JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 June Volume 8 Number 4
http://doi.org/10.9770/jssi.2019.8.4(10)

Scopus®

CHALLENGES ON INTRODUCING INFORMATION SECURITY STANDARDS: A CASE STUDY

Olzhas Murashbekov

Ministry of Internal Affairs of the Republic of Kazakhstan, Almaty, Utepova Street, 29, 050060, Kazakhstan

E-mails: murashbekov@bk.ru

Received 11 January 2019; accepted 10 April 2019; published 30 June 2019

Abstract. The article discusses the current state and prospects for the further development (modernization) in the area of information security (IS) in Kazakhstan. Special attention is paid to the challenges that may arise when taking cyber security measures in relation to special requirements of standards to security and an independent IS audit at essential objects of the information and communication infrastructure (EOICI).The purpose of the study is to analyze the challenges on introducing modern standards of IS in the context of forming the national cyber security system in the Republic of Kazakhstan. The study has determined that the current challenges on introducing modern IS standards to maintain a high level of cyber security are related to the underdevelopment of the regulatory framework for the list of EOICI, the creation of an IS audit system and an information and analytical system to form national IS indicators. Recommendations have been given, and areas for the further study have been identified.

Keywords: national security; information security; cyber security; information security standard; essential objects of the information and communication infrastructure; information security audit; national indicators of information security

Reference to this paper should be made as follows: Murashbekov, 0. 2019. Challenges on introducing information security standards: a case study, *Journal of Security and Sustainability Issues* 8(4): 665–674. http://doi.org/10.9770/jssi.2019.8.4(10)

JEL Classifications: O31

1. Introduction

It is difficult to overestimate the importance of information for the security (IS) of the modern world. IS is often of high priority for a country, because it defines, on the one hand, the protection and, as a result, the sustainability of the main areas of the society's (country's) activity with respect to dangerous information impact (destabilizing, destructive, vulnerable, etc.) and, on the other hand, the intensity of the society's development in a particular area through the effective use of knowledge accumulated by the humanity (Polyakov, 2016, p. 11).

The analysis of scientific references about IS shows that most experts agree that IS is an integral part of the national security and is

1) The protection of vital interests of an individual, society and state, which minimizes the harm caused by incomplete, untimely and unreliable information or negative information influence, due to the negative consequences of information technologies, as well as due to unauthorized distribution of information,

2) The state of security of the information environment/space that ensures its formation, use and development in the interests of citizens, organizations, and the state (Vladimirova, 2012, p. 48).

Officially IS is defined in the Law of the Republic of Kazakhstan "On the National Security of the Republic of Kazakhstan" (2012). This is the protection of the information space of the Republic of Kazakhstan, as well

as the rights and interests of the person and citizen, society and state in the information area from real and potential threats, which ensures sustainable development and information independence of the country.

According to A.S. Grachev, A.A. Kortnev, and K.A. Lazunin, IS is the ability of the system to withstand accidental or deliberate internal and external threats – the ability to protect subjects from the impact of negative information, i.e., it is primarily associated with the activities of the state, because in most cases it goes about certain unauthorized actions with information (Grachev, Kortnev, Lazunin, 2017, p. 95).

There is no doubt that the main institution that acts as an IS agent is the state that takes security measures through a number of certain political institutions. Political IS measures include identification of unilateral and multilateral interests through the exchange of information and negotiations, objective informing about the essence of conflicts and crisis problems by mass media (MM), creation of conditions for the professional activity of MM in tension areas to provide the international community with reliable information and to form the relevant world opinion, informational support of political (referendums) and electoral processes, analytical monitoring over the compliance with fundamental human rights and freedoms, and informational contacts with opposition groups, nongovernmental organizations in order to efficiently achieve consensus between the confrontation parties (Horne, 2016; Kantemirova et al., 2018).

One of the IS components is cyber security. The International Telecommunications Union (ITU) defines it as follows: cyber security is a set of means, strategies, security principles, security guarantees, risk management approaches, actions, professional training, practical experience, insurance and technologies that can be used to protect cyberspace, resources of an organization and a user (Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity, 2018).

