

In addition to paying constant attention to victims, the subsection systematically organizes the following three types of outreach day events:

1. Days of assistance to victims in the framework of the special process of justice and peace;
2. Special assistance to victims of gender-based violence;
3. Psychosocial support for victims in hearings held as part of the special process of justice and peace [3].

Список використаних джерел

1. Government Support: Colombia. URL: <https://www.un.org/victims/terrorism/en/node/598>.
2. Terrorism in Colombia. URL: <https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine/article/abs/terrorism-in-colombia/0F0319D9696D9B2BA5BA1EBC43665F01>.
3. Legal Resources available to Victims. URL: <https://www.un.org/victims/terrorism/en/node/598>.

Литвиненко Д.,

здобувач ступеня вищої освіти

бакалавра Національної академії

внутрішніх справ

Консультант з мови: Гіпська Т.

COUNTERING CYBERCRIME IN UKRAINE

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

The fight against crime is especially relevant in the conditions of martial law, where the main task is to repel hacker attacks of the aggressor country on important state and other bodies, which occurred during the full-scale invasion of Ukraine and until now.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers [2].

Cybercrime includes many types of actions that are committed against the victim, namely:

1. Email and internet fraud.
2. Identity fraud (where personal information is stolen and used).

3. Theft of financial or card payment data.
4. Theft and sale of corporate data.
5. Cyberextortion (demanding money to prevent a threatened attack).
6. Ransomware attacks (a type of cyberextortion).
7. Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
8. Cyberespionage (where hackers access government or company data).
9. Interfering with systems in a way that compromises a network.
10. Infringing copyright.
11. Illegal gambling.
12. Selling illegal items online. Soliciting, producing, or possessing child pornography [2].

Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters. Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur [1].

Therefore, the legislation on cybercrimes and their countermeasures must be constantly improved in order to ensure the safety of the public from fraudsters.

Cybercriminals that target computers may infect them with malware to damage devices or stop them working, also they may also use malware to delete or steal data, or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers.

Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images [2].

Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data [2].

Therefore, in order to ensure the safety of Ukrainian citizens in the Internet space, the first steps were taken on July 27, 2009, to establish the Cyber Police Department of the National Police of Ukraine.

Although the fight against cybercrime in Ukraine is at an early stage and is not as developed as in other countries, including the United States, the first steps to create a cybercrime response have already been taken and are actively developing.

At the same time, our government is paying more and more attention to this issue. In particular, in October 2015, the Cyber Police was established as a structural unit of the National Police of Ukraine, which protects human and civil rights and freedoms, the interests of society and the state from criminal offenses in cyberspace; takes measures to prevent, detect, stop and solve cybercrime, and raise public awareness of cybersecurity [3].

The main tasks of the Cyberpolice are:

1. Participation in the formation and implementation of the state policy on preventing and combating criminal offenses, the mechanism of preparation, commission or concealment of which involves the use of electronic computers, systems and computer networks and telecommunication networks.

2. Assist other units of the National Police in preventing, detecting and suppressing criminal offenses in accordance with the procedure provided for by applicable law.

After the full-scale invasion, cyberpolice activities expanded to the information front, but many IT professionals joined the cyberpolice forces and together with the cyberpolice are fighting back against the aggressor country.

Someone sends complaints about enemy resources, someone develops information systems that ensure the information security of our internal resources, someone tells us about the rules of cyber hygiene. All of this helps survive and win the information war." Together with volunteers, the cyber police have developed information systems and solutions that now help with communication and improve protection against attacks by hackers from the aggressor country [4].

Cybersecurity is a practical activity aimed at protecting computer systems and networks from cyberattacks. It covers the entire range of measures, from password management to computer security tools based on machine learning technologies, and it also allows you to reliably perform trading operations, communicate and view content online. Therefore, it is important to always remember about cyber hygiene, which is the key to successful protection.

Список використаних джерел

1. The role of cybercrime law. URL: <https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html>.

2. What is cybercrime? How to protect yourself from cybercrime. URL: <https://www.kaspersky.com/resource-center/threats/whatcybercrime>.

3. Кіберзлочинність в Україні. URL: <https://equity.law/press-center/publications/1169.html>.

4. Протидія російському ворогу в інформаційному просторі ключове завдання Кіберполіції в умовах війни. URL: <https://cyberpolice.gov.ua/news/protydiya-rosijskomu-vorogu-vinformaczi-jnomu-prostorikiberpolicziyi-v-umovax-vijnny-8148/>.

Дукань Н.,

*здобувач ступеня вищої освіти
бакалавра Національної академії
внутрішніх справ*

Консультант з мови: Волік О.

**INVESTIGATION OF WAR CRIMES.
INTERNATIONAL EXPERIENCE**

War crimes can take various forms, including attacks on civilians, indiscriminate attacks, use of prohibited weapons, and targeting of essential civilian infrastructure such as hospitals and schools. Violations of human rights, including extrajudicial executions, torture, and displacement of civilians, are also of concern. Investigating war crimes is a complex and challenging process that involves adherence to legal standards, preservation of evidence. It's important to note that investigating war crimes requires a high level of expertise, resources, and often international collaboration. The political and security context can also influence the feasibility and success of such investigations. Coordination with international bodies and adherence to legal standards are crucial for the credibility and legitimacy of the investigation process.