IT Production: Monitoring Economic Security in Supply Chain Management

Maksim Dombrovsky[1], Svetlana Doguchaeva[2*], Sergey Bratanovsky[3]

[1]*Department of Entrepreneurship and Economic Security, Perm State National Research University, Russian Federation*
[2]*Department of Data Analysis, Decision-making and Financial Technology, Financial University under the Government of the Russian Federation, Moscow, Russian Federation*
[3]*Plekhanov Russian University of Economics, Moscow, Russian Federation*
Corresponding author: svetlanadoguchaeva@yandex.ru

***Abstract*– The rapid development of computer information technologies affected all spheres of human life. Therewith, unlawful distortion, falsification, destruction or disclosure of some information, as well as disorganization of information processing and transmission, cause serious material and moral damage to many subjects involved in the automated information interaction. The purpose of this research is to analyze the problems of economic security in distributed software development. In the legal practice of foreign countries, protection of computer programs is a controversial issue. This study involves a numerical analysis of the relationship between the International Property Rights Index (IPRI) and the Information and Communication Technology (ICT) Development Index. The analysis also touched upon the informal impact on economic security in the field of information and communication technologies. The correlation between the International Property Rights Index (IPRI) and the ICT Development Index (IDI) across countries is between 0.32 and 0.52. In the USA, Germany, Belgium, India, the correlation between the growth rate of IDI and the growth rate of IPRI is negative due to the high growth rates of IDI over striding the growth rates of IPRI. This article offers an innovative approach to the organization of block chain-based software development.**

***Keywords*–** *economic security, intellectual property, distributed development, software, block chain*

1. Introduction

Modern software projects travel a non-easy way from developers working at individual parts to the manufacturer. In the case of a code being lost or disclosed before manufacturing, or when information leaks to competitors, developers experience economic losses [1-15]. In addition to this, there is a danger of unlawful or unauthorized use of someone else's code by ordinary developers. This entails the emergence of claims by the third parties of intellectual property infringement. These threats necessitate a thorough study of the economic security control in software development management. In the legal practice of foreign countries, protection of computer programs is not a simple matter [16-18].The United States was the first country to legally protect computer programs. In 1980, the Computer Software Copyright Act was adopted. The next ten years were marked by the series of similar actions. Regulations similar to this Act were adopted in Australia (1984), Japan, Great Britain, France and Germany (1985), Spain (1987), Canada (1988) and China (1990). Nowadays, software products are protected by copyright at the international level [19, 20]. This is enshrined in the Berne Convention for the Protection of Literary and Artistic Works, in the WIPO Copyright Treaty (1996), in the EU Directive on the Legal Protection of Computer Programs (1991), and in the WTO Agreement on Trade Related Aspects of Intellectual Property Rights [21-24].Any software project that implies the use of components created outside the project can be called a project with a supply chain [25-29]. Components can be made inside or outside the company responsible for the project. The software security characteristics in the supply chain have a significant and long-lasting impact on the security of software created within the framework of a project. In traditional software development projects (including waterfall and iterative ones), software security characteristics in the supply chain are usually evaluated by development teams [24]. Such an evaluation involves the review of component's documentation, the search for documents related to licensing and support, and security testing. The Software Supply Chain Report is an overview of the financial implications of data leakage in 2017[17]. According to this report, data leakage cost companies an average of USD 4 million, 29% higher than in 2016. The study showed that each compromised data record takes 158 US dollars. In highly regulated industries, such leaks are even more expensive. For example, the cost of health care data has risen by 100 US dollars in 2016 reaching 355 US dollars per compromised record in 2017.The problem of securing

