2. Salomatin AY Fighting corruption in the United States in the XIX century and the state modernization / / Jurisprudence. − 2001. − № 3. S. 196 [Електронний ресурс]. – Режим доступу: https://ua.usembassy.gov/committing-fight-corruption-ukraine/

3. Mikhailov LV Fighting corruption in the U.S. (80 years) / / Questions of history. − 1994, − № 5.S. 149. [Електронний ресурс]. – Режим доступу: https://nabu.gov.ua/en

4. Corruption Perceptions Index 2016: Results [Електронний ресурс]. – Режим доступу: https://www.transparency.org/ news/feature/corruption_perceptions_index_2016/

5. Official website of the company GAN [Електронний ресурс]. – Режим доступу: http://www.ganintegrity.com/

6. Dzhumabekov Z. A. Foreign experience of combating corruption in the system of state service: scientific article / National Academy of Sciences of the Kyrgyz Republic, 2015. – 117–119 p

[Електронний ресурс]. – Режим доступу: https://interactive-science.media/en/article/466443/discussion_platform

Кропивницька В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Гіпська Т.

FIGHT AGAINST CYBERCRIME

The growing statistics of crimes committed in cyberspace demonstrate the ineffectiveness of cybercrime mechanisms, as the cross-border nature of high-tech crimes makes it impossible to combat them effectively within national legal systems alone. That is why, since the end of the twentieth century. States have begun the process of cooperation within various international organizations to counter the threats posed by the latest technologies.

Cybercrime is an evolving form of transnational crime. The complex nature of the crime as one that takes place in the border-less realm of cyberspace is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime and their victims can be located in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response.

The International Criminal Police Organization makes a direct and important contribution to the establishment of international cooperation in the fight against high-tech crime. This organization takes various measures

to support member states in the fight against cybercrime. It provides support to investigations, as well as technical assistance, advice on best investigative practices and training.

INTERPOL has a Global Group of Experts on Cybercrime, which includes experts in various areas of the fight against high-tech crime. According to the Interpol Global Complex for Innovation, the organization coordinates transnational investigations and operations against cybercrime. The Cyber Fusion Centre brings together law enforcement and IT professionals to provide intelligence. In addition, it has a digital forensics laboratory and separate working groups on cybercrime [2].

Within the framework of the European Union, a comprehensive Europe Action Plan and EU substantive law was harmonized through a number of directives. The European Union's cybersecurity strategy, adopted in February 2013, aims to build capacity to prevent cyber threats, including cybercrime and cyberterrorism. The fight against high-tech crime is one of the main priorities of the European Police Office [3].

UNODC promotes long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action. Specifically, UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime [3].

From the point of view of the fundamental legal doctrine - cybercrime consists of criminal acts committed with the help of electronic information and communication means. In other words, cybercrime can be any traditional offline crime (such as theft, fraud, money laundering), but committed on the Internet. Some researchers also single out "hybrid" or "cyber-driven" crimes and cyber-dependent crimes, which have only been made possible by the development of the Internet and related digital technologies. A number of countries have developed special laws aimed at combating cybercrime. For example, Germany, Japan and China have amended the relevant provisions of their criminal codes to describe and combat cybercrime.

EU experience. Some crimes, such as terrorism, human trafficking, sexual abuse of children and drug trafficking, have largely moved to the digital world or been controlled from the Internet. Due to this, the investigation of criminal cases in most of such criminal offenses has a digital component.

The EU has focused its efforts on the above types of cybercrime, and the Council of Europe Convention on Cybercrime has led to the emergence of the following acts:

- directive on Combating Sexual Exploitation of Children on the Internet;
- directive on attacks on information systems;
- regulatory proposals and directives promoting cross-border access to electronic evidence for criminal investigations;
- non-cash fraud directive;
- proposal on temporary regulation of the processing of personal and other data in order to combat sexual violence against children [2].

The European Cybercrime Center has also been set up by Europol and acts as a key body in the fight against cybercrime in the EU. Its aim is to bring together European cybercrime expertise to support cybercrime investigations in the Member States.

Cybercrime is one of the most prolific forms of international crime, with damages set to cost the global economy USD 10.5 trillion annually by 2025, according to Cybersecurity Ventures.

Speaking at the CYBERUK conference in London, UK Foreign Secretary Dominic Raab said: "We are working with like-minded partners, to make sure that the international order that governs cyber activity is fit for purpose. Our aim should be to create a cyberspace that is free, open, peaceful and secure, which benefits all countries and all people. We want to see international law respected in cyberspace, just like anywhere else. And we need to show how the rules apply to these changes in technology, the changes in threats, and the systemic attempts to render the internet a lawless space" [2].

Assessment coordinated by INTERPOL with partners and member countries in Africa found that each act of Internet fraud targeting businesses enabled cybercriminals to steal an average of USD 2.7 million from companies and USD 422,000 from individuals.

The UK's support for INTERPOL's cyber initiative in Africa underlines its commitment to this fight and will be an important piece of the global security architecture to combat cybercrime.

The creation of INTERPOL's new cybercrime desk comes at a time when cybercriminals are attacking the computer networks and systems of individuals, businesses and global organizations when cyber defences might be more vulnerable due to the shift of focus to the pandemic crisis.

The project will provide opportunities to take regular pulse checks on cybercrime in Africa and to publish annual threat landscape assessments that will underpin operational activities.

With UK funding for the two-year initiative amounting to almost GBP 3 million, the Africa cybercrime initiative will be implemented by the

Cybercrime Directorate at the INTERPOL Global Complex for Innovation in Singapore [2].

Urgent measures that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

Список використаних джерел:

1. **Council of Europe.** [Електронний ресурс]. – Режим доступу: https://www.coe.int/en/web/cybercrime/international-cooperation

2. INTERPOL desk targets cybercriminals and Internet fraud in Africa. [Електронний ресурс]. – Режим доступу: https://www.interpol.int/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa

3. United Nations. [Електронний ресурс]. – Режим доступу: https://www.unodc.org/unodc/en/cybercrime/index.html

Кубишин І.,
здобувач ступеня вищої освіти бакалавра Національної академії внутрішніх справ
Консультант з мови: Ващук А.

FOREIGN EXPERIENCE IN COMBATING CYBERCRIMES COMMITTED WITH THE RANSOMWARE

Today, the global problem of the international community is cybercrime, the number of which is growing every year. Utilities and other critical infrastructure are a popular target for cyber attacks.

Since the beginning of 2020, there have been several high-profile attacks by various groups on large corporations, including critical infrastructure operators. Colonial Pipeline has been hit by cybercriminals, resulting in gasoline shortages in several US states. [1] The Washington Police Department, District of Columbia, hackers blocked secret files from the department and demanded $ 4 million to prevent data leaks. The Russian group said they had collected 250 GB of files, including information about informants and the history of the department's staff. The Comparitech report shows that in 2020, 92 attacks by individual ransomware affected more than 600 individual clinics, hospitals and organizations and more than 18 million patient records. Comparitech estimates that the attacks cost nearly $ 21 billion. [2]

Thus, it can be concluded that the need to sharply strengthen cybersecurity around strategically important infrastructure needs to be addressed.

Numerous attacks have led to a significant investment in the development of cybersecurity software products, the creation of teams of