конкурентного статусу як самого підприємства, так і його прямих та потенційних конкурентів. Для вирішення цього завдання доцільно проводити постійний моніторинг конкурентного статусу та фінансової безпеки підприємства.

Література:

1. Бєлоусова Л. І. Вплив стратегічного управління та обраної стратегії на конкурентоспроможність промислового підприємства [Електронний ресурс] / Л. І. Бєлоусова, Н. О. Марченко // Вісник Східноукраїнського національного університету імені Володимира Даля. - 2016. - № 3. - С. 7-11.
2. Бучинська Т. В. Конкурентоспроможність персоналу як основний чинник підвищення ефективності діяльності підприємства [Електронний ресурс] / Т. В. Бучинська // Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. - 2016. - Вип. 10(1). - С. 74-77.
3. Давидова О. Ю. Формування конкурентного статусу підприємства: функціональні аспекти [Електронний ресурс] / О. Ю. Давидова // Проблеми системного підходу в економіці. - 2014. - Вип. 50. - С. 41-48.
4. Ковадло К. Економічна спроможність як чинник конкурентного статусу підприємства [Електронний ресурс] / К. Ковадло, В. Бокій // Вісник Київського національного торговельно-економічного університету. - 2015. - № 2. - С. 47–57.
5. Ковадло К. Л. Механізм підвищення конкурентного статусу підприємства [Електронний ресурс] / К. Л. Ковадло // Вісник Чернігівського державного технологічного університету. Серія : Економічні науки. - 2014. - № 1. - С. 34-38. - Режим доступу: http://nbuv.gov.ua/UJRN/Vcndtue_2014_1_7.
6. Мельник Т. С. Удосконалення теоретико-методичних засад управління конкурентоспроможністю підприємства та оцінки його конкурентного статусу [Електронний ресурс] / Т. С. Мельник // Збірник наукових праць Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна. Проблеми економіки транспорту. - 2015. - Вип. 9. - С. 19-29.
7. Пічугіна Т. С. Дослідження конкурентного статусу підприємства сфери послуг як основа розробки маркетингової стратегії [Електронний ресурс] / Т. С. Пічугіна, Л. М. Яцун, В. М. Селютін, В. А. Куценко // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг. - 2010. - Вип. 1. - С. 545-553.
8. Терованесова О. Ю. Формування конкурентного статусу підприємств машинобудування: ресурсно-діяльнісний підхід [Електронний ресурс] / О. Ю. Терованесова // Науковий вісник Ужгородського університету. Серія : Економіка. – 2015. – Вип. 2. – С. 234-240.
9. Трайкун Ю. М. Вплив логітики на конкурентоспроможність підприємства [Електронний ресурс] / Ю. М. Трайкун, Н. Є. Муромець // Молодий вчений. - 2016. - № 1(1). - С. 178-181.

Semenova K. D.,
Candidate of Economic Sciences, Associate Professor
Tarasova K. I.
Candidate of Economic Sciences, Lecturer
Odessa national economic university, Ukraine

STATISTICAL RESEARCH OF GLOBAL CYBER-RISKS: THE COST OF CYBER-CRIME

The article analyzes global cyber-risks and their effect on the economy. The types of cyber-risks impeding various areas of life are characterized and their negative influence is shown. The state of the digital world of today is analyzed: positive effects and problems of the informatization of society are marked. The basic issues of cyber-risks are outlined and recommendations for their management at the micro and macro levels are provided.

Keywords: *risk, cyber-risk, risk management, internet, cyber-attack, cyber-crime, breach, cyber-security.*

Our world today is in the midst of the greatest information revolution in the history of humanity. Hereby, more than 40 % of the world's population has access to the internet web, with more and more users coming online each day [1, p. 2].

During the last decade, the number of internet users has grown more than by 3 times – from 1 billion in 2005 to an estimated 3.2 billion at the end of 2015. Presently typical day in the life of internet users consists of 207 billion of sent e-mails, 4.2 billion of Google searches, 2.3 GB of web traffic, 152 million of Skype calls and 36 million of Amazon purchases [1, p. 6]. It means that businesses, people, and even governments are now more connected than ever before. The

information revolution has brought and immediate private benefits such as easier access to the information, better convenience, free digital products, and new different forms of leisure.

