militaire de Nuremberg, établi par la Charte de Londres (art. 6, c). Ce terme a été soutenu par le juriste britannique de renom Hersch Lauterpacht.

Il faut souligner que la nouvelle incrimination était destinée à juger les responsables des atrocités exceptionnelles commises pendant la Seconde Guerre mondiale, notamment les crimes les plus graves qui englobent l'ensemble de la communauté internationale. Cette nouvelle incrimination sera également utilisée pour assigner des hauts dirigeants du régime showa devant le Tribunal militaire international pour l'Extrême-Orient.

Aux termes de l'article 6c du statut du Tribunal militaire international de Nuremberg, le crime contre l'humanité est défini comme « l'assassinat, l'extermination, la réduction en esclavage, la déportation, et tout autre acte inhumain inspirés par des motifs politiques, philosophiques, raciaux ou religieux et organisés en exécution d'un plan concerté à l'encontre d'un groupe de population civil» [3].

Dès lors ce crime appartient aux concepts fondamentaux du droit. On notera que la définition de cette qualification s'est faite au cours des années après la Seconde Guerre mondiale. Le crime contre l'humanité est mieux défini grâce à l'article 7 du Statut de Rome de la Cour pénale internationale [4].

Список використаних джерел

1. Jean-Philippe Feldman, Crime contre l'humanité, dans Dictionnaire de la culture juridique, dir. Denis Alland et Stéphane Rials, éd. PUF, 2003.

2. La documentation française, *Justice pénale internationale : Quelle justice pour quels crimes : Définitions des crimes*, lire en ligne.

3. La documentation française, Justice pénale internationale : *Quelle justice pour quels crimes* : Définitions des crimes, lire en ligne.

4. Rapport fait au nom de la Commission des Affaires étrangères sur la proposition de loi de M Didier Migaud et plusieurs de ses collègues (n° 895), relative à la reconnaissance du génocide arménien de 1915, par M. Réné Rouquet, Député [archive], sur assemblee-nationale.fr, 1998.

Первак В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Драмарецька Л.**

CYBERCRIME AND THE FIGHT AGAINST IT IN POLAND

Nowadays, the use of information technology has no limits. The virtual space takes over everything from the real one in a row, including crime in its new forms and manifestations. In the legal world, some have even personally encountered cybercrime. It includes various types of crimes committed using a computer and the Internet. The object of cybercrimes is personal data, bank accounts, passwords and other personal information.

In Poland, cybercrimes include copyright and related rights violations, fraud, illegal actions with transfer documents, payment cards and other means of accessing bank accounts, equipment for their production;

evasion of taxes, duties, i.e. mandatory payments, importation, production, sale and distribution of pornographic items, illegal collection for the purpose of use or apply of information constituting a commercial or banking secret.

In recent years, Poland has demonstrated a consistent state policy of combating cyber threats. Poland became aware of the danger of cyber threats after large-scale cyber attacks in 2012. At that time, the work of government websites was paralyzed, and the mass protests that began in the streets swept through the network through massive DOS attacks.

The consequences that followed revealed several gaps, such as the weakness of the state's telecommunications and information provision, as well as the low awareness of state officials and their reluctance to acknowledge the problem. Some of them publicly stated that government websites do not work because too many people visit them. For a long time, the authorities' efforts to combat cyber threats were insufficient. However, a series of large-scale attacks against the background of the absence of a single coordinated decision-making center became the impetus for action.

There were 4 factors that positively influenced the solution to this problem:

1) the adoption of amendments to the legislation that allow the introduction of a state of emergency in the country in the event of an attack in virtual space, introduced a legal innovation, so to speak;

2) the authorities agreed with the inexpediency of functioning of several institutions for combating cyber threats, which only duplicated each other;

3) in 2016, the National Cyber Security Center was created within the framework of the Ministry of Digitalization. Its key task was the prevention of threats, response to them and coordination of actions. The work of the center is a successful example of public-private partnership in the field of cyber protection;

4) Poland has developed a new cyber security strategy. It predicts that by 2020 the authorities will guarantee the safety of citizens, subjects of economic activity and state institutions in the field of cyber security.

Poland's system does not mean that it has coped with threats, but according to the National Cyber Security Center, the number of incidents is decreasing. However, the increase in the number of messages is an indicator of the growing awareness of users who are able to report it. Poland was one of the countries against which Russian hackers waged cyber wars. In particular, they stole information from state institutions.

Ukraine's path in this struggle can be compared to Poland's. We have repeatedly encountered Russian-inspired cyberattacks. The most famous of them were the attempts to interfere with the work of the CEC server in 2014, Oblenergo servers in 2016, as well as the websites of the State Treasury, the Ministry of Finance and other state institutions.

The legislative base of Poland is an important component, which is why this country has moved from words to actions. Therefore, countering

cybercrime and the level of cyber security are currently one of the priority directions in the country's policy. But for a comprehensive fight against this problem, joint efforts of the state, citizens and the international community are needed.

Список використаних джерел

1. Cybercrimes: types and tools for fighting against them. URL: https://gurt.org.ua/articles/34602/.

2. Poland: experience in cybercrime counteracting. URL: https://www.epravda.com.ua/columns/2017/10/12/630044/.

3. Cybercrime counteracting. URL: https://alebank.pl/cyberbezpieczenstwo-w-firmach-walka-z-cyberprzestepczoscia-jest-w-polsce-nieskuteczna/?id=292344&catid=32532&cat2id=32533&cat3id=22872.

4. Cybercrimes: where and what for. URL: https://www.pomaturze.pl/news/cyberprzestepczosc+gdzie+moze+cie+spotkac/1690/.

Перекрест І.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Сторожук О.**

CRIMINAL BRIBERY AND CORRUPTION LIABILITY UNDER GERMAN LAW

Bribery and corruption are regulated under the German Criminal Code (Strafgesetzbuch). On one hand corruption of public officials is unlawful in circumstances where an individual person offers, promises or grants a public official an advantage for the accomplishment of an act which is contrary to his or her duty (Section 334 of the Criminal Code – Strafgesetzbuch) or in accordance with his or her duty (Section 333 of the Criminal Code). These rules apply regardless of whether the act has occurred or have yet to occur. On the other hand the public official acts unlawful in these situations if they accept an advantage (Sections 331 and 332 of the Criminal Code).

Is commercial bribery and bribery of foreign agents illegal?

Corruption in the course of business and trade is also unlawful (Section 299 of the Criminal Code). It occurs if, during the course of a business transaction, an employee or agent intentionally demands, allows himself to be promised, or accepts a benefit for himself or another as consideration for giving an unfair preference in the competitive purchase of goods or commercial services. To be guilty of active commercial bribery, the defendant must have acted «for competitive purposes» to obtain «an unfair preference in the purchase of goods or commercial services». Passive commercial bribery requires the recipient to accept (or allow to be promised) a briber «as consideration 55 for according an unfair preference to another in the competitive purchase of goods or commercial services».

Further, active commercial bribery of foreign employees/agents requires the defendant to act «in order to obtain or retain an unfair