кутской области (Иркутск) Научная библиотека : http:// http://cyberleninka.ru/article/n/professionalnyy-risk-meditsinskih-rabotnikov#ixzz46RBPgOVD.
9. Приказ Минтруда России от 25.12.2012 N 625н "Об утверждении Классификации видов экономической деятельности по классам профессионального риска" (Зарегистрировано в Минюсте России 25.12.2012 №26385) : http:// http://www.consultant.ru/document/cons_doc_law_140637.
10. Ахмерова С.Г. Профессиональные заболевания педагогов Электронный журнал "Менеджер образования». Портал информационной поддержки руководителей образовательных организаций// http://www.menobr.ru/article/36246-professionalnye-zabolevaniya-pedagogov.
11. European Court of Human Rights; Chamber judgment Sorguç v. Turkey 23.06.09 Press Release — Chamber Judgments 23/06/2009: http: // http://hudoc.echr.coe.int/eng?i=003-2771377-3044351#{"itemid":["003-2771377-3044351"]}.
12. European Court of Human Rights; Revista de Psicología del Trabajo y de las OrganizacionesVolume 30, Issue 3, September–December 2014, Pages 95–96 Universidad de Sevilla, España Received 6 November 2014, Accepted 6 November 2014, Available online 17 December 2014: http: // http://www.sciencedirect.com/science/article/pii/S1576596214000176.
13. Чикирева И. П. Профессиональные риски: совершенствование механизмов профилактики производственного травматизма и профессиональной заболеваемости (перспективы развития законодательства) // ЕВРАЗИЙСКИЙ ЮРИДИЧЕСКИЙ ЖУРНАЛ 2016, №2 (93), С. 196-199. http: // http://www.eurasialaw.ru/index.php?option=com_content&view=article&id=8095:-2-93-2016&catid=521:-2-93-2016-&Itemid=848.

DIGITAL SINGLE MARKET STRATEGY EXPERIENCE: CYBERSECURITY ENSURING FOR THE SUSTAINABLE DEVELOPMENT OF RUSSIA

E.V. Stolbova
a 2d year student of Law department
the Institute of State and Law Tyumen State University
katherine.stolbova@ya.ru
Research supervisor:
S.S. Racheva
Associate professor of Foreign Languages
and Intercultural Professional Communication
Department for Law and Economics
the Institute of State and Law Tyumen State University
PhD in Education Master of Law

Abstract

In this research, the cybersecurity formation issue in the Russian Federation is examined. The topicality of the theme is provoked by the mass character of hacker attacks that represent public threat not only for an every single person but also for the whole state. Moreover, the cyberthreat phenomenon is not regulated legally or economically that bounds an opportunity of perpetrators' bringing to account.

The novelty of the research appears to be in the Digital Single Market Experience appealing to the Russian legal development and is aimed to view the potential in the European progress.

Key words: Digital Single Market strategy, cybersecurity ensuring of Russia, hacker attacks, cybersecurity regulation of Russian Federation, cybersecurity strategy of Russian Federation, the Directive of the European Parliament and of the Council, Cybersecurity Strategy of the European Union.

1. Introduction

"Further cybersecurity assurance of Russia straightly depends on the stakeholder interaction level: state, scientific — research institutions, developers and info communicational producer decisions, customers and consumers" [1].

According to the Kaspersky Lab statistics, 28, 7% of cyber local threat is expected to be measured in Russia for only a month relatively to the world. Addressing to the web-threat, the Russian Federation takes the 3rd place worldwide, which is 20, 3% for a month [2].

It goes without saying that there are several approaches of the "cybersecurity" definition. "Cybersecurity is a battery of conditions that provide the safety of all cyberspace forms from the maximum amount of the threats and objectionable consequences of the malicious impacts" [3]. This definition is secured in the Concept of the cybersecurity strategy of the Russian Federation Project. However, the main goal is not to protect users from the greatest amount of attacks but to provide comfortable and productive surrounding for the users, customers, sellers and other consumers. This definition persuades to create even more threats to fight it. Moreover, cybersecurity contains obligatory aspects such as cyberspace and connections between parties of the public relations. In respect of this condition, it is necessary to change the approach for cybersecurity in order to clarify the destination and significance of this phenomenon.

Furthermore, cybersecurity is meant to defense citizens from the leaking and publication of the personal data, fraud, blackmailing, dangerous data spreading and citizen infrastructure attack. The online-banking system, system or online sales blocking and hack attacks on the private websites could influence all types of enterprises. The state appears to be under the huge pressure while key state systems are under attack such as e-Government or federal bodies' websites.