For example, in Kenya after the introduction of the digital pay system M-Pesa, the sending remittances decreased by 90%. The online platform of e-commerce Alibaba accelerates efficiency of the economy of China through the reduction of coordination costs.

But have new technologies generated faster economic growth and are the countries reaping sizable digital dividends? Arises and another question – will the information technologies continue to bring economies to innovation and prosperity? In so far, developing technologies bring not only new possibilities but also – new risks called cyber ones [2, p. 197].

Cyber-risks appear in many forms, all of which can represent major threats to doing business. Enterprises increasingly face new exposures, including third-party damage, business interruption and different regulatory consequences. Cyber-risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems [3, p. 1]. However, this definition must be broadened. We consider that the most accurate definition of cyber-risk was given by CRO Forum who described "cyber-risk" to mean: "Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber-security incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information − be it related to individuals, companies, or governments." [4].

The 2016 Global Risk Report labels the increase of cyber dependency as one of the long-term trends that will contribute to amplifying global risks. Moreover, the cyber-attacks were ranked in the top 10 global risks. The scope, scale, and impact of them are growing rapidly: the estimated annual cost to the global economy from cyber-crime in 2016 totaled 445 billion $ [5, p. 4]. It is also prognosticated that the cost of data breaches will reach 2.1 trillion $ by the end of 2019 [6, p. 6].

Various researches' data show that 2016 sets new records in the field of ICT:

- There were 4,149 breaches reported during the year that exposed over 4.2 billion records.
- Top 10 breaches exposed 3 billion records combined.
- Ninety-four breaches of the year exposed more than million records.
- There were 102 countries reporting at least one data breach in 2016.
- The Top 10 economies accounted for 64.4% of the breaches.
- Six breaches of 2016 have taken their place on the Top 10 List of All Time Largest Breaches [5,7].

It is clear that the impact of cyber-attacks is also moving from the virtual to the physical world. In 2015, a hack on three Ukrainian power distribution companies caused outages to 80,000 energy customers. [8, p. 6].

All those facts actualize the problem of cyber-risks and make them the object of research of a set of organizations and individual scientists. The most widely known experts in the area of cyber-risks are the Ponemon Institute, Hewlett Packard Enterprise, Risk Based Security Inc., Allianz Global Corporate & Specialty, Marsh & McLennan Companies, PriceWaterHouseCoopers etc. that often publish handbooks on the problems of digital world.

The aim of the article is to quantify the economic impact of cyber-risks and observe their trends of development over the time.

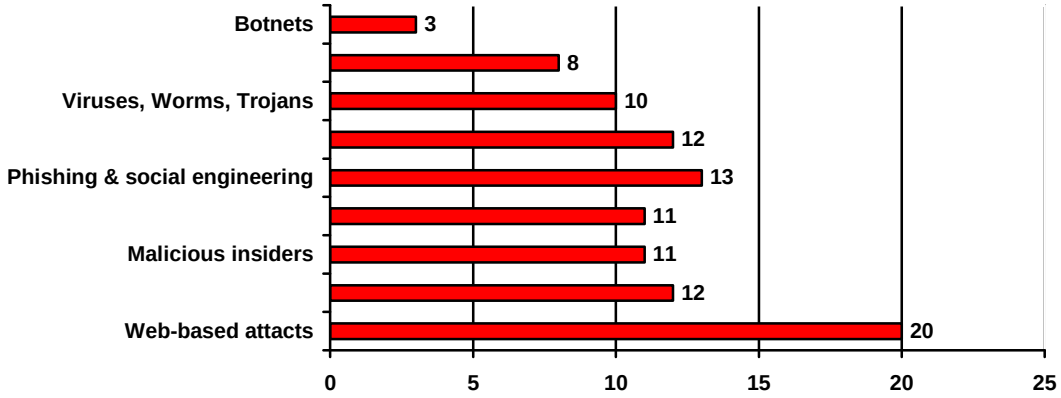
In the past 20 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual: it was found that 80 % of the total value of the Fortune 500 today consists of intellectual property and other intangibles [8, p. 4]. Along with the rapidly expanding "digitization" of corporate assets, there has been a corresponding digitization of the corporate risk which led to the occurring cyber risk. In turn, this risk can vastly affect the competitive position of the enterprise in the market, enterprise's stock price, and shareholder value.

