Список використаних джерел

1. Law of Ukraine "On the National Police". Verkhovna Rada of Ukraine, 2015. Retrieved from https://zakon.rada.gov.ua/laws/show/580-19.

2. Verkhovna Rada of Ukraine. Amendments to the Law on the National Police during Martial Law. Verkhovna Rada of Ukraine. 2022. Retrieved from https://zakon.rada.gov.ua/laws/show/2102-20.

3. Ministry of Internal Affairs of Ukraine. Reform of the National Police during Martial Law. Ministry of Internal Affairs. 2022. Retrieved from https://mvs.gov.ua/en/news/national-police-reforms-2022.

4. Europol. Cooperation between Europol and the National Police of Ukraine during Martial Law. Europol. 2022. Retrieved from https://www.europol.europa.eu.

5. Interpol. International Collaboration with Ukraine's National Police: A Response to Transnational Crime during Wartime. Interpol. 2022. Retrieved from https://www.interpol.int.

6. National Police of Ukraine. Specialized Units in Response to Wartime Threats. National Police of Ukraine. 2023. Retrieved from https://www.npu.gov.ua/en/news/special-units-in-martial-law.

7. Ministry of Justice of Ukraine. Changes in Legislation and New Powers of the National Police During Martial Law. Ministry of Justice. 2022. Retrieved from https://minjust.gov.ua/en.

8. United Nations Office on Drugs and Crime. Ukraine's National Police and War Crimes Documentation. UNODC. 2023. Retrieved from https://www.unodc.org.

Сокол Д.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Василенко О.В.**

COUNTERING AND FIGHTING CYBERCRIME IN EUROPE

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. Europe, as a leading region in digital technology and innovation, faces an increasing number of cyber-attacks aimed at disrupting critical infrastructure, stealing confidential information, and causing financial damage. There is a massive economic and social impact on governments, businesses and individuals worldwide. Phishing, ransomware and data breaches are just a few examples of current cyberthreats, 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. Combating this threat is becoming more challenging due to the continuous evolution of techniques and methods employed by criminals. Cybercrimes

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

Cybercrime is a broad term that encompasses many malicious activities exploiting digital technologies, affecting individuals, businesses and governments worldwide. Cybercrime involves unlawful actions executed using computers or the internet, focusing on attacking networks, stealing data, or committing fraud. This encompasses activities like unauthorized system access, identity theft, and online scams [1].

Understanding the most common types of cybercrime is key to fighting it. Consider some of the most common:

1) A DDoS attack targets websites and servers by disrupting network services in an attempt to exhaust an application's resources. The perpetrators behind these attacks flood a site with errant traffic, resulting in poor website functionality or knocking it offline altogether. DDoS attacks are wide-reaching, targeting all sorts of industries and company sizes worldwide. Certain industries, such as gaming, ecommerce, and telecommunications, are targeted more than others. DDoS attacks are some of the most common cyberthreats, and they can potentially compromise your business, online security, sales, and reputation [2].

2) Ransomware is a type of malicious software, or malware, that threatens a victim by destroying or blocking access to critical data or systems until a ransom is paid. Historically, most ransomware targeted individuals, but more recently, human-operated ransomware, which targets organizations, has become the larger and more difficult threat to prevent and reverse. With human-operated ransomware, a group of attackers use their collective intelligence to gain access to an organization's enterprise network. Some attacks of this kind are so sophisticated that the attackers use internal financial documents they've uncovered to set the ransom price [3].

3) Identity theft, as it states, is when someone steals another person's identity, i.e. personal information such as a social security number, with the intent to commit fraud, usually for economic gain. Obviously aware that they have stolen another person's identity, the offender's intention is to use it to create new accounts or tamper with existing accounts under the stolen identity. All sensitive personal information is at risk, as the person committing the crime will have access to a list of resources connected to the stolen identity. These resources can then be used to create accounts in industries such as medical, financial, insurance and so on [4].

4) Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. It asks the consumer to provide personal identifying information. Then a scammer uses the information to open new accounts, or invade the consumer's existing accounts [5].