Referring to the analysis of international experience, the authors state that various regulatory documents define cyber security as

A set of organizational, legal, technical and educational measures aimed at ensuring continuous functioning of cyberspace (Cyberspace Protection Policy of the Republic of Poland),

The desired state of the information technology security when the risks to the cyberspace are minimized to the acceptable level (Cyber Security Strategy of Germany),

The desired state of an information system when it can counteract the challenges of cyberspace that may affect the accuracy, integrity and confidentiality of the data stored or processed by this system (Strategy for Security and Information Systems Defense of France), and

Protection of information systems that enter the cyberspace from attacks, ensuring the confidentiality, integrity and availability of the information processed in this space, detection and counteraction to attacks and cyber incidents (National Cyber Strategy of Turkey) (van der Meulen, 2015; Lisin, 2018; Shvetsova et al., 2018).

Table 1 shows legislative acts regulating cyber security in European countries.

Table 1. Legislative Acts Regulating Cyber Security (van der Meulen, 2015)

Country	Cyber strategy	Responsible authorities
Austria	National ICT Security Strategy (2012), Cyber Security Strategy (2013)	Lead group on cybersecurity, Expert Center against Cybercrime
Great Britain	National Cyber Security Strategy (2011)	Office of Cyber Security and Information Assurance, Center for the Protection of National Infrastructure
Spain	National Cyber Security Strategy (2013)	National Cryptologic Center, National Intelligence Center, National Security Service
Italy	Basics of the National Cyber Security Strategy (2013)	President of the Council of Ministers
Germany	Cyber security Strategy (2011)	Federal Office of Information Security
Poland	National Cyber Security Strategy (2007)	Ministry of National Defense, Internal Security Service
France	Strategy for the Security and Protection of Information Systems (2011)	National Service of Information Technologies Security
Czech Republic	National Cyber Security Strategy for 2015 – 2020	National Security Department, National Center of Cyber Security

Source: Compiled by authors

Most countries define the following main threats to the national cyberspace:

– Cyber espionage and military operations the state is aware of and supports. All technologically advanced states and corporations become an object of cyber espionage that aims at capturing state or industrial secrets, personal data or other valuable information,

– Use of the Internet for terrorist purposes. Terrorist groups use the Internet for propaganda and recruiting supporters.

– Cybercrime: theft of personal data and laundering of the illegally obtained funds. Attackers sell information on bank card numbers, passwords, and malware.

– As a rule, the national legislation of most countries regulates the issues related to personal data protection (Canada, the Netherlands, Sweden, and Finland), protection of e-commerce, security of electronic transactions and payment instruments (the USA, Canada, Poland, and Italy), and protection of important infrastructure objects and information systems (France) (Pupillo, 2018; Chernova et al., 2017; Sagiyeva et al., 2018).

Today most European countries are actively modernizing their own security sectors in compliance with the challenges, especially taking into account the potential of using the Internet. It comes with active reformation of management systems by the relevant security sector, normalizing the regulatory field, which should ensure the integrity of the state policy in this area; active explanatory work among the population on dangers of cyber threats; the increase in the number of units engaged in the cyber defense system; and strengthening the control over the national information space.

On October 6, 2016, by the Decree of the President of Kazakhstan, the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan (hereinafter referred to as the MDAI RK) was established (2016). One of the main activities of the MDAI RK is to pursue the state policy in IS in the area of informatization and communication (cyber security). By the same Decree, the Government of the Republic of Kazakhstan was ordered to establish the Committee for Information Security (hereinafter referred to as the CIS) that would actually fulfill functions of the authorized body (regulator) on developing the state policy in the area of the national IS.