The cost of cyber-risk also rapidly grows. According to the Ponemon Institute's study, the total cost of cyber-crime during 2016 in Russia increased by 29 %, in the United States – by 19 %,

in Japan and the United Kingdom – by 14 %, in Germany – by 8 %. In Ukraine this number exceeds 25 % [7].

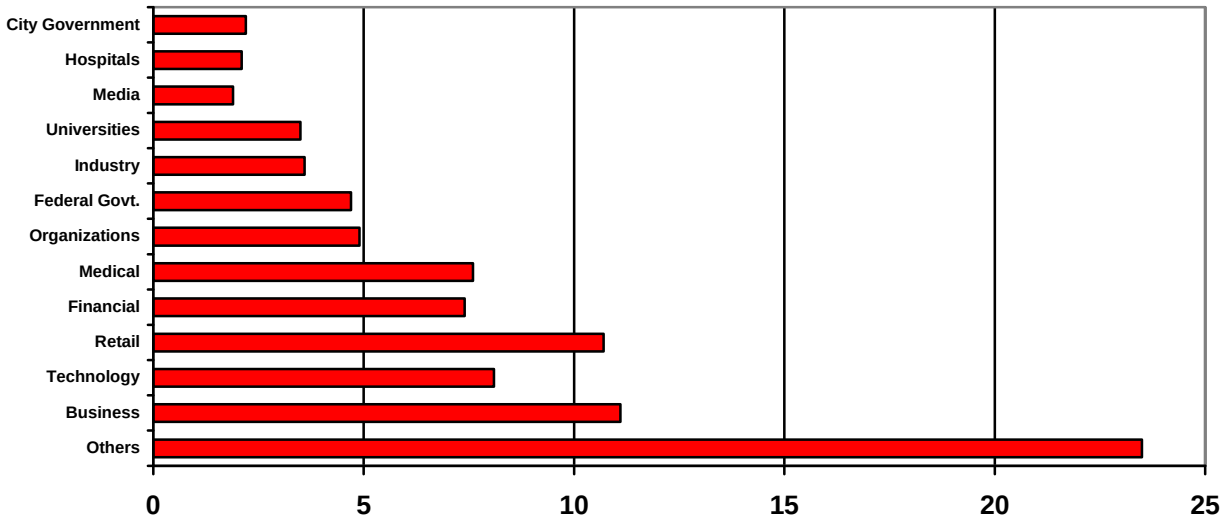
Enterprises nowadays view cyber-risks in the same way they consider other critical risks – in terms of a risk-reward trade-off. This is especially difficult in the cyber arena because of the complexity of cyber threats that has grown drastically. Enterprises are faced with the increasingly sophisticated events that outstrip traditional defenses. As the complexity of these attacks increases, so does the risk they pose to the companies. The top 10 cyber-risk types and their frequency of occurrence are presented in Figure 1.

Figure 1. Top 10 cyber-risks' incidents in 2016, % [4,9]



The potential effects of cyber-risks are expanding well beyond information loss, and include significant damage in other areas. As of now, enterprises are subject to the attackers who are part of very sophisticated teams that deploy increasingly targeted malware against systems and individuals in multi-staged, stealthy attacks. These attacks, sometimes referred to as APTs (for advanced persistent threats), were first deployed against government entities and defense contractors. More recently, they have migrated throughout the economy, meaning that virtually any organization is at risk. The average impact of cyber-risk by sectors of the economy is situated in Figure 2.

Figure 2. The impact of cyber-risk by sector of economy, % [1,4]

