Using information systems, the German police can quickly respond to digital threats and conduct effective investigations.

These information systems thus play a key role in the fight against crime in Germany, providing the police with powerful tools for data collection and analysis.

The German police have an important role in the fight against corruption, actively working on the prevention and investigation of corruption crimes. One of the main aspects is the destruction of the financial base of criminal groups through the confiscation of property and the fight against money laundering. Strengthening the legal framework and preventing officials from abusing their position are important measures. In addition, the police use innovative information systems, such as POLIS and INPOL, which allow the analysis of criminal activity, gang structures, and help in the fight against terrorism, financial fraud and cybercrime. Modern technologies, including artificial intelligence, are used to analyze large volumes of data and speed up investigations. Thus, thanks to interdepartmental cooperation and the use of modern systems, the German police ensure effective counteraction to corruption and other crimes.

Список використаних джерел

1. Титаренко О.О. Досвід Німеччини в програмуванні протидії злочинності в сучасних умовах. Право і суспільство. 2019. № 4. С. 267–274.

2. Чередниченко О. Ю. Організаційно-економічний аспект використання досвіду створення та діяльності антикорупційних структур країн ЄС в роботі щодо запобігання та протидії корупції в Україні. Вісник економіки транспорту і промисловості. 2017. Вип. 58. С. 239–247.

3. Науковий вісникт 3'2023 ISSN 2311-8040 Львівського державного університету внутрішніх справ.

4. Інформаційні поліцейські системи Німеччини, та їх використання: URL.: https://www.bka.de/DE/UnsereAufgaben/ Ermittlungsunterstuetzung/

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

USE OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS IN FOREIGN COUNTRIES

The Code of Criminal Procedure of Ukraine does not contain a special procedure for the use of electronic evidence. Meanwhile, the main order of proof was formed more than half a century ago and is oriented

towards obtaining traditional means of proof. So, in terms of using electronic traces as means of proof and ways of displaying legally significant information contained in them, they are so specific that traditional procedural forms of proof are no longer relevant and outdated in modern conditions. In some other countries, the place of electronic evidence was previously established, thanks to the spread of general rules unification principle of their application in civil and economic proceedings. The implementation of general provisions gives an opportunity to develop uniform cross-industry rules for the use of electronic evidence in any process. Some foreign countries use just this approach.

In the Anglo-Saxon legal system, there is no clear division of evidence into types. Evidence law is based on typical problem situations. The evidence law of the USA, in fact, is a consolidation of the most important and landmark court decisions, a generalized practice and has a prohibitive nature, that is, it indicates in which cases the evidence cannot be recognized as admissible one. Therefore, for American lawyers, it does not matter whether electronic evidence is an independent type of evidence [1, p. 2].

Federal Rules of Evidence adopted in 1975, are considered the main normative act on the regulation of evidence in the United States. Art. 401 of Federal Rules of Evidence states that evidence is admissible if it can make the presence of any fact that affects the qualification of the offense more likely or less likely than in the absence of this evidence. Article 402 of Federal Rules of Evidence interprets digital evidence as data and media storing the data [2]. Such a broad definition of the concept of evidence has long allowed the use of electronic evidence in the US criminal process.

Legislative regulation of electronic evidence in Great Britain is governed by the Police and Criminal Evidence Act of 1984. According to Art. 19 of the specified Law, the police may demand any information, including the one in electronic form. The main condition is that the electronic evidentiary information is relevant to the commission or prevention of crimes, as well as when its removal contributes to the concealment, loss, falsification or destruction of evidence in any form [3].

All digital evidence is subject to the same rules and laws that apply to documentary evidence. In addition, this issue is also regulated by the Computer Misuse Act, which contains criminal law regulations on computer crimes and other crimes committed using a computer as an instrument of crime, criminal procedural provisions of search, seizure of electronic evidence, powers of law enforcement agencies [4]. In general, in Great Britain, such a separate type of evidence as electronic one is not distinguished, but it is only about the procedures and rules for submitting electronic documents.

