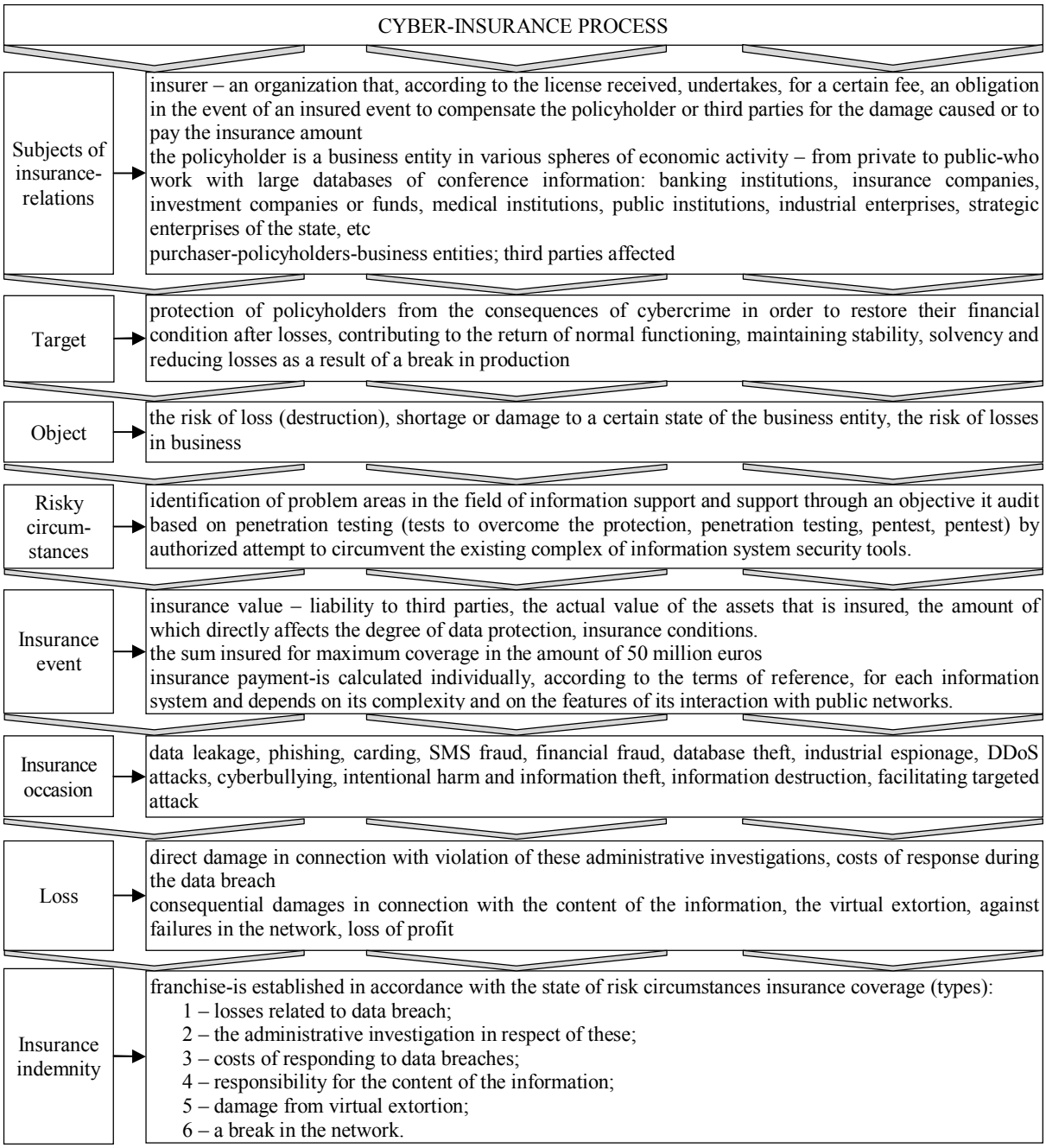

Fig. 1. Organizational cyber-insurance process sample
Source: own elaboration

2. administrative investigation of data-administrative investigation of data - losses of the policyholder in connection with the investigation as a result of violation of legislation or other legal acts in

connection with the processing of data or corporate information for which the policyholder is liable in an amount not exceeding the cost of protection;

3. costs of response in case of data breach - costs of response and preventive software and technical expertise, restoration of the reputation of the policyholder and individuals, messages of data subjects, monitoring, recovery of electronic data and programs;
4. liability for the content of information-losses of the policyholder as a result of public disclosure caused by an error, false statement, misleading statement or omission in connection with their activities in the field of multimedia, which lead to violation of copyright, ownership, slogan, trademark, trade name, domain name violation, plagiarism, violation of publishing rights or misappropriation or theft of ideas; any misrepresentation, public disclosure of facts of private life made without intent, as a result of a recorded, spoken or broadcast statement, including, but not limited to, emotional distress or mental pain in connection with such acts; or invasion, invasion of privacy, unlawful invasion or deprivation of property, Commission of an offense or unauthorized seizure of information;
5. losses from virtual extortion-money paid by the policyholder with the written consent of the insurer to limit or terminate the security threat that may otherwise cause damage to the policyholder; and the cost of the investigation to determine the cause of the security threat. At the same time, losses from virtual extortion do not include any payments to persons responsible for security risks.
6. interruption of the network-losses from failures in the network in the amount of lost profits (income that had to be received, reduced by the amount of expenses that had to be carried out).

In order to protect personal data from theft, hackers, human errors and many other decisions of the insurance company, it is necessary to provide clients with access to the services of companies specializing in cybersecurity and cybercrime investigation, legal advice and anti-crisis PR. It is a tool to prevent losses and overcome the consequences of data leakage. It provides professional, round-the-clock financial assistance to employees, customers and their families who have been affected by identity theft.

Conclusions

Taking into account the conducted researches it is established that in modern conditions of development it is necessary to develop measures aimed at protection of information, telecommunication and information-telecommunication systems of enterprises of different spheres of economic activity and corresponding resources from cyberattacks and cyber threats. One of the important factors in the development of the country's economic potential, the main spheres of its economic activity and their enterprises is cybersecurity: if the state makes some progress in the field of cybersecurity, it is a sign of a favorable investment climate for attracting external donor financial assets, which in turn contributes to the more effective development of both enterprises and the country's economy as a whole.

Regarding to the management of cyber-risks in Ukraine most enterprises could be ahead of the curve. Market participants should interact, despite the organizational, sectorial, and even national borders, to identify cyber-risks firewall risks, to create risk maps and test them, increasing the sustainability of enterprises and improving risk management.

That is why the authors propose an organizational model of the process of cyber insurance, which allows minimizing the consequences of the crisis caused by data leakage. In order to provide a more complete package of services to domestic insurance companies, it is necessary to provide clients with access to the services of companies specializing in cybersecurity and investigation of cybercrime, legal advice and anti-crisis PR. It is also advisable for insurance companies to create expert staffs of specialists with many years of experience in the field of cybersecurity and information technology, to build a partner ecosystem with industry leaders, which will identify potential cyber threats to the client, objectively assess risks and offer solutions understandable to the market.

Thus, cyber insurance is a special type of insurance of liability and property of policyholders, which are economic entities of different spheres of economic activity, which work with large databases of conference information, which allows minimizing the consequences of the crisis caused by data leakage.

Abstract

The main resource of modern enterprises is information, the violation of the basic properties of which can become a serious danger for enterprises in the conditions of the growing number of threats and vulnerabilities during the Informatization of society. Such threats include cybercrime, which affects the loss of corporate data, intellectual property or customer data. In addition, the consequences of such threats include regulatory penalties and loss of reputation to the complete loss of business. Cybersecurity is one of the important factors in the development of the economic potential of the country, the main areas of its economic activities and their enterprises, so the issues of ensuring the protection of information risks and cybersecurity of enterprises from unauthorized access to internal information of the company is very important, the decision of which will contribute to the products of the insurance market, namely. Taking into account the existing theoretical approaches to the formation of the virtual insurance market in domestic and foreign practice and the legally uncertain nature of the basic concepts of its structure, it is necessary to conduct research with the analysis of cybercrime, systematization of cyber-risks and the rationale for the development of cyber-insurance in Ukraine.

The aim of this work is to study cyber-insurance as a tool of minimizing informational risks of enterprises in the context of global economic development and the information society. The study systematizes the cyber-risks types and characteristics that, in contrast to the traditional risks can get to the business worldwide and in virtually every business process. Cyber-risks features and possible losses from them, to minimize or eliminate that there are three main areas: security technology solutions, educational work in the sphere of counteraction and prevention of cyber-crimes, as well as cyber-insurance. The main normative legal acts regulating the issues of cybersecurity in Ukraine are revealed. Taking into account the conducted research, the organizational model of the process of cyber insurance was determined, which presents the subjects of insurance relations, the purpose and subject of insurance, risk circumstances, insurance event and insurance event, damage and insurance payments. According to the authors, cyber insurance is a special type of insurance of liability and property of policyholders, which are economic entities of different spheres of economic activity, which work with large databases of conference information, which allows to minimizing the consequences of the crisis caused by data leakage.

Список літератури:

1. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. Актуальні проблеми економіки. Київ, 2015. № 9. С. 421-427.
2. Wang S.S. Integrated Framework for Information Security Investment and Cyber Insurance. Режим доступу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674.
3. Kesan J.P. & Hayes C. (2017). Strengthening cybersecurity with cyber insurance markets and better risk assessment. Minnesota law review. 102(1), 191-276. Режим доступу: https://www.researchgate.net/publication/322295117_Strengthening_cybersecurity_with_cyberinsurance_markets_and_better_risk_assessment.
4. Malhotra Y. (2015). Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-atRisk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era. New York: Suny Polytechnic Institute. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547.
5. Shackelford, S. J. (2012). Should Your Firm Invest in Cyber Risk Insurance? Business Horizons. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1972307.
6. Страхування кібер-ризиків. URL: https://ehow.com.ua/strahuvannya/strahuvannya-kiber-rizikiv.html.
7. European Commission. URL: https://ec.europa.eu/commission/index_en.
8. Zecurion. URL: http://www.zecurion.ru/about/licenses/.
9. Національний банк України. URL: https://www.bank.gov.ua/.
10. Cisco. URL: https://www.cisco.com/c/uk_ua/index.html
11. Міжнародний союз електрозв'язку. URL: http://www.itu.int.
12. Марутян Р. Україна посіла 56 місце у глобальному індексі кібербезпеки. URL: https://matrix-info.com/2017/06/28/ukrayina-posila-56-mistse-u-globalnomu-indeksi-kiberbezpeky/.
13. Івашина Н. В. Кібер-страхування: новий інструмент страхового ринку. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доп. XXV міжнар. наук.-практ. конф. MicroCAD-2017, м. Харків, 17-19 трав. 2017 р.: у 4 ч. / за ред. проф. Сокола Є.І. Харків: НТУ «ХПІ» Ч. IV. С. 208.
14. Wallet One. URL: https://www.walletone.com/uk/wallet/security/.
15. Грицишин В. Найпопулярніші способи електронних крадіжок з пластикових карт. URL: https://korupciya.com/najpopulyarnishi-sposobi-elektronnix-kradizhok-z-plastikovix-kart/.
16. Чернишов Г. М. До питання про визначення фінансового шахрайства. Науковий вісник Ужгородського національного університету. Серія Право. Ужгород, 2014. Вип. 26. С. 230-234. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/8013/1/ДО%20ПИТАННЯ%20ПРО%20ВИЗНАЧЕННЯ%20ФІНАНСОВОГО%20ШАХРАЙСТВА.pdf.
17. Кіберполіції попереджає українців про нові схеми смс-шахраїв. Сьогодні. 2017. 29 верес. 2017. URL: https://ukr.segodnya.ua/ukraine/kiberpoliciya-preduprezhdaet-ukraincev-o-novyh-shemah-sms-moshennikov-1059751.html.
18. Кібератаки. Як захистити бізнес від нової зброї? URL: https://www.insa.com.ua/uk/blog/kiberataki-kak-zashhitit-biznes-ot-novogo-oruzhiya/.
19. Cyber Security. URL: Forum https://runet-id.com/event/csf18/.
20. Кібер-страхування: новий інструмент ризик-менеджменту. URL: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu.
21. Страховка от кибер-рисков. URL: https://habr.com/company/ruvds/blog/326530/.
22. Страхування від кібер-атак: тепер і на європейському ринку. URL: https://www.dw.com/uk/страхування-від-кібер-атак-тепер-і-на-європейському-ринку/a-16950877.
23. Ільчук В.П., Парубець О.М., Сугоняко Д.О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. Ефективна економіка. 2018. № 5. URL: http://www.economy.nayka.com.ua/pdf/5_2018/5.pdf.

