In general, the work of law enforcement agencies consists in maintaining order in society and the state as a whole. The police are working hard to achieve this goal both in the conditions of martial law and during peaceful life.

Список використаних джерел

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII.

2. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII.

3. Про правовий статус осіб, зниклих безвісти із змінами, внесеними згідно із Законами № 113-IX від 19.09.2019, ВВР, 2019, № 42, ст. 238 № 2191-IX від 14.04.2022: Закон України від 12.07.2018 № 2505-VIII.

4. Про внесення змін до деяких законів України щодо присвоєння спеціальних звань поліції під час дії воєнного стану: Закон України від 24.03.2022 № 2151-IX.

5. Про Дисциплінарний статут Національної поліції України: Закон України від 15.03.2018 № 2337-VIII.

6. Хатнюк Ю. А. Актуальні проблеми організації охорони громадського порядку: курс лекцій. Львів: Львівський державний університет внутрішніх справ, 2020. 168 с.

Ковандра А.,
здобувач ступеня вищої освіти
бакалавра Національної академії
внутрішніх справ
Консультант з мови: **Зубенко В.**

LAW ENFORCEMENT VERSUS CYBERCRIME

Over the years the criminal landscape has changed dramatically. The worldwide online cyber crime realm is increasingly displacing conventional forms of property crime, such as burglary and robbery, blurring the lines between traditional crime and cybercrime. With the exception of some violent crimes, it is becoming more and more evident that almost every conceivable crime, in this day and age, has a cyber element to it.

To discuss cybercrime, we will first define crime, which is an act or omission that harms any social, political, moral or legal good that is punishable by law.

Cybercrime is a type of crime involving a computer or a computer network. Warren Buffett describes cybercrime as the

"number one problem with mankind" and said that it "poses real risks to humanity" [3].

Cybercrime is one of those notions that did not exist 30 years ago.

The question is often asked how cybercrime came about. Normally this is related to the invention of the computer and computer network but also the internet. As soon as it was widely recognized that computers store something of value (information), criminals saw an opportunity.

The availability of virtual spaces to public and private sectors has allowed cybercrime to become an everyday occurrence.

Cybercrimes, which differ significantly from conventional crimes in many dimensions, are frequently difficult to identify and prosecute. Technology is changing the environment every day, it affects the civilian and military infrastructure in all sectors. We can note the effects of that through the cyber-attacks that the United States of America, Ukraine and other countries were exposed to, which were announced in various media.

One of the major reasons for the increase in cyber crime is technological innovation. Technology is expanding rapidly and in many cases is unpredictable, cybercrime has been expanding, with such innovations, to affect virtually all other criminal activities.

In this digital age, it is more important than ever for communities to learn of the dangers of cybercrime, and how to protect themselves from it. This is where law enforcement is needed.

Due to the intense activity of cyber criminals, authorities in many countries have long been looking for legal and technological solutions to effectively combat computer crime.

In the United States, the FBI leads the national effort to counter cybercrimes, including cyberterrorism, espionage, computer hacking, and major cyber fraud. The FBI continuously adapts to meet the challenges posed by online criminals.

Moreover, the FBI has the support of cybersecurity specialists working in embassies around the world and collaborates with international institutions that fight against cybercrime.

For a long time, Poland has been developing units operating in the field of cybersecurity, both civilian and military ones. The Central Office for Combating Cybercrime, which performs tasks related to the creation of conditions for the effective detection of perpetrators of crimes, committed with the use of modern information and communication technologies, has been operating under the auspices of the National Police Headquarters for many years.

In Ukraine similar bodies also exist-in particular, Department of Cyber policies of the National Police of Ukraine.

As with all Ukrainian police, the number one challenge that the Cyber Police Department faces is ensuring that the law is followed.

The law enforcement agency typically focuses its efforts on online fraud, scams, and other forms of financially-motivated cybercrime. But when Russian invaded Ukraine in February, the Cyber Police started seeing a surge in new types of attacks.

We primarily focus on countering distributed denial-of-service [DDoS] attacks and attacks against media organizations, analyzing the enemy's information space, collecting information regarding cyber incidents, developing projects to support the army and volunteers, and safeguarding information resources. We also focus on international cooperation, and securing our operational work at an appropriate level across key areas including the banking sector, online fraud, cybercrime, and crimes relating to illegal content.

Methods of cybercrime detective work are dynamic and constantly improving, whether in closed police units or in international cooperation framework.

During investigations of cybercrimes and cyber incidents, the Cyber Police Department exchanges information with international law enforcement agencies through communications channels with Europol and Interpol.

INTERPOL Cyber Fusion Center has begun a collaboration with cybersecurity key players to distribute information on the latest online scams, cyber threats and risks to internet users.

The cyber front of the Russo-Ukrainian War is highly dynamic and continues to evolve. The lessons learned are already informing our knowledge of cyber warfare and are likely to remain a key subject of study in the coming decades for anyone interested in cyber security. Indeed, Estonian PM Kaja Kallas recently published an article in The Economist claiming that Ukraine is "giving the free world a masterclass on cyber defense" [1].

Список використаних джерел

1. Russia's invasion of Ukraine is also being fought in cyberspace. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/russias-invasion-of-ukraine-is-also-being-fought-in-cyberspace.

2. Blueline. Policing cybercrime. URL: https://www.blueline.ca/policing-cybercrime/.

3. Wikipedia. Cybercrime. URL : https://en.wikipedia.org/wiki/Cyber crime.

4. Scientific research. Enhancing Police Officers' Cybercrime Investigation Skills Using a Checklist Tool. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=124124.

5. The Impact Of Cyber Crimes And How Law Enforcement Is Adapting. URL: https://saltcommunications.com/news/law-enforcement-adapting-to-cyber-crime/.

6. How Ukraine's Cyber Police fights fraud, scams, and attacks on critical infrastructure. URL: https://therecord.media/how-ukraines-cyber-police-fights-fraud-scams-and-attacks-on-critical-infrastructure.

7. Law Enforcement Versus Cybercrime. URL: https://warsawinsti tute.org/law-enforcement-versus-cybercrime/.

Козубенко А.,
здобувач ступеня вищої освіти
бакалавра Національної академії
внутрішніх справ
Консультант з мови: **Зубенко В.**

PROTECTION OF CITIZENS' RIGHTS AND ENSURING LAWFULNESS BY THE POLICE DURING WARTIME

In times of war and conflict, the role of the police becomes particularly complex, as they are tasked with maintaining law and order while upholding the rights of citizens. This article examines the most important task of protecting the rights of citizens and ensuring the legitimacy of the militia during wartime. It delves into the unique challenges law enforcement officers' face, the need to balance security and civil liberties, the legal frameworks that guide their actions, and the importance of specialized training and strategies.

The primary role of the police during wartime is to maintain law and order within the constraints of the conflict. Their responsibilities may extend to enforcing curfews, regulating movement, and responding to civil disturbances that can arise in times of crisis [1].

This role can encompass a range of responsibilities that are crucial for preserving stability and protecting citizens' rights:

– Enforcing Curfews: One of the fundamental tasks of the police during wartime is to enforce curfews. Curfews are imposed to restrict civilian movement during certain hours, typically during the night or in areas of heightened conflict. This measure helps minimize the risk of individuals being caught in the crossfire or engaging in activities that could exacerbate the conflict. Police officers are