2. Загальна декларація прав людини, прийнята Генеральною Асамблеєю ООН від 10 груд. 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
3. Рішення Конституційного Суду України від 28 січ. 2016 р. № 955-VIII зі змінами від 12 лип. 2019 р. № 5-р(I)/2019. URL: https://zakon.rada.gov.ua/laws/show/va05p710-19#Text
4. Рішення Конституційного Суду України від 1 чер. 2016 р. № 2-рп/2016. URL: https://zakon.rada.gov.ua/laws/show/v002p710-16#Text
5. Конституція України від 28 чер. 1996 р. Відомості Верховної Ради України. 1996. № 30.
6. Конвенція про захист прав людини і основоположних свобод від 04 лист. 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
7. Про правовий режим воєнного стану: Закон України від 12 трав. 2015 р. Відомості Верховної Ради України. 2015. № 28. Ст. 250.

УДК 343.98(043.2)

Grekova L., Senior Lecturer,
Loetska S., student of higher education first (bachelor) level,
National Aviation University, Kyiv, Ukraine

TO THE ISSUES OF THE PROBLEMS OF DIGITAL FORENSICS AND WAYS TO RESOLVE

At the present, the evolution of digital technologies, electronic communications, the Internet has caused a significant impact on the entire legal system has led to the development of scientific knowledge about the investigation of crimes related to computer information, the study of digital evidence and methods for searching for digital information. Nowadays digital forensics is developing rapidly. Its purpose is to obtain evidence from digital storage that exist on various devices - from mobile phones to servers, establishing facts (circumstances) that are important for pre-trial investigation bodies or the court, based on a study of the patterns of progress and operation of computer tools and systems that ensure the implementation of information processes.

In our opinion, one of the main problems in the investigation of criminal cases, the facts associated with obtaining digital evidence are the evidence base of, is that they represent a separate, specific group of evidence that cannot be classified as traditional material or personal, have a specific procedure and environment for its creation, and which have specific qualities, in particular, they are quite easy to destroy (both intentionally and accidentally) or make faking. In addition, in cases where they are a crime weapon, it is often difficult, and sometimes impossible, to find and identify. In this connection, the main task of investigating cases of this category is to establish the indisputable

authenticity of such type of evidence (must meet the requirements of relativity and admissibility).

Furthermore, the ability to quickly change the content of the site, the physical location of servers on the territory of other states, the use of anonymous software packages are factors that significantly complicate the possibility of fixing, and in the future, the study of digital information [1, p. 259]. These factors not only significantly complicate the investigation, but also lead to significant time consuming.

A striking example of this situation is the investigation of a large-scale hacker attack, the largest in the history of the country, was beganing on June 27, 2017, when Ukraine was attacked by a virus called PetyaA. As the results of a joint investigation by the Cyber Police and third-party computer security specialists, it was established that the damage to the information systems of Ukrainian companies occurred due to an update of the software designed for reporting and document management - "MEDoc", through making changes to the ZvitPublishedObje.dll library. The active and most destructive phase of the attack began from the M.E.doc program’s automatic update system. A day after the start of the attack, 23 criminal cases is being investigated on couse the facts of unauthorized interference in electronic computers. As of June 29, 2017, 1 508 legal entities and individuals, organizations of the private sector and the public sector of the country applied to the National Police of Ukraine with reports of the facts of blocking the operation of computer equipment using an encryption virus. Specialists from the Department of Counterintelligence Protection of State Interests in the Sphere of Information Security of the SBU were involved in the investigation with aim to identify the methods for carrying out this cyberterrorist attack, identify the sources of the attack, its perpetrators, organizers and customers. Interaction has been organized with partner law enforcement agencies, intelligence agencies of foreign countries and international organizations specializing in cybersecurity, including the US FBI, the UK National Crime Agency (NCA), Europol, as well as leading cybersecurity institutions of some other countries.

Despite a large-scale investigation, it was only in 2018 that the CIA in its report stated with a high degree of probability that the military intelligence of the Main Intelligence Directorate of the Russian Federation (GRU) was involved [2]. And only in 2021, information appeared about four legal entities and six individuals affiliated with the Russian special services, involved in the development of components of the PetyaA virus, who administered it, moderated it, organized cyber attacks on critical infrastructure facilities in our country. Aforementioned subjects are included in the US sanctions lists and are charged by the USA in a criminal proceeding for carrying out these cyber attacks [3].

Forensic recommendations to prevent this kind of crime can be careful verification of people who have access to server-type servers with M.E.Doc updates, making special technological and technical decisions, related to software safety at the stage of its design. Moreover it can be control of compliance with the rules and principles of computer ethic by all members of the organization, etc.

Contacting an appropriate specialist can be considered factor contributing to the rapid investigation of such criminal cases to clarify, draw up a correct list of issues that can be resolved during a forensic computer-technical examination.In addition it is obvios simplify the procedure for international cooperation of special forces to combat cybercrime by making the necessary changes to legislative acts, develop scientific methods for determining time, authors of writing computer programs, what changes and at what stage itwas introduced, will make shortter the time of investigation also.

Literature

1. D.M. Tsehan. Tsifrovi dokazy: poniattia, ocoblyvosty, ta mictse u systemi dokazuvannia. *Науковий вісник міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2013. № 5. С. 256-260.

2. TSRU: kiberataku virusom Petya v Ukraine organizuyut rossiyskiye víys'koví URL: https://lb.ua/society/2018/01/13/387139_tsru_kiberataku_virusom_petya.html (date of access 11.01.2023)

3. RNBO naklala sanktsiyi na prychetnykh do rozrobky virusu notPetya. URL: https://lb.ua/news/2021/06/18/487421_rnbo_naklala_sanktsii_prichetnih.html (date of access 11.01.2023)

УДК 343.9(043.2)

Дідківська Г.В., д.ю.н., професор,
Державний податковий університет, м. Ірпінь, Україна

ОКРЕМІ ІСТОРИЧНІ АСПЕКТИ СТАНОВЛЕННЯ ПРАВООХОРОННИХ ОРГАНІВ

На сьогодні, історія вивчає виникнення і розвиток судових і правоохоронних органів як однієї з державних структур і одного із засобів забезпечення соціальної регуляції; політологія досліджує проблеми судових і правоохоронних органів, виходячи з їх місця і ролі у здійсненні політичної влади; соціологія досліджує судові і правоохоронні органи як певний соціальний інститут, у контексті їх соціальної обумовленості, соціальної ролі і призначення. Для юриспруденції система судових і правоохоронних органів та її складові є одними з найбільш значущих державно-правових явищ, які мають значну питому вагу і місце в її