UDC 004.056.1

Peculiarities of the legal regulation of cybersecurity in the National Laws of Lithuania, Russia and the USA: cybersecurity strategies

Stitilis Darius
Full Doctor of Law, professor,
head of the committee of the "Right of new technologies" program,
Mykolas Romeris University,
P.O. Box 08303, Ateities str., No. 20, Vilnius, Lithuania;
e-mail: stitilis@mruni.eu

Klisauskas Valdas
Assistant,
Mykolas Romeris University,
P.O. Box 08303, Ateities str., No. 20, Vilnius, Lithuania;
e-mail: v.klisauskas@gmail.com

Abstract

Purpose – To analyse the legal/regulatory framework of cybersecurity in the Republic of Lithuania, the Russian Federation and the United States of America to the extent it is related to cybersecurity strategies.

Methodology – Several different methods were used to carry out the research: the authors used the method of comparison to research the legal framework of cybersecurity (cybersecurity strategies) of Lithuania, Russia and the United States of America (hereinafter – the USA). The method of empirical analysis of legal documents was used to determine the strategic legal regulation of cybersecurity in force in Lithuania, Russia and the USA. The research included the analysis of the legal regulatory acts – cybersecurity strategies – of the Republic

of Lithuania, the Russian Federation and the USA. This method allows, after performing the analysis of the official documents, to accurately identify and describe the relevant relationship among the existing legal regulations. When using references to academic literature, the authors used the method of deduction, allowing to draw sufficiently reliable conclusions. For the analysis of concepts, the authors used the latest academic literature and dictionaries.

Findings – The research has revealed that information technologies are dynamic. In our opinion, the governments of the Republic of Lithuania, the Russian Federation and the USA cannot stand still and must go forward to align their legislative and technical framework with the changing information technologies by ensuring their protection at international level.

Research limitations – Although the analysis of the legal regulation of cybersecurity can be done by analysing and comparing the legal acts of different levels, the research was carried out by comparing only the key, strategic legal acts – national programs of Lithuania, Russia and the USA.

Practical implications – The results of the research can be applied to draw up new legislation or to make amendments to the existing legal acts with regard to cybersecurity.

Originality/Value – The article presents a research which is new in Lithuania. The analysis of the legal acts of the Republic of Lithuania, the Russian Federation and the USA regulating cybersecurity has not been conducted yet. The results of this research fill in this void.

Research type – presentation of the research, presentation of the approach.

Keywords

Cybersecurity, cybersecurity strategies, legal regulation.

Introduction

As information technologies develop and advance forward, there arise limitless opportunities for the development of the global Internet, transfer and storage of information in cyberspace. However, this also leads to negative consequences, such as the loss of important electronic information or even cybercrime. The security

of electronic information, also called as cybersecurity, also requires coherent and detailed legal regulation.

Cyberse[1]curity is even described as "the cornerstone of the information society"[2]. Recently, all countries all over the world are increasingly focusing on the security of electronic information, and the Republic of Lithuania, the Russian Federation and the USA are not the exception. Top state leaders also speak out about the importance of cybersecurity. "To create a mechanism for information sharing in order to better protect critical information systems, we have established a communication channel and information sharing arrangements between our computer emergency response teams", – Barack Obama and Vladimir Putin, Presidents of the USA and Russia agreed on the improvement of cybersecurity during their discussions at the Group of Eight (G8) summit.[3]

When attending the Munich Security Conference, Dalia Grybauskaitė, President of the Republic of Lithuania, pointed out that cybersecurity issues are no longer a matter of NATO's competence only – they are becoming increasingly important to the European Union as well. Not only with regard to protection of countries, their institutions and organizations, but also of individuals which is growing more and more urgent[4]. Thus, from the above statements it can be seen that cybersecurity is one of the countries' priority areas in order to manage them effectively, by ensuring continuous state and social processes as well as the security of citizens.

Cybersecurity strategies are one of the key documents in the legal regulation of cybersecurity (Štitilis D., Paškauskas Ž., 2007).[5] These are the cor-

1 Danyushina, Yu.V. (2011), "Kommunikativnaya bezopasnost' v gosudarstvennom i delovom upravlenii" ["Communicative safety in the state and business management"], *Language. Philology. Culture*, No 1, pp. 66-80.

