DOI: http://dx.doi.org/10.34069/AI/2020.28.04.8

Cyber insurance: the current situation and prospects of development

Киберстрахование: современная ситуация и перспективы развития

Received: January 25, 2020 Accepted: March 16, 2020

Written by:
Kurmaiev Petro[29]
https://orcid.org/0000-0001-9464-0380
Seliverstova Liudmyla[30]
https://orcid.org/0000-0002-2231-0558
Bondarenko Olena[31]
https://orcid.org/0000-0002-5990-2522
Husarevych Nataliia[32]
https://orcid.org/0000-0002-8266-8498

Abstract

The aim of the article is to analyze current trends in the development of cyber insurance. The following methods of scientific research were used in the preparation of the article: generalization, correlation analysis, comparative analysis. The authors analyze in detail the main trends in the spread of cybercrime. The correlation analysis between the number of registered cybercrimes in a particular country and its GDP, the number of business entities, indicated the lack of correlation between the studied indicators. It states that the most common types of cybercrime are: hacking, unauthorized access, accidental exposure, insider and physical theft. The sectoral analysis of the distribution of cybercrime has revealed a decrease in the share of financial companies while increasing the share of health care companies. It is noted that cyber insurance is one of the effective preventive measures that minimize the negative effects of cybercrime intervention. The article presents segmentation of the cyber insurance market by geography and size of insurance companies. The results of the analysis showed the dominance of US companies in the cyber insurance market. It is stated that the sectoral distribution of cybersecurity policy purchasers in general follows the trends of the sectoral distribution of cybercrime. The volume of cyber insurance,

Аннотация

Целью статьи является анализ современных тенденций развития киберстрахования. При подготовке статьи использованы методы научного исследования: обобщение, корреляционный анализ, компаративный анализ. Авторами подробно проанализированы основные тенденции распространения киберпреступлений. Проведенный корреляционный анализ зависимости между количеством зарегистрированных киберпреступлений в конкретной стране и ее ВВП, количеством субъектов предпринимательства, указал на отсутствие связи между исследуемыми показателями. Указывается, что наиболее распространенными видами киберпреступлений являются: хакерство, неавторизированный доступ, непреднамеренное воздействие, инсайдерская, материальная кража. Отраслевой анализ распределения количества киберпреступлений показал уменьшение доли финансовых компаний при одновременном росте доли компаний, работающих в сфере здравоохранения. Отмечается, что киберстрахование является одной из эффективных превентивных мер, которые позволяют минимизировать негативные последствия воздействия киберпреступников. В статье проведена сегментация рынка

[29] D.Sc.habil. (Economics), Assistant Professor in Economics, Department of Finance, Accounting and Economic Security, Pavlo Tychyna Uman State Pedagogical University, Ukraine
[30] D.Sc.habil. (Economics), Professor, Department of Finance, Kyiv National University of Trade and Economics, Ukraine
[31] D.Sc.habil. (Economics), Professor, Department of Marketing, Kyiv National University of Trade and Economics, Ukraine
[32] PhD (Economics), Assistant Professor in Economics, Department of Finance, Kyiv National University of Trade and Economics, Ukraine

expenses of insured legal entities is analyzed. The main trends in the development of cyber insurance have been identified. The factors that hold back the development of cyber risk insurance have been identified. The main ones include the following: high level of information entropy in the process of cyber risk assessment, lack of a single standard for filling insurance services in the field of cyber insurance. It is noted that in the medium term the cyber insurance market is prospective for insurance companies. This is caused by the increasing scale of cyber threats and the costs associated with cyberattacks.

Key Words: cybercrime, cyber insurance, insurance market, cyber risk, sectoral analysis.

киберстрахования по географическому признаку и по размерам страховых компаний. Результаты анализа показали доминирование компаний США на рынке киберстрахования. Указывается, что отраслевое распределение покупателей полисов киберстрахования в целом повторяет тенденции отраслевого распределения совершенных киберпреступлений. Проанализированы объемы киберстрахования, расходы застрахованных юридических лиц. Определены основные тенденции развития киберстрахования. Идентифицировано факторы, сдерживающие развитие страхования киберрисков. К основным из них отнесены: высокий уровень энтропии информации в процессе оценки киберриска, отсутствие единого стандарта по наполнению страховой услуги в сфере киберстрахования. Указывается, что в среднесрочной перспективе рынок киберстрахования является перспективным для страховых компаний. Это обусловлено ростом масштаба киберугроз и расходов, связанных с кибератаками.

