of committing a crime or to deliver persons in need of medical care to medical institutions, or to travel to the crime scene [2];

An important feature of provision public safety and order by the National Police of Ukraine under martial law is effective interaction with volunteers, territorial defense units, namely in accordance with Clause 3 of Article 3 of the Law of Ukraine "On Basics of National Resistance":

1) response and taking the necessary measures defense of the territory and protection of the population in certain territory before the deployment of within such territory of the troop group(forces) and/or groups of joint forces, intended for conducting hostilities actions to repel armed aggression against Ukraine;

2) participation in the protection and defense of important objects and communications, other critical infrastructure objects, determined by the Cabinet of Ministers of Ukraine [1].

Список використаних джерел

1. Закон України «Про основи національного спротиву» від 22.05.2024р. стаття №3 пункт №3. URL: https://ips.ligazakon.net /document/T211702?an=29

2. Постанова Кабінету Міністрів України «Питання запровадження та здійснення деяких заходів правового режиму воєнного стану» від 08.07.2020 № 573. URL: https://zakon.rada.gov.ua /laws/show/573-2020-%D0%BF#Text

3. Про затвердження Положення про функціональну підсистему забезпечення публічної (громадської) безпеки і порядку, безпеки дорожнього руху єдиної державної системи цивільного захисту: Наказ МВС України від 04.10.2019 № 835. URL: https://zakon.rada.gov.ua /laws/show/z1199-19#Text

4. Про затвердження Порядку організації взаємодії Національної гвардії України та Національної поліції України під час забезпечення (охорони) публічної (громадської) безпеки і порядку: Наказ Міністерства внутрішніх справ України від 10.08.2016 № 773. URL: https://ips.ligazakon.net/document/re29353

Гуменюк М.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Волік О.**

COMBATING CYBERCRIME INTERNATIONAL EXPERIENCE

Cybercrime is one of the most significant threats to the modern world, especially for countries in the Americas with advanced infrastructure and high levels of digitalization. Cyberattacks impact both the public and private sectors, threatening national security, the economy, and citizens' privacy. Major threats include financial fraud, data theft, phishing, and

ransomware attacks. Combating cybercrime requires coordinated efforts across legislation, technology, and international cooperation.

Countries in the Americas have seen a significant increase in cybercrime. According to data from Cybersecurity Ventures, cybercrime-related losses continue to grow annually, and this trend is expected to persist. North America, especially the United States, is one of the most affected regions by cyberattacks, but Latin American countries are also facing increasingly sophisticated threats. Major types of cyberattacks include phishing, DDoS attacks, financial fraud, identity theft, attacks on critical infrastructure, and ransomware.

The United States leads in developing a legal framework to combat cybercrime in the region. Key laws include [1]:

– Computer Fraud and Abuse Act (CFAA) – the primary law governing criminal liability for unauthorized access to computer systems.

– Cybersecurity Information Sharing Act (CISA) – allows private companies to share cyber threat information with the government to improve response capabilities.

– U.S. Agencies' Role – The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) are responsible for ensuring cybersecurity at the national level.

Fighting cybercrime requires international cooperation, as most crimes cross national borders. In the Americas, international initiatives include:

– Organization of American States (OAS) – coordinates between regional countries, promoting information sharing and cybersecurity policy development.

– Budapest Convention – an international treaty that some countries in the Americas have joined to facilitate cooperation and standardize cybercrime laws.

– Training Programs and Technology Exchange – the U.S., Canada, Brazil, Argentina, and others conduct joint training programs to improve the skills of cybersecurity professionals.

Developing cybersecurity infrastructure is a key component in combating cybercrime. In the U.S., multiple cybersecurity centers, such as the National Cybersecurity Center, are dedicated to protecting critical infrastructure. Programs like the National Initiative for Cybersecurity Education (NICE) are designed to enhance the skills of cybersecurity personnel and increase the number of professionals in the field.

Modern technologies are crucial tools in the fight against cybercrime:

Artificial Intelligence (AI) enables real-time detection and response to threats.

Big Data Analytics helps identify anomalies and potential threats.

Blockchain is being implemented to ensure transaction transparency and reduce fraud risks [1].

Ransomware attacks are a severe threat to the Americas. In the U.S., the Ransomware Task Force coordinates actions to prevent these attacks. Strategies include prohibiting ransom payments to cybercriminals, increasing accountability for cooperating with such groups, and developing assistance plans for companies affected by attacks.

The private sector is a primary target for cyberattacks. Many small and medium-sized businesses have limited resources for protection. To improve business security, cybersecurity standards like the NIST Cybersecurity Framework are widely implemented, helping businesses combat phishing, data theft, and malware [2].

In Latin American countries, resources to combat cybercrime are limited, but these nations are actively developing legal frameworks and cooperating with international organizations. For example:

Brazil and Mexico are creating national cybersecurity strategies and strengthening cyber-policing.

With support from international organizations like the UN and OAS, Latin American countries are developing technological capabilities and improving the skills of professionals [3].

Education is an essential component of cybercrime prevention. American countries conduct cybersecurity awareness programs for students and national campaigns that educate citizens about phishing threats, identity theft, and safe internet use.

Therefore combating cybercrime in the Americas requires a comprehensive approach that includes legislative initiatives, international cooperation, technology development, specialist training, and public awareness. Only through joint efforts can American countries effectively respond to cyber threats and protect critical infrastructure, businesses, and citizens' personal data from cyberattacks.

Список використаних джерел

1. Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It. Ecco, 2020.

2. Melnick, Jaime, and Donald McLellan. Combating Cybercrime and Cyberterrorism: Challenges and Trends in the Americas. Springer, 2020.

3. Kshetri, Nir. Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan, 2023.