implementation of human rights in policing has been on the agenda. These will include co-operation schemes on training with the South African Police and the Palestinian Police Force.

Список використаних джерел

1. Human rights and the police, seminar proceedings, Strasbourg, 6–8 December 2005, Council of Europe Publishing. 184 p.

2. Danish police. URL: http://ukraine.um.dk/uk/about-denmark-ukr/political-and-social-affairs-ukr/.

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

COMBATING CYBERCRIMES IN UKRAINE IN CONDITIONS OF WAR

War, as one of the greatest upheavals of humanity, exerts a particularly powerful influence on the state of crime in general and on its individual types. Cybercrime is not an exception, but rather the opposite – it is a vivid example of how socially dangerous acts can simultaneously act as a mass destructive phenomenon of society and a powerful tool of the enemy's so-called «hybrid war».

Since the beginning of the Russian Federation's invasion of Ukraine, the number of cybercrimes has increased significantly, both for self-serving motives and for ideological and propaganda ones. According to the legislation of Ukraine, Cybercrime (computer crime) is a socially dangerous criminal act in cyberspace and/or with its use, responsibility for which is provided by the law of Ukraine on criminal responsibility and/or which is recognized as a crime by international treaties of Ukraine.

Among the cybercrimes committed for the purpose of illegal enrichment, carding, phishing, skimming, etc., which were already quite common, should be noted. However, new ones were added to them – fake charity for the needs of the army and wounded soldiers, offers to evacuate or rent housing for refugees and internally displaced persons, fraud related to the trade in non-existent ammunition, weapons, as well as from the preparation of documents that allegedly give enable men to avoid mobilization and even cross the border.

In the conditions of an armed conflict, a cybercriminal is not only a thief or a fraudster, but also a potential saboteur, collaborator and recruiter, that is, a full-fledged combat unit of enemy forces that uses Ukrainian cyberspace to weaken the state's defense capabilities and demoralize Ukrainians. Since the beginning of the full-scale invasion, several cases of large-scale hostile cyberattacks have already become known. They consist of vanous actions such as disrupting, denying or destroying computers and computers networks [1, p. 75].

The Armageddon group's cyber attack on the state bodies of Ukraine, which is a mailing of HTML files, the opening of which leads to the creation of an archive on the computer with a file called «Regarding the facts of persecution and killing of Prosecutor's Office employees by the Russian military in the temporarily occupied territories.lnk». Opening it establishes control over the computer and allows hackers to steal all personal data.

On March 23, 2022, the enemy tried to attack the state institutions of Ukraine using the Cobalt Strike Beacon program, which infects a computer if it is opened, and on April 4, it was reported that e-mails with the name «Military criminals of the Russian Federation.htm» were distributed, the opening of which leads to that attackers establish remote control over the device.

Thus, the issues of cyber security are extremely important for the Ukrainian state at the present stage, which is primarily due to the need to resist illegal encroachment on the information space of Ukraine, preservation of information resources, protection of the population from negative information influence and more [2, p. 129].

The responsibility for combating cybercrimes are on the Department of Cyberpolice of the National Police of Ukraine. According to the information on the official website of the mentioned body, its tasks include: implementation of the state policy in the field of cybercrime counteraction; timely informing the public of the emergence of new cybercriminals; implementation of software tools for the systematization of cyber incidents; responding to requests from foreign partners [3, p. 3].

Since the invasion of Russia on the territory of Ukraine, the load on cyber police units has increased significantly. Currently, they conduct active preventive work with the population, the purpose of which is to warn about possible criminal schemes of criminals and inform the population about ways to protect personal data.

As a conclusion, we can say that cybercrime as a set of culpable socially dangerous acts in the field of information and computer technologies began to grow actively from the moment of the invasion of the Russian Federation into Ukraine and for the second time – from the moment of the start of full-scale military operations. This is directly related to the emergence of new levers of influence of criminals on citizens – the desire to help the army and compatriots, problems with logistics and housing, the desire to evade military service, etc. And also the Russian use the cyberspace as a secondary battlefield. However, Ukraine is making significant efforts to respond in a timely and appropriate manner to the growing level of cybercrime both at the level of work of law enforcement units and at the legislative level.

Список використаних джерел

1. Vorobets K. The main directions of cybercrime prevention in Ukraine. Eur. JL & -Pub. Admin, 2019. P. 75–79.

2. Cherniavskyi S., Babanina V., Mykytchyk O., Mostepaniuk L. Measures to combat cybercrime: analysis of international and Ukrainian

experience. *Cuestiones Politicas*, Vol. 39, Nº 69 (Julio - Diciembre) 2021. P. 115–132

3. Borko A., Nehodchenko V., Volobuieva O., Kharaberiush I., Lohvynenko Y. Figting against cybercrime: problems and prospects in Ukraine and the world. *Journal of Legal, Ethical and Regulatory.* Issues Volume 22, Special Issue 2, 2019. P. 1–5

Маринич В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Богуцький В.**

THE WORK OF LAW ENFORCEMENT AGENCIES IN THE WORLD

In the difficult conditions of radical reform of the system of internal affairs of Ukraine, the experience of the police of the Federal Republic of Germany can be quite useful. The German Federal Police is a federal law enforcement agency in Germany, which is subordinated to the German Ministry of the Interior. Regular police forces, the state police, exist in each federal state and are subordinated to the state governments.

Tasks:

– Security of the order, which includes passport checks (only at airports, as all neighbouring countries are part of the Schengen area) and maritime border protection. As Germany is a member of the Schengen Agreement, the German Federal Police is part of the European Border and Coast Guard Agency.

– Protection of federal buildings, such as the Bellevue Palace, the residence of the Federal President of Germany, the buildings of the Federal Constitutional Court and the Federal Supreme Court.

– Responding to significant domestic events.

– Security of international airports and railways.

– Countering terrorism (GSG 9).

– Activities of air marshals (law enforcement officers in airplanes, whose task is to prevent the hijacking of aircraft by terrorists).

– Supporting international police missions of the UN and the European Union, for example in Kosovo and Afghanistan.

– Protection of some German embassies.

– Provision of rescue operations by helicopters.

Special units:

– Aviation unit, which is directly subordinated to the Main Directorate in Potsdam. It has 5 aviation squadrons in the cities of Fülendorf (north), Bloomberg (east), Fuldatal (center), Oberschleissheim (south) and Sankt Augustin (west), which have 132 helicopters at their disposal. Its duties include: border surveillance, surveillance of railway facilities, assistance during serious incidents and disasters in Germany and abroad, aerial search operations, search for missing persons, search for criminals,