2 Schjolberg, S., Ghernaouti-Hele, S. (2011), "A Global Treaty on Cybersecurity and Cybercrime. Geneva", available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

3 "Agenda of the meeting on cybersecurity held between Barack Obama and Vladimir Putin, Presidents of the USA and Russia. 2013, Northern Ireland", available at: http://en.rian.ru/russia/20130618/181726010/Cybersecurity-High-on-Agenda-of-Obama-Putin-Meeting.html

4 "Press release of Dalia Grybauskaitė, President of the Republic of Lithuania. 2012, Munich", available at: www.president.lt/lt/spaudos_centras_392/pranesimai_spaudai/kibernetinis_ir_energetinis_saugumas_-_lietuvos_prioritetas.html

5 Štitilis, D., Paškauskas, Ž. (2007), "State's Electronics Information Security Strategy – One of Key Electronic Information Security Regulatory Instruments: Com-

nerstone legal acts, on the basis of which the legislative framework in the area of cybersecurity is developed. All of the above-mentioned countries have already adopted strategic legal acts, guidelines for ensuring the legal regulation of cybersecurity. Lithuania has the Cybersecurity Programme for 2011-2019, approved by the Resolution of the Government of the Republic of Lithuania[6]. Russia also has the Doctrine of the Information Security of the Russian Federation[7] that was adopted in 2000. The USA has the International Strategy for Cyberspace[8] that was adopted in 2011. It should also be noted that in 2013 the Cybersecurity Strategy of the European Union[9] was also adopted in the European Union (hereinafter – the EU). As can be seen in Lithuania and in Russia and in the USA, there is a strong focus on solving this problem and this is evidenced by the adopted strategic legal acts. Thus, it can be said that Russia and the USA do pay attention to the threats related to cybersecurity. In view of the experience gained by the Russian Federation and the USA in the field of cybersecurity, we believe that it would be appropriate to more thoroughly analyse the strategic legal acts regulating cybersecurity in Lithuania, as a member of the EU, as well as those in Russia and the USA, and to draw adequate conclusions.

Strategic Legal Acts in the Field of Cybersecurity in Lithuania, Russia and the USA

Every policy-making process in every relevant field, at both national and international levels, starts from initiatives, strategies or concepts. So, in this article we will discuss the strategic – legal regulation of public relations in the field of cybersecurity in Lithuania, Russia and the USA (we will analyse strategies), since the development of a more detailed

parative Analysis", *Jurisprudencija*, No. 2(92), pp. 37-45.

6 "Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 "On the Approval of the Programme for the Development of Electronic Information Security (Cybersecurity) for 2011-2019", *Valstybės žinios*, No. 83-4033, 2011; No. 106 (correction).

7 "Doctrine of the Information Security of the Russian Federation" ["Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii"], available at: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

8 "International Strategy for Cyberspace", available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

9 "Cybersecurity Strategy of the European Union, 2013, Brussels", available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

legal framework depends on this. Taking into consideration the purpose of this research paper, strategies will be analysed from a comparative perspective.

In Lithuania, the first National Strategy for the Security of Electronic Information in the Information Systems of Public Institutions was approved in 2006 and remained in force until 2008[10]. This Strategy was limited to the public sector. The currently effective Programme for the Development of Electronic Information Security (Cybersecurity) for 2011–2019 (hereinafter – the Lithuanian Programme) was approved by Resolution No. 796 of the Government of the Republic of Lithuania of 29 June 2011[11]. This Lithuanian Programme outlines the main problems of electronic information security (cybersecurity), determines the objectives and tasks for the development of electronic information security (cybersecurity). The objectives and tasks set out in this Programme are focused on both the public and private sectors. In Russia, the Doctrine of the Information Security of the Russian Federation, approved by the President of the Russian Federation on 9 September 2000[12] (hereinafter – the Russian Doctrine), is the strategic document that defines the state policy in the field of cybersecurity. The Russian Doctrine is intended to conceptualize the Russian public sector's policy in the field of electronic information security.

It should be noted that currently the temporary working group of the Information Society Council of the Russian Federation is preparing the Russian cybersecurity strategy, which, according to Ruslan Gattarov, will be simple and understandable for every citizen[13]. However, we have failed to find the draft of this cybersecurity strategy in public space, therefore in this article we will refer to the Russian Doctrine of 2000.

In the USA, great attention is also paid to ensuring cybersecurity. One of the most recent strategic documents re-

10 However, this strategy was limited to the sector of public institutions.

11 "Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 "On the Approval of the Programme for the Development of Electronic Information Security (Cybersecurity) for 2011-2019", *Valstybės žinios*, No. 83-4033, 2011; No. 106 (correction).

12 "Doctrine of the Information Security of the Russian Federation" ["Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii"], available at: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

13 "Press Release of the Council of the Russian federation", available at: http://council.gov.ru/press-center/news/14575/

lated to cybersecurity in the USA is the International Strategy for Cyberspace (hereinafter – the USA Strategy), adopted in 2011.[14] From the very title of this Strategy we can see that the USA, being aware of the benefits and threats of the "global" Internet, seeks to ensure cybersecurity internationally. Thus, this Strategy identifies the core principles and policy priorities in the area of cybersecurity, by emphasizing that only diverse collaboration between the public and private sectors, international collaboration can reduce the threats of cyber incidents and ensure cybersecurity. So, we would like to point out that this Strategy is focused on both the private and public sectors.