According to the Concept of Cyber Security adopted on June 30, 2017 (Decree of the Government of the Republic of Kazakhstan No. 407, 2017), nowadays a set of national and harmonized technical standards in IS is being updated. In terms of compliance with IS, this primarily includes the development of relevant legal acts, the creation of a unified (universal) system of cyber threat indicators and the implementation of a national IS audit

system at essential cyber defense objects. In addition, the main subjects of the national cyber security should also be subject to audit that should be independent, regular and carried out in accordance with international auditing standards.

At the same time, according to the Law of the Republic of Kazakhstan "On Standardization" adopted on October 5, 2018 (2018), the principle of voluntary choice of standards (clause 1 Article 4) is approved unless otherwise established by the legislation of Kazakhstan. Thus, according to this legal norm, all cyber defense objects on the territory of Kazakhstan are a priori free in choice, use, and even in the development of IS standards. However, according to the second part of the same norm, there are restrictions for the Unified Requirements in Information and Communication Technologies and IS (hereinafter referred to as the Unified Requirements) approved by Decree of the Government of the Republic of Kazakhstan No. 832 dated December 20, 2016 (2016), and they are important enough. Thus, the Unified Requirements approve a special mode of standardization, certification, auditing, and responsibility for complying with the requirements of information and cyber security for EOICI.

The purpose of the study is to analyze problems on introducing modern IS standards in the context of forming the national cyber security system of the Republic of Kazakhstan.

The hypothesis of the study is as follows: the current problems of introducing IS standards to maintain a high level of cyber security are associated with the underdevelopment of the regulatory framework for the list of EOICI, the creation of an IS audit system and an information and analytical system for the formation of national IS indicators.

According to the results of the study, it is possible to conclude that the goal set in the study has been achieved

2. Methods

The study methodology is based on expert discussion related to determining the problems of introducing modern IS standards in the context of forming a national cyber security system of the Republic of Kazakhstan by using the moderation method.

Thirty-seven experts, employees of the CIS of the MDAI RK, as well as the management of private IT companies involved in ensuring cyber security of enterprises and organizations participated in the expert discussion.

The experts were challenged to define the main problems of introducing modern IS standards (cyber security).

The expert discussion aimed at determining the importance of the problem arising in this aspect. At the same time, the use of moderation instruments allowed managing and channeling the discussion.

The results of the discussion were processed by defining the main problems of introducing modern IS standards during the discussion and assessing the consistency of expert opinion according to the concordance coefficient (W).

3. Results

During the expert discussion by using the moderation method, three main problems of introducing modern IS standards (cyber security) were identified:

– Underdeveloped list of EOICI,

– Need to create an IS audit system, and

– Need in an information and analytical system to form national IS indicators.

Table 2 shows the consistency of expert opinion on the importance of each of the problems (calculation of the concordance coefficient).

Table 2. Calculation of the Concordance Coefficient

	Problem			
	EOICI	IS audit	System of IS national indicators	Σ
Sum of ranks (Σx_i)	42	70	110	222
Deviation from the average sum of ranks ($x - x_{av}$)	-32	-4	36	-
Squares of deviations of rank sums $(x - x_{av})^2$	1,024	16	1,296	2,336

Source: Compiled by authors

W = 12 S / m2 (n3 – n), where m is the number of experts,

$W = 12 \cdot 2{,}336 / 372 (33 - 3) \approx 0.853$

Thus, it is possible to consider that the experts' opinions on the importance of each problem are rather coordinated.

Discussion

According to Kaspersky Lab, the CIS cybercrime market doubles every two years, and Kazakhstan has become one of the top ten countries by the number of users attacked by mobile banking Trojans (position 10), mobile extortionists Trojans (position 3), miners (position 4), where users underwent the highest risk of being infected via the Internet (position 10). (Development of information threats in the second quarter of 2018. Statistics, 2018) At the same time, for the first nine months of 2018 about 1.5 thousand cybercrimes were registered in the financial sector of Kazakhstan. The level of crimes has increased five times over the past three years (Cybersecurity strategy in the financial sector of the Republic of Kazakhstan for 2018 – 2022, 2018).