subjects in an information sphere of relations and protecting their legitimate interests has sharp angles due to a number of objective reasons. These are the expanding application scope of computer technology and the increasing level of trust in information systems [27]. The very approach to the term "information" has also changed. This term is increasingly used to name a product, the cost of which is higher than the cost of a computer system that runs it [28, 30]. No sooner had been market relations introduced than the creation and provision of information services turned into a competition with industrial espionage. There is no doubt that computer systems must be protected at all stages of their life cycle, given the fact that a computer is in every house and every man has the ability to remotely access computer networks and systems. The most relevant and significant are those threats, the source of which is the users and the company's employees, who have made the software [8]. This trend is brought up not only in various studies of the largest audit companies but also in the annual reports on offences in the field of information security. For a customer, code-reuse attacks are a powerful threat that is used extensively to gain control over modern programs [3]. These attacks use program errors to redirect program control to existing but unplanned code sequences. Protection against such attacks become a popular research topic [1, 2, 7]. The main protection methods are control flow integrity(CFI) [13], code randomization [14], and code pointer integrity [15].According to a research report from Forrester [25, 10], the most well-known personal data protection tools are the cloud data protection solutions, which are good for creating an additional value at the maturity stage of the product life cycle. Tokenization, Big Data Encryption, and Data Access Governance are effective and necessary at the growth stage. The cost of ownership of these technology products is sufficiently high. At the survival stage, specialists use Consent/Data Subject Rights Management, Data Privacy Management Solutions, and Data Discovery and Flow Mapping. The ownership of such technologies costs a medium price. Data Classification, Enterprise Key Management, Application-Level Encryption ensure a moderate success when creating an additional value of the company. These technologies are in use at the stages of growth and maturity. The least effective is Enterprise Rights Management, which is used at the stage of product maturity. In distributed outsourcing software development, there are a number of typical problems. These problems are associated with the distribution of work among the contractors, with the execution control, and with the evaluation and integration of results. The latter must be done with possible threats to economic security kept in mind. The purpose of this research is to analyze the threats in supply chain management that exist in the sphere of IT products and to analyze the related control solutions.

2. Materials and Methods

Supply chain management is a formal term for managing the physical and information flow of materials, finished products and goods in the supply chain. Modern conditions of supply chain management require advanced business processes, the latest technology, and technology/copyright protection in software development. This study selects and justifies recommendations for the safe development of IT products. To accomplish this objective, the study addresses the relationship between the level of intellectual property rights (IPR) protection and the pace of ICT development. The interesting issue is what the relationship is there between the level of economic development and the maturity of legal regulation processes, especially in the field of ICT. To answer this question, it is advisable to consider not just indicators of economic development but to assess the influence of the shadow economy. The entrepreneurship develops in an environment, which, to some extent, is in the shadows. Even countries with a developed system of economic relations are not immune to informal operations. The shadow economy is a complex socio-economic phenomenon that encompasses all socio-economic relations, and above all, the reproduction sector. This is the place where entrepreneurship hides from the government. The size of the shadow economy directly depends on the economic, political and social level of development. In countries with developed market economies, the proportion of enterprises without shadow operations is much higher than in countries in transition. On the other hand, the booming ICT sector is a field for informal activity, especially in countries with an immature legislative system. The indicator reflecting the level of IPR protection, commonly known as the International Property Rights Index (IPRI), has been monitored by the Property Rights Alliance since 2007 [16]. The grading scale of IPRI is [0 to 10], where "10" is the highest value and "0" is the lowest value. This study examines the2010/2018 dynamics of IPRI in the United States, the Russian Federation, Germany, Belgium, and India (Table 1).

Table 1. International Property Rights Index, adapted from [16]

Year	USA	Russia Federation	Germany	Belgium	India
2010	8.461	4.583	8.233	8.122	5.289
2011	8.400	5.000	8.100	8.000	5.500
2012	8.300	4.800	8.100	8.000	5.400
2013	8.300	4.900	8.100	8.100	5.500
2014	8.333	4.767	8.133	8.600	5.267
2015	8.436	4.841	8.094	8.026	5.349
2016	8.632	4.841	8.230	8.247	5.625
2017	8.715	4.943	8.376	8.452	5.866
2018	8.700	5.216	8.343	8.177	5.802

