l'échelle locale et régionale. Il porte une lourde responsabilité en matière de sécurité des personnes et des biens. Il est le représentant de l'État dans la gestion des affaires de police et est en contact direct avec les citoyens [3].

La préfecture doit s'adapter en permanence à l'évolution des modes opératoires des délinquants et aux nouvelles menaces (terrorisme, cybercriminalité...).

Les citoyens ont des exigences de plus en plus fortes en matière de sécurité et de qualité de service. La préfecture doit travailler en étroite collaboration avec les autres services de l'État, les collectivités locales et les partenaires privés [1].

Pour conclure il faut dire que la préfecture de police de Paris est une institution essentielle pour la sécurité et le bon fonctionnement de la capitale française. Son rôle est complexe et multiforme, et elle doit faire face à des défis constants.

Список використаних джерел

1. Préfecture de Police. URL: https://www.prefecturedepolice.interieur.
2. Préfecture de police Paris. URL: https://www.pagesjaunes.fr/pros/01672222
3. Préfecture de police (Paris). URL: https://fr.wikipedia.org/wiki/Pr%C3%A9

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

FIGHTING CYBERCRIME IN EUROPE

Technical innovation can be harnessed for social good, but just as readily for nefarious ends. This is truer of cybercrime than of perhaps any other crime area. And cybercriminals are also getting more aggressive. According to the most recent Internet Organised Crime Threat Assessment (IOCTA), cybercrime is becoming more aggressive and confrontational. This can be seen across the various forms of cybercrime, including high-tech crimes, data breaches and sexual extortion.

Cybercrime is one of the EU's priorities in the fight against serious and organized crime as part of EMPACT 2022–2025.

Cybercrime is a growing problem for countries, such as EU Member States, in most of which internet infrastructure is well developed and payment systems are online.

But it is not just financial data, but data more generally, that is a key target for cybercriminals. The number and frequency of data breaches are on the rise, and this in turn is leading to more cases of fraud and extortion.

The sheer range of opportunities that cybercriminals have sought to exploit is impressive. These crimes include: using botnets—networks of

devices infected with malware without their users' knowledge;creating «back doors» on compromised devices to allow the theft of money and data, or remote access to the devices to create botnets;creating online fora to trade hacking expertise; bulletproof hosting and creating counter-anti-virus services;laundering traditional and virtual currencies;committing online fraud, such as through online payment systems, carding and social engineering;various forms of online child sexual exploitation;the online hosting of operations involving the sale of weapons, false passports, counterfeit and cloned credit cards, and drugs, and hacking services [1].

Legal Framework:

Cybercrime Convention

The convention aims to help in the fight against crimes that can only be committed through the use of technology, where the devices are both the tool for committing the crime and the target of the crime, and crimes where technology has been used to enhance another crime, such as fraud. It provides guidelines for any country developing domestic laws on cybercrime and serves as a basis for **international cooperation** between parties to the convention.

The first additional protocol aims to criminalise the dissemination of racist and xenophobic material through computer systems, along with racist and xenophobic-motivated threats and insults.

The second additional protocol aims to provide common rules at international level to enhance cooperation on cybercrime and the collection of evidence in electronic form for criminal investigations or proceedings.

The decision authorizes European Union (EU) Member States to ratify the second additional protocol in the interest of the EU [2].

The EU has implemented various directives and regulations to enhance cybersecurity, such as **the Network and Information Security (NIS) Directive** is a legislative framework designed to enhance cybersecurity across the European Union by establishing a high common level of security for network and information systems. It builds upon the original NIS Directive, expanding its scope and strengthening requirements to better address evolving cyber threats. The directive mandates an "all-hazards" approach, meaning that entities must be prepared to address a wide range of threats, from cyberattacks to physical disruptions, ensuring comprehensive protection and resilience in their operations [3].

European Union (EU) citizens and regulators have created the strongest and most effective legal framework for compliance with data protection standards to date, the General Data Protection Regulation (GDPR)These laws impose stricter security requirements on businesses and organizations, helping to prevent cyber attacks [4].

