3. Code pénal Replier Chapitre II : Des atteintes à l'intégrité physique ou psychique de la personne. Articles 222-1 à 222-67. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165282/#LEGISCTA000047052746.

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

## METHODS AND AUTHORITIES OF FIGHTING CYBERCRIME: US AND EU EXPERIENCE

Rapid development of high technologies including information technologies, significantly increases and facilitates the activities of criminals.

There is a series factors that contribute to the development of cybercrime, in particular, the low socio-economic level of a certain state, the imperfection of the legislative framework, the corruption of subjects of power, military conflicts, the lack of international partnership agreements on cooperation to overcome cybercrime, etc. The USA and most of the EU member states in their strategies carry out the issue of combating cybercrime is at the forefront. It was the USA that became the first country to adopt the relevant law and create a National Cyber Security Strategy. The reason for writing this document was the terrorist attack of September 11, 2001. The strategy was part of a more general strategy for ensuring national security. In addition, according to experts' estimates, it is in the USA that the annual losses of corporations from crime exceed 200 billion dollars USA, and 6 billion dollars from computer crimes. USA, so the issue of combating cybercrime is extremely important for this country, to combat cybercrime in the USA, special units and departments were created:

1) United States Secret Service (USSS), which was created in 1865 to investigate and prevent counterfeiting. However, its functions have evolved over the years, and today the US Secret Service fights economic and computer crimes.

2) US federal agency subordinate to the US Department of Homeland Security (subordinated in 2003, before that it was subordinate to the US Treasury). It forms interaction between

services, law enforcement agencies (federal level, state level, local levels), privat sector, academic community, which in their turn detect and prevent cybercrimes.

3) A military unit that operates in cyberspace.

4) National Cyber Defense Division of the US Department of Homeland Security.

5) Department of computer crime and intellectual property.

6) Internet police, network police Along.

With the USA, the active fight against cybercrime is carried out in the countries of the European Union. In the EU, the necessary regulatory and legal foundation for the protection of cyberspace has been created. The EU cyber security strategy was adopted in 2013. Its feature is that the strategy covered various aspects of cyberspace, including the internal market, justice, domestic and foreign policy, and personal data protection.

In Directive 95/46 EC of the European Parliament and of the Council On the protection of natural persons with regard to the processing of personal data and on the free movement of such data" dated October 24, 1995, it is indicated that the principles of protection should be applied to any information relating to an identified person or a person who can be identified, while in order to determine whether a person can be identified, all means, the use of which the controller or any other person is likely to be expected to identify the person (Article 26), to ensure the legality of the processing of personal data, must be taken into account must, among other things, be carried out with the permission of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official powers, or in the legitimate interests of a natural or legal entity, provided that the interests or rights and freedoms of the data subject are taken into account.

It is necessary to mention certain documents of the Council of Europe, such as: Recommendation No. R(91)10 On the transfer to third parties of personal data that are at the disposal of public authorities. Recommendations No. R(99)5 Regarding the protection of privacy life on the internet. Recommendation No. R(97)18 On the Protection of Personal Data Collected and Recorded for Statistical Purposes. Recommendations No. R(2000) 13 On the European policy of access to archives. Recommendations No. R(95)4 On protection of personal data in the field telecommunications,

especially in telephony. All these acts are aimed at ensuring respect for private life, information and correspondence, and also determine the conditions under which it is allowed to limit the relevant right of a person. The fight against cybercrime is one of the most urgent problems of the modem world, and it requires a comprehensive and coordinated approach at different levels. Experience of the United States of America and Europe Union in this area can serve as an important source of learning for other countries and regions. Both entities recognized the need to improve legislation to combat cybercrime and created numerous regulatory acts regulating this aspect. An important part of the fight against cybercrimes is investigation in cyber defense and cyber education. The US and the EU are devoting significant resources to developing and strengthening cyber infrastructure and capabilities to detect and respond to cyber threats.

Summarizing, the experience of the US and the EU in the fight against cybercrime shows that effective protection against cyber threats requires a combination of legal, technical and organizational measures. This includes strong legislation, cooperation between sectors, investment in cyber defense and the ability to respond to new and evolving threats. Achieving this goal is important for ensuring security and stability in the digital world.

***Список використаних джерел***

1. Dnipropetrovsk Regional Universal Scientific Library. URL: https://old.libr.dp.ua/site-libr/?idm=1&idp=184&ida=1898.

2. The secret of the success of the USA in the field of information security.

3. Problems of combating cybercrime: international experience and Ukrainian realities. URL: http://molodyvcheny.in.ua/ files/journal/2019/ 12.1/13.pdf.

4. Protection of personal data in the modern world. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/30929/1/ЗАХИСТ%20ПЕРСОНАЛЬНИХ%20ДАНИХ%20У%20СУЧАСНОМУ%20СВІТІ.pdf.