The Information and Communication Technology (ICT) Development Index is a composite index that serves to monitor and compare developments in information and communication technology (ICT) across countries. The ICT development is currently one of the most important indicators of a country's economic and social well-being [19, 20]. An analysis of the correlation between the IPRI and the ICT Development Index (IDI) will help assess the mutual influence of the legislative framework development on the protection of intellectual property rights and the pace of ICT development in the country. Specialists advise calculating this correlation between countries and between the growth rates. Additionally, the level of the shadow economy in studied countries should also be assessed because its size significantly affects the possibility of legal IPR protection. Once the state of IPR protection is analyzed, it is necessary to develop measures to stabilize and improve the development of economic security in supply chain management in the IT production.

3. Results

The IT products go through a complex supply chain (from developers to the consumer). Therefore, there is a need to secure and protect the product when it moves through it. In the USA, Germany and Belgium, IPR protection is at a higher level. These countries scored more than 8 points out of 10. In Russia, IPRI shows a positive trend, reaching 5.216 in 2018, 0.633 points higher than in 2010. Finland in 2018 ranks highest with an IPRI score of 8.69. In India and the Russian Federation, IPRI is not high enough. In in the United States and Germany, IPRI scores were on an increasing trend until 2017. In India, the Russian Federation and Belgium, the IPRI shows improvements followed by a decline, which happens to be a pattern (Figure 1).

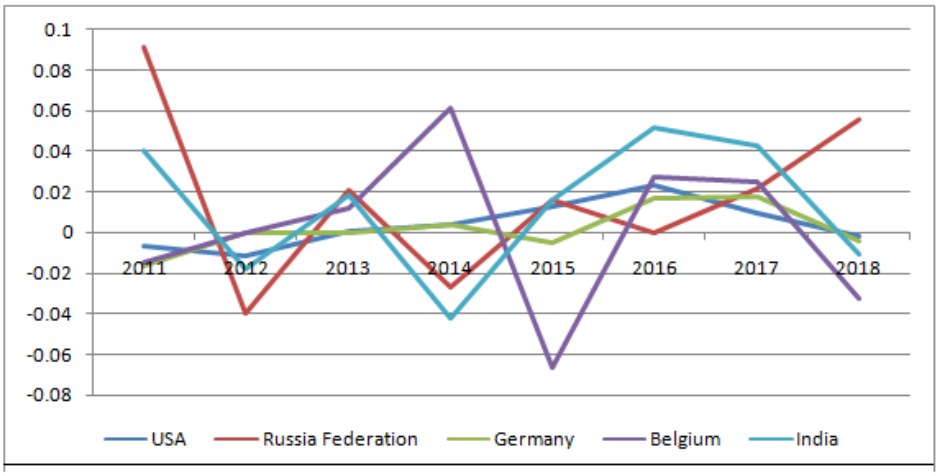

Figure 1.IPRI Growth Rates

The IDI that serves to monitor and compare developments in information and communication technology (ICT) across countries. The level of ICT development today is one of the most important indicators of the state's economic and social well-being [18, 19, 20].

Table2.ICT Development Index, adapted from [20]

Year	USA	Russia Federation	Germany	Belgium	India
2010	7.30	5.57	7.28	6.76	2.14
2011	7.48	6.00	7.39	6.89	2.10
2012	7.90	6.48	7.72	7.33	2.89
2013	8.02	6.70	7.90	7.57	3.05
2015	8.19	6.91	8.22	7.88	2.69
2016	8.13	6.91	8.20	7.7	2.65
2017	8.18	7.07	8.39	7.81	3.03

Table 3 shows the correlation between IDI and IPRI for some countries and correlation between the growth rate of IDI and the growth rate of IPRI.

Table3. Correlation Coefficient

Indicator	USA	Russia Federation	Germany	Belgium	India
Correlation between IDI and IPR	0.324119	0.523035	0.377496	0.436146	0.472717
Correlation between the growth rate of IDI and the growth rate of IPRI	-0.8526	0.159181	-0.35249	-0.48189	-0.61806

The obtained data did not confirm the hypothesis of a close relationship between the level of ICT development and the IPRI scores. The correlation between the growth rate of IDI and the growth rate of IPRI is negative because the existing mechanisms of legal regulation are not able to react fast enough to changes that occur in the software market. This is evident from the higher growth rates of IDI against the lower growth rates of IPRI. The initial stages of distributed software development are often carried out in countries with cheaper labor and low levels of economic development. In such countries, the shadow economy is usually huge. According to data given in [18], the share of shadow GDP in developed countries does not exceed 12-15%, but in countries with a low level of economic development, it reaches 64%. Figures 2 and 3 show the average estimates of the size of the shadow economy in percent of GDP for developed countries and for countries with a high informal part, respectively.

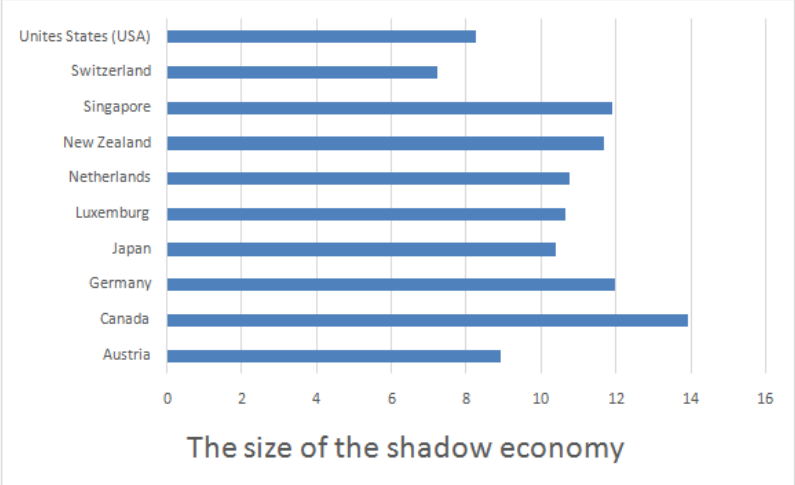

Figure 2. The Average Size of the Shadow Economy in Developed Countries, adapted from [18]

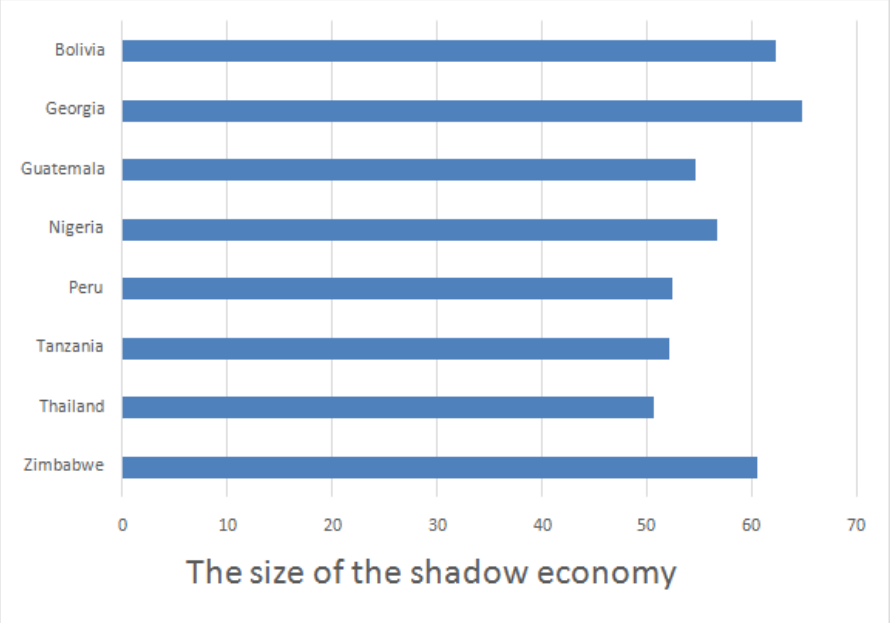

Figure3. The Average Size of the Shadow Economy in Countries with Struggling Economies, adapted from [18]