The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online

crime. Since its establishment in 2013, EC3 has made a significant contribution to the fight against cybercrime and it has been involved in many high-profile operations and hundreds of operational-support deployments. C3 offers operational, strategic, analytical and forensic support to Member States' investigations. For each of the cybercrime types mentioned above, EC3:

- serves as the central hub for criminal information and intelligence;
- supports operations and investigations by Member States by offering operational analysis, coordination and expertise;
- provides highly specialized technical and digital forensic support capabilities to investigations and operations;
- provides support to EU crisis management structures, within the scope of Europol's mandate, and facilitates the operational, technical and strategic collaboration between law enforcement agencies (LEAs) and other relevant cyber communities and EU institutions, bodies and agencies (e.g. Eurojust, EEAS, ENISA, CERT-EU, Commission, Council, etc.);
- provides 24/7 operational and technical support to LEAs for immediate reaction to urgent cyber incidents and/or cyber crises via stand-by duty and the EU Law Enforcement Emergency Response Protocol (EU LE ERP);
- hosts and facilitates the efforts of the Joint Cybercrime Action Taskforce (J-CAT) in combating cybercrime;
- supports training and capacity-building, in particular for the relevant authorities in Member States;
- provides a variety of strategic analysis products that enable informed decision-making on combating and preventing cybercrime;
- provides a comprehensive outreach function connecting law enforcement authorities tackling cybercrime with the private sector, academia and other non-law enforcement partners;
- contributes to the preparation and delivery of standardised prevention and awareness campaigns and activities in the cybercrime-mandated areas [5].

Funded by the European Commission and working in close cooperation with Europol-EC3 and CEPOL, both members of the Advisory Group, ECTEG activities aim to:

- Support international activities to harmonize cybercrime training across international borders.
- Share knowledge, expertise and find training solutions.
- Promote standardization of methods and procedures for training programmes and cooperation with other international organizations.
- Collaborate with academic partners to establish recognized academic qualifications in the field of cybercrime and work with

universities that have already created such awards making them available across international borders.

- Collaborate with industry partners to establish frameworks whereby their existing and future efforts support law enforcement by the delivery of training, harmonized into an effective programme, making best use of available resources.
- Provide training and education material and reference trainers to international partners, supporting their efforts to instruct law enforcement on cybercrime issues globally [6].

Cybercrime is a serious threat that is on the rise. As we share more and more business and personal information online, criminals find new ways to steal and use that data for illegal purposes and financial gain.As this risk continues to grow in our daily lives, it's important to understand how cybercrime has become such a major problem, why we're all so vulnerable to it, and what steps we can take to protect ourselves.

Список використаних джерел

1. Cybercrime. URL: https://www.europol.europa.eu/

2.Convention on cybercrime. URL: https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html

3.The NIS 2 Directive URL: https://www.nis-2-directive.com/

4.The European Union General Data Protection Regulation URL: https://www.stimson.org/2024/the-european-union-p rotection-regulation/

5.The European Cybercrime Centre (EC3) URL: https://www.europol.europa.eu/about-europol/european-cybercrime- ec3

6. European Cybercrime Training and Education Group URL: https://www.ecteg.eu/

Бандура Б.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Драмарецька Л.**

COUNTERACTING CYBERCRIME IN GERMANY

Today, the world is more digitally connected than ever before. Criminals take advantage of this online transformation to target weaknesses in online systems, networks and infrastructure. There is a massive economic and social impact on governments, businesses and individuals worldwide.

Phishing, ransom ware and data breaches are just a few examples of current cyber threats, while new types of cybercrime are emerging all the time. Cybercriminals are increasingly agile and organized – exploiting new technologies, tailoring their attacks and cooperating in new ways.

Cybercrimes know no national borders. Criminals, victims and technical infrastructure span multiple jurisdictions, bringing many challenges to investigations and prosecutions [1].