Liashenko Yelyzaveta,
cadet of the 3rd year of the Institute № 2
of the National Academy of Internal Affairs,
specialty «Law»

Language Adviser:
Vasylenko Olena,
Professor of the Legal Linguistics Department
of the National Academy of Internal Affairs,
Candidate of Pedagogical Sciences,
Associate Professor

ACTIVITY OF LAW ENFORCEMENT AGENCIES IN THE INVESTIGATION OF CYBERCRIME IN CANADA

A cybercrime is a criminal infraction that uses the computer or network as the source, tool, target or place of a crime. The main types of cybercrime police investigate are:

1. Crimes against persons (luring, child pornography, harassment, extortion, threats, false messages hate propaganda bullying defamatory libel suicide 1inducement
2. Crimes against property unauthorized use of a computer fraud computer virus.

Every day there are news stories about the latest victims of data breaches and identity theft and of information technology systems crippled by cyber attacks. Private citizens, businesses, and government organizations are all at risk of falling under attack, and police departments are far from immune. Across the Canada, state and local law enforcement organizations have dealt with threats to their IT systems and data, many lacking the expertise and knowledge to respond quickly and mitigate the damage [4].

Fraud and scams are almost certainly the most common form of cybercrime, including malicious cyber threat activity such as phishing, result in significant financial losses. According to the CAFC there were 70,878 reports of fraud in Canada with over $530 million stolen in 2022 [1]

Law enforcement agencies in Canada actively investigate cybercrimes through specialized units like the Royal Canadian Mounted Police (RCMP) National Cybercrime Coordination Centre and the Canadian Anti-Fraud Centre. The Royal Canadian Mounted Police's (RCMP) National Cybercrime Coordination Centre coordinates responses to cybercrime and provides guidance to Canadian police. They are the only federal organization with the mandate and authority to investigate criminal

offences related to cybercrime and typically investigate international cybercrime and cybercrime with a national security implication [3].

The RCMP has a broad mandate when it comes to investigating and apprehending criminals in the online world, or otherwise disrupting cybercrime activity. The RCMP Cybercrime Strategy is therefore broad in scope and reflects the role of cyber in several law enforcement areas. The RCMP Cybercrime Strategy's vision is to reduce the threat, impact and victimization of cybercrime in Canada through law enforcement action. The following three pillars are identified within the strategy to guide the RCMP's efforts in combating cybercrime: identify and prioritize cybercrime threats through intelligence collection and analysis; pursue cybercrime through targeted enforcement and investigative action; and, support cybercrime investigations with specialized skills, tools and training [2].

The criminal exploitation of new and emerging technologies requires new policing measures to keep pace in a digital era. The same technologies that people and organizations use for legitimate purposes may be used by criminals to mask their online activities and evade detection from law enforcement. Police must often find technical solutions to decrypt, unlock or otherwise deal with encryption technologies, re-routed Internet Protocol (IP) addresses and other technical roadblocks that criminals exploit to cover their digital tracks and commit cybercrimes.

To varying degrees, cybercrimes affect Canadians in real and harmful ways. For law enforcement, addressing cybercrime requires broad-based domestic and international police cooperation, engagement with public and private sector organizations, and integrating new technical skills and tools with traditional enforcement measures.

In conclusion, it can be inferred that law enforcement agencies in Canada are actively engaged in investigating cybercrimes, collaborating both domestically and internationally. They employ advanced technologies and specialized units to detect and prosecute cybercriminals, aiming to ensure the safety of internet users in Canada.

References:

1. Baseline cyber threat assessment: Cybercrime. Canadian Center for Cyber Security.

2. Royal Canadian Mounted Police Cybercrime Strategy. RSMP-grc.gc.ca.

3. Cyber Security Incidents in Canada. URL.: https://gowlingwlg.com/en/insights-resources/articles/2023/reporting-cyber-security-incidents-canada/.

4. Cyber security emerging challenge for law enforcement. URL.: https://www.policechiefmagazine.org/cybersecurity-for-all-law - enforcement/.

Nesterova Maria,
cadet of the 1st year of the Institute № 1 of the National Academy of Internal Affairs, specialty «Law enforcement activity»

Language adviser:
Loputko Olena,
Associate Professor of the Legal Linguistics Department
of the National Academy of Internal Affairs, Candidate of Pedagogical Sciences, Associate Professor

RELATIONSHIP BETWEEN ECONOMIC AND ORGANIZED CRIME IN MODERN SOCIETY

Thanks to the presence of stable social connections, the possibility of free movement of people, money and goods, there has been an evolution not only in social and cultural development, but also in the development of illegal actions, including those that can be classified as organized crime, terrorism, etc. Economic crime associated with organized crime is the focus of attention not only of the authorities of Ukraine, but also of other states. In addition to government bodies of different countries, international organizations and institutions also deal with the problems of this type of crime. The connection between economic and organized crime, a subtype of which can be considered economic, is directly proportional, since the development of any of these types of crime entails the development of another type, since economic crime developed with the development of the economy and business, information and communication technologies. Legal, as well as related criminological and criminological and other related scientific disciplines do not have a common opinion on the concept and definition of organized crime. However, theorists of these scientific disciplines generally agree that organized crime began to develop along with the development of modern states. One of the most influential and cited foreign theorists dealing with organized crime is Howard Abadinsky. Abadinsky views organized crime as “a non-ideological association existing