the appeal of citizens, officials, other police officers, mass media or the direct detection of a disciplinary offense by a police official.The term of official investigation is 15 days, but can be extended up to 30 days. During the investigation, the police officer may be suspended from his post.

If a police officer is found guilty of a disciplinary offense, one of the following disciplinary sanctions may be applied to the police officer: reprimand, reprimand, severe reprimand, warning of incomplete service compliance, demotion in special rank by one level, dismissal from the position, dismissal from police service.

All in all, as we can see there are some real changes to the current legislation in the field of law enforcement activity. Thus, we should promote and develop these changes in order to improve the conditions for our police forces.

Список використаних джерел

1. National police as a component of the security. URL: https://science.lpnu.ua/law/all-volumes-and-issues/volume-10-number-137-2023/ national-police-component-security-and-defence.

2. Law of Ukraine about National Police. URL: https://cis-legislation.com/document.fwx?rgn=78349.

3. Martial law regime. URL: https://ukraineinvest.gov.ua/en/response-to-war/helpdesk/martial-law/.

Хізанов О.,
здобувач ступеня вищої освіти
бакалавра Національної академії
внутрішніх справ
Консультант з мови: **Романов І.**

APPOROCHES TO COMBATE CYBERCRIME AND CYBERTERTORISM: THE EXPERIENCE OF THE USA AND THE EUROPEAN UNION

Cyberspace has become an important part of modern life where we do electronic financial transactions, exchange personal information, and manage important systems like energy and transportation, but as the number of users and the amount of data increases, cyberspace has become the perfect place for cybercriminals to do cybercrime, to steal confidential information and to harm computer systems, and to take advantage of the threat, the United States and the European Union to fight cybercrime, and the Cyberspace has become a field for fighting criminals and law enforcement.

Part 1: American Experience

The U.S. information security development began early in the 19th century. It was during this time that a new U.S. legislation was created in the outside information security area, including an array of federal laws, laws of states and norms, together creating a legal basis for the creation and implementation of state security policies. The basics of them are the National Defense Strategy (2003), a review of cybersecurity (Cyber Security Review, 2009), the Imitations of all – national cyber security issues (2010), the Strategy of the U.S.

Part 2: European Union Experience

In Budapest in 2001, 35 states (Council of Europe countries, as well as Australia, the Dominican Republic, Japan, Panama, and the USA) signed the Convention on Cybercrime, which remains the most relevant international treaty to this day. The Convention calls for the protection of people and their rights against cybercrime. Ukraine ratified the convention in 2005.

The signing of the document was due to the need to cooperate with the state in the investigation or reinvestigation of criminal offenses related to computer systems and data, or for the purpose of collecting evidence in electronic form, although cybercrimes, for the most part, are transnational innature.

Currently, only 10 of the 27 countries of the European Union are currently pursuing cyber security strategies. Currently, the European Strategy of Cybertech, United Kingdom, Finland, France, and the Netherlands has been developed. The European Union is giving great attention to cyber security and cybersecurity. In the context of Digital Europe, European Strategy, which defines the priorities and strategy for the fight against cybercrime. The European Agency for Cybersecurity (ENISA) is an example of how to regulate personal data in the European Union. It calls for high-level cybersecurity and provides high-level frauds.

There are also special cybercrime systems in the EU. They can be divided into two groups in general. The first group is for the formation and implementation of national policy in the fight against cybercrime. The second group is for preventing and investigating crimes in cyberspace. The National Security Policy for cybersecurity policy is for organizing a general complement or foreordination. Yes, the General Competitive Agency is the Finland Security Committee, the Center for National Information Administration, the National Safety Management for Safety and Prevention of Terrorism, the Ministry of Administration and the introduction of Digital Technology in Poland. The series of

foreign countries has also created special organs that are the implementation and policy implementation of cybersecurity policy. This is how the National Service for Information Administration, the National Information Administration, and the Management of Technology, are also available.

So the United States and the European Union have a lot in common with their approach to cybercrime, both of which recognize the importance of co-operation between sectors, including public and private sectors, and they are also actively working on building and improving legislation aimed at counteracting cybercrime.

The fight against cyberspace crime is an important task for modern society, and the United States and the European Union are implementing different approaches to the problem by choosing a combination of legal, technical, and organizational action. Both regions are trying to ensure high levels of cyber security and to cooperate at an international level to achieve this goal. In further research we can take a closer look at specific examples of successful measures and their effect on the reduction of cybercrime.

Список використаних джерел

1. Секрет успіху США у сфері інформаційної безпеки. URL: https://doi.org/10.29038/2524-2679-2018-01-66-71.

2. Закон про Комп'ютерний Закон США. Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

3. Європейська Стратегія Кібербезпеки, Європейська Комісія.

4. Загальний Регламент про Захист Даних (GDPR), Регламент (ЄС) 2016/679.

5. Проблеми боротьби з кіберзлочинністю. міжнародний досвід та українські реалії. URL: http://molodyvcheny.in.ua/ files/journal/ 2019/12.1/13.pdf.

6. Кіберзлочинність: актуальна судова практика. URL: https://biz. ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika.