

*Тимошенко А.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Василенко О.*

INTERNATIONAL EXPERIENCE IN THE FIGHT AGAINST CYBERCRIME: LESSONS FOR UKRAINE

In today's world, digital technologies have become an integral part of our lives. From the moment we wake up and check our smartphones to working days spent in front of the computer, technology accompanies us everywhere. Gadgets are no longer just a means of communication or entertainment, they have become our personal assistants, facilitating everyday life, work, study and even interaction with government structures. People cannot imagine life without technologies that provide convenience and speed in everything. But is this comfort safe? In recent years, the world has witnessed how technological advances have created not only conveniences, but also new threats. Every day, countries are subjected to powerful cyberattacks, from attempts to steal personal data to hacking strategic facilities. In recent years, Ukraine has strengthened its cyber security, but international experience in this area will be an important source for improving the cyber security system.

The US was one of the first countries to realize the importance of cyberspace defense at a strategic level. It is this country that can become an example to follow, because it has shown that effective legislation is the basis of the fight against cybercrime. The Computer Fraud and Abuse Act (CFAA) allows prosecution for hacker attacks and other crimes related to computer systems. The Electronic Communications Protection Act (ECPA), which provides protections for communications in storage and in transit. The strategy, adopted on March 2, 2023, has improved the state of national cybersecurity in the United States, as it speaks of the importance and need for strong cooperation, especially between the public and private sectors, as it is essential for the security of cyberspace. The strategy also provided for the expansion of investments in research and development in the field of cyber security, which contributed to increasing the resistance of the national information infrastructure to attacks.

It is this key experience that Ukraine can gain from such a progressive country in this field – the USA. Cooperation between the state and the private sector, the development of a modern legislative framework, investment in innovative technologies and a proactive approach to identifying threats are all critical components for creating a sustainable cyber defense system. In the conditions of constant cyberattacks that Ukraine is experiencing, this US experience can be an important step towards strengthening national security in the digital space.

In addition to the United States, many new approaches and methods of ensuring cyber protection can be borrowed from such a progressive country as Israel. Israel is famous for its advanced cyber security infrastructure and innovative technologies in the field of cyber defense. Since its inception as a nation facing constant threats of war, Israel has created its own unique challenges and opportunities to become a global leader in cyber security.

The need to defend itself against hostile neighbors has pushed Israel to develop superior military capabilities, with a particular focus on cyber defense. The Israel Defense Forces (IDF) has established specialized units, such as Unit 8200, dedicated to intelligence gathering and cybersecurity [3]. By merging the National Cyber Staff and the National Cyber Defense Directorate into a single National Cyber Defense System, Israel has achieved collaboration between government, business and universities that encourages innovation and knowledge sharing. A good example of the success that is currently developing in Ukraine is investment in human capital, because cyber security education starts at an early age thanks to specialized programs in schools.

European countries actively use the Budapest Convention, which is a key international treaty aimed at combating cybercrime. Adopted in 2001, this convention establishes general rules for the participating countries regarding the criminalization of cybercrimes, the implementation of procedural measures for their investigation, and also ensures effective international cooperation. Any country may make use of the Budapest Convention as a guideline, check list or model law. Today, it plays an important role in strengthening global cyber security and harmonizing legislation in the field of protection against the latest cyber threats. Ukraine is also among the countries that use and support the convention, currently there are 76 such participating countries.

Obviously, our country is at the initial stage of implementing institutions and mechanisms in the field of cyber security, but Ukraine meets new challenges almost every day and works to prevent such crimes. Given the best European and American experience, Ukraine can significantly strengthen its defense against cyber threats. This requires complex efforts of both government bodies, the IT sector and civil society. Thus, on January 16, 2024, the Verkhovna Rada of Ukraine adopted in the first reading as a basis the project of the Law of Ukraine "On Amendments to the Criminal Code of Ukraine on Establishing Criminal Liability for Unauthorized Interference, Sale or Distribution of Information Processed in Public Electronic Registers and Strengthening Criminal Liability under during the period of martial law for criminal offenses in the field of use of information and communication systems", this draft law contributes to combating the factors of cybercrime and ensures legality in the information field [5].

It is worth hoping that the current state authorities will not stop there, will borrow the experience of other European countries and the USA and participate in international cooperation on cyber security issues.

Список використаних джерел

1. McNicholas E. R., Angle K. J. Cybersecurity Laws and Regulations Report 2024 USA. *International Comparative Legal Guides International Business Reports*. URL: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa>.

2. National Cybersecurity Strategy. ONCD. The White House. URL: <https://www.whitehouse.gov/oncd/national-cybersecurity-strategy/>.

3. Abhishek P. Evolution of Israel as a Cybersecurity Powerhouse: From *Warfare to Cyberspace*. URL: <https://www.linkedin.com/pulse/>.

4. Budapest Convention – Cybercrime. *Cybercrime*. URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

5. Myronenko V. The army of cyber warriors: international legal experience in the field of combating cyber crime. *Mind.ua*. URL: <https://mind.ua/openmind/20270195-armiya-kibervoyiniv->.

Тимчишин П.,

здобувач ступеня вищої освіти бакалавра

Національної академії внутрішніх справ

Консультант з мови: **Романов І.**

**COMPARATIVE ANALYSIS OF PUBLIC SAFETY MEASURES
IN WARTIME: UKRAINE AND INTERNATIONAL EXPERIENCE**

The comparative analysis of public safety measures during wartime reveals diverse approaches that different nations take to maintain order, protect civilians, and support national security. In Ukraine, the Russian invasion has prompted a rapid escalation of public safety initiatives designed to respond to both traditional military threats and modern hybrid warfare tactics, which include cyberattacks, disinformation, and targeted disruptions of civilian infrastructure. Ukraine's response combines traditional defense with innovative strategies, drawing lessons from international practices and developing new frameworks suited to its unique situation.

Ukraine's public safety measures have intensified through coordinated efforts between military, police, and local defense forces. One of the primary initiatives includes territorial defense units that consist of civilian volunteers and reservists, enabling rapid responses to emergencies and bolstering the national army's capacity to counter aggression. These units operate alongside regular military forces, providing local intelligence and assisting in securing infrastructure. In comparison, countries like Israel have longstanding frameworks for citizen involvement in public safety, where civilian preparedness and rapid mobilization are institutionalized through organized defense networks. Israel's system includes community-