Ключевые слова: киберпреступление, киберстрахование, страховой рынок, киберриск, отраслевой анализ.

Introduction

The development of information technology creates the preconditions for virtualization of all types of business activities. During the 2000s, the use of information technology has come a difficult way from performing functions related, mainly, to communication and computational processes to the use of artificial intelligence in decision-making, modeling. The use of information technology in business helps reduce transaction costs due to the more efficient organization of communication channels and business processes. At the same time, along with the obvious positive effect of the information technologies use, there are accompanying negative manifestations. We are talking about cybercrime. That means the cases of national and international legislation violation in the virtual space and / or with the use of information technologies. Given the further virtualization of business activity, the relevance of finding tools to minimize the negative effects of cybercrime will increase. One such tool is cyber insurance.

The aim of the article is to analyze current trends in the development of cyber insurance

Literature review

The general issues of digitization and innovation to various sectors of the economy are discussed in articles Kurmaiev & Bayramov (2017), Razumova & Levina (2019).

The authors Böhme R. & Schwartz G. (2010) analyzed the main modern models of cyber insurance. The following specific characteristics of cyber risk are identified: correlated risk, interdependent security, information asymmetry. The authors point to a discrepancy between the arguments for cybersecurity as an online security tool and analytical information about the current state of the cyber insurance market to perform its functions. The scenario of the negative impact of the cyber insurance market on the incentives to improve security is indicated.

The article (Shetty, Schwartz, Felegyhazi, Walrand, 2010) examines the impact of cyber insurers on information security. The authors consider cybercrime protection at the individual and global levels. It is noted that cyber insurance has a positive impact on the security of specific insured entities. At the same time, cyber insurance does not affect security on the WAN.

The authors (Marotta, Martinelli, Nanni, Orlando & Yautsiukhin, 2017) summarized the basic information about cyber insurance, highlighted the unique characteristics of this type of insurance. The algorithm of analysis of the market of cyber insurance is offered. Prospective areas of research have been identified. This will allow to reveal the issues of cyber insurance more fully.

Bolot J., Lelarge M. (2009) highlight the feasibility of using cyber insurers. The focus is on the individual cyber risks that insurance companies do not work with. The influence of the factors that determine the volume of investments in cybersecurity is analyzed. The authors note that insurance is an important component of cyber risk management.

The study (Franke, 2017) focuses on the cyber insurance market in Sweden. Using the interview method, the author interviewed 15 subjects of the insurance and reinsurance market. The obtained information allowed us to cover the underwriting process, to summarize the data on insurance premiums. It is noted that one of the main reasons for refusal in cyber insurance is the low level of information security of the client. It is stated that cyber insurance can be an effective tool to minimize the negative effects of cyber risk.

The team of authors (Woods & Simpson, 2017) examines the practice of cyber insurance from public-private partnerships. The mutually beneficial nature of the cooperation between cyber insurers and public authorities is noted. The authors analyze the nature of government institutions impact on the functioning of the cyber insurance market.

Hayel Y., Zhu Q. (2015) note that cyber insurance is a promising tool for minimizing cybercrime losses. The authors propose a cyber insurance model that takes into account the interaction between users, attackers and insurance companies. The basic characteristics of the optimal insurance policy are determined.

The work (Böhme & Kataria, 2006) proposes a two-level classification of correlation properties of cyber risks. According to the authors, the first level is the in-house correlation of cyber risks; it means the correlation of failures / threats in the internal network (Intranet). The second level is global-scale risk correlation. The authors found that cyber risks are different in the first and second levels of the proposed classification. It is noted that the intrinsic correlation of cyber risks has an impact on the insurance decision making, and the global one - on the process of determining the premium by insurers.

Methodology

The method of generalization was used in the preparation of the article. Its application has allowed us to identify common approaches to the use of cyber insurance tools. The method of correlation analysis allowed us to study the degree of interdependence between the number of registered cybercrime and GDP, the number of business entities in individual countries. The method of comparative analysis allowed to compare the indicators that characterize cybercrime and cyber insurance.

In addition, materials from the analytical studies of Identity Theft Resource Center, Wipro Limited, Kaspersky Lab and others were used.

Results and discussion

Development of information technologies, virtualization of entrepreneurial activity is important components of business processes organization of modern companies. Today, it is difficult to find a company that does not use information technology in its activities. A similar situation is observed for individuals for whom online services have become a part of life. Interesting are the results of the study (West, 2016), which showed that the losses of the economy of 19 countries, in which in 2015-2016 the Internet disconnected, amounted to 2.4 billion USD. In particular, India's economy lost 0.96 billion USD as a result of 70 days of shutdowns over the period. 2.75 days of Internet shutdown caused 35.1 million USD loss in Turkey's economy.

In turn, informatization of the economy has led to the emergence and spread of illegal acts in this area (cybercrime). Cybercrime has become an integral part of today's information society.
Having started its history in the 1970s with password and hacking programs, using the advances of modern science, cybercrime has become a global threat to the economic security of legal businesses.

In our opinion, it is advisable to consider cybercrime as a separate specific type of non-legal (criminal) business.

The rapid development of new technologies has contributed to the growth of quantitative and value indicators of cybercrime. The financial flows generated by cybercrime are the largest,

compared to other types of illegal activity. Thus, according to experts (Morgan, 2019), the volume of the cybercrime market in 2015-2016 was 3 trillion USD, compared with 1.13 trillion USD (maximum estimated value) for the pirated products market, 0.65 trillion USD (maximum estimated value) for drug trafficking (May, 2017).

Cybercrime is a universal concept that combines many types of unlawful activity using information technology and / or computer technology.

Summarizing the above-mentioned information allows us to distinguish the following major cybercrime trends:

- object-oriented - development of software and algorithm of actions for a specific object;
- changing the focus of cyber-attacks - less protected entities in the non-financial corporations sector are preferred;
- growth of the share of personal and individuals accounting data and legal entities in the overall structure of the stolen information;
- changing the attitude of companies to be targeted by cybercrime.

An analysis of cybercrime geography has made it possible to identify countries, companies and individuals who are most often the target of cybercrime. The first group of countries, where more than 40% of all cybercrimes are recorded, are: the USA and Canada. The second group of countries consists of Great Britain, India, Australia. Third group of countries includes China, Germany, Norway, Sweden and South Africa.

We conducted a correlation analysis of the relationship between the number of reported cybercrime and GDP (current USD) countries (World Bank, 2019). The correlation coefficient was 0.28, indicating that there is no correlation between the studied indicators.

Similarly, there was no statistically significant correlation between the number of cybercrime reported and the number of business entities in the above-mentioned countries.

To our point of view, the extension of the offenses geography is indicative of the selective nature of cybercrime.

At the same time, as it was mentioned above, the leader of cybercrime attacks was the United States. In the Table 1 the dynamics of indicators that characterize cyber-attacks on US companies is shown.

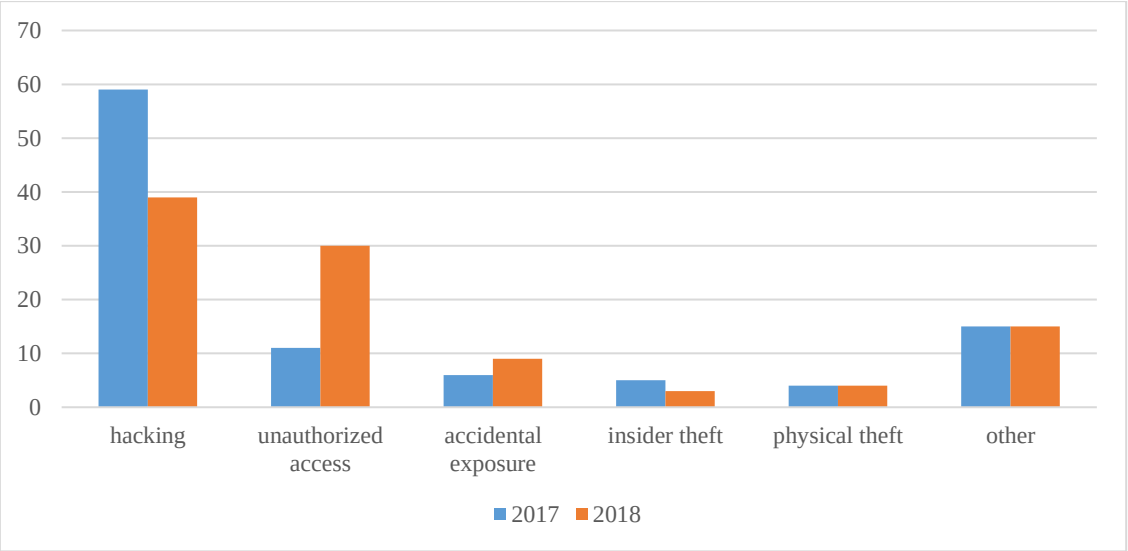
Table 1. Correlation of Cyber-Attacks and General Losses

