police law enforcement agencies, whose officers are not police officers, but still enforce laws, and other bodies with solely investigatory powers.

Miscellaneous Police Forces mostly have their foundations in older legislation or common law. These are responsible for policing specific local areas or activities, such as ports and parks [7].

Summarizing our theoretical research, we should note that the law enforcement bodies of Ukraine and Great Britain have similar bodies and functions as well as differences in their structure and activity.

Список використаних джерел

1. Закон України про Національну Поліцію. URL: https://zakon.rada.gov.ua/laws/show/580-19.

2. Закон України про Прокуратуру. URL: https://zakon.rada.gov.ua/laws/show/1697-18.

3. Закон України про Службу Безпеки України. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

4. Правоохоронні органи Великобританії. URL: https://studopedia.com.ua/1_316312_pravoohoronni-organi-velikobritanii.html.

5. Правоохоронні органи держави: поняття, ознаки, система і загальна характеристика. URL: https://studfile.net/preview/5483510/page:3/.

6. Про державний захист працівників суду і правоохоронних органів від 23.12.1993р. № 3781-XII (редакція 24.11.2021). URL: https://protocol.ua/ua/pro_dergavniy_zahist_pratsivnikiv_sudu_i_pravoohoronnih_organiv/.

7. List of law enforcement agencies in the United Kingdom, Crown Dependencies and British Overseas Territories. URL: https://dbpedia.org/page/List_of_law_enforcement_agencies_in_the_United_Kingdom,_Crown_Dependencies_and_British_Overseas_Territories.

Нестерчук Я.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Гіпська Т.**

SECURITY OF PERSONAL DATE

Data security is the process of protecting sensitive information from unauthorized access. It includes all of the different cybersecurity practices you use to secure your data from misuse, like encryption, access restrictions (both physical and digital), and more. Data security has always been important. Security had always been central for the protection of confidentiality, integrity and availability of personal data.

With the increasing use of online and mobile applications, the advances of analytics and the Internet of Things, the need for data security is more important than ever, considering the risks of new exposed system vulnerabilities and cyber-attacks, as well the vast opportunities for data combination and end users' tracking. Still, security is not just about the

application of one or more measures and no security measure alone can provide an adequate protection level for personal data. On the contrary, security for personal data needs to follow a thorough and continuously monitored framework of controls, both technical and organizational, appropriate to the nature of the data processing and the associated risks [1].

Over the last years, an increasing number of personal data breaches has been reported, especially relating to online systems and services. Such breaches can lead (and have led) to serious impact on the affected individuals' private lives, including humiliation, discrimination, financial loss, physical or psychological damage or even threat to life. It is, thus, of critical importance that the data controllers and processors have all the necessary mechanisms in place both for preventing data breaches, as well as for encountering them on time and in an appropriate way.

In each country, the methods and laws regarding the protection of personal information are slightly different, but the goal is always the same - to protect personal data. Consider, for example, the security of personal data in the United States. The United States has a patchwork and ever-changing web of laws governing data privacy. While there's no comprehensive federal privacy decree, several laws do focus on specific data types or situations regarding privacy. Without a holistic statute, however, it can be unclear what protections are in place for the various types of personal information with which companies. Despite the lack of a comprehensive privacy framework, organizations that process or store data are still responsible for staying up-to-date on the latest regulations to ensure compliance.

The internet has revolutionized our lives and work, providing unprecedented access to information and communication. However, along with this increased connectivity comes new risks to privacy. Thankfully, data privacy laws govern the collection, use, and disclosure of personal data and set standards for how businesses need to handle sensitive data. The Federal Trade Commission (FTC) is the principal enforcer of these laws in the U.S. In recent years, the FTC has taken several enforcement actions against companies that have misled consumers about their data security and privacy practices.

The United States and Europe have the most comprehensive data security and privacy laws; the EU's General Data Protection Regulation (GDPR) came into effect in 2018, while the California Consumer Privacy Act (CCPA) took effect in 2020. GDPR and CCPA set strict standards for how service providers must handle personal data, including ensuring that data collection is transparent, secure, and obtained with the concerned individual's consent. The standards also provide individuals the right to know what personal data is collected about them and allow them to access it and request its deletion.

The main difference between CCPA and GDPR is that GDPR applies to any organization that processes or intends to process EU citizens' sensitive data, regardless of location. GDPR compliance is mandatory for any organization that processes the personal data of EU citizens, regardless

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;