There is interesting experience of the People's Republic of China (hereinafter – PRC) regarding the use of electronic evidence. In 2012, electronic evidence was equated with existing evidence in the CCP of the

People's Republic of China, although the Criminal Procedure Law did not disclose this concept [5].

The regulation "On solving some issues regarding the collection, obtaining and analysis of electronic data in criminal cases" defines electronic evidence as information collected in the framework of a criminal case, stored and transmitted in electronic form, which can be evidence in a criminal case. Article 2 of the specified Regulations refers to electronic evidence in a criminal case: websites, blogs (online diaries), microblogs, pages in social networks, application identifiers (for example, WeChat), forums, online drives (online storage). Also important are communications on the Internet and communication networks, for example, mobile messages, e-mails, messages from messengers, messages in groups. Identification information obtained during user registration on the site, electronic transactions, registration logs [4] are especially important. The regulation also defines the procedure for obtaining such evidence by only two investigators and in compliance with the procedural form and technical standards.

It should be emphasized that international organizations play an important role in the development of rules regarding electronic evidence. Thus, in 2019, Interpol held a meeting on electronic evidence, where not only the main problems, the use of electronic evidence in the process of proving were identified, but also recommendations were made to both legislative and law enforcement agencies.

Consequently, the use of electronic evidence in criminal proceedings is a complex area of law that continues to evolve. While they offer powerful tools for law enforcement, they also pose significant challenges related to privacy, reliability, and cross-border collaboration. As countries continue to adapt to the digital age, the development of a robust legal framework and international cooperation will be essential to ensure the effective and fair use of electronic evidence in the pursuit of justice. In the conditions of Ukraine's aspiration to become a full member of the EU and to be at the center of international arena, the adoption of regulations at the EU level on electronic evidence will contribute to effective cross-border cooperation of EU member states in criminal cases, which, given the growth of cybercrimes, is becoming more and more relevant. In the process of joining the EU, Ukraine should not only strengthen cooperation with member states in criminal cases, but also ensure compliance of national legislation with the EU acquis in the field of criminal justice, which requires taking into account the experience of European countries.

Список використаних джерел

1. Rothstein P.F. Evidence: State and Federal Rules. St. Paul, 1991. 669 p.

2. Washington State Courts - Court Rules. Washington State Courts Washington Courts. URL: https://www.courts.wa.gov/court_rules/?fa=court_rules.list&group=ga&set=ER.

3. Police and criminal evidence act 1984. Legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/1984/60/contents.

5. Common Criteria Certification for Information Technology (IT) Security. UL Solutions.

6. Criminal Procedure Law of the People's Republic of China. 2012. URL: http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/13/content_1384067.htm.

Білик І.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Романов І.**

INTERNATIONAL COOPERATION IN COMBATING CYBERCRIME: THE EXPERIENCE OF EUROPOL AND INTERPOL

In recent years, international cooperation has become pivotal in addressing the growing complexities of cybercrime. Europol and Interpol, as the leading international organizations in crime prevention, have developed specific approaches and initiatives to foster cross-border collaboration. Highlighting the strengths and difficulties of such cooperation, with an emphasis on effective practices and existing limitations, allows us to outline modern approaches to cybercrime prevention.

Europol and Interpol have established numerous frameworks to streamline cross-border cybercrime investigations. Operations like Operation Blackfin and Operation Neptune, led by Europol, represent successful joint efforts to dismantle cybercriminal networks involved in various types of online crime, such as financial fraud and identity theft. Additionally, Interpol's Cyber Fusion Centre offers a global hub for intelligence-sharing, bringing together expertise from law enforcement agencies worldwide. Such operations underscore the importance of a unified approach to identify, track, and apprehend cybercriminals.

Despite advances in cooperation, differences in legal standards and data-sharing regulations remain significant barriers. Countries vary widely in their cybercrime legislation, complicating evidence collection and prosecution across borders. For instance, data protection laws in the EU pose unique challenges in collaborating with regions with less stringent data regulations. The Budapest Convention on Cybercrime has attempted to provide a framework for alignment, yet not all countries are signatories, limiting its effectiveness.