УДК 1751

Діана Артурівна ТУПОТІНА,
здобувач вищої освіти 2 курсу
факультету підготовки фахівців для органів досудового розслідування
Дніпропетровського державного університету внутрішніх справ

AUTHORITIES RESPONSIBLE FOR REGULATION OF CYBER CRIME IN UKRAINE, COMPARISON WITH OTHER COUNTRIES

Cybersecurity means the desired end state in which cyberspace is reliable and in which its functioning is ensured. Cybersecurity includes measures for functions and critical infrastructure aimed at achieving predictive management capabilities and, where necessary, resilience to cyber threats and their consequences that could cause significant harm or threat to Ukraine or its population. In the summer of 2017, government agencies and Ukrainian companies were exposed to a massive cyberattack, the Petya virus. A. It was one of the largest cyberattacks in Ukrainian history. The attack showed that the state was completely unprepared for cyber threats. The Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (Registration № 2126) is a positive normative legal act, as it defines the legal and organizational bases of ensuring the protection of the vital interests of the Ukrainian state in the field of cybersecurity and defines the principles of coordination of their activity of state bodies on cybersecurity.

Within its mandate, the Security Service of Ukraine is obliged to prevent, detect, terminate and solve crimes against the world and security of humanity in cyberspace, to combat cyberterrorism and cyber espionage. The SBU is also empowered to conduct secret inspections of critical infrastructure.

The National Bank is defined by law as a regulator of cybersecurity in the banking sector. To this end, it has the right to set its own standards in this area and to have them checked for compliance. But I would like to emphasize that this is already happening – the banking sector has long introduced the international standard of information security ISO-27001.

In general terms, the development of information and communication technologies goes beyond their legal regulation, and it is possible that new

aspects of their development will emerge that will require regulation at national and international legal level, but any emerging issues will be related in one way or another. the problems of cross-border internet management, its safe use and taking measures against the illegal use of the Internet.

The cyberspace that we strive for encourages innovation and supports entrepreneurs, connects individuals and strengthens community; influences the activities of governments and promotes the "transparency" of governments; stands at the heart of fundamental freedoms and ensures privacy; it promotes understanding, refines behaviors and enhances national and international security. To support such an environment, the best practical form is international cooperation, which is the first principle.

National Security Authorities around the world have developed and are currently developing their cyber defense capabilities, that is, measures designed to identify and prevent cybercrime and mitigate the effects of these cybercrimes in the event of their occurrence.

The United States' approach to international cyberspace is based on the belief that networking technologies have enormous potential for the country and the world. For the past three decades, the United States of America has watched how these technologies revolutionize our economy and transform our daily lives. They also watched as problems from the outside penetrate into cyberspace, such as exploitation and aggression. Adapting to these challenges, the United States adheres to such principles regarding international cyberspace that would open up opportunities for innovation, stimulating economic development, and improving the quality of life at home and abroad. This work will be based on principles that are vital not only to US foreign policy but also to the future and to the Internet as such. The United States will help build capacity in the field of cybersecurity abroad bilaterally, within multilateral organizations, so that each country has the means to protect its digital infrastructure, strengthen the global networks, establish closer cooperation on a consensus-building basis secure and reliable network.

Ensuring the safety of society is a key task of public authorities and important functions of our society must be protected in all situations. Being an information society, Finland is dependent on information networks and systems and is therefore extremely vulnerable in terms of disruptions that affect their functioning. Cyberspace is the international term for such an interdependent, multi-purpose electronic data processing environment. Cyberspace should be seen as both an opportunity and a resource. Secure

cyberspace simplifies the planning of its activities for both individuals and organizations, which in turn stimulates economic activity. A well-functioning environment also enhances Finland's attractiveness to foreign investors.

Thus, international cooperation is a key point in eliminating the legal vacuum that exists between the development of information technology and the response to it. The process of developing events at the international level, as experience shows, is itself a complex problem. However, this is the only way to ensure the security of users and the state against electronic attacks, as well as to effectively investigate and prosecute cybercrime.

Список бібліографічних посилань

1. «Ми ведемо війну з Росією»: повний текст закону України про кібербезпеку // Obozrevatel : сайт. 06.10.2017. URL: https://www.obozrevatel.com/ukr/tech/digest/mi-vedemo-vijnu-z-rosieyu-povnij-tekst-zakonu-ukraini-pro-kiberbezpeku.htm (дата звернення: 25.04.2020).
2. Шаховал О., Лозова І., Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. Захист інформації. 2016. № 1, т. 18. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/10113 (дата звернення: 25.04.2020).
3. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник національної академії державного управління при Президентові України*. Серія «Державне управління». 2015. № 4. С. 50–56.
4. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших : інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України / Європейський інформаційно-дослідницький центр. Київ, 2016. 37 с. URL: https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf (дата звернення: 25.04.2020).

Одержано 29.04.2020