24. Директива про секретність та електронні комунікації: Директива 2002/58/ЄС Європейського Парламенту та Ради від 12.07.2002 L 201/38. Дата оновлення: 12.07.2002. URL: https://nkrzi.gov.ua/images/upload/58/19/6f96b8148ef15842f70cba3dd98f055b.pdf.
25. Конвенція про кіберзлочинність від 23.11.2001. Ратифікація від 07.09.2005 №2824-IV. URL: http://zakon.rada.gov.ua/laws/show/994_575.
26. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Дата оновлення: 05.10.2017. URL: http://zakon.rada.gov.ua/laws/show/2163-19
27. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016. Дата оновлення: 15.03.2016. URL: http://zakon.rada.gov.ua/laws/show/96/2016.
28. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 01.01.2017. URL: http://zakon. rada. gov. ua/laws/show/2657-12.
29. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. Дата оновлення: 19.04.2014. URL: http://zakon.rada.gov.ua/laws/show/80/94-вр.
30. Про авторське право й суміжні права: Закон України від 23.12.1993 № 3792-XII. Дата оновлення: 22.07.2018. URL: http://zakon.rada.gov.ua/laws/show/3792-12.
31. Про поширення примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних: Закон України від 23.03.2000 № 1587-III. Дата оновлення: 04.10.2018. URL: http://zakon.rada.gov.ua/laws/show/1587-14.

References:

1. Bratiuk, V.P. (2015). The essence of cybercrime and insurance against cyber-risk in Ukraine. Actual problems of economics, 9, 421-427 [in Ukrainian].
2. Wang, S.S. (2017). Integrated Framework for Information Security Investment and Cyber Insurance. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674 [in English].
3. Kesan, J.P. & Hayes, C. (2017). Strengthening cybersecurity with cyber insurance markets and better risk assessment. Minnesota law review. 102(1), 191-276. Retrieved from: https://www.researchgate.net/publication/322295117_Strengthening_cybersecurity_with_cyberinsurance_markets_and_better_risk_assessment [in English].
4. Malhotra, Y. (2015). Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-atRisk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era. New York: Suny Polytechnic Institute. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547 [in English].
5. Shackelford, S.J. (2012). Should Your Firm Invest in Cyber Risk Insurance? Business Horizons. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1972307 [in English].
6. Insurance of cyber-risk (2018). Retrieved from: https://ehow.com.ua/strahuvannya/strahuvannya-kiber-rizikiv.html [in Ukrainian].
7. European Commission. Retrieved from: https://ec.europa.eu/commission/index_en [in English].
8. Zecurion. Retrieved from: http://www.zecurion.ru/about/licenses/ [in Russian].
9. National Bank of Ukraine. Retrieved from: https://www.bank.gov.ua/ [in Ukrainian].
10. Cisco. Retrieved from: https://www.cisco.com/c/uk_ua/index.html [in Ukrainian].
11. International Telecommunication Union. Retrieved from: http://www.itu.int [in English].
12. Marutian, R. (2017). Ukraine ranked 56th in the global index of cyber security Retrieved from: https://matrix-info.com/2017/06/28/ukrayina-posila-56-mistse-u-globalnomu-indeksi-kiberbezpeky/ [in Ukrainian].
13. Ivashyna, N.V. (2017). Cyber Insurance: New Insurance Market Tool. Information Technologies: Science, Technology, Technology, Education, Health: Theses of the XXV Report of the International Scientific and Practical Conference MicroCAD-2017, Kharkiv, Kharkiv, Ukraine, 17-19 May 2017, 208 [in Ukrainian].
14. Wallet One, available at: https://www.walletone.com/uk/wallet/security/ [in Ukrainian].
15. Hrytsyshyn, V. (2016). The most popular ways of electronic theft of plastic cards. Retrieved from: https://korupciya.com/najpopulyarnishi-sposobi-elektronnix-kradizhok-z-plastikovix-kart/ [in Ukrainian].
16. Chernyshov, H.M. (2014). On the issue of identifying financial fraud. Scientific herald of Uzhgorod National University. Series Law. no. 26. pp. 230-234. Retrieved from: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/8013/1/ДО%20ПИТАННЯ%20ПРО%20ВИЗНАЧЕННЯ%20ФІНАНСОВОГО%20ШАХРАЙСТВА.pdf [in Ukrainian].
17. Cyberpolice warns Ukrainians about new schemes of SMS-scammers (2017). Today. Retrieved from: https://ukr.segodnya.ua/ukraine/kiberpoliciya-preduprezhdaet-ukraincev-o-novyh-shemah-sms-moshennikov-1059751.html [in Ukrainian].
18. Cyberattacks. How to protect business from new weapons? (2017). Retrieved from: https://www.insa.com.ua/uk/blog/kiberataki-kak-zashhitit-biznes-ot-novogo-oruzhiya/ [in Ukrainian].