"Most cyber attacks are designed to steal information — primarily intellectual property and trade secrets. Data theft and business disruption are the most expensive cyber threats," explains Cynthia Provin, president of Thales e-Security, Inc. in the maga-

zine article “The invisible enemy”. The cybercrime without state regulation would transform into cyber-espionage to cyber-sabotage to cyber-war [4].

2. Legislation gaps of cybersecurity ensuring

In spite of the fact that the prevalence of cybercrimes increases with enormous rate, the lack of suitable norms of Russian legislation is obvious. The analysis of the federal law “On the information, information technology and on information protection” indicates the absence of definite law norms that could guarantee secure web-space and contain a responsibility for every malicious activity. Nevertheless, the federal law “On the personal data”, the federal law “On the commercial data” and other legal acts establish the rights that should be protected. Similarly, “The Doctrine of information security of the Russian Federation” was adopted in 2000. No doubt that this act is virtually outdated and requires an up-to-date version.

The Concept of the cybersecurity strategy of the Russian Federation Project present itself as an attempt to define a real place of cybersecurity in the information security structure and to coordinate public relations in the cyberspace. Unfortunately, this act tends to be a project without legal power, so it could not endorse effective digital security.

“The problem of the cybersecurity in our country is especially keenly mostly because of weak legislation base. Actually, well-formulated and fixed holistic approach to the national cybersecurity does not exist nowadays” [5].

3. Digital Single Market strategy: a global cybersecurity experience

In the light of the cybercrime rapid growth for the last two decades, the European Commission had adopted a Digital Single Market strategy on 6 May 2015 that should be fully implemented until the end of the 2016. The essential assignment of this document rests on three key pillars: creating better access for users to digital goods and service, making the conditions and a high-level playing field for digital networks and the potential increase of the digital economy.

“A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence” [6].

The required conditions have to be based on the full-scale and ubiquitous legal acts as well as on the trust and security. In the framework of the global project as known as Digital Single Market strategy some acts are being prepared to be formally approved that is equally important: Directive of the European Parliament and of the Council and Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

A Directive of the European Parliament and of the Council is normative legal act in the development process. A proposal of a Directive defines fundamental principles, technically, the basement of the digital legislation. In particular, it:

- lays down an obligation for the Member States making them responsible for the risks affecting network and information systems;
- establishes security requirements;
- applies complete and well-established definitions;
- sets frameworks on network and information security (NIS);
- initiates cooperation between competent authorities;
- regulates security of the networks and information systems of public administration and market operators.

An absence of the state as a responsible party is a significant disadvantage of Russian legislation system since there is a duty of federal bodies to ensure a cybersecurity in the country.

Security requirements are fixed in the Article 14 and include the obligation of the State “to ensure that public administrations and market operators take appropriate technical and organizational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations” [7].

The Directive establishes the definition of the “security” mentioning that it is an ability (not the conditions) of a network and information systems to withstand and resist an accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of information or the related services.

On balance, network and information security are fully supported by Member State in their territories relying on the National NIS strategy that should address cybersecurity issues for maintaining a high-level NIS. Research and development plans are described with governance framework and general methods on preparedness, response and recovery. In addition, each state shall set up a Computer Emergency Response Team responsible for handling emergency incidents and supply them with all kind of useful sources.

Moreover, the competent authorities of Member States with the European Commission organize cooperation network supporting NIS strategies and national NIS cooperation plans and preventing the risk and incidents on the early stage. It is vital to note that in conformity with the Directive, Member State take significant place in cybersecurity ensuring process by delegating powers to state bodies, authorities, special subjects. This approach allows a state to be a central figure in social relations.

By and large, the Directive of the European Parliament and of the Council is estimated to be a key act that conducts hand in public relations in the field of cybersecurity in the following Member States in consideration of current increasing threat in the cyberspace.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace comprises the elements of Digital Single Market strategy delineating basic principles, vital challenges that should be overcome and a suitable legislation system. The Strategy invokes to remain principles and values the European Union upholds not only in the real world but also online. The rights of the users’ personal data, freedoms, privacy and the legitimate interests to be protected prevail to be unsafe nowadays as the private sector owns the significant part of the cyberspace. Based on this, the EU have to guarantee safe access for everyone. The concept of control absence by any entity in the digital world is emphasized in the Strategy. Non-government stakeholders suppress the idea of the democratic and efficient multi-stakeholder governance. Besides, it is self-evident that all the relevant actors need to remonstrate a digital threat protecting themselves and share the responsibility while taking action.