The above reinforces the urgency of analyzing the problem of introducing modern IS (cyber security) standards. Speaking about the underdevelopment of the EOICI list, the experts state that it is necessary to ensure the following for all EOICI:

• Mandatory IS requirements (as set by the Government of Kazakhstan), including those to their creation, commissioning, operation and modernization, taking into account international standards and the specifics of the industry the relevant EOICI belong to,

• Mandatory independent IS audit, and the procedure and requirements to it must be also centrally approved by the Government of Kazakhstan, and

• Responsibility of owners and/or managers of enterprises, institutions and organizations included in the list of EOICI to ensure cyber protection of their communication and technological systems, to protect technological information in accordance with the requirements of the law, to promptly report cyber security incidents, and to organize an independent IS audit at such objects.

As on April 2019, due to the lack of legal acts and bylaws, all these requirements to EOICI are practically not specified, as well as there is no system and the list of EOICI.

At the same time, state information resources or sensitive information should be processed in the system using a comprehensive IS system with confirmed compliance. Obviously, almost all future EOICI are included here, which in its turn means that in accordance with the Unified Requirements, today they must comply with the requirements of the national standard ST RK GOST R ISO/MEK 15408-2006 "Information Technology.

Methods and Means of Security. Criteria for Assessing the Security of Information Technology".

However, in any case, the obligation to use ST RK GOST R ISO/MEK 15408-2006 is caused not by referring to EOICI as a cyber security object, but by the mode of access to the information processed in the system. Thus, obviously, a considerable number of EOICI will fall under the effect of the above standard, but, firstly, not all of them, and secondly, above all, these will be government agencies and departments.

Meanwhile, Kazakhstan continues harmonizing and introducing modern international IS standards, above all, a series of international standards ISO/IEC 27000, developed by the International Organization for Standardization (ISO) together with the International Electrotechnical Commission (IEC) that is constantly supplemented by new documents. The series is a model (framework) for the development, implementation, operation, monitoring, analysis, support and improvement of the information management system both at the general level (27001) and in certain sectors and industries – finance, transport, energy, healthcare, telecom operators, cloud computing, infrastructure projects, auditing and certification, etc. (Lipina et al., 2017; Limba et al., 2017; Luhn rt al., 2017).

The implementation of an IS management system (ISMS) in accordance with ISO/IEC 27000 makes it possible to optimize the protection of information resources and management of risks for these resources. Due to this, and also due to upgrading of standardization systems and procedures for ordinary cyber security objects, as a whole, the situation in this area is developing optimally.

However, the issues related to forming the basis of EOICI, including the "membership conditions" in it and methods of protection, remain problematic and much urgent at the same time. Due to the fact that the recently adopted Cyber Security Concept provides much stricter and more responsible requirements and the compliance with cyber security for EOICI as compared to other cyber security objects, the method and criteria for forming the list of EOICI have become special in Kazakhstan (it will directly influence the choice of objects that will and will not fall under these strict standards).

The experts formulated two criteria. According to them, the information and telecommunication system (ITS) of an object can be referred to as essential infrastructure. They are 1) a list of industries that are strategically important for the functioning of the economy and the security of the state, society and population, 2) the nature of possible negative effects in various areas in case of a cyber attack on ITS.

In the experts' opinion, it is also necessary to scale "negative impact" on the ITS of an object (for example, duration, territorial coverage, estimated losses, threat to the national security, etc.) and, according to this scale, referring it to essential/non-essential infrastructure.

However, the experts explain that if such assessment is made by the CIS of the MDAI RK based on the lists provided by the executive authorities and other interested bodies in a nonpublic manner and guided by extremely vaguely defined criteria (which allows for their arbitrary interpretation), it seems to be a rather controversial approach, because the procedure for creating the first national registry of EOICI, apparently, requires more extensive communications and consultations – including with the nongovernmental sector. As for preparing the above offers by the sectoral executive authorities, it would be much more efficient if it involved the participation of specialists in the area of national security and ICT and relevant specialists.

