if they're customers or not. There are also no entity revenue or processing threshold requirements for GDPR [2].

Generally speaking, privacy laws fall into two categories: vertical and horizontal. Vertical privacy laws protect medical records or financial data, including details such as an individual's health and financial status. Horizontal privacy laws focus on how organizations use information, regardless of its context. The types of data covered by these laws include fingerprints, retina scans, biometric data, and other personally identifiable information such as names and addresses. While both vertical and horizontal privacy laws play an essential role in protecting individuals' privacy rights, many view vertical policies as more effective because they're better at targeting specific risks [2].

The federal government passed the U.S. Privacy Act of 1974 to enhance individual privacy protection. This act established rules and regulations regarding U.S. government agencies' collection, use, and disclosure of personal information.

The main principles of this law is that U.S. citizens have the right to access their personal data kept by government agencies and request changes if they believe the information is inaccurate. Government agencies grant users data access based on their role in their company. Individuals must know how agencies use their personal data upon collection.

Список використаних джерел

1. European Union. Security of personal data. URL: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data.

2. The Privacy, Data Protection and Cybersecurity Law Review: United Kingdom. URL: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/united-kingdom.

Новік М.,
здобувач ступеня вищої освіти бакалавра
Донецького державного
університету внутрішніх справ
Консультант з мови: **Мамонова О.**

INTERNATIONAL COOPERATION IN THE FIELD OF COMBATING COMPUTER CRIME

Considering the fight against computer crime from the perspective of international cooperation, we will identify the following features:

1) cross-border nature – this feature is expressed in the fact that the criminal has the possibility of authorized access to any system through the Internet, regardless of state borders;

2) the specified criminal offense has a high level of latency due to the difficulty of detecting this offense and the reluctance of victims to report the commission of an offense against them;

3) lack of established mechanisms in investigation and international assistance.

One of the important events of Ukraine on the path of interstate cooperation was the ratification of the Convention on Cybercrime on September 7, 2005, which provides for the provision of powers sufficient to effectively combat crimes in the field of information and telecommunication technologies at both the domestic and international levels, the conclusion of agreements on effective international cooperation. In accordance with this Convention, the parties cooperate by applying relevant international documents on international cooperation in criminal matters, agreements concluded on the basis of unified or reciprocal legislation, as well as domestic legislation for the purpose of investigating or prosecuting criminal offenses related to computer systems and data, collecting evidence in electronic form [1, p. 131].

In order to solve the problems of international cooperation in combating computer crime, it is necessary to agree on a strategy that will take into account the proposals and objections of all parties involved in it.

It is also worth paying attention to the meeting of the Ukraine-NATO joint working group, which took place on December 8, 2010, as a result of which directions for further cooperation in the field of cyber defense were determined, in particular, Ukraine envisages the following measures:

1) establishment of consultative mechanisms;

2) exchange of experience regarding legislative provision and regulation;

3) development of operational cooperation mechanisms in crisis situations;

4) establishment of a system of information exchange regarding cyberspace monitoring;

5) cooperation in eliminating the negative consequences of a cyberattack.

Next, it is advisable to consider the experience of different countries in combating computer crimes.

The creation of new units in the field of combating cybercrime, in particular computer fraud, is practiced in such countries as: Australia, Belgium, Belarus, Great Britain, Denmark, Estonia, India, Ireland, China, South Korea, Lithuania, Luxembourg, Macau, Malaysia, the Netherlands, Germany, Norway, South Africa, Peru, Poland, Portugal, USA, Singapore, Slovenia, Thailand, Finland, Czech Republic, Switzerland, Sweden, etc. [2].

Currently, Australia has a government telecommunications committee that regulates the country's Internet policy [3]. On the basis of the Ministry of Public Policy of China, a unit was formed to provide «control over the Internet» in China [4]. The Indian Cyber Crime Investigation Service employs professional hackers to carry out its functions. In England, the National Hi-Tech Crime Unit (NHTCU) has been established. This unit consists of forty specially trained agents located in the

main office in London and forty-six territorial investigators [5]. In the Czech Republic, the detection and investigation of cybercrimes, in particular computer fraud, is carried out by the Bureau of the Criminal Police and Investigative Service, but in the near future it is planned to create special regional units.