Concerning the priorities of the EU, the Strategy determines precedent ones to be able to withstand challenges:

- achieving cyber resilience;

- drastically reducing cybercrime;
- developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- develop the industrial and technological resources for cybersecurity;
- establish a coherent international cyberspace policy for the European Union and promote core EU values.

4. International cybersecurity cooperation

Cyber resilience allow of all the relevant actors to collaborate with each other due to the fact that a cooperation provides capabilities development as the cybersecurity efficiency boosting is vital need.

Obviously, digital resilience as well as cybercrimes confrontation is unattainable without a strong legislation for common requirements establishment to obligate Member States to ensure cybersecurity becoming progress. The regulation of the national NIS competent authorities has to be implemented with support of the legal norms. The private sector should also coordinate itself and be technically and perfectly prepared to reflect a cyber threat on its own. In addition, users have to be aware of the obstacles and malicious activities they could come across by making proper decisions and taking simple steps.

"Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders — the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative crossborder approach to respond to this growing threat" [8].

Fortunately, cybercrime could be effectively tackled by dint of powerful legislation. The first stage are The Council of Europe Convention on Cybercrime also known as the Budapest Convention and a Directive on combating the sexual exploitation of children online and child pornography.

Cyber defense policy is a summary of capacity development aspects, dialogue establishment between civilian and military actors in the European Union, international partners and organizations. It is supported by the scientific research and development. R&D investment and innovation would support a strong policy in a line with fulfilling technical gaps.

Digital products does make a security a priority. However, Information and Communication Technology (ICT) products are located outside the EU that could cause certain dependence. Therefore, it is necessary to stimulate a cybersecurity products market for the competitive development.

Cybersecurity is inseparable from the international cooperation. "One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance" [8].

The European Commotion in the framework of the Cybersecurity Strategy developed an interdependence scheme to show visually importance of the connections.

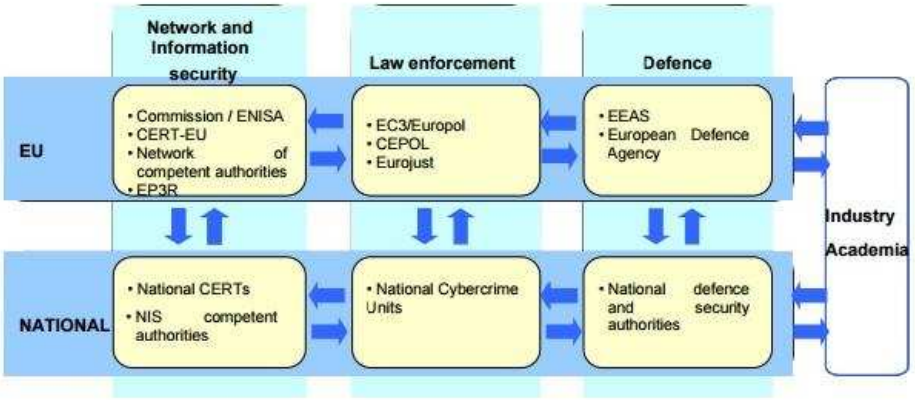

Table 1. An interdependence scheme

Three general pillars of online security were involved: NIS, law enforcement and defence. By the same token, Russian approach should be changed in order to recreate national digital security structure and to systemize the relations of state bodies, organizations and authorities.

Uniquely, Digital Single Market strategy combined aspects of a scale plan in unification, proportionality, mutual responsibility and the effectiveness of the presentation of variety.

It would be giddily to ignore such a global threat as a cyberterrorism and cybercrime. Although the ways of cybercrime confrontation are not written in the Strategy documents clearly, the European Commission launched an EU Forum where major IT companies were invited to set a limit on the terrorist propaganda and to explore measures to address the concerns of law enforcement authorities on new encryption technologies. Due to the future ambitions, the Commission determines key actions: countering radicalization, updating the Framework Decision on terrorism, cutting the financing of criminals, enhancing dialogues with the IT industry, strengthening the legal framework on firearms, reinforcing tools to fight cybercrime and enhancing the capacities of Europol [9].