In addition, according to the experts, it is necessary to provide mechanisms for continuous monitoring and updating the list of EOICI, which is necessary, taking into account the dynamics of socio-economic changes, on the one hand, and the escalation of cyber threats, on the other hand. The international experience proves it. At the same time, according to the experts, it is necessary that the formation of the EOICI list does not create prerequisites for excessive and unreasonable burden on small and medium-sized enterprises most of which must not be referred to as the essential infrastructure. In this regard, one of the experts (Sergey K., 34 years old) insists that "when preparing legislative offers for introducing responsibility for the violation of the requirements

to cyber defense", it is necessary "to clearly define the subjects that are the owners (managers) of EOICI" "based on their importance, in particular, for the national security and defense of the state".

In addition, the experts believe that the dynamics of the modern processes do not allow "clearly defining" such "subjects" once and forever. Therefore, there should be a clear and understandable methodology and a thoroughly coordinated system of the most specific (up to approving accurate indicators wherever possible) criteria for classifying cyber defense objects as EOICI. It will also have to be reviewed periodically, but at reasonable intervals. It is important that this system allows for the minimum possible number of ambiguous interpretations. This would help to optimize the process of forming the final registry, and would reduce the risks of interdepartmental fights, duplication of powers and corrupt practices. In the future, the EOICI registry, as well as the methodology for its formation will obviously have to be adjusted directly in practice, in the "real-time mode".

The identification, categorization and registration of EOICI are a difficult problem not only in Kazakhstan, but also in other states. It is solved very differently in various countries. There is considerable international experience that is being studied in some places in Kazakhstan, although mostly superficially, in the context of a broader perspective. At the same time, the urgency of the problem and the unsatisfactory level of its legal understanding indicate the need in further scientific and analytical study in this area.

According to the expert opinion, in the area of cyber security, it is necessary to form a list of international standards in the area of electronic communications, information protection, information and cyber security that must be translated and harmonized. Besides, it is necessary to implement their standards and introduce the IS audit system in government agencies and essential infrastructure objects. As a part of these plans, the CIS must develop a number of draft regulations regarding the implementation of the IS audit system, ensure the implementation of IS audit at essential infrastructure objects, set requirements to IS auditors, determine the order of their certification (recertification), coordinate, organize and carry out the audit of the security of EOICI communication and technological systems for vulnerability.

Thus, the CIS must develop a Concept for the introduction of the IS audit system that should define the basic principles for introducing and implementing the IS audit system in Kazakhstan, a procedure for certifying IS auditors, their training and appraisal, and relevant control over the completeness and adequacy of service provision in this area at set intervals after the certificate is submitted, as well as systematization and generalization of the IS audit results by submitting reports to central and specialized authorities. In addition, a model for the IS audit system functioning should be offered and the main stages of its implementation in Kazakhstan should be defined.

At the same time, according to the experts, it is supposed to accredit auditors/auditing organizations for checking IS according to the modern international standard ISO/IEC 17024-2014 "Conformity assessment. General requirements for personnel certification bodies" that was confirmed and enacted in Kazakhstan in 01.01.2017. It is supposed to audit IS management systems (ISMS) in accordance with the ST RK ISO/IEC 27001-2015 standard that is generally consistent with international practices.

The idea of experts about "creating an information and analytical system for forming the national IS indicators" can be also considered as relevant to the current European standards and practices. Kazakhstan does not pay special professional attention (with some exceptions) to this issue, while the world is actively conducting relevant research and development. For example, IS indicator complexes were developed and standardized several years ago by the European Telecommunications Standards Institute (ETSI), an influential international nonprofit organization that brings together representatives of the European and global telecom industry and is officially recognized by the European Commission as the leading agency in the development of industry standards. The international standard ISO/IEC 27004-2016 is also devoted to monitoring, measuring, analyzing and evaluating security in IS management (i.e., defining technologies based on quantitative indicators – quality characteristics). The above ETSI methodology was developed in accordance with it.