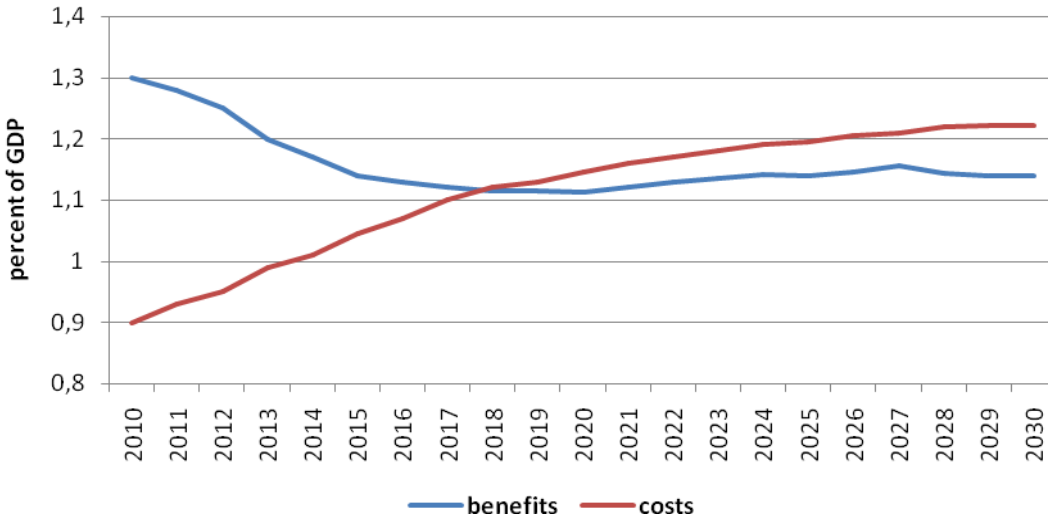


Nevertheless, in any area, the information theft is the most extensive consequence of a cyber-crime. In most cases it results in business disruption (39 %), information loss (35 %) and profit loss (21 %) [9, p. 16]. One of the defining characteristics of cyber-attacks is that they can penetrate virtually all of a company's perimeter defense systems, such as firewalls or intrusion detection systems. In other words, if a skilled hacker targets an enterprise's systems, they will almost certainly breach them [8, p. 4].

But not only large companies are at risk: although small and medium-sized enterprises believe that they are too insignificant to be a target, that opinion is deeply wrong. In fact, the majority of cyber-attacks are levied against smaller organizations that have fewer security resources. In addition to being targets in their own right, smaller firms are often an attack pathway into larger organizations via customer, supplier, or joint venture relationships, making vendor and partner management a critical function for all interconnected entities [8, p. 5].

At the same time, some researchers think that, so far, cyber-space has been safe enough, secure enough and more data breaches, more disclosures of critical vulnerabilities will only come in the future [10, p. 2]. A future where the annual costs of being connected will outweigh its benefits. According to Zurich Insurance Group and the Atlantic Council's models, annual cyber-security costs in high-income economies like the U.S. have already begun to outweigh the annual economic benefits arising from global connectivity. For all economies, the inversion of costs and benefits is expected to occur within the next five years (Figure 3).

Figure 3. ICT cyber benefits and costs, global annual totals, 2010-2030 [13]



Moreover, prognostications of future losses can become even more chilling: according to a certain study, between $9 trillion and $21 trillion of global economic value creation in the next five to seven years could be at risk if organizations and governments are unable to adopt successful strategies to combat cyber threats [8, p. 5].

But, there is a positive side. Whereas the cyber costs tend to be experienced as 'one-time deals', cyber benefits tend to deliver positive effects after they originally left for many years to come.

Based on current tendencies of development of our digital world, scientists also made a prediction as touched to the four possible variants of future, symbolically named Cyber Shangri-La, Independent Internet, Leviathan Internet and Clockwork Orange Internet [10, p. 18-21]. The substance of those possibilities is expressed in table 1.

It's hard to say which variant of future is more likely to come. But more and more scientists make gloomy predictions. The threat of cyber-risk will continue to rise, and it's up to the governments and businesses to choose their policy to make one of these predictions to come true.

In light of the above, we make a conclusion that cyber-risk is one of the most complex problems of the present and it requires expert managing. The problem of cyber-risk management can be viewed at the macro and micro levels.

At the macro level governments should encourage next-generation security projects and aim for an intermediate situation called a strategy of dynamic stability. In this case, a strong and resilient internet is driven by a healthy non-state sector, supported when needed by governments.

Therefore, high-income countries especially should increase funding and cooperation on risk management, and demonstrate exceptional caution in using the internet for intelligence and military

purposes. It is also necessary to encourage cross-border digital trade and avoid location-specific or market restrictions on where ICT equipment is made. Even if such protectionist market restrictions make policy sense in the short run, they import physical borders, which will similarly reduce trade and hurt national and global GDP growth.