The informal economy can bring serious consequences to economic security, especially in software development. Informal activities are neither protected nor properly regulated. The growth prospects may be compromised due to the lack of information and social infrastructure. Because copyright protection is not properly delivered in some countries, the recommendation is to use other technologies. Currently, many major experts in authorship and ownership consider block chain technology a technology with good prospects [22]. In the light of the last study from IBM [26], the block chain technology seems to be pushing its way to the top most important information security technologies. The block chain and distributed registries found their application in the registration and confirmation of property rights. The information stored in the block chain is automatically encrypted. Thus, any information within the block is inaccessible to outsiders and useless to the individual developer. The block chain is a technology that changes the principle of doing business in many fields. It allows managing data much easier and in a more convenient way. The use of block chain provides confidence and transparency. This is a reliable way to store important information and securely enter into transactions, including those related to software development.

4. Discussion

Those, who adhere to the principles of supply chain management, see significant improvements in quality and productivity. Organizations that choose to ignore the security of components delivered through their supply chains suffer from the growing technical and security debt [31]. This comes with snowballing liability problems. A large number of cloud software systems are facing security threats, and even the sophisticated security tools and mechanisms are not able to detect it. Such prevailing problem necessitates the monitoring and controlling of the software development process and its maintenance. Security is considered to be one of the nonfunctional requirements that have significant effect on the architectural designing of the cloud software as a service. The evaluation results showed appearance of a significant number of security vulnerabilities in the early stages of software development life cycle, including developer espionage [4].Code virtualization built upon virtual machine technologies is emerging as a viable method for implementing code obfuscation to protect programs against unauthorized analysis [5]. On the one hand, many forms of lightweight static analysis have difficulties with even basic obfuscation schemes, which explains the unbroken popularity of obfuscation among malware writers. On the other hand, more expensive analysis techniques, in particular when used interactively by a human analyst, can easily defeat many obfuscation. [9]. Modern VM-based protection approaches use a fixed scheduling structure where the program always follows a single, deterministic execution path for the same input [5, 6]. Such approaches, however, are vulnerable in certain scenarios where the attacker can reuse knowledge extracted from previously seen software to crack applications protected with the same obfuscation scheme. As a result, software obfuscation for the purpose of intellectual property protection remains highly challenging [9]. It is important to produce software systems in a manner that is both efficient and secure. In this context, psychological trust of software

is a pertinent aspect of research [8]. It is also important to explore a personality as a moderator of the trustworthiness-reuse relationship to recruit right personnel for the software production. While the majority of security practice is focused on post-development products and enterprise approaches, some have sought to change the focus of security from the networks we manage to the systems we build [11, 12]. Thus, Heitzenrater proposed an initial model that captures the secure software engineering investment as a means of reducing defender uncertainty regarding vulnerabilities, while raising the cost to the attacker. This approach is instantiated as a companion process to traditional security models, and we use the Iterated Weakest Link (IWL) model of post-deployment security investment. The results indicate an increased return on security investment, as well as reduced post-deployment costs [11].Thus, it's possible to conclude that components of the program code must be secured not only while they go through the supply chain but also when they are being made. In this regard, the blockchain technology offers great promise for the software engineering applications.

Currently, distributed software development uses the blockchain system, which is almost impossible to crack. The GitHub platform hosts 24 million developers (as of October 2017) and houses projects for about 86.000 blockchain programs [21]. People use the platform due to the inefficiency of existing solutions, which are based on the principles of centralization and do not provide the necessary level of transparency and reliability. Instead of them, users tend to use blockchain. With this technology, users can ensure that all modules and subprograms, which they are going to use in the project, come from a proven and reliable source and meet all the necessary requirements. The use of blockchain raises standards, improves methods for developing software products and makes the work with freelancers more effective.