Year	Losses, USD	Number of Cyber-Attacks	Price of One Cyber-Attack, USD
2015	1070700000	288012	3717,55
2016	1450700000	298728	4856,26
2017	1418700000	301580	4704,22
2018	2706400000	351973	7689,23

Source: Federal Bureau of Investigation, 2019

Thus, according to Table 1, in the US, cybercrime losses increased more than 2.5 times during 2015-2018, although the number of cyber-attacks increased by only 22%. The average cost of losses from 1 cyber-attack during the analyzed period increased from 3717,55 USD to 7689.23 USD. The losses from cyber-attacks in the other countries listed above, especially the first and second groups, are similar in terms of the amount of losses.

The most common types of cybercrime are the following: hacking, unauthorized access, accidental exposure, insider and physical theft. The structure of cybercrimes by their types is shown in Fig. 1



Source*: Identity Theft Resource Center, 2019*

Fig. 1. Breaches by type

Analysis of Fig. 1 shows that hacking accounts for the largest share of cybercrime, with its share accounting for 39% of cybercrimes in 2018. Most often, hacking was done by sending a phishing e-mail virus, activating which resulted in the loss of control over the data. At the same time, the share of this group of crimes decreased by 20% during 2018. First of all, this is due to the increased level of protection, due to the use of letter filtering programs and to the improvement of the functioning of cyber-threat centers. The share of unauthorized access to devices and information networks other than hacking increased by 19 points during the period 2017-2018, accounting for 30% at the end of the period. The share of other types of cybercrime in the overall structure did not fluctuate significantly - about 3-9%.

Analysis of the distribution of cybercrime by industry revealed the following trends.

First of all, there is a significant decrease in the share of business companies operating in the financial sector in the overall industry structure of cybercrime. According to estimates (George, 2019), their share has dropped to 17% of total cybercrime.

Secondly, the share of healthcare companies has increased significantly. The increase was 17% during 2016-2018 (George, 2019; *Identity Theft Resource Center, 2019*).

This means that cybercriminals will refocus on companies in those industries that satisfy three conditions: low basic level of cyber defense, high public resonance, and high level of financial capacity.

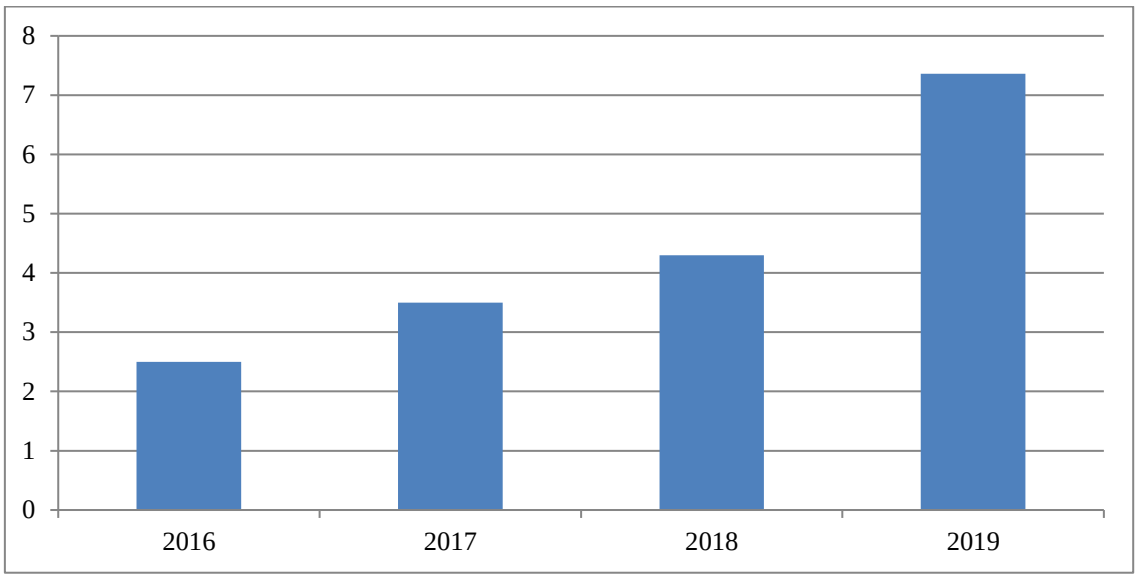
According to a survey conducted by W. Schwab, M. Poujol (2018), 77% of respondents rated the likelihood of a cyber security incident at companies as “Very likely” and “Quite likely”. That is why the mechanisms of combating cybercriminals and their activities are the most relevant.

Among the preventive measures that minimize the negative effects of cybercrime intervention, it is advisable to single out cyber insurance.

With the development of cyber threats and cyber-attacks, insurance has become a significant risk management tool for both state and non-state enterprises. This is a promising direction for the development of insurance business, since the creation of insurance protection programs, in addition to the direct compensation of losses, greatly contributes to improving the level of information security of the company as a whole or of individual business processes.

Cyber insurance is a dynamic segment of the global insurance market. Undoubtedly, this type of insurance is considered as a method of risk management and protection against various threats that arise in the implementation of e-commerce and the use of information technology. The first cyber risk insurance contracts were signed in 2010-2011. This topic was actively discussed at the annual Davos

Forum in 2012. But the active growth of this type of insurance began several years later, following massive cyber-attacks on corporate and government resources in the USA. The dynamics of cyber insurance in the world in 2016-2019 is shown in Fig. 2.



Source: Marsh, 2017, Grand View Research, 2019; Mordor Intelligence, 2020

Fig. 2. Dynamics of Cyber Insurance in the World in 2016-2019, Billion USD

Throughout 2016-2019, there has been a steady increase in cyber insurance in the world. Thus, in 2016, the amount of cyber insurance amounted to 2.5 billion USD, in 2017 this figure reached 3.5 billion USD (an increase of 40%), in 2018 - 4.3 billion USD (compared to the previous year) 23%), 7.36 billion USD in 2019, up 71% from 2018. In general, over the period 2016-2019, the volume of cyber insurance in the world has increased by 194.4%.

The geographical segmentation of the cyber insurance market that we have conducted has shown that 62% of the global cyber insurance market is in the USA, 16% in the UK, 14% in the global market belongs to the EU, 8% - in other countries.

The 2018 FICO Country Cyber Insurance Market Survey (FICO, 2019) shows that the largest number of cyber risk insurers is in the UK. For example, in the UK, in 2017, the number of companies with specific cyber-risk coverage was 61%, in 2018, this figure increased by 29% to 90%. In the USA in 2018, 76% of companies had specific coverage, up 41% from 2016.

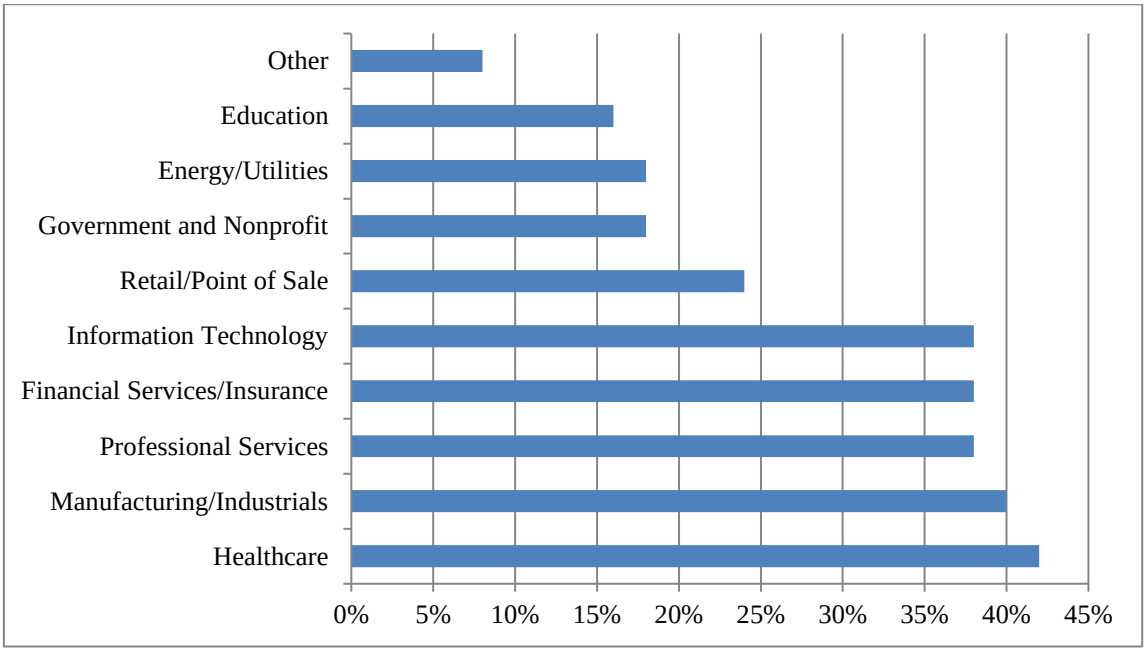
Scandinavia has seen a slow spread in cyber insurance: in Sweden, the percentage of companies with cyber risk insurance has increased by only 1%, and this is the country with the lowest levels - only 57% has cyber risk insurance.