In 2011, the Russian Federation, as well as the United States, adopted strategic documents, such as the Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space[15] and the Department of Defense Strategy for Operating in Cyberspace[16]. We will not, however, discuss these documents here, because they are intended only for the regulation of only a narrow area of cybersecurity.

Analysis of Strategic Legal Acts on Cybersecurity in Lithuania, Russia and the USA

1) Programme for the Development of Electronic Information Security (Cybersecurity) for 2011–2019 of the Republic of Lithuania.

When analysing the Lithuania Programme, its paragraph 2 stipulates a rather specific and ambitious strategic objective to be achieved by 2019 – the development of the security of electronic information in Lithuania, ensuring cybersecurity in order to achieve, in the year 2019, a 98 per cent level of compliance of state-owned information resources with legislative requirements on electronic information security (cybersecurity), reduction to 0.5 hour of the average time of response to critical infor-

14 "International Strategy for Cyberspace", available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

15 "The conceptual views on the activities of the Armed Forces of the Russian Federation in the information space" ["Kontseptual'nye vzglyady na deyatel'nost' Vooruzhennykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve"], available at: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

16 "Department of Defense Strategy for Operating in Cyberspace. 2011, Washington", available at: www.slideshare.net/DepartmentofDefense/department-of-defense-strategy-for-operating-in-cyberspace

mation infrastructure incidents and a 60 per cent level of the Lithuanian residents who feel secure in cyberspace.[17]

To summarize the provisions set forth in paragraphs 6-10 of the Lithuanian Programme, it can be stated that this Programme establishes the following objectives and tasks to be achieved:

– To ensure the security of state-owned information resources. In order to achieve this objective, the following tasks shall be implemented: to improve the coordination and supervision of electronic information security (cybersecurity); to improve the regulatory framework of electronic information security (cybersecurity); to expand and improve a secure national information infrastructure; to promote the implementation of electronic information (cybersecurity) projects; to develop international cooperation in the area of electronic information security (cybersecurity).

– To ensure an efficient functioning of critical information infrastructure. In order to achieve this objective, it is necessary to implement the task of ensuring the security of critical information infrastructure.

– To seek to ensure the cybersecurity of the Lithuanian residents and persons staying in Lithuania. In order to achieve this objective, the following tasks must be implemented: to enhance the culture of protection of electronic information security (cybersecurity); to strengthen Lithuania's cyberspace security; to ensure the protection of Lithuania's virtual cyber perimeter from external cyber attacks; to reinforce the security of services delivered in cyberspace.[18]

In addition to the objectives and tasks to be achieved, the Annex to the Lithuanian Programme also stipulates the assessment criteria for the Programme's implementation and their indicators to be attained in 2011, 2015 and 2019, as well as the institutions responsible for the implementation of the above criteria. It should be noted that the established indicators of the assessment criteria are specific and ambitious, but it is not clear how realistic they are, because most of the indicators have not been assessed at all until the adoption of the Lithuanian Programme, for example, the Programme provides that, by the year 2015, the level of information resources using the secure infrastructure will reach 70 per cent, and

17 "Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 "On the Approval of the Programme for the Development of Electronic Information Security (Cybersecurity) for 2011-2019", *Valstybės žinios*, No. 83-4033, 2011; No. 106 (correction).

18 Ibid.

by 2019 – 100 per cent, although it is not known what this indicator was in 2011. In our view, taking into consideration the fact that indicators of the most of the assessment criteria are not known, it had to be stipulated in the Lithuanian Programme that the first assessment would have to be done much earlier than 2015, in order to determine the initial values of relevant indicators (i.e., to assess the current situation), and only then it would be possible to consistently establish the indicators to be attained in further years to come.

In addition, in our opinion, some of the indicators may be difficult to accurately assess at all, for example, as laid down in the Programme, the percentage of the Lithuanian population who feel secure in cyberspace in 2015 should reach 40 per cent, and in 2019 – already 60 per cent, though it is not clear how this feeling of security will be evaluated. Although the Lithuanian Programme devotes much attention on raising the society's awareness in the field of electronic information, it lacks, in our opinion, more specific measures to combat certain problems, such as the use of pirated programming software, which is really relevant. According to the data of the global research (In a year, more than half of Internet users were affected by viruses and malicious software, 2010), commissioned by Microsoft Corporation, three-quarters of computer users agree that the use of illegal software is unsafe. According to the data of the research of Internet users (Viruses and malicious software interfere with the work of more than half of the users in Lithuania, 2010), conducted in Lithuania by Synopticom, more than half of the users in Lithuania use illegal software. In the Lithuanian Programme, a more profound analysis might also be made of the current situation, identifying the potential threats and reasons due to which the achievement of the relevant objectives might be put at risk, since it could make it easier to plan the steps necessary for the objectives and tasks to be achieved.