5. Conclusion

The software supply chain management is a must-have for all modern organizations. The ICT is developing at a rapid pace, stimulating the emergence of a variety of intellectual property products. In the country's economic development, the protection of intellectual property plays a significant role, which is evident from the 80% share of the intellectual capital in the national wealth of developed countries [23]. However, despite the low level of shadow economy in developed countries, the legal framework alone is not enough to protect the intellectual property rights, especially in the climate of rapidly developing ICTs. The obtained data did not confirm the hypothesis of a close relationship between the level of ICT development and the IPRI scores. The value of a correlation between two indices was in the range of 0.32-0.52 across countries. The correlation between the growth rate of IDI and the growth rate of IPRI was negative in the USA, Germany, Belgium, and India. The reason was probably the gap between the higher growth rates of IDI and the lower growth rates of IPRI. The software customers do not receive full protection of intellectual property rights, as it does not cover the protection against code copying and against the introduction of foreign programs into the software. We advise using a blockchain technology to develop software [32].To sum up, the existing mechanisms of legal regulation are not able to react fast enough to changes that occur in the software market, and this is when the latter requires new, innovative approaches, such as the blockchain technology.

References

[1] Omoronyia, I., Ferguson, J., Roper, M., & Wood, M. *A review of awareness in distributed collaborative software engineering*. nSoftware: Practice and Experience, 40(12), 1107-1133, 2010.

[2] Mckone-Sweet, K., & Lee, Y.-T. *Development and Analysis of a Supply Chain Strategy Taxonomy*. Journal of Supply Chain Management, 45(3), 3–24, 2009.

[3] Andreas, F., &Bodden, E. *ROPocop—Dynamic mitigation of code-reuse attacks*. Journal of Information Security and Applications,29, 16-26, 2016.

[4] Aljawarneh, S. A., Alawneh, A., &Jaradat, R. *Cloud security engineering: Early stages of SDLC*. FutureGenerationComputerSystems,74, 385-392, 2017.

[5] Kuang, K., Tang, Z., Gong, X., Fang, D., Chen, X., & Wang, Z.*Enhance virtual-machine-based code obfuscation security through dynamic bytecode scheduling*. Computers&Security,74, 202-220, 2018.

[6] Hosseinzadeh, S., Rauti, S., Laurén, S., Mäkelä, J. M., Holvitie, J., Hyrynsalmi, S., & Leppänen, V. *Diversification and obfuscation techniques for software security: A systematic literature review*. Information and Software Technology, 104, 72-93, 2018.

[7] Ge, X., Talele, N., Payer, M., & Jaeger, T. *Fine-grained control-flow integrity for kernel software*. Security and Privacy (EuroS&P), 2016 IEEE European Symposium on. IEEE, 2016.

[8] Ryan, T. J., Walter, C., Alarcon, G. M., Gamble, R. F., Jessup, S. A., &Capiola, A. A. *Individual differences in trust in code: The moderating effects of personality on the trustworthiness-trust relationship*. InternationalConferenceonHuman-ComputerInteraction. Springer, Cham, pp. 370–376, 2018.

[9] Schrittwieser, S., Katzenbeisser, S., Kinder, J., Merzdovnik, G., & Weippl, E. *Protecting software through obfuscation: Can it keep pace*

*with progress in code analysis?*ACM Computing Surveys (CSUR), 49(1), 4, 2016.

[10] TechRadar™: *Data Security and Privacy*, Q4 2017, Forrester Research, Inc., October 4, 2017.

[11] https://www.forrester.com/report/TechRadar+Data+Security+And+Privacy+Q4+2017/-/E-RES123881

[12] Heitzenrater, C., Böhme, R., & Simpson, A. *The days before zero day: Investment models for secure software engineering*. Proceedings of the 15th Workshop on the Economics of Information Security (WEIS), 2016.

[13] Dang, Y., Zhang, D., Ge, S., Huang, R., Chu, C., &Xie, T. *Transferring code-clone detection and analysis to practice*. Proceedings of the 39th International Conference on Software Engineering: Software Engineering in Practice Track. IEEE Press, 2017.

[14] Muhammad, K. *The Effects of Electronic Human Resource Management on Financial Institutes*. Journal of Humanities Insights, 02(01), 01-5, 2018.

[15] Abadi, M., Budiu, M., Erlingsson, Ú.,& Ligatti, J. *Control-flow integrity principles, implementations, and applications*. ACM Transactions on Information and System Security (TISSEC), 13(1), 4, 2009.

[16] Larsen, P., Homescu, A., Brunthaler, S., & Franz, M. *SoK: Automated software diversity.*2014 IEEE SymposiumonSecurityandPrivacy (SP). IEEE, 2014.

[17] Kuznetsov, V., Szekeres, L., Payer, M., Candea, G., Sekar, R., & Song, D.*Code-pointer Integrity. In USENIX Conference on Operating Systems Design and Implementation* (OSDI), 2014.

[18] International Property Right Index Report, 2018. [Electronic resource]. Assess mode: http://www.internationalpropertyrightsindex.org/

[19] State of the Software Supply Chain Report (2017). [Electronic resource]. Assess mode: https://www.sonatype.com/2017-state-of-the-software-supply-chain-report

[20] ICT Development index 2017 https://www.itu.int/net4/itu-d/idi/2017/index.html.

[21] *Measuring the Information Society Report* Volume 1 2017https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

[22] ICT development index. https://knoema.com/search?query=ict%20development%20index&source=HomePage

[23] The blockchain project development: basic steps. [Electronic resource]. Assess mode: https://coinnet.ru/razrabotka-blokchejn-proektov/

[24] Ito, K., & O'Dair, M. *A critical examination of the application of blockchain technology for intellectual property management.*Businesstransformationthroughblockchain, 2, 2018.

[25] Khodakov, V. E. *The impact of human capital and other socio-economic factors on the development of regional economic systems.* Problems of Information Technology, 21, 2017. (in Ukrainian).

[26] Akbari, A., Abbasian, M., & Jansooz, P. *Application of RAP Model in measuring the capabilities of attracting sources in the economy: A case study of the tourism sector in Sistan and Balucestan*. UCT Journal of Social Sciences and Humanities Research, 1(4), 12-15, 2013.

[27] Security issues when deploying DevOps. (In Russian). [Electronic resource]. Assess mode: https://www.ibm.com/developerworks/ru/library/d-security-considerations-devops-adoption/index.html

[28] Manshin, G. G., Artamonov, V. A., & Artamonova, E. V. *10 technologies to protect information and keep personal datasafe*. (In Russian). [Electronic resource]. Assess mode: http://itzashita.ru/publications/10-tehnologiy-informatsionnoy-bezopasnosti-i-konfidentsialnosti-personalnyih-dannyih.html

[29] *The Benefits of Blockchain to Supply Chain Networks. Watson Customer Engagement*. IBM Corporation, 2017

[30] Mohamed, B., Youness, K. I., & Mohamed, M. *Taking account of trust when adopting cloud computing architect*ure. Cloud Computing Technologies and Applications (CloudTech), 2016 2nd International Conference on. IEEE, 2016.

[31] Ulesko, I. N. *Ways to hide malware from antivirus programs using Windows scripts*. Novosibirsk, 2014. (In Russian). [Electronic resource]. Assess mode: https://nsu.ru/xmlui/bitstream/handle/nsu/1423/Text_UleskoIN.pdf

[32] Kitch, E. W. "*The law and economics of rights in valuable information*. WhoOwnsKnowledge?Routledge, pp. 35-76, 2017.