Taking into account such world experience and the general orientation of the Kazakh sectoral legislation to international standards, it would be logical to harmonize or confirm the relevant standards by the Gosstandart of the Republic of Kazakhstan, formally put them into action, and further develop national IS indicators based on them, as well as to introduce the information and analytical system to form them. This way is typical, for example, for EU and many other countries. The practice shows that it provides the minimum cost with the maximum effect: safety standards are complied with, IS is strengthened and, due to the unified nature of standards, international/cross-border exchanges are not restrained.

However, some experts offer another approach:

– The creation of a "central part" (and later "territorial parts") of an information-analytical system for the formation of national IS indicators that will provide an opportunity to monitor and inform central and specialized authorities of Kazakhstan "on the status of IS in certain institutions, regions, and the state, as a whole",

– The creation of an integrated IS system (ISIS) with the confirmed correspondence in the information-analytical system of forming the national IS indicators,

– Periodic "works on reviewing threats to information" in this information-analytical system, assessment of its sustainable functioning and "if necessary, an increase in the capacity of the system".

In this case, the experts say, first of all, about creating a specialized intradepartmental (controlled by CIS) administrative-bureaucratic vertical that covers the whole territory of Kazakhstan, supervisory control functions and the possibility of further expansion ("capacity increase") based only on the relevant intradepartmental decision.

It is necessary to note that the idea of a "system to form the national IS indicators" correlates little with the Cyber Security Concept that does not mention a system of national IS indicators.

The approach to solving the key issue offered by some experts – IS audit in Kazakhstan – is ambiguous. Some experts consider the following variant as the only true: "introducing an IS audit system at the national level and using IS audit services that can be provided by national (the context makes it clear that it is in contrast to international, according to the "or-or" principle) auditors (companies)". It is necessary to state that such model does not meet both international standards and the most successful international practices of carrying out the IS audit. It is well known that the activities of international audit companies (including sensitive areas, such as verification of EOICI IS) in the modern world are one of the foundations and constants of the adequate functioning of states and economies. The idea of refusing, even minimizing their participation in the IS audit at Kazakh objects, based on national security considerations, is somewhat ambiguous, because it can considerably narrow down the possibilities of creating modern audit mechanisms.

Some experts consistently pursue the idea of creating a closed cycle unified IS audit system (from training centers for auditors to a network of certified auditing institutions) as a part of CIS on the whole territory of Kazakhstan. Its scope would allow "monitoring the protection of information resources in the state, which would provide online information about the real state of IS in certain institutions, regions and in the state as a whole". To a large extent, it complies with the requirements of the Cyber Security Concept. At the same time, it is necessary to take into account that attempts to create an IS audit system by using a similar model in the real life will cause an excessive concentration of relevant functions and resources in one department, which in its turn will generate a whole range of risks – administrative, regulatory, economic, etc.

Conclusion

1. Currently the national cyber security system of Kazakhstan, as well as its components such as IS standardization and certification and the associated regulatory and legal framework (bylaws) are being formed.

2. The modernization of the relevant legislation (the Kazakh Law "On Standardization"), as well as institutions and standardization procedures for ordinary cyber defense objects contributed to developing the situation in this area in the optimal direction — the IS standardization base is becoming more and more modern and diversified in Kazakhstan, industry international standards are being actively harmonized.

3. The cyber security remains potentially problematic. It includes the cyber defense of the objects related to EOICI, more precisely, the mandatory audit of compliance with the IS standard (and mandatory) requirements by such objects.

4. One of the ways to solve the problem is to organize consultations and establish cooperation between CIS specialists and reputable auditing companies (such as PricewaterhouseCoopers or Ernst & Young), specialized international organizations (such as ENISA or ISACA), and industry professional associations. Such interaction aims at searching for a confirmed mode of the IS audit system that would meet international standards in this area.

5. Despite the fact that the formation of the IS audit system will be directly related to the activities of a significant pool of (future) nongovernmental EOICI, it is necessary to consider the feasibility of organizing a number of consultations between the subjects of the national cyber security system (chaired by the CIS) and the responsible representatives of those nongovernmental objects that are the most important for ensuring the information security and, in general, the national security of Kazakhstan in order to:
a) Coordinate positions on the conceptual vision of the IS audit system,
b) Elaborate practical issues related to functioning of this system directly in relation to nonstate EOICI.

6. It is necessary to ensure the publicity of reports (as an annual report) of subjects of the national cyber security system of Kazakhstan about the state of implementing the provisions of the Cyber security strategy.

7. In order to properly protect EOICI from cyber attacks, it is essential to additionally study the international expertise in this area, recommendations of specialized international organizations, and the possibility of using them in Kazakhstan. In the future, taking into account the studied material, it is necessary to form a confirmed regulatory framework regarding the identification, registration and categorization of EOICI.

References

Chernova, V. Y.; Zobov, A. M.; Starostin, V. S.; Butkovskaya, G. V. 2017. Sustainable marketing communication strategies of Russian companies under the import substitution policy, Entrepreneurship and Sustainability Issues 5(2): 223-230. http://doi.org/10.9770/jesi.2017.5.2(5)

Grachev, A.S., Kortnev, A.A., Lazunin, K.A. (2017). Obshchiye problemy obespecheniya informatsionnoy bezopasnosti gosudarstva v sovremennom sociume [Common problems of state information security in the modern society]. Information and Space, 3, 94 – 97.

Guide to developing a national cybersecurity strategy – Strategic engagement in cybersecurity. (2018). http://handle.itu.int/11.1002/pub/811cf62d-en

Horne, C.A. (2016). A theory on information security. Australasian Conference on Information Systems, Wollongong, 11.

Yedinye trebovaniya v oblasti informatsionno-kommunikatsionnyk tekhnologiy i obespecheniya informatsionnoy bezopasnosti. Utv. postanovleniyem Pravitelstva RK ot 20 dekabrya 2016 goda No. 832 [Uniform requirements in the area of information and communication technologies and information security. Approved by Resolution of the Government of the Republic of Kazakhstan dated December 20, 2016 No. 832] https://tengrinews.kz/zakon/pravitelstvo_respubliki_kazahstan_premer_ministr_rk/kultupa/id-P1600000832.

Kantemirova, M.A.; Dzakoev, Z.A.; Alikova, Z.R.; Chedgemov, S.R.; Soskieva, Z.V. 2018. Percolation approach to simulation of a

sustainable network economy structure, Entrepreneurship and Sustainability Issues 5(3): 502-513. https://doi.org/10.9770/jesi.2018.5.3(7)

Limba T.; Agafonov K.; Paukštė L.; Damkus, M.; Plėta T., 2017. Peculiarities of cyber security management in the process of internet voting implementation, Entrepreneurship and Sustainability Issues 5(2): 368-402. http://doi.org/10.9770/jesi.2017.5.2(15)

Lipina, S.A., Lochan, S.A., Fedyunin, D.V., Bezpalov, V.V. (2017). Government promoting communication tool in innovation development of companies. European Research Studies Journal, 20(4B), 536 – 547. http://doi.org/10.11214/thalassinos.20.07.040

Lisin, E.; Kurdiukova, G.; Ketoeva, N. 2018. Sustainability issues of territorial power systems in market conditions, Entrepreneurship and Sustainability Issues 6(2): 1041-1052. http://doi.org/10.9770/jesi.2018.6.2(38)

Luhn, A.; Aslanyan, S.; Leopoldseder, Ch.; Priess, P. 2017. An evaluation of knowledge management system‘s components and its financial and non-financial implications, Entrepreneurship and Sustainability Issues 5(2): 315-329. http://doi.org/10.9770/jesi.2017.5.2(11)

