УДК 330.131.7:[316.772.3:004.738.5]
JEL Classification: D85

Eshchenko E.O.
Postgraduate Employee
V.N. Karazin Kharkiv National University

RISKS OF FUNCTIONING OF THE NETWORK COMMUNITIES OF ELECTRONIC SPACE AND THEIR ADMINISTRATION

The risks of the economic system in the context of the impact of network communities of electronic space have been analyzed. There has been also made a systematization of these risks. On the basis of this analysis possible ways of risk administration have been identified.

Keywords: risk, informatisation, network communities of electronic space, risk administration.

Єщенко Є.О. РИЗИКИ ФУНКЦІОНУВАННЯ МЕРЕЖЕВИХ СПІЛЬНОТ ЕЛЕКТРОННОГО ПРОСТОРУ ТА ЇХ АДМІНІСТРУВАННЯ
У статті проведено аналіз ризиків господарської системи у контексті впливу мережевих спільнот електронного простору. Також здійснено їх систематизацію. На основі цього були визначені можливі шляхи їх адміністрування.
Ключові слова: ризики, інформатизація, мережеві спільноти електронного простору, адміністрування ризиків.

Ещенко Е.О. РИСКИ ФУНКЦИОНИРОВАНИЯ СЕТЕВЫХ СООБЩЕСТВ ЭЛЕКТРОННОГО ПРОСТРАНСТВА И ИХ АДМИНИСТРИРОВАНИЕ
В статье проведен анализ рисков хозяйственной системы в контексте влияния сетевых сообществ електронного пространства. Также осуществлена их систематизация. На основе этого были определены возможные пути их администрирования.
Ключевые слова: риски, информатизация, сетевые сообщества электронного пространства, администрирование рисков.

Introduction. In contemporary society relations in all spheres of activity are getting network character. Network communities have become a reality on a global scale. Proliferation of such structures is accompanied by an increase in the intensity of communications and causes many serious problems associated with the security of the individual, society and state. Over the past 10 years there have been evolutionary changes in the forms and types of risk and the nature of their control. As a consequence, the characteristics of many new forms of risk often do not allow to use traditional methods of risk assessment and management, or traditional policy applied at the institutional or governmental level.

Analysis of recent research and publications. Problems of network organization of economic interactions are considered by V. Auzan, A. Gritsenko, A. Nekless, O. Yaremenko V. Sobolev, I. Strelets. Among foreign researchers there should be highlighted works of such scholars as M. Castells, Ph. Kotler, D. Stonehouse. Important theoretical developments in the field of scientific study of the risks and threats to information security have been made by foreign scientists: P. Molander, A. Riddle, D. Ronfeldom, P. Wilson and domestic researchers: S. Bukharin, A. Manoilo, I. Panarin, S. Parinov V. Prokofiev.

Risks of the global economy have been considered particularly closely recently. The World Economic Forum (WEF) since 2007 has made expert risks assessment. But there does not exist a system analysis of them. Network communities become the dominant form of economic relations, transform the market institutions and the risks, that they produce, constitute the relevant range of risks of economic system and require appropriate regulation.

The purpose of the investigation is to analyze and make a systematization of the risks of the economic system under the influence of network communities of electronic space and thereby to identify possible ways of their administration.

Results. The emergence of the network economy is associated with the development of information technology, that leads to the evolution of modern economic systems, the development of non-market mechanisms of regulation and network organizational structures.

The uncertainty of the functioning and development of the global economy, which has a network nature, requires an analysis of the risks and their consideration in economic practice.

The previous years World Economic Forum analyzed global risks. This year WEF experts place the emphasis on risks caused by information technologies [10]. An in-depth risk analysis is being made, and the main risk-generate factor is the stability of growing electronic networks.

Network communities of electronic space, despite the significant benefits and positive properties, have a negative side, the probability of which is a dangerous risk today. The network nature of the relationship increases the hazard of such risks, because they will be spread with lightning speed, as the «infection», affecting all network participants.

Risks of the economic system as a result of functioning of network communities of electronic space can be classified by several parameters [2, p. 4].

By occurrence of risk-generate factors:
- spontaneously arisen;
- purposefully created.