19. Cyber Security Forum. Retrieved from: https://runet-id.com/event/csf18/ [in Russian].
20. Cyber Insurance: A New Risk Management Tool (2017). Retrieved from: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu [in Ukrainian].
21. Cyber Risk Insurance. Retrieved from: https://habr.com/company/ruvds/blog/326530/ [in Russian].
22. Insurance against cyber attacks: now on the European market. Retrieved from: https://www.dw.com/uk/страхування-від-кібер-атак-тепер-і-на-європейському-ринку/a-16950877 [in Ukrainian].
23. Ilchuk, V.P., Parubets, O.M. & Suhoniako, D.O. (2018). Innovative approaches to the development of the cyber insurance market in Ukraine. Efficient economy. № 5. Retrieved from: http://www.economy.nayka.com.ua/pdf/5_2018/5.pdf [in Ukrainian].
24. Directive 2002/58/EC of the European Parliament and of the Council "Directive on Secrecy and Electronic Communications". Retrieved from: https://nkrzi.gov.ua/images/upload/58/19/6f96b8148ef15842f70cba 3dd98f055b.pdf [in Ukrainian].
25. "Convention on Cybercrime". Retrieved from: http://zakon.rada.gov.ua/laws/show/994_575 [in Ukrainian].
26. Law of Ukraine "About the basic principles of providing cyber security of Ukraine". Retrieved from: http://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].
27. Decree of the President of Ukraine "Cybersecurity Strategy of Ukraine". Retrieved from: http://zakon.rada.gov.ua/laws/show/96/2016 [in Ukrainian].
28. Law of Ukraine "About information". Retrieved from: http://zakon. rada. gov. ua/laws/show/2657-12 [in Ukrainian].
29. Law of Ukraine "On the protection of information in information and telecommunication systems", available at: http://zakon.rada.gov.ua/laws/show/80/94-вр [in Ukrainian].
30. Law of Ukraine "About copyright and related rights". Retrieved from: http://zakon.rada.gov.ua/laws/show/3792-12 [in Ukrainian].
31. Law of Ukraine "About the distribution of copies of audiovisual works, phonograms, videograms, computer programs, databases". Retrieved from: http://zakon.rada.gov.ua/laws/show/1587-14 [in Ukrainian].

Посилання на статтю:
Demyanchuk M. A. Cyber-insurance as a tool for minimizing the informational risks of the enterprise in the conditions of global economic development and society informatization / M. A. Дем'янчук, Н. Д. Маслій, В. В. Станкова // Економіка: реалії часу. Науковий журнал. – 2018. – № 5 (39). – С. 41-51. – Режим доступу до журналу: https://economics.opu.ua/files/archive/2018/No5/41.pdf. DOI: 10.5281/zenodo.2570060.

Reference a Journal Article:
Demyanchuk M. A. Cyber-insurance as a tool for minimizing the informational risks of the enterprise in the conditions of global economic development and society informatization / M. A. Demyanchuk, M. D. Maslii, V. V. Stankova // Economics: time realities. Scientific journal. – 2018. – № 5 (39). – P. 41-51. – Retrieved from https://economics.opu.ua/files/archive/2018/No5/41.pdf. DOI: 10.5281/zenodo.2570060.