2) Doctrine of the Information Security of the Russian Federation.

The Russian Doctrine provides basically 2 groups of national interests (objectives) in the sphere of information security. Having analysed Article 1 of the Russian Doctrine, it can be presumed that the first group of interest (objectives) has been distinguished according to whom these interests relate:

– Interests of a person – realization of constitutional rights to access to information, protection of personal information, and the possibility to use information, in a manner not forbidden by

the law, for physical, spiritual and intellectual development, etc.;

– Interests of a society – ensuring interests of a person in the sphere of information security, creation of a legal social State, achievement and maintenance of social consent, etc.;

– Interests of the State – creation of conditions for harmonious development of Russian information infrastructure, preparation of necessary laws and procedures, development of international cooperation, etc.[19]

When analysing the content of the interests included in the second group, it can be presumed that this group has been distinguished according to the importance of interests:

– Observation of constitutional rights and freedoms of a human being and a citizen in the field of obtaining information and its use.

– Ensuring security of home policy of the State in order that Russian and international public is provided with trustworthy information on the home and foreign policy of the Russian Federation.

– Promotion of the development of modern information technologies as well as of the means of information industry of the Russian Federation in the field of telecommunications and communications in order that this industry is capable of satisfying the demands of both domestic and external markets.

– Protection of information resources from illegal access, ensuring security of information infrastructure.[20]

Article 9 of the Russian Doctrine sets out the following priority measures in the sphere of ensuring information security:

– working out and introduction of mechanisms to facilitate the implementation of the norms of law regulating relations in the sphere of information, and also development of the conception for ensuring the legal protection of information security;

– working out and introduction of mechanisms for increasing efficiency of government direction of activities of governmental mass media, carrying out government information policy;

– adoption and realization of Federal programs, providing for formation of generally accessible archives of information resources of federal authorities and government authorities, upgrading legal culture and computer literacy of citizens, development of infrastructure

19 "Doctrine of the Information Security of the Russian Federation" ["Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii"], available at: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

20 Ibid.

of the unified information space of the Russian Federation, complex opposition to threats of information war, etc.;

– development of the system of training personnel to be employed in the sphere of ensuring information security of the Russian Federation;

– harmonization of domestic standards in the sphere of informatization and ensuring information security, etc.[21]

In our opinion, the wording of the objectives and priority measures set forth in the Russian Doctrine is rather non-specific and declarative. Lithuanian scientists also say that the Russian Federation formally gives considerable attention to safety information, including legislation. However, the provisions are declarative, so they sound more like slogans rather than specific measures for ensuring information security (Štitilis et al, 2011). Volchinskaya E. (2008), when analysing the role of the State in ensuring information security, notes that, in her opinion, the majority of the measures specified in the Russian Doctrine are impracticable, for example, in Russia, there is no state policy developed in this sphere, as well as no target federal program drafted yet.[22]

The Russian Doctrine also additionally lays down the methods of ensuring information security of the Russian Federation. They are divided into legal, organizational, technological and economic. Legal methods of ensuring information security of the Russian Federation include working out legal acts, governing relations in information sphere, and normative and methodological documents on matters, related to ensuring information security of the Russian Federation. Organizational and technological methods of ensuring information security of the Russian Federation include the following: strengthening activities of law enforcement authorities; working out and usage of information protection means and methods of control of efficiency of these means; development of protected telecommunications systems, increase of reliability of special software; creation of systems and means of preventing illegal – unsanctioned access and damage to and destruction or modification of information, etc. Economic methods of ensuring information security of the Russian Federation include the following: working out programs of ensuring information security of the Russian Federation and determination of the order of

21 Ibid.

22 Volchinskaya, E.K. (2008), "The Role of the State in Ensuring Information Security" ["Rol' gosudarstva v obespechenii informatsionnoi bezopasnosti"], http://elibrary.ru/item.asp?id=13609231

their financing; improvement of the system of financing works, connected with realization of legal, organizational and technical methods of information protection, creation of an insurance system of information risks of physical persons and legal entities, etc. In our opinion, such provision of the methods of ensuring the state's information security in a strategic document is redundant and unnecessary, because in the strategic documents of this kind, the most important actions to be carried out should be stated in articles on measures.

3) The International Strategy for Cyberspace of the USA.

