Джунь С.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Волік О.**

US EXPERIENCE IN COMBATING CYBERCRIME

Rapid technological progress in society leads not only to new opportunities but also to a new type of crime — cybercrime. Therefore, countries are obliged to maintain security in cyberspace by protecting their citizens from this new form of criminal activity. Control in the digital environment is somewhat more complicated, because with modern technologies and methods of bypassing controls, such as VPNs or specialized software, maintaining cybersecurity is becoming increasingly difficult. However, thanks to the NCSI website, we can assess the cybersecurity index and analyze which countries are leaders in this field. According to data on the NCSI website, the United States has an index of 84.17, which is a high result [1].

To ensure cybersecurity, the state establishes cybersecurity agencies and implements various laws, including the Computer Fraud and Abuse Act (CFAA) in the United States, which provides for criminal liability for unauthorized access to computer systems [2]. Initially adopted in 1986, the law prohibits various cybercrimes such as hacking, intentional damage to computer systems, and unlawful use of passwords. The CFAA can be applied in both criminal and civil cases, although its broad wording and application—particularly regarding "exceeding authorized access"—have been the subject of debate and calls for reform. This is unsurprising, given that the law is nearly 40 years old while technology continues to evolve rapidly and relentlessly. In addition to this Act, there are several others, such as the Identity Theft and Assumption Deterrence Act, Wire Fraud, the Cybersecurity Information Sharing Act, Cyberstalking statutes, and more. Legislation continues to adapt to new needs for citizen protection, creating a new era in the development of law.

Furthermore, agencies such as the National Security Agency (NSA) and the Department of Homeland Security (DHS) are actively operating in the United States, coordinating cybersecurity policy. The activities of these law enforcement bodies are guided by the National

Cybersecurity Strategy. The U.S. also has an Internet Crime Complaint Center that collects reports of internet-related crimes from the public. Using such complaints, the ICCC team works on asset recovery. Its main functions include collection, analysis, public awareness, and referrals [3, p. 154].

In addition, the United States has well-developed public–private partnerships. The government collaborates with business representatives—particularly in critical infrastructure and information technology—to exchange information on cyber incidents. The U.S. also has extensive international cooperation, entering into bilateral agreements to combat cybercrime and to facilitate information sharing.

Researchers emphasize that the U.S. has a comprehensive system of agencies that combat cybercrime:

1. U.S. Cyber Command (USCYBERCOM) — a branch of the U.S. Armed Forces that conducts cyber warfare operations and manages and protects military computer networks;

2. The United States Computer Emergency Readiness Team (US-CERT) — part of the National Cybersecurity Division of the Department of Homeland Security, which provides security information and works to eliminate vulnerabilities in security systems;

3. The Computer Crime and Intellectual Property Section (CCIPS) — a unit of the U.S. Department of Justice that investigates computer crimes and intellectual property violations, specializing in the seizure of digital evidence [4, p. 212].

In conclusion, the United States demonstrates a comprehensive and multi-layered approach to ensuring cybersecurity, combining robust legislation, specialized governmental agencies, and active public–private as well as international cooperation. The evolution of laws such as the CFAA, alongside additional federal acts, reflects the state's continuous efforts to adapt its legal framework to the rapidly changing technological landscape. Institutional structures, including the NSA, DHS, USCYBERCOM, US-CERT, and CCIPS, form an integrated system aimed at preventing, investigating, and responding to cyber threats. While the increasing complexity of cyberspace presents ongoing challenges, the coordinated strategies and mechanisms implemented in the United States position the country among the global leaders in combating cybercrime and enhancing national cyber resilience.

References:

1. NCSI : Ranking URL: https://ncsi.ega.ee/ncsi-index/?order=rank&type=c

2. United States Congress. Computer Fraud and Abuse Act of 1986, 18 U.S. Code § 1030. Fraud and related activity in connection with computers. Enacted: 1986. URL: https://www.law.cornell.edu/uscode/text/18/1030

3. Колосов, О. О. (2023). Особливості протидії кіберзлочинам у Сполучених Штатах Америки. *Ірпінський юридичний часопис*, (1(10), 151–160. URL: https://doi.org/10.33244/2617-4154-1(10)-2023-151-160

4. Орлов О.В., Онищенко Ю.М. Узагальнення міжнародного досвіду створення державної системи попередження та запобігання злочинам у мережі інтернет. *Теорія та практика державного управління*. 2014. Вип. 2. С. 212-219.

Домбровська В.,
здобувач ступеня вищої освіти бакалавра
Донецького державного
університету внутрішніх справ
Консультант з мови: **Черньонков Я.**

PROBLEMATIC ISSUES OF THE PROCEDURAL USE OF POLYGRAPH EXAMINATION CONCLUSIONS AS A SOURCE OF EVIDENCE IN ORGANIZED CRIME

Organised crime (OC) poses a significant threat to Ukraine's national security and public order. Due to its high level of secrecy, rigid hierarchy, corruption connections, and active resistance to investigation (including the use of countermeasures), traditional forensic methods often prove insufficient. In this context, the polygraph examination serves as a highly informative tool capable of verifying the reliability of provided information. Despite its widespread application, the procedural status of polygraph results in criminal proceedings remains uncertain and controversial. This inconsistency is the main problem. In the absence of explicit regulation in the Criminal Procedure Code (CPC) of Ukraine, courts often treat the results of polygraph