The USA market is dominated by several major insurers, including AIG, Chubb and XL Group, which own 40% of the cyber insurance market. Other insurance companies, such as Beazley, CNA Financial, Liberty Mutual, BCS Insurance, Axis Capital and Zurich American Insurance, hold significantly smaller market shares. According to a study (Snyder, 2019), 10 leading companies accumulate more than 100 million USD in annual insurance premiums, and about 10 others collect monthly insurance premiums of 25 million USD to 100 million USD.

The segmentation of the cyber insurance market by size of insurance companies has demonstrated the dominance of insurers with assets in excess of 100 million USD. Yes, 69.5% of the cyber insurance market was held by five leading cyber insurers (Snyder, 2019): Chubb 325.8 million USD (16% market share; 98% packaged), AXA US 255.9 million USD (12.6% market share; 100% standalone), AIG 232.6 million USD (11.4% market share; 99.9% standalone), Travelers 146.2 million USD (7.2% market share; 77.2% standalone), Beazley 110.9 million USD (5.5% market share; 90.9% standalone).

The PartnerRe & Advisen 2018 survey (PartnerRe & Advisen, 2018) showed an increase in interest in cyber risk insurance among medium-sized enterprises, although in 2014-2017, the major buyers of cyber insurance policies were mainly large enterprises. The above-mentioned demonstrates the growing awareness of the importance and need for cyber-risk protection.

The sectoral segmentation of the market for buyers of cyber insurance policies is shown in Fig. 3.



Source: PartnerRe & Advisen, 2018

Fig. 3. Industry segmentation of cybersecurity buyers in 2018, %

According to the data shown in Fig. 3, the largest number of buyers of cyber insurance policies belongs to the health sector (42%), the second place belongs to the industry (40%), the third - to the professional services, financial services, insurance and information technologies (38% each).

It is advisable to highlight the following major problems of cyber insurance. They are:

- high level of entropy of information in the process of cyber risk assessment;
- the individual nature of pricing for insurance services;
- lack of a single standard for filling insurance services in the field of cyber insurance;
- limited coverage of cyber insurance policies to cover risks;
- availability of other risk coverage policies;
- lack of qualified cybersecurity experts;
- the emergence of new cyber security and cyber-attacks;
- the indifference and illiteracy of business owners and staff about the need to protect against cyber-attacks.

Despite the fact that nowadays there are sufficiently effective means of protection against certain types of cybercrime (means of detecting problems in the Software, SIEM solution, network screening, anti-DDO services), in our opinion, only cyber insurance can compensate for possible losses from damage, destroying or stealing corporate and customer data, and overcoming a business crisis that may result from cyber risk.

According to PartnerRe & Advisen (PartnerRe & Advisen, 2018), the number of cyber insurance policies will continue to grow, as the main reasons for purchasing cyber coverage (in 2018, as in previous years) were:

- reaction to perpetrators of cyber-attacks;
- experience of information and financial losses associated with cyber risks.

In the medium term, the cyber insurance market is prospective for insurance companies. This is due to the fact that the scale, level of danger and costs associated with cyber-attacks are increasing, regardless of whether such attacks are aimed at corrupting data and systems or stealing confidential information, such as trade secrets or personal data.

Thus, according to estimates, the amount of cyber insurance in 2025 will be 27.83 billion USD, with a CAGR of 24.3% over the period 2020-2025 (Grand View Research, 2019). This will be linked to the growing number of digital technologies created and implemented, including in the areas of digital security and privacy management, cyber threats.

