и обратная связь.

Анализ характеристик (доминант) элементов дискурса показывает их взаимопроникновение и взаимозависимость. Так, статусно-ролевые характеристики субъектов права влияют на мотивы и цели коммуникации, темы высказываний и социально-коммуникативная активность субъекта определяет порядок действий в рамках определенной вербальной деятельности и может определять принципы и способы принятия решений. В свою очередь мотивы и цели субъектов в правовом дискурсе определяют тему, жанр, композицию и языковые средства информации, мировоззрение и ценности субъектов права определяются ментальностью общества и определяют статусно-ролевые позиции. В свою очередь индивидуальные особенности субъекта влияют на социально-коммуникативную активность, мировоззрение и ценности [1, с. 140].

Таким образом, овладение методологическими принципами правового дискурса выводит современное юридическое образование на новый тип диагностико-правовых и обучающих технологий.

Литература

1. Храмцова Н.Г. Дискурс – правовой анализ: от теории к практике применения: монография / Н.Г. Храмцова. – Курган: Изд-во Курганского гос. ун-та, 2012. – 180 с.

2. Григорьева В.С. Дискурс как элемент коммуникативного процесса: прагмалингвистический и когнитивный аспекты: монография / В.С. Григорьева. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2007. – 288 с.

UDC 340:608.3:001.102:438(043.2)

Kunyk A.M., Master,
National Aviation University,
Wroclaw, the Republic of Poland
Scientific advisor: Myronets O.M., Senior Lecturer

CYBERSECURITY POLICY IN THE REPUBLIC OF POLAND

Social and economic development is more and more dependent on fast and unhindered access to information and its use in the management, production and service sector and by public entities. Continuous development of network and information systems, including analyzing larger data sets, helps develop communications, commerce, transport, or financial services. We create and shape social relations in cyberspace, and the Internet has become a tool for influencing the behavior of social groups, as well as exerting influence in the political sphere [1, p. 4].

In the face of globalization, the cyberspace security has become one of the key strategic objectives in the area of security of each country. At a time of free

movement of people, goods, information and capital – the security of a democratic country depends on the development of mechanisms which allow preventing and combating threats to the cyberspace security [2, p. 4].

The number and severity of cyber attacks are on the rise, and companies simply cannot rely on their governments to protect them. In fact, quite the opposite is true. Governments are increasingly requiring corporations to defend themselves and, by extension, the state as a whole [3]. Nowadays the following cybercrimes are known to the Police in Poland: unauthorized access to the system and/or interception of information, data interference, computer sabotage, system interference, misuses of devices, computer fraud, copyright offence, pornography [4, p. 6].

Poland, like China and Singapore, is the latest example of a nation that has passed far-reaching cyber security legislation to better ensure that its critical infrastructure is protected [3]. To fight against cyber crimes, prevent violation of human rights and improve security in the whole county, Poland adopted the National Framework of Cyber security Policy of the Republic of Poland for 2017-2022. It is a strategic document in a continued process of actions taken by the governmental administration, aimed at raising the level of cyber security in the Republic of Poland, including the Policy for the Protection of Cyberspace of the Republic of Poland adopted by the government in 2013 [1, p. 5].

Today Polish Penal Code provides a wide range of offences that specifically relate to a computer system and data as the objects of offending. The following offences against confidentiality, integrity and availability of computer data and systems can be distinguished: - illegal access to a computer system (article 267 § 1 and 2), - illegal interception (article 267 § 3), - data interference (articles 268 and 268a), - system interference (articles 269 and 269a), - misuse of devices (article 269b) [4, p. 8].

The mentioned above Policy specific objectives foresee: 1). Increased capacity for nationally coordinated actions to prevent, detect, combat and minimize the impact of incidents which compromise the security of ICT systems vital to the functioning of the state; 2). Enhanced capacity to counteract cyber threats; 3). Increasing the national potential and competence in the area of security in cyberspace; 4). Building a strong international position of the Republic of Poland in the area of cyber security [1, p. 7].

The Government of the Republic of Poland notices the essence of new cyberspace hazards that continue to evolve and are acquiring more considerable significance, in connection with transferring subsequent spheres of human life and activity into the virtual dimension. Currently, new technologies and the Internet play an essential role in social and economic life. These are critical resources for all sectors of the economy are based on them. For this reason, it is extremely important to strengthen our resilience to cyber incidents so that the economy and society may function smoothly, and develop [5, p. 2].

In 2022, Poland will be more resilient to attacks and threats from

cyberspace. Thanks to a combination of internal and international activities, Poland's cyberspace will provide (constitute) a secure environment enabling the State to carry out their functions and allowing Poland to fully utilize the potential of the digital economy, while at the same time respecting the rights and freedoms of the citizens [1, p. 7].

The initiatives presented in the Communication deserve support, although in many points they should be particularized by the European Commission. On this note, Poland stresses the need for conducting deepened analysis as to whether the establishment of new structures is truly necessary and whether the tasks planned in the Communication could be rather implemented by the already existing structures/bodies. At the same time, Poland declares active participation in the actions undertaken at the EU level [5, p. 13].

In conclusion, we have to admit that the directions of cyber security in Poland are rather effective and important for the development of the whole Polish society. According to the mentioned Policy, education in the area of cyber security should begin at the early stage of education. The safe use of cyberspace will form a core part of the curriculum. It is also planned to develop and launch refresher courses for computer science teachers and to implement adequate changes in postgraduate education for teachers [1, p. 21]. We support such a position and insist on the great importance of further informational culture development and improvement in Poland.

Literature

1. National Framework of Cyber security Policy of the Republic of Poland for 2017-2022. Warsaw. 2017. 28 p. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (date of access: 22.01.2019).

2. Cyberspace protection policy of the Republic of Poland. Warsaw. 25 June 2013. 26 p. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ ncss-map/copy_of_PO_NCSS.pdf. (date of access: 22.01.2019).

3. Michael Bahar, Trevor J. Satnick, Pawel Lipski, Daria Gęsicka. Legal alert: Poland implements comprehensive cyber security legislation. URL: https://www.lexology.com/ library/detail.aspx?g=4f3fe69d-17a4-4ff6-a466-8a0e 5002 ea02. (date of access: 22.01.2019).

4. Andrzej Adamski. Cybercrime Legislation in Poland. 26 June 2015. URL: http://www.cybercrime.umk.pl/files/files/Cybercrime%20Legislation%20_PL_2010. pdf. (date of access: 22.01.2019).

5. The position of the polish government. 22 July 2016. URL: https://www.gov.pl/documents/31305/0/pl_position_cyber_ec_com_eng.pdf/baa0818 6-708b-5b43-9965-c7d1bbb7e1d1. (date of access: 22.01.2019).