Recently, the USA has been paying a lot of attention to cybersecurity. Professor Mary Ellen O'Connell says that it is time to turn to cyber disarmament and start the application of peaceful security measures, i.e., education of users, etc.[23]

Parts I and II of the USA Strategy set out the general principles of human rights that must be respected in cyberspace as well – these are the principles of fundamental freedoms, privacy, protection of property from crime, the right to self-defense, etc.[24] The norms of international cyberpolicy are also stated here as being essential for the formation of secure cyberspace – global interoperability, network stability, reliable access, multi-stakeholder governance, cybersecurity due diligence.[25]

Part III of the USA Strategy defines the tasks of the USA cybersecurity policy with the help of which it is sought to implement cybersecurity. After a more thorough analysis of the tasks, it can be seen that these tasks are closely related to one another. These tasks could be divided into the following several priority directions in ensuring cybersecurity:

– development of information technologies;

– collaboration between the public and private sectors;

– encouragement of the fight against violations of law and crimes in cyberspace;

– implementation, availability and promotion of new information technologies;

– national and international education and training in the sphere of cybersecurity;

23 O'Connell, M.E., "Cyber Security without Cyber War. 2012, Oxford", available at: http://jcsl.oxfordjournals.org/content/17/2/187.full

24 "International Strategy for Cyberspace", available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

25 Ibid.

– international collaboration.[26]

In our opinion, the main objective of this Strategy is international collaboration on cybersecurity. In this Strategy, international collaboration is the cornerstone on which the main opportunity for ensuring cybersecurity is based. This objective is also observed by Georgij Korsakov, who states that the main focus of this Strategy is on international collaboration in the field of electronic information security, with emphasis on the USA government's strategic approach towards cybersecurity[27].

Parts I and II of the USA Strategy provide an overview of the general features of cyberspace policy, formation of an approach, naming of certain objectives, but do not identify any specific measures for the implementation of certain goals and objectives. Part III of the above Strategy outlines the policy priorities in the field of cybersecurity. As it can be seen, there are quite a lot of priorities identified which, however, are intertwined with one another. As can be seen from the identified priorities, this Strategy is applicable to both the public and private sectors. Professor Mary Ellen O'Connell stresses that at this time, in the field of ensuring cybersecurity, there is a heavy dependence on the private sector. Therefore, the application of the Strategy to the private sector is reasoned and logical[28].

Much attention is paid to the reduction of cybercrime and terrorism. As in most strategic documents of other countries, such as Russia, Lithuania and others, the Strategy sets out the legislative and technical development initiatives for ensuring cybersecurity. The Strategy encourages international collaboration, collaboration between the public and private sector institutions, and exchange of best practices, with emphasis on the need for training in this area. Thus, as we can see, the strategic directions of the USA are similar to those of other countries. However, it is stated in the USA Strategy that cybersecurity can be fully guaranteed only through collaboration among all countries. It is emphasized that only by working together internationally it is possible to ensure the security and stability of the "global" Internet, which does not have any borders and boundaries.

26 Ibid.

27 Korsakov, G.B., "The role of information weapons in military and political strategy of the USA" ["Rol' informatsionnogo oruzhiya v voenno-politicheskoi strategii SShA"], available at: http://elibrary.ru/item.asp?id=17358664

28 O'Connell, M.E., "Cyber Security without Cyber War. 2012, Oxford", available at: http://jcsl.oxfordjournals.org/content/17/2/187.full

It must be added that the USA Strategy neither provides any analysis of the current situation in the field of cybersecurity nor gives any reference point, which would serve as a basis for judging the implementation of this Strategy.

Similarities and Differences in Cybersecurity Strategies of Lithuania, Russia and the USA

The Lithuanian Programme and the USA Strategy were both adopted at around the same time – in 2011, whereas the Russian Doctrine was adopted considerably earlier – in 2000. When assessing the objectives of the above strategic legal acts, it can be seen that the legal acts of Lithuania, Russia and the USA contain similar objectives related to the security of information resources, effective functioning of the information infrastructure, and personal security in cyberspace. The USA Strategy, as distinct from the strategic legal acts of other countries, singles out the main objective – international collaboration in ensuring cybersecurity. The exclusive objective which can also be found in the Russian Doctrine is development of the concept of the area of electronic information security. It also should be noted that the legal acts of Lithuania and the USA are intended for both the public and the private sectors, while the Russian Doctrine is focused exclusively on the public sector. In our opinion, national strategies must apply to both the public and private sectors.