Conclusions

The first quarter of the XXI century was marked by rapid development and global spread of information technologies. This process is accompanied by actualization of cyber-risks, including those caused by the activity of cybercriminals. The study showed a trend towards increasing cybercrime and damage. The authors point to the prospect of cyber-risk insurance, given the possibility of minimizing the negative effects caused by cybercriminals.

During 2016-2019, the global cyber insurance market has shown a growth trend, despite the problematic aspects of its current functioning. The growth of this market is primarily due to the awareness of the need for cyber risk insurance and the increasing number of cyber-attacks in the world. The authors point out that the main catalysts for the development of the cyber insurance market in the medium term will be: an increase in the technological level of cyber threats, the need for further improvement of data protection legislation.

Bibliographic references

Böhme, R. & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. Workshop on the Economics of Information Security, June, 1-36

Böhme, R., & Kataria, G. (2006). Models and Measures for Correlation in Cyber-Insurance. Workshop on the Economics of Information Security, June, 1-26

Bolot, J. & Lelarge, M. (2009). Cyber Insurance as an Incentivefor Internet Security. In M. E. Johnson (Ed.), Managing Information Risk and the Economics of Security (p. 269-290). Boston: Springer

Federal Bureau of Investigation (2019). IC3 Annual Report Released. Retrieved from https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219/

FICO (2019). Who has cyber risk insurance worldwide? Retrieved from https://www.fico.com/blogs/who-has-cyber-risk-insurance-around-world

Franke, U. (2017). The cyber insurance market in Sweden. Computers & Security, 68, 130-144

George, J.V. (Ed) (2019). State of Cybersecurity Report. Bangalore: Wipro Limited

Grand View Research (2019). Cyber Insurance Market Size, Share & Trends Analysis Report By Organization. Retrieved from https://www.grandviewresearch.com/industry-analysis/cyber-insurance-market

Hayel, Y., Zhu, Q. (2015). Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks. In M. Khouzani, E. Panaousis, G. Theodorakopoulos (Eds.), Decision and Game Theory for Security. Lecture Notes in Computer Science (p. 22-34). London: Springer

Identity Theft Resource Center (2019). End-Of-Year Data Breach Report Identity. San Diego: Theft Resource Center

Kurmaiev, P. Yu., Bayramov, E. A. (2017). Current trends of financing of innovative activity entities in Ukraine. Scientific Bulletin of Polissia, 2(10), 55-62.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. & Yautsiukhin, A. (2017). Cyber-insurance survey. Computer Science Review, 24, 35-61. doi.org/10.1016/j.cosrev.2017.01.001

Marsh (2017). Global Insurance Market Index (Second Quarter 2017). New York: Marsh LLC

May, C. (2017). Transnational Crime and the Developing World. Washington: Global Financial Integrity

Mordor Intelligence (2020). Cyber Security Insurance Market - Growth, Trends, Forecast (2020 - 2025). Retrieved from https://www.mordorintelligence.com/industry-reports/cyber-security-insurance-market

Morgan, S. (2019). 2019 Official Annual Cybercrime Report. Sausalito: Cybersecurity Ventures

PartnerRe & Advisen (2018). Survey of Cyber Insurance Market Trends. New York: PartnerRe & Advisen

Razumova, Y. & Levina, E. (2019). Digitalization of the transport and logistics market: integration of information systems. Russian experience in introducing digital

technologies in the organization of logistics processes. Amazonia Investiga, 8(22), 269-279. Retrieved from https://www.amazoniainvestiga.info/index.php/amazonia/article/view/428

Schwab, W., Poujol, M. (2018). The State of Industrial Cybersecurity 2018. Munich: CXP Group Company

Shetty, N., Schwartz, G., Felegyhazi, M. & Walrand, J. (2010). Competitive Cyber-Insurance and Internet Security. In T. Moore, D. Pym, C. Ioannidis (Eds.), Economics of Information Security and Privacy (p. 229-247). Boston: Springer

Snyder, A. (Ed.) (2019). Cyber Insurers Are Profitable Today, but Wary of Tomorrow's Risks Oldwick: AM Best

West, D. M. (2016). Internet shutdowns cost countries $2.4 billion last year. Washington: Center for Technological Innovation at Brookings

Woods, D. & Simpson, A. (2017). Policy measures and cyber insurance: a framework. Journal of Cyber Policy, 2, 209-226, DOI: 10.1080/23738871.2017.1360927

World Bank (2019). GDP (current US$). Retrieved from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?type=shaded&view=map