Targeted hazards can be large-scale as well as of local effects. Purposeful risks, for example, include 1) cyber attacks (according to the report «2013 Cost of Cyber Crime Study» the average annual damage from cyber attacks is 11.56 million US dollars [4]). 2) malicious software, which includes viruses, worms, «Trojan horses» (computer programs that can harm your computer and data stored on it) [2, p. 5]. The number of using malware cyber attacks aimed at stealing financial data increased by 27,6% to 28,4 million in 2013. Number of attacked users was 3,8 million people (there is an 18,6% increase over the year). The proportion of users faced financial attacks that use malware was 6,2% of the total attack in 2013. Compared to 2012 the figure has risen by 1,3 percentage points [7]. 3) cyber fraud – a type of cybercrime, which aims to trick

users (hacker illegally gains access and uses the user's personal information (bank account numbers, passport details, codes, passwords, etc.) to cause material and financial damage).

By a factor of information integrity the following risks can be identified [2, p. 5]:

– information theft (the risk that an attacker can obtain information through the social networking site that will allow him to carry out an attack on a corporate network (socio-technical attack); phishing – the theft of confidential information and money with their redirection to fraudulent websites; interception of communications – made for the purpose of their viewing, copying or modification).

According to «Kaspersky Lab» in 2013 about 39,6 million people faced with phishing. In 2013 the majority of locked by «Kaspersky Lab» phishing attacks occurred in the United States: users from that country took over 30,8% of all attacks. They are followed by Russia (11,2% of attacks) and Germany (9,32%) [9].

Most of the attacks in 2013 occurred in social networks – about 35,4%. Fake bank sites, payment systems and online stores – 31,45% of attacks. The third place with 23,3% – e-mail services [9].

– information system breaking (risk of the account hacking on the social network; unauthorized access to computers and computer networks; disruption of the network. They are dangerous in terms of causing property damage as well as damage to the reputation of the company);

– malicious misrepresentation or spreading the false information (disinformation, intimidation or blackmail).

By the impact on the individual [2, c. 6]:

– content-risks (risks associated with the consumption of the information published on the Internet that includes any illegal or inappropriate content (pornography, propaganda of extremism, drugs, gambling, religious sects, suicide, etc.);

– communication risks (activity related to interpersonal users relationships, probability of being subjected to insults and attacks from the other members of the community, including illegal contact (grooming), cyberstalking, cyberbulling etc.);

– psychological risks (abnormality of adequate perception of reality; social networking addiction; increased opportunities for deception and manipulation of consciousness).

By subjects that can be under cyber risk [2, c. 6]:

– global economic community;
– national economic system;
– public administrations;
– manufacturers;
– consumers.

Consumer risks – an abuse of consumer rights on the internet. They include: the risk of purchasing poor quality goods, various fake, counterfeit products, the loss of money without purchasinge a product or service, theft of personal information to cyber-fraud, etc. [8].

Risks for Business:

Risks for current or potential employees of the company can be separately identified [2, c. 6]:

– more and more HR-recruiters use social media in order to clear up their competitors' record.

– information announced by the user of a social network can be used by the employer to put pressure on him or dismiss.

For a company the following risks exist:

– risks and threats, causing material damage (accidental or deliberate attacks faced by enterprise networks due to careless actions of employees who use social networking sites during working hours; reduced productivity due to time-consuming to visit social networking sites and chat there; financial losses due to leakage of important information).

– reputational risks (network communities can act as a «field» for competitive intelligence and industrial espionage; the discrediting of competitors in network communities; and with the increasing freedom of self-expression the possibility of employees' affection on the company's image also increases).

According to «Allianz» experts in 2014 awareness of cyber crime and reputational risks has increased the most. Cyber crime has made the biggest jump in the rating of «Barometer of Risk», rising from 15 to 8th place, and reputational risks have moved from 10th position to 6th [5].

For public administration [2, c. 7]:

– economic espionage;

– potential modification of internal or public information, including the disruption of websites, etc.

It should be noted that the risks caused by information and communication technologies and the network nature of the interactions in the modern world appear at the macro level (for the national economy as a whole):

– threat to national security, the possibility of information attack and isolation;

– the growth of the shadow economy;

– an increase in unemployment rate, a decrease in tax revenues as a result of piracy, phishing, etc.

Risk-generated factors in terms of the level and timing of administrative actions [2, c. 7]:

– strategic cyber risks;
– operational.

Strategic risks – threats that may lead to a significant reduction in sustainable development and security of companies.

For most companies across sectors and regions the risks of cyber attacks are strategic risk: cyber attacks are more risky than other types of technological risks. Some managers consider internal threats as great risk as external attacks [10, p. 11]. Financial institutions are particularly sensitive – about 80% of them believe that cyber stability is a «strategic risk», compared to about a half of the other institutions [10, c. 13].

Operational risks – network communities create problems for the staff: in spite of the positive effects of corporate environment and establishment of informal communication in the team there is still the problem of loss of productivity due to time-consuming of visiting social networking sites and chat there. Besides social networking creates a significant burden on the Internet channel and slows a work of applications needed for business networking.

As the risks of network communities of electronic space arise at four levels: micro, meso, macro and mega-levels, then the risk management can be carried out at different levels [3, c. 4]:

– at the supranational level (global);
– at the state level;
– at the company level;
– at the personal level.

A variety of factors that affect the cyber resilience and economic stability is enormous, and the analysis of possible outcomes should take into account the degree of uncertainty. This leads to the development of various protective mechanisms and institutions. Experts identify three scenarios depending on the implementation of cyber risks and attitudes of business entities [10, p. 24]:

Scenario one: muddling into the future. Cyber threats increase, but sophistication of institutions does not. Businesses continue to reach the way they have in the past and the attack vendors continue to group together and increase in their relative sophistication.

Scenario two: backlash against digitization, prompted by proliferating cyberattacks. Fears about cyber security slow down cooperation and trust. Sophisticated attack vectors are disseminated to a wider range of actors with some harboring truly destructive intent. This ripples into implications for consumer purchasing habits, limiting business strategies and severely inhibiting government regulations. The companies' innovation slows and productivity decreases. Over time, there may be reduction in the effectiveness of international trade and distribution of corporate resources.

Scenario three: accelerated digitization thanks to robust cyber resilience. Technology and security become enablers to growth. Governments come together in the face of an ever increasing threat to facilitate the dramatic uplift in institutional capability and international cooperation.

Obviously, following the third scenario will form the basis of sustainability to global risks, including cyber risks. However, a necessary condition is the coherence of the measures as well as adaptation to these scenarios of regulatory actions at national level. And this adaption should be carried out to a global regulation, to the interests of the business environment and civil society.

Ukraine has taken disparate attempts to form a national information space and to protect it (July 6, 2010: Ukraine ratified the basic European standards in the field of protection of personal data; December 9, 2010: by Presidential Decree № 1085/2010 «On optimization of central executive bodies» the State Service of Ukraine on the protection of personal data was formed as the central body of executive power in Ukraine; experts of the National Institute for Strategic Studies under the President of Ukraine during 2012-2013 developed the project «Strategy for cyber security of Ukraine» [6]). However, it should be admitted that to form the modern national information space of Ukraine, which would meet new challenges and threats, it is necessary to take a number of system activitions in the conceptual, legal and institutional directions.

Besides the important point is the fact that in network communities of electronic space effective protection of personal data depends on the user no less than the national controller or a provider of online services. For this purpose the user must also be responsible, considerate, have certain knowledge for the proper use and combination of security tools available to him, observe the rules of use of network resources, etc. In other words, it is a kind of online user safety culture and it is need to be promoted on a global scale.

In this connection it is necessary to carry out the following steps to enhance stability and leveling cyber risk [3; 6; 10]:

At the national level:

– improve the level of international cooperation in the field of cyber security at the national and departmental levels;

– help to prevent the militarization of electronic space;

– promote the creation of international rules for the government policy in electronic space and improving the international legal framework in this area;

– further development of legislation, relevant national standards, clear definition of terms, concepts and categories in the field of information and security policy;

– establish mandatory requirements for cyber defense of critical national information infrastructure facilities regardless of ownership as well as protection orders and monitor of its compliance;

– strengthen the technical and technological capabilities, scientific and human potential of the Ukrainian Security Service, the intelligence agencies and the State Service for Special Communications and Information Protection in electronic space;

– strengthen the fight against cyber terrorism and cyber espionage, protection of their manifestations of critical national information infrastructure facilities;

– promote the development of network teams to respond to computer emergencies;

– develop and coordinate research in the field of cybersecurity;

– create favorable conditions for young professionals in the IT field, which should facilitate their employment in Ukraine;

– provide changes to the curriculum and programs of middle and high schools, the training of scientific and scientific-pedagogical staff, aimed at informing the target groups of cyber threats and methods to combat them;

– develop a nation-wide program to improve public awareness of cyber threats;

– work to harmonize national and international policies surrounding the prosecution of cybercrime.

At the level of business:

– integrate cyber resilience into enterprise-wide risk management and governance processes and responsibilities;

– provide differentiated protection based on importance of assets;

– deploy active defenses to uncover attacks proactively;

– continuous testing to improve incident response;

– enlist front-line personnel – helping them understand value of information assets;

– increase investments in cybersecurity technical education;

– foster partnerships with the government, universities and the private sector to develop the skills, etc.;

At the level of society and the individual user:

– protection of personal data;

– responsibly, carefully, improving special knowledge, use and combine the available security tools;

– keep the rules on the use of network resources;

– there is a need for a dialogue between the private, public and civil structures to develop a coordinated combination of policy and market mechanisms.

Conclusion. Therefore, the impact of network communities of electronic space on the functioning and results of economic entities appears in the probability of achieving/failing to achieve goals, i.e. risks that must be considered because network communities of electronic space are increasingly becoming the defining form of economic relations and, accordingly, a factor of stability/instability. Risks and threats caused by network communities of electronic space have been systematized on the following criteria: the rise of factors, that cause risks (spontaneously arisen; purposefully created); a factor of information integrity (information theft; information system breaking; malicious misrepresentation or spreading the false information); risk-generated factors in terms of the level and timing of administrative actions (strategic cyber risks; operational risks); the impact on the personality (con-

tent-risks; communication risks; psychological risks); subjects that may be under cyber risks (global economic community; national economic system; public administrations; manufacturers; consumers).

The spread of information technology and network logic of economic relations through virtualization involves more and more participants, including countries and entire regions of the world. Depending on the awareness of the reality of the risks produced by network communities of electronic space, there could be defined possible options and implications for economic systems, which consist in passive and active (proactive and reactive) actors' response. Reduction in risks for the economic system from the activity of network communities makes it necessary to interface institutional change in management strategies of network communities of electronic space at the global and national level to integrate the efforts of government, civil society and business.

REFERENCES:

1. Аналітична доповідь Національного інституту стратегічних досліджень «Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти» [Электронный ресурс]. – Материал с сайта www.niss.gov.ua. – Официальный веб-сайт. – Режим доступа : http://www.niss.gov.ua/public/File/2013_table/1010_dopov.pdf.
2. Ещенко Е.О. Риски хозяйственной системы: влияние сетевых е-сообществ / Е.О. Ещенко // Экономика и Финансы. – 2014. – № 7.
3. Ещенко Е.О. Управление рисками кибер устойчивости в глобальной экономике / Е.О. Ещенко // Экономика и Финансы. – 2014. – № 8-9. – С. 3-8.
4. Исследование: среднегодовой уровень ущерба от кибератак вырос на 78% [Электронный ресурс]. – Материал с сайта Портал «Центр информационной безопасности». – Официальный веб-сайт. – Режим доступа : http://www.bezpeka.com/ru/news/2013/10/24/cyberattacks-survey.html.
5. Кибер-риски становятся глобальным трендом [Электронный ресурс]. – Материал с сайта Портал «Капитал». – Официальный веб-сайт. – Режим доступа : http://kapital.kz/tehnology/14251/kiber-riski-stanovyatsya-globalnym-trendom.html.
6. Проект «Стратегії забезпечення кібернетичної безпеки України» [Электронный ресурс]. – Материал с сайта www.niss.gov.ua. – Официальный веб-сайт. – Режим доступа : http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf.
7. Развитие информационных угроз в первом квартале 2014 года [Электронный ресурс]. – Материал с сайта ЗАО «Лаборатория Касперского». – Официальный веб-сайт. – Режим доступа : http://www.securelist.com/ru/analysis/208050839/Razvitie_informatsionnykh_ugroz_v_pervom_kvartale_2014_goda.
8. Рекомендации «Безопасный Интернет» [Электронный ресурс] / Под общей ред. Н. К. Солоповой, к.п.н., доцента, проректора по учебно-методической работе и информатизации ТОИПКРО. – Тамбов : ТОИПКРО, 2011. – 191 с. – Режим доступа : http://www.vsosh2.info/wp-content/uploads/2012/12/bezopasnyi-internet-dlya-pedagogov.pdf.
9. Финансовые киберугрозы в 2013 году. Часть 1: фишинг [Электронный ресурс]. – Материал с сайта ЗАО «Лаборатория Касперского». – Официальный веб-сайт. – Режим доступа : http://www.securelist.com/ru/analysis/208050836/Finansovye_kiberugrozy_v_2013_godu_Chast_1_fishing.
10. Risk and Responsibility in a Hyperconnected World / World Economic Forum Report 19 Jan 2014 [Электронный ресурс]. – Материал с сайта World Economic Forum. – Официальный веб-сайт. – Режим доступа : http://reports.weforum.org/hyperconnected-world-2014/.