The Lithuanian Programme does not distinguish the competences of any particular institutions in the field of cybersecurity, and only indicates the specific Lithuanian institutions and the specific objectives and tasks established in the Programme for the implementation of which they are responsible. Coordination of the Lithuanian Programme's implementation, reviewing of the tasks laid down in the Lithuanian Programme and changes in the levels of task assessment criteria, and updating of the Programme is the responsibility of the Ministry of the Interior. The institutions and bodies responsible for the implementation of the objectives and tasks of the Lithuanian Programme are as follows: Office of the Prime Minister, Communications Regulatory Authority, State Data Protection Inspectorate, Police Department under the Ministry of the Interior, Ministry of National Defence, Ministry of Transport and Communications, Ministry of Finance, Ministry of Education and Science, and Ministry of Economy. In our opinion, the Lithuanian Programme quite clearly and specifically indicates

the tasks that need to be implemented in order to achieve the appropriate level of cybersecurity. However, what we missed in the Programme was the "reference point" from which it would be possible to assess the already achieved level of cybersecurity. Thus, in order to conduct an informal assessment of the measures and their benefits, there had to be carried out an assessment of the current situation, which is called by us the "reference point".

Meanwhile, the Russian Doctrine makes a rather clear distinction among the competences of legislative, executive and judicial governance institutions in the field of information security. The Doctrine details the functions to be performed in this field by the President of the Russian Federation, State Duma of the Russian Federation, Government of the Russian Federation, Security Council of the Russian Federation, Federal executive authorities, interdepartmental and governmental commissions, appointed by the President of the Russian Federation and the Government of the Russian Federation, institutions of local governments, judicial authorities, etc. This Russian Doctrine, the same as the Lithuanian Programme, identifies the key problems in information security, establishes the objectives, principles and directions in the field of ensuring information security in the Russian Federation. However, unlike the Lithuanian Programme, the Russian Doctrine pays much more attention to the description of the condition of information security, potential threats, and the identification of sources of these threats, and it also identifies the peculiarities of ensuring information security in different spheres of public life (e.g., economy, home and foreign policy, science and technology, etc.), but it does not provide any assessment criteria according to which it would be possible to decide whether the Doctrine is implemented successfully or not. The Doctrine additionally lays down the methods of ensuring information security of the Russian Federation. They are divided into legal, organizational, technological and economic. Legal methods of ensuring information security of the Russian Federation include working out legal acts, governing relations in information sphere, and normative and methodological documents on matters, related to ensuring information security of the Russian Federation. Organizational and technological methods of ensuring information security of the Russian Federation include the following: strengthening activities of law enforcement authorities; working out and usage of information

protection means and methods of control of efficiency of these means; development of protected telecommunications systems, increase of reliability of special software; creation of systems and means of preventing illegal – unsanctioned access and damage to and destruction or modification of information, etc. In our opinion, such a division of the methods of ensuring information security is very useful, because it helps getting a more complete picture of the methods of ensuring information security and the types of means for ensuring cybersecurity. As an example, we can mention the fact that even university programs on cybersecurity are divided into the following three categories: managerial, legal and technical.

The USA Strategy does not indicate any specific institutions or heads of state responsible for the implementation of certain priority areas. In our opinion, the Strategy lacks the description of the current situation and describes it only in broad outline, without assessing the current cybersecurity situation, which is covered but only in general terms, without reference to any factual circumstances. This legal act also identifies very useful directions in ensuring cybersecurity, one of which is the organization of education and training in the sphere of cybersecurity at both national and international levels. This strategic legal act is a big step forward in the field of cybersecurity.

In our opinion, in order to develop and implement effective policy in the field of cybersecurity, the Lithuanian Programme also should specify not only the institutions responsible for the implementation of specific measures, but also should make a clear separation between each institution's functions in this field. It should also be added that the ensuring of cybersecurity at international level that is outlined in the USA Strategy is a particularly beneficial and positive step. It should be emphasized that it is not possible to ensure cybersecurity in one or another country, since this has to be done at international level, through immediate collaboration among countries, exchange of best practices, and by joining international agreements or by signing new ones. Attention should also be paid to the dynamism of technologies, thus educational priorities are important not only nationally, but also internationally.

When analysing the strategic legal acts of Lithuania, Russia and the USA in the field of cybersecurity, we observed the following positive and negative features of the strategies that we would like to distinguish as good and bad practices:

The bad practice, in our opinion, is that in order to not formally assess the measures carried out and their benefits, there had to be carried out an assessment of the current situation, the description of which we have failed to find in any of the strategic legal acts.

The good practice, in our view, is the following:

1. The Lithuanian Programme indicates the specific objectives as well as the methods for achieving them, and also the institutions responsible for the implementation of these objectives;

2. The Russian Doctrine specifically describes potential threats and sources of these threats, as well as possible methods for opposing these threats. Also, the Russian Doctrine provides a detailed description and clear division of the methods of ensuring information security (cybersecurity) (organizational, technological, and legal).