The study of the experience of the United States of America requires special attention. One of the features is the establishment at the legislative level of the obligation of state bodies to notify the relevant federal or local cybercrime units of all cases of unauthorized access to individual files or databases in order to respond to them in a timely manner. The USA became one of the first countries in the world to take measures regarding criminal liability for committing crimes in the field of information technologies, where this category of crimes appeared earlier than in other countries [6, p. 29]. The Federal Bureau of Investigation (hereinafter – FBI) acts as the main subject of ensuring cyber security in the entire territory of the USA.

In implementing the cybercrime program, the FBI works closely with the Department of Defense and the Department of Homeland Security, which often handle similar tasks. In order to obtain information about computer crimes as quickly as possible, the FBI has created the Internet Crime Complaint Center, where both victims and third parties, by filling out a special online form or simply by calling, can to provide information about committed crimes on the Internet [7, p. 199].

Also under the direction of the FBI was the establishment of the «Internet Center», which takes complaints of criminal offenses on the Internet and provides the public with reports on suspects, computer fraud schemes and how to overcome them. In particular, the official website contains advice on preventing computer fraud, which includes the following topics:

1) Business E-Mail Compromise (BEC);
2) Database fraud (Data Breach);
3) Denial of Service (DoS);
4) Malicious software (Malware/Scareware);
5) Phishing (Phishing/Spoofing).

Information is analyzed and disseminated for investigative and intelligence purposes among law enforcement officers and to inform the public [8].

Therefore, the implementation of international cooperation in the field of combating computer fraud plays a significant role, as it increases the effectiveness of detection and investigation of computer fraud thanks to international experience and a unified countermeasure strategy.

Список використаних джерел

1. Актуальні питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф., м. Харків, 10 груд. 2013 р. МВС України, Харк. нац. ун-т внутр. справ. Х. : ХНУВС, 2013. 272 с.

2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

3. Аналітичний огляд організації роботи поліції зарубіжних країн щодо протидії злочинам у сфері високих технологій. Матеріали з сайту Укрбюро Інтерполу. URL: ttp://26308.ncbinter.web11. ukraine.com.ua/?p=275.

4. Спецслужбы задержали интернет-мошенников из Украины. Матеріали з сайту Корреспондент.net. URL: http://www.korrespondent.net/ main/93952.

5. Всеукраїнський прес-центр Німеччина створює центральне управління по боротьбі з інтернет-злочинністю. Матеріали з сайту Всеукраїнський прес-центр. URL: http://presscenter.ukrinform.ua/ news48879.html.

6. Державне регулювання суспільних відносин в мережі Інтернет. Матеріали з сайту referaty.pp.ua. URL: http://www.referaty.pp.ua/ abstracts/ua/pravo/pravo_23914.php.

7. Поляруш О.О. Використання мережі Інтернет як каналу інформаційно психологічного впливу. К. 2005. № 21. С. 218–227.

8. Лапта С. П. ФБР у боротьбі з кіберзлочинністю. Актуальні питання протидії кіберзлочинності та торгівлі людьми : матеріали всеукр. 188 наук.-практ. конф. (Харків, 27 листоп. 2017 р.) / МВС України ; Харків. нац. ун-т внутр. справ. Харків, 2017. С. 197–199.

Ньорба А.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Скриник М.**

THE SPECIFICS OF THE FUNCTIONING OF CIVIL LAW IN COMPENSATION FOR NON-PROPERTY DAMAGE IN EUROPEAN COUNTRIES

Among the rights enshrined in the fundamental Chapter II of the Constitution, there is a right to compensation damage It is noted that everyone has the right to material compensation at the expense of the state or local self-government bodies and moral damage caused by illegal actions or inaction of state bodies authorities, local self-government bodies, their officials and officials during the exercise of their powers. Such provisions are enshrined in European constitutional acts. Declaration of the right to moral compensation damage is a common vector of the development of democratic and legal countries, and, despite this, some countries, in particular in the countries of the European Union, have such an institute effective, thorough on a consistent judicial basis practice, but unstable and ambiguous in the Ukrainian legal space.

Currently, the main development trends institution of compensation for moral damage there is a movement in the direction of overcoming conceptual contradictions regarding the foundations of such an institution and gaps in regulation. To such problems, in particular, uncertainty can be counted circle of persons who can claim compensation for moral damage,