5. Final statements

In summary, the Russian Federation legislation does not properly suit to the up-to-date cybersecurity regulation needs. Legal acts have to be reconsidered according to the digital conditions. European experience by way of Digital Single Market strategy seems to make great intentions for the future and to effect in a productive way on the reality. To our way of thinking, Russian state bodies should pay special attention on the following aspects:

- establishing the exact definition of the fundamental terms;
- expansion and clarification of the actual Russian legislation;
- the need of the real state responsibility existence;
- establishing special security requirements for organizations, state and users;
- cooperation between competent authorities;
- development of the stakeholders' cyber resilience;
- development of the cyber defence policy.

The stated norms and definitions are able to stabilize the unregulated social relations so as to increase a crime level and to avert further illegal activity prosperity. The reason of the state obligation to be responsible for cybersecurity norms realization is a practical demand as the state activities need to be organized too.

The number and contingent of active users increase exponentially that causes urgent changes of cybersecurity methods to fight with digital offenders successfully.

"The more people rely on the internet the more people rely on it to be secure. A secure internet protects our freedoms and rights and our ability to do business. It's time to take coordinated action — the cost of not acting is much higher than the cost of acting" [10].

References

1. Zgoba Artem, Dmitry Markelov, Pavel Smirnov. Cybersecurity, threats, calls, solutions [Digital source] // Zgoba Artem, Dmitry Markelov, Pavel Smirnov. — "Cybersecurity issues" №5 / 2014. P. 30-39. Date of access: 05.04.2016. — URL: http://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya.
2. Secure List Statistics [Digital source] // Kaspersky Lab ZAO. Date of access: 03.04.2016. — URL: https://securelist.ru/statistics/.
3. Mikhail Bezkorovainy, Alexander Tatuzov. Cybersecurity — approaches to the definition [Digital source] // Mikhail Bezkorovainy, Alexander Tatuzov. — "Cybersecurity issues" №1 / 2014. P. 22-28. Date of access: 05.04.2016. — URL: http://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya.
4. Trefor Moss. The invisible enemy [Digital source] // Trefor Moss. — Internet Journal "Defence: Cybersecurity". P. 2-4. Date of access: 04.04.2016. — URL: https://www.thalesgroup.com/sites/default/files/asset/document/p2-5_cybersecurity_final.pdf.
5. Mikhailova Alena. The problems of cybersecurity in Russia and the solution ways [Digital source] // Informational — legal portal "Garant". Date of access: 03.04.2016. — URL: http://www.garant.ru/article/520694/.
6. "A Digital Single Market Strategy for Europe" [Digital source] // Adopted in Brussels, 6.5.2015 // EUR-lex: Access to European Union Law. Date of access: 03.04.2016. — URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192.
7. Proposal for a Directive of the European Parliament and of the Council // Adopted in Brussels, 7.2.2013. P. 24.
8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // Adopted in Brussels, 7.2.2013. P.9.
9. Commission takes steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime [Digital source] // The European Commission Press Release Data Base. Date of access: 05.04.2016. — URL: http://europa.eu/rapid/press-release_IP-15-4865_en.htm.
10. EU Cybersecurity plan to protect open internet and online freedom and opportunity [Digital source] // The European Commission Press Release Data Base. Date of access: 05.04.2016. — URL: http://europa.eu/rapid/press-release_IP-13-94_en.htm.

ПРАВО НА ОБРАЩЕНИЕ: СУЩНОСТЬ, СТАНОВЛЕНИЕ, ПРОБЛЕМЫ РЕАЛИЗАЦИИ

Н.А. Ткаченко,
магистрант ИГиП ТюмГУ
направление «Юриспруденция»
nadezda.zaharowa@yandex.ru
Научный руководитель:
Д.О. Тепляков,
доцент кафедры конституционного и муниципального права ИГиП ТюмГУ,
кандидат юридических наук

Право на обращения является составным элементом обеспечения участия граждан Российской Федерации в управлении делами государства и местного самоуправления, а также служит своеобразным каналом обратной связи, позволяющим органам власти оценивать положение дел в стране.

В настоящее время институт права на обращение находится в процессе модернизации и совершенствования. В условиях становления правового государства и повышения правового сознания право на обращение приобретает особую значимость, являясь отражением народовластия и укрепления правового статуса человека.

Федеральным законом от 2 июня 2006 года №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» [1] обращение граждан определяется как направленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления.

Отмечая значимость функций права на обращение, Мещерягина В.А. рассматривает институт обращения граждан как: средство (осуществления и охраны прав личности; укрепления связи органов государственной власти, органов местного самоуправления с населением; разрешения противоречий в общественной и политической жизни; общественного контроля за