Table 1

Alternative worlds: scenarios of international development

Variant of future	Characteristics	Impact on the economy
Cyber Shangri-La	Newly created technologies create benefits faster than costs are accumulated. The cyber defense mechanisms are easier and cheaper, their improvement becomes faster than offences arise.	ICT becomes the main driver of innovation process; it benefits among the world as nearly all firms have access to similar technologies. Global cooperation on cyber- security is relatively high.
Independent Internet	ICT companies continue to develop new e-defenses but cyber-terrorists still thrive.	ICT is an important driver of innovation but there is a risk of rising income inequality between countries in the future. As for now, the ICT globalization is high.
Leviathan Internet	Cyber-security decreases all over the world. Most of the nations have predominantly open internet borders and from time to time suffer from cyber-attacks. Some countries, like China and Russia, choke off their national borders so that all the information and attacks have difficulty penetrating.	There is little trust between friendly countries. Some nations close off their national e-borders which lead to the ICT inequality. The impact on the economic development is fairly modest with stably growing GDP. But this growth is far lower than it could have been with open borders.
Clockwork Orange Internet	Cyber offence mechanism is unstoppable. ICT usage is very limited and is reserved only for those people who are rich enough to pay for proper security measures.	The international cooperation is limited due to the lack of trust between countries. The cost of the digital economy is rising much faster than dividends of them. Most heavily by cyber-crimes are affected higher-income countries and so-called 'middle economies'.

At the micro level the problem of cyber-risk management and cyber-security is a serious issue affecting virtually all levels of significant entrepreneur activity. Enterprises need to continuously assess their capacity to address cyber-risks, both in terms of their own fiduciary responsibility as well as their oversight of management's activities, and many will identify gaps and opportunities for improvement. Managers should seek to approach cyber-risk from an enterprise-wide standpoint; understand the legal ramifications for the company as well as the board itself; ensure directors have sufficient agenda time and access to expert information in order to have well-informed discussions with management; and integrate cyber-risk discussions with those about the company's overall tolerance for risk.

The problem of cyber-risks is not a problem of one. It's a problem of all mankind, and it is necessary to fight together at all levels of our existence.

References:

1. Global Economic Prospects. June 2016. Divergences and Risks [Electronic resource]. – 2016. – № 26. – Available at: http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf (date of appeal: 09.02.17). – Title screen.
2. Тарасова К. І. Global cyber risks and alternative variants of future / К. І. Тарасова // Інноваційні технології та інтенсифікація розвитку національного виробництва / Матеріали ІІІ міжнар. наук.-практ. конф. 20-21 жовтня 2016 р. Ч2. – Тернопіль : Крок, 2016. – С. 197-199.
3. Cyber risk appetite: Defining and Understanding Risk in the Modern Enterprise [Electronic resource]. – Available at: https://www.rsa.com/content/dam/rsa/PDF/2016/05/h15150-cyber-risk-appetite-wp.pdf (date of appeal: 09.02.17). – Title screen.
4. Cyber resilience – The cyber risk challenge and the role of insurance [Electronic resource]. – 2014. – Available at: http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance/ (date of appeal: 09.02.17). – Title screen.
5. Allianz Risk Barometer Top Business Risks 2016. - Allianz SE and Allianz Global Corporate & Specialty SE. – 2016. [Electronic resource]. Available at: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf (date of appeal: 09.02.17). – Title screen.

6. MMC Cyber Handbook 2016. Increasing resilience in the digital economy. [Electronic resource]. – 2016. – Available at: https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf (date of appeal: 09.02.17). – Title screen.
7. Data Breach QuickView Report. 2016 Data Breach Trends – Year In Review. [Electronic resource]. – 2017. – Available at: https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf (date of appeal: 09.02.17). – Title screen.
8. Cyber-risk oversight. Director's handbook series. 2014 Edition. [Electronic resource]. – 2014. – Available at: https://na.theiia.org/standards-guidance/Public%20Documents/NACD-Financial-Lines.pdf (date of appeal: 09.02.17). – Title screen.
9. 2015 Cost of Cyber Crime Study: Global. – 2015. – Available at: http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf (date of appeal: 09.02.17). – Title screen.
10. Risk Nexus. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures [Electronic resource]. – 2015. – Available at: http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf (date of appeal: 09.02.17). – Title screen.