

Paket prohramm “Dekanat” [Software Package “Dean’s Office”]. Retrieved from: <http://www.politek-soft.kiev.ua/ru/index.php?do=products&product=deanery> [in Ukrainian].

Mariia Nadolna, Anastasiia Rudenko
Vasyl’ Stus Donetsk National University
Vinnytsia

Research Supervisor: I.Y. Zhdanova, PhD in Criminal Law, Assoc. Prof.
Language Advisor: O.O. Odintsova, Senior Lecturer

INTERPOL ACTIVITIES TO COORDINATE COOPERATION TO FIGHT CYBER CRIME

Introduction. In today’s world, information technology has spread to all areas of society, providing access to a large amount of information that becomes a weapon in the hands of criminals. Therefore, high-tech crime occupies a special place among socially dangerous acts and is one of the threats to the global security of mankind.

Thus, Yu. Maksymenko notes that the formation of the information society has both undoubted positive and certain negative consequences. On the one hand, the transfer of large amounts of information has accelerated, its processing and implementation have accelerated. On the other hand, the spread of illegal collection and use of information, unauthorized access to information resources, illegal copying of information in electronic systems, theft of information from libraries, archives, banks and databases, violation of information processing technologies, launch of viruses, destruction are serious concerns and modification of data in information systems, interception of information in technical channels of its source, manipulation of public and individual consciousness, etc. The transformation of society into information has changed the status of information. Today, it can be both a means of security and a threat and danger [1].

In developed countries, the economic losses from the progression of cybercrime are measured in very significant amounts. For example, according to Interpol, the losses of European economies from cybercriminals amount to 750 billion euros annually. According to LACNIC, which analyzes Internet activity, US cybercrime losses range from \$20 billion to \$140 billion, or about 1% of the country’s GDP, and in Latin America, cybercrime losses are \$1.1 billion [2].

According to Interpol, the rate of increase in crime on the global computer network is the highest compared to other types of crime, including drug and arms trafficking [3].

Therefore, the urgency of this problem is due to the fact that high-tech crime requires a concerted international effort to combat it. Thus, the importance of Interpol's activity as a universal international organization that coordinates the cooperation of states on this issue is growing.

Review of recent publications. Some aspects of the development and formation of information relations, the implementation of the fight against cybercrime were considered by leading domestic scientists M. Budakov, V. Butuzov, M. Galamboy, R. Kalyuzhnyy, V. Kovalenko, Ya. Kondratiev, B. Kormich, Yu. Maksymenko, A. Marushchak, G. Novitsky and foreign experts A. Robert, K. Osakwe, T. Blentan, D. Banisar and others. The issue of Interpol's activities in the field of high technologies was researched by N. Moroz.

Objectives of the paper. The purpose of this study is to determine the role of Interpol in coordinating international cooperation against the spread of cybercrime and search for methods to prevent cybercrime.

Results of the research. Today in Ukraine there are certain laws and regulations of various levels that regulate the cybersecurity of the state. We can distinguish the Law "On the State Service for Special Communications and Information Protection of Ukraine" as of 23.02.2006, the Law "On Information" as of 02.10.1992, the Law "On State Secrets" as of 21.01.1994, the Law "On Information Protection in Information and Telecommunication Systems" as of 05.07.1994, and the Law "On Fundamentals of National Security of Ukraine" as of 19.06.2003. It is also worth noting that currently there are two strategic documents: the National Security Strategy of Ukraine and the Doctrine of Information Security of Ukraine.

An organization such as Interpol deals with international security issues. In Ukraine, the Cabinet of Ministers issued a resolution "On the National Central Bureau of Interpol".

The International Criminal Police Organization (Interpol) is an international organization that searches for a certain person and ensures the exchange of information between the police departments of different countries in the fight crimes [4]. Cybercrime is also one of its sphere of activity. Interpol offers states support in the investigation of cybercrime, works on the development of new innovative technologies and develops actionable intelligence to prevent and counter cybercrimes.

This organization makes a direct and important contribution to establishing international cooperation in the fight against high-tech crime. Interpol takes a variety of steps to support States Parties in the fight against cybercrime, as well as providing support to investigations, as well as providing technical assistance, guidance on best investigative practices and training. INTERPOL has a Global Group of Experts on Cybercrime, which includes experts in various areas of the fight against high-tech crime. According to the Interpol Global Complex for Innovation (IGCI), the organization coordinates transnational investigations and operations against cybercrime (for example, such as Unmask (2012), Strikeback (2014), Aces (2015), Simbobotnet (2015), Singapore (2017)).

The CyberFusionCentre (CFC) brings together law enforcement and IT professionals to provide intelligence. In addition, INTERPOL has a digital forensics laboratory and separate working groups on cybercrime [5]. In his work, S. Schjolberg said that an important step in establishing cooperation in the fighting cybercrime was

the holding of the 1979 Paris Conference and the First International Conference of Interpol on Cybercrime [6].