3. The USA Strategy names international collaboration as the key method for ensuring cybersecurity.

Conclusions

1. The Programme for the Development of Electronic Information Security (Cybersecurity) of the Republic of Lithuania establishes rather specific and ambitious objectives, tasks and criteria for the assessment of the Programme's implementation, while the wordings of the objectives and priority measures laid down in the Doctrine of the Information Security of the Russian Federation, the same as in the International Strategy for Cyberspace of the USA, seem rather declarative and non-specific, and also, unlike the Programme for the Development of Electronic Information Security (Cybersecurity) of the Republic of Lithuania, these two documents do not provide any assessment criteria according to which it would be possible to decide whether the Doctrine of the Information Security of the Russian Federation and the International Strategy for Cyberspace of the USA are implemented successfully or not.

2. The Programme for the Development of Electronic Information Security (Cybersecurity) of the Republic of Lithuania (as currently done in the Doctrine of the Information Security of the Russian Federation) does not clearly distinguish the competences of any particular institutions (both public and municipal authorities) in the field of cybersecurity.

3. The International Strategy for Cyberspace of the USA outlines the ensuring of cybersecurity at international

level, which is a particularly beneficial and positive step. In our opinion, it is not possible to ensure cybersecurity in one or another country, since this has to be done at international level, through immediate collaboration among countries, exchange of best practices, and by joining international agreements or by signing new ones.

4. The above strategic legal acts of Lithuania, Russia and the USA in the field of cybersecurity formally describe the current situation in the field of cybersecurity, but lack a more profound analysis of the current situation, without which it is not possible to accurately assess the achievements made in the field of ensuring cybersecurity.

5. The above strategic legal acts of Lithuania, Russia and the USA in the field of cybersecurity draw attention to the dynamism of technologies, therefore, one of the key tasks in order to ensure cybersecurity is education and training in this field at both national and international levels.

References

1. "Agenda of the meeting on cybersecurity held between Barack Obama and Vladimir Putin, Presidents of the USA and Russia. 2013, Northern Ireland", available at: http://en.rian.ru/russia/20130618/181726010/Cybersecurity-High-on-Agenda-of-Obama-Putin-Meeting.html
2. "Cybersecurity Strategy of the European Union, 2013, Brussels", available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
3. Danyushina, Yu.V. (2011), "Kommunikativnaya bezopasnost' v gosudarstvennom i delovom upravlenii" ["Communicative safety in the state and business management"], *Language. Philology. Culture*, No 1, pp. 66-80.
4. "Department of Defense Strategy for Operating in Cyberspace. 2011, Washington", available at: www.slideshare.net/DepartmentofDefense/department-of-defense-strategy-for-operating-in-cyberspace
5. "Doctrine of the Information Security of the Russian Federation" ["Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii"], available at: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

6. "Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 "On the Approval of the Programme for the Development of Electronic Information Security (Cybersecurity) for 2011-2019", *Valstybės žinios*, No. 83-4033, 2011; No. 106 (correction).
7. "International Strategy for Cyberspace", available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
8. Korsakov, G.B., "The role of information weapons in military and political strategy of the USA" ["Rol' informatsionnogo oruzhiya v voenno-politicheskoi strategii SShA"], available at: http://elibrary.ru/item.asp?id=17358664
9. O'Connell, M.E., "Cyber Security without Cyber War. 2012, Oxford", available at: http://jcsl.oxfordjournals.org/content/17/2/187.full
10. "Press release of Dalia Grybauskaitė, President of the Republic of Lithuania. 2012, Munich", available at: www.president.lt/lt/spaudos_centras_392/pranesimai_spaudai/kibernetinis_ir_energetinis_saugumas_-_lietuvos_prioritetas.html
11. "Press Release of the Council of the Russian federation", available at: http://council.gov.ru/press-center/news/14575/
12. "Resolution No. 189 of the Government of the Republic of Lithuania "Regarding the Approval of the Implementation Measures of the 2008–2012 Programme of the Government of the Republic of Lithuania" of 25 February 2009", *Official Gazette*, 2009, No. 33-1268.
13. Schjolberg, S., Ghernaouti-Hele, S. (2011), "A Global Treaty on Cybersecurity and Cybercrime. Geneva", available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf
14. Štitilis, D. (2011), *Electronic Crimes: A Methodological Tool*, Mykolas Romeris University, Vilnius, p. 83.
15. Štitilis, D., Pakutinskas, P., Dauparaitė, I., Laurinaitis, M. (2011), "Legal Environment in Order to Prevent Identity Theft: Comparative Analysis of the Legal Acts of the USA and Lithuania", *Social Technologies*, No. 1(1), p. 68.
16. Štitilis, D., Paškauskas, Ž. (2007), "State's Electronics Information Security Strategy – One of Key Electronic Information Security Regulatory Instruments: Comparative Analysis", *Jurisprudencija*, No. 2(92), pp. 37-45.
17. "The conceptual views on the activities of the Armed Forces of the Russian Federation in the information space" ["Kontseptual'nye vzglyady na deyatel'nost' Vooru-

zhennykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve"], available at: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle
18. Volchinskaya, E.K. (2008), "The Role of the State in Ensuring Information Security" ["Rol' gosudarstva v obespechenii informatsionnoi bezopasnosti"], http://elibrary.ru/item.asp?id=13609231