Cybercrime is one of the most prolific forms of transnational crime. Highly complex cyber threats such as Malware, Distributed Denial-of-Service (DDoS) and Ransomware bring new challenges to law enforcement – including large volumes of data, cross-border investigations, and new areas of technical knowledge.

Given the constant evolution of the cybercrime landscape, police agencies need to share information and knowledge with their counterparts around the world to develop a timely, intelligence-based response.

To achieve this, the European Union Agency for Cybersecurity (ENISA) was established in 2004. It cooperates with EU countries and institutions and helps to make the EU more resilient against cyber-attacks, in particular by contributing to cyber policy, operational cooperation and capacity building. Current key topics include fostering cloud computing security, ensuring the robustness of critical infrastructure against attacks as well as providing resources regarding the cybersecurity [6]. Additionally, the European Union's law enforcement agency Europol established the European Cybercrime Centre (EC3) in 2013, to 'help protect European citizens, businesses and governments from online crime'. It has since been involved in high-profile operations as well as on-the-spot operational support, and also made cybercrime one of its priority areas.

Given this increase in the frequency of cybercrime and the growing digital connectedness of the EU, a 2019 Regulation on cybersecurity (replacing the 2013 Cybersecurity Act) aims at ensuring the proper functioning of the internal market and a high level of cybersecurity, cyber resilience and trust within the Union. In the course of adopting the regulation, the European Parliament highlighted the importance of a common response to cyber-attacks, helped by expertise provided through the European Union Agency for Cybersecurity. This is also meant to facilitate operational cooperation between EU countries. The European Parliament had previously adopted a resolution on the fight against cybercrime in October 2017, where it underlined that fighting cybercrime should be first and foremost about safeguarding and hardening critical infrastructures and other networked devices and not only pursuing repressive measures [7].

The Commission presented a new cybersecurity strategy. The strategy aims to bolster Europe's collective resilience against cyber threats. Specifically, the Commission put forward legislative proposals on the security of network and information systems and on the protection of critical infrastructure. Both proposals aim to address both cyber and physical resilience of critical entities and networks: the European Parliament and EU countries are working on these proposals.

In conclusion, the ongoing digital transformation has made the world more interconnected, but it has also created new vulnerabilities that cybercriminals exploit. Europe, as a leader in digital innovation, faces

significant challenges from cyber-attacks targeting critical infrastructure and sensitive information. The economic and social impacts of cybercrime are profound, affecting governments, businesses, and individuals worldwide. With the continuous evolution of cyber threats and the increasing sophistication of cybercriminals, combating cybercrime requires a comprehensive and coordinated approach. To enhance cybersecurity, it is essential to implement innovative technologies, strengthen critical infrastructure, and foster resilience against cyber threats. Legislative efforts, such as the EU's new cybersecurity strategy, aim to bolster the collective defense against cyber-attacks and ensure a high level of cybersecurity within the Union. As the cybercrime landscape continues to evolve, ongoing research, cooperation, and proactive measures will be vital in safeguarding the digital future of Europe and the world.

Список використаних джерел

1. Types of Cyber Crime: A Guide to Prevention & Impact. URL: https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/
2. What is a DDoS attack? URL: https://www.microsoft.com/en-gb/security/business/security-101/what-is-a-ddos-attack
3. What is ransomware? URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-ransomware
4. Identity Theft URL: https://www.idnow.io/glossary/identity-theft/
5. Phishing Scams and How to Spot Them. URL: https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams
6. Fighting cybercrime in the two Europes. URL: https://shs.cairn.info/revue-internationale-de-droit-penal-2006-3-page
7. What is the EU doing to combat cybercrime. URL: https://epthinktank.eu/2021/03/25/what-is-the-eu-doing-to-combat

Старовойт А.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Сторожук О**.

TECHNOLOGICAL INNOVATIONS IN COUNTER-TERRORISM: THE EXPERIENCE OF ISRAEL

Israel’s counter-terrorism strategies are renowned for their use of cutting-edge technologies to detect, prevent, and respond to terrorist threats. Due to its unique geopolitical position, Israel has been at the forefront of developing and implementing technological innovations in national security. This thesis will explore the technological tools Israel has pioneered to combat terrorism, focusing on intelligence gathering, cybersecurity, and advanced monitoring systems.