To coordinate cooperation in the fight against cybercrime, Interpol can apply various activities which we will consider. First, it is important for the General Assembly to adopt regulations relating to cybercrimes. Such acts include various resolutions, which are set out on the official website of Interpol.

Secondly, the organization's activities are manifested in the creation of units within the structure of Interpol, which are responsible for the implementation of cooperation in the field of high technology. The Interpol Innovation Centre is headquartered in Singapore and aims to research, develop and implement the latest approaches to combating international crime. It consists of scientists, analysts, law enforcement and technology professionals. Interpol also has the ability to coordinate transnational cybercrime investigations and operations, both locally and remotely. In addition to this unit, there is a Cyber Fusion Centre (CFC), which consists mainly of analysts. It publishes reports to warn countries of new or imminent cyber threats [7].

Third, the most important is the creation, organization, implementation of joint programs to stop crime in the field of high technology. Known operations of Interpol are "Cryptojacking", "Operation Night Fury", "The ASEAN operation", "AMERICAS", and others. For example, Operation "The ASEAN" combined the experience of the police and the private sector to detect management and control servers that distribute various types of malware, leading to the detection of nearly 270 compromised websites, including government portals [8].

Conclusion. The research allows us to conclude that cybercriminals are becoming more agile, exploiting new technologies at lightning speed, adapting their attacks to new methods and cooperating with each other in various ways. The Interpol-Europol 8th Cybercrime Conference, held in October 6, 2020, aimed to solve future problems in this sphere. The events of 2020, which covered the whole world, reminded us that strong partnerships are central to the fight cybercrime. Such problems can be solved only flexibly and actively, uniting all the efforts of states.

References

1. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. ... канд. юрид. наук : 12.00.01. Київ, 2007. 20 с.

Maksymenko Yu.Ye. Teoretyko-pravovi zasady zabezpechennia informatsiinoi bezpeky Ukrainy [Theoretical and legal principles of information security of Ukraine]: avtoref. dys. ... kand. yuryd. nauk: 12.00.01. Kyiv, 2007. 20 s. [in Ukrainian].

2. Колесніков А., Зяйлик М. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. 2017. №1. С. 26-29

Kolesnikov A., Ziailyk M. Ekonomiko-pravovi zasady rozvytku kiberzlochynnosti ta metodiv borotby z neiu [Economic and legal principles of cybercrime development and methods of combating it]. 2017. №1. S. 26-29. [in Ukrainian].

3. Интерпол: киберпреступления являются самой опасной криминальной угрозой. [Электронный ресурс]. Режим доступа: <http://www.virusovnet.org/main/309>

Interpol: kiberprestupleniia yavlyayutsa samoy opasnoy kryiminalnoy uhrozoy [Interpol: Cybercrime is the most dangerous criminal threat]. Retrieved from : <http://www.virusovnet.org/main/309>. [in Russian].

4. Орлова О. О. Интерпол та Європол: співвідношення діяльності організацій та співробітництво з Україною // Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали IV Міжнар. наук.-практ. конф. (м. Дніпро, 13 березня 2020 р.). Дніпро : ДДУВС, 2020. С. 52-53.

Orlova O. O. Interpol ta Yevropol: spivvidnoshennia diialnosti orhanizatsii ta spivrobitnytstvo z Ukrainoiu [Interpol and Europol: Correlation of activities of organizations and cooperation with Ukraine] // Mizhnarodna ta natsionalna bezpeka: teoretychni i prykladni aspekty : materialy IV Mizhnar. nauk.-prakt. konf. (m. Dnipro, 13 bereznia 2020 r.). Dnipro : DDUVS. 2020. S. 52-53. [in Ukrainian].

5. Роль міжнародних організацій у протидії кіберзлочинності. [Електронний ресурс]. Режим доступу: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

Rol mizhnarodnykh orhanizatsii u protydii kiberzlochynnosti [The role of international organizations in combating cybercrime]. Retrieved from : https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

6. Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva / S. Schjolberg // Journal of International Commercial Law and Technology. 2008. Vol. 1, Issue 12. P. 1–19. Retrieved from : https://www.cybercrimelaw.net/documents/cybercrime_history.pdf

7. Interpol. Cybercrime: Future-oriented policing projects. 2019.

8. Interpol. Retrieved from: <https://www.interpol.int>

Anhelina Horbatiuk

Vasyl' Stus Donetsk National University

Vinnytsia

Research Supervisor: O. P. Pysmenna, PhD in Law, Assoc. Prof.

Language Advisor: O. V. Zubenko, Lecturer.

ADMINISTRATION OF JUSTICE BY A JUDGE: ETHICAL PRINCIPLES

Introduction. Modern life has rapid progress in various public spheres and our country is now at a decisive stage in its development. Society has high demands for the integrity and effective performance of all government institutions. This places