Особенности правового регулирования кибербезопасности в национальных законах Литвы, России и США: стратегии кибербезопасности

Штитилис Дарюс
Доктор юридических наук, профессор,
заведующий комитетом программы «Право новых технологий»,
Университет Миколаса Ромериса,
08303, Литва, Вильнюс, ул. Атейтес, 20;
e-mail: stitilis@mruni.eu

Клишаускас Валдас
Ассистент,
Университет Миколаса Ромериса,
08303, Литва, Вильнюс, ул. Атейтес, 20;
e-mail: stitilis@mruni.eu

Аннотация

В статье анализируется правовая база кибербезопасности Литовской Республики, Российской Федерации и Соединенных Штатов Америки относительно стратегий кибербезопасности. Результаты исследования могут быть применены при разработке нового законодательства или внесения изменений в существующие правовые акты по кибербезопасности.

Ключевые слова

Кибербезопасность, стратегии кибербезопасности, правовое регулирование.

Библиография

1. Волчинская Е.К. Роль государства в обеспечении информационной безопасности. [Электронный ресурс]. – Режим доступа: http://elibrary.ru/item.asp?id=13609231
2. Данюшина Ю.В. Коммуникативная безопасность в государственном и деловом управлении // Язык. Словесность. Культура. – 2011. – № 1. – С. 66-80.
3. Доктрина информационной безопасности Российской Федерации. [Электронный ресурс]. – Режим доступа: www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm
4. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. [Электронный ресурс]. – Режим доступа: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle
5. Корсаков Г.Б. Роль информационного оружия в военно-политической стратегии США. [Электронный ресурс]. – Режим доступа: http://elibrary.ru/item.asp?id=17358664
6. Agenda of the meeting on cybersecurity held between Barack Obama and Vladimir Putin, Presidents of the USA and Russia. 2013, Northern Ireland. Available at: http://en.rian.ru/russia/20130618/181726010/Cybersecurity-High-on-Agenda-of-Obama-Putin-Meeting.html
7. Cybersecurity Strategy of the European Union, 2013, Brussels. Available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
8. Department of Defense Strategy for Operating in Cyberspace. 2011, Washington. Available at: www.slideshare.net/DepartmentofDefense/department-of-defense-strategy-for-operating-in-cyberspace
9. Government of the Republic of Lithuania Resolution No. 796 of 29 June 2011 «On the Approval of the Programme for the Development of Electronic Information Security (Cybersecurity) for 2011–2019» // Valstybės žinios (Official Gazette). – No. 83-4033. – 2011; No. 106 (correction).

10. International Strategy for Cyberspace. 2011, Washington. Available at: www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
11. O'Connell M.E. Cyber Security without Cyber War. Available at: http://jcsl.oxfordjournals.org/content/17/2/187.full
12. Press release of Dalia Grybauskaitė, President of the Republic of Lithuania. 2012, Munich. Available at: http://www.president.lt/lt/spaudos_centras_392/pranesimai_spaudai/kibernetinis_ir_energetinis_saugumas_-_lietuvos_prioritetas.html
13. Press Release of the Council of the Russian federation, 2013, Moscow. Available at: http://council.gov.ru/press-center/news/14575
14. Resolution No. 189 of the Government of the Republic of Lithuania «Regarding the Approval of the Implementation Measures of the 2008–2012 Programme of the Government of the Republic of Lithuania» of 25 February 2009. – Official Gazette. – 2009. – No. 33–1268.
15. Schjolberg S., Ghernaouti-Hele S. A Global Treaty on Cybersecurity and Cybercrime. Available at: http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf
16. Štitilis D. Electronic Crimes: A Methodological Tool. – Vilnius: Mykolas Romeris University, 2011. – P. 83.
17. Štitilis D., Pakutinskas P., Dauparaitė I., Laurinaitis M. Legal Environment in Order to Prevent Identity Theft: Comparative Analysis of the Legal Acts of the USA and Lithuania. – Social Technologies. – 2011. – No. 1(1). – P. 68.
18. Štitilis D., Paškauskas, Ž. State's Electronics Information Security Strategy – One of Key Electronic Information Security Regulatory Instruments: Comparative Analysis // Jurisprudencija. – 2007. – No. 2(92). – Pp. 37-45.