Polyakov, V.P. (2016). Aspekty informatsionnoy bezopasnosti v informatsionnoy podgotovke [Aspects of information security in information training]. Moscow: FSBSE “IUO RAO”, 135. http://iuorao.ru/wp-content/uploads/2017/08/%D0%9F%D0%BE%D0%BB%D1%8F%D0%BA%D0%BE%D0%B2-%D0%B2%D0%B5%D1%80%D1%81%D1%82%D0%BA%D0%B0.pdf

Postanovleniye Pravitelstva Respubliki Kazakhstan ot 30 iyunia 2017 goda No. 407 “Ob utverzhdenii Kontseptsii kiberbezopasnosti (“Kibershchit Kazakhstan”)” [Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407 “On Approving the Concept of Cyber Security (“Kazakhstan Cybershield”)] http://base.spinform.ru/show_doc.fwx?rgn=98630

Pupillo, L. (2018). EU Cybersecurity and the paradox of progress. CEPS Policy Insight, 2018-06. https://www.ceps.eu/system/files/PI2018_06_LP_ParadoxProgress.pdf

Razvitiye informatsionnyh ugroz vo vtorom kvartale 2018 goda. Statistika [Development of information threats in the second quarter of 2018. Statistics] https://securelist.ru/it-threat-evolution-q2-2018-statistics/90919.

Sagiyeva, R,; Zhuparova, A.; Ruzanov, R.; Doszhan, R.; Askerov, A. 2018. Intellectual input of development by knowledge-based economy: problems of measuring in countries with developing markets, Entrepreneurship and Sustainability Issues 6(2): 711-728. http://doi.org/10.9770/jesi.2018.6.2(17)

Shvetsova, O.A.; Rodionova, E.A.; Epstein, M. Z. 2018. Evaluation of investment projects under uncertainty: multi-criteria approach using interval data, Entrepreneurship and Sustainability Issues 5(4): 914-928. http://doi.org/10.9770/jesi.2018.5.4(15)

Strategiya kiberbezopasnosti finansovogo sektora Respubliki Kazakhstan na 2018 – 2022 gody. Utverzhdena Postanovleniyem Pravleniya Natsionalnogo Banka Respubliki Kazakhstan ot 29 oktyabrya 2018 goda No. 281 [Cybersecurity strategy in the financial sector of the Republic of Kazakhstan for 2018 – 2022. Approved by Resolution of the Board of the National Bank of the Republic of Kazakhstan dated October 29, 2018 No. 281] http://base.spinform.ru/show_doc.fwx?rgn=111254

Ukaz Prezidenta Respubliki Kazakhstan ot 6 oktyabrya 2016 goda No. 350 “Ob obrazovanii Ministerstva oboronnoy i aerokosmicheskoy promyshlennosti Respubliki Kazakhstan” [Decree of the President of the Republic of Kazakhstan dated October 6, 2016 No. 350 “On Establishing the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan”] https://online.zakon.kz/Document/?doc_id=35551363

van der Meulen, N. (2015). Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. – Brussels. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

Vladimirova, T.V. (2012). Informatsionnaya bezopasnost: k metodologicheskim osnovaniyam analiza voprosa [Information security: on the methodological basis for the analysis of the issue]. Informational Community, 5, 47 – 52. ISSN: 1606-1330

Zakon Respubliki Kazakhstan ot 5 oktyabrya 2018 goda No. 183-VI “O standartizatsii” [Law of the Republic of Kazakhstan dated October 5, 2018 No. 183-VI “On Standardization”]. https://online.zakon.kz/Document/?doc_id=38448599#pos=49;-255

Zakon Respubliki Kazakhstan ot 6 yanvarya 2012 goda No. 527-IV “O natsionalnoy bezopasnosti Respubliki Kazakhstan” (s izmeneniyami i dopolneniyami po sostoyaniyu na 28.12.2018 g.) [Law of the Republic of Kazakhstan dated January 6, 2012 No. 527-IV “On the National Security of the Republic of Kazakhstan” (amended as on December 28, 2017)] https://online.zakon.kz/Document/?doc_id=31106860#pos=3;-255