UDC 343.9(043.2)

Shyian Yu.V., applicant for the first (bachelor's) level,
National Aviation University, Kyiv, Ukraine
Supervisor: Grekova L., Senior Lecturer

INTERNET NETWORK AS A CARRIER OF FORENSIC INFORMATION ABOUT CYBERCRIME

Digital and information technologies are in constant development and act not only as means of communication, but also as tools for concluding contracts, means of payment, as well as ways to carry out various operations. The Internet system opens up ample opportunities for communication and exchange of information of any nature. That is, we can say that the Internet network has become one of the most favorable environments for the development of social relations. However, the improvement of information technology and the development of the Internet network has led to the emergence of a new type of crime – cybercrime.

Note that cybercrime is often used along with the concept of computer crime. However, according to the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine", cybercrime (computer crime) is a socially dangerous guilty act in cyberspace and / or with its use, the responsibility for which is provided for by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine [1].

Cybercrime is not limited to the framework of crimes committed on the global Internet, it applies to all types of crimes committed in the information and telecommunications sphere, where information, information resources are the subject of criminal encroachments, the electronic environment in which criminal offenses are committed.

Cybercrimes are characterized by a specific picture of traces. At the scene, simultaneously with the usual traces, there should be virtual traces that are in the memory of electronic devices. Virtual traces are traces of any actions in the information space of computer and other digital devices, their systems and networks. In the theory of forensic science, there are different opinions about what should be understood by virtual traces: 1) virtual traces as a change in an automated information system; 2) virtual traces in terms of physical and quantum theory; 3) virtual traces as a result of logical and mathematical operations with binary code and many others. Until now, there is no exact definition of virtual footprints. The authors consider the question from different points of view: some from the point of view of human influence on computer systems, others from the point of view of physical connections of computer systems, others – from the point of view of performing certain operations [2].

In today's conditions, there is a tendency to increase illegal materials (information) in social Internet networks. Often, criminals flaunt the result of their illegal actions and record their criminal activities. There are also offenders who use the Internet as a means of committing their crimes, often to maintain criminal ties. Information on the Internet makes it possible to identify the identity of the offender, the situation, the scene of the incident, accomplices, tools, helps to identify important circumstances that are important in criminal proceedings. Offenders, acting as the creator and distributor of their own content and consumer of someone else's, inevitably leave virtual traces of their activities in cyberspace. According to such traces, it is possible to establish not only the physical parameters of the time and place of committing an action, but also with a high degree of probability to solve a number of diagnostic problems for the formation of the psychological profile of the reflected subject of predicting his future behavior [3, p. 6].

Internet networks are a valuable source of forensic information that can guide the investigator to make tactical decisions when investigating cybercrime. Forensic information in such networks is a set of data, messages and information about the sources and mechanism of occurrence of ideal and material traces related to a criminal event, obtained on the Internet using special means, in order to establish the circumstances of a criminal event in criminal proceedings. However, both the detection and investigation of this category of crimes remains quite a difficult task for most law enforcement officers, and this is mainly due to their lack of preparedness to work with a new type of evidence contained directly on digital media and on the Internet.

The investigation of such crimes has its own specifics and is complicated by their increased latency. There is a problem of reviewing computer systems, technical devices that contain information. Also complicated is the procedure for extracting, investigating and fixing traces of cybercrime. This is facilitated by insufficient technical support of pre-trial investigation bodies, operational units [4, p. 102-103].

Based on the foregoing, it can be noted that the Internet network can undoubtedly act as a source of forensic information both in relation to cybercrime and other types of crimes where they are present. Traces of crime left on digital information have certain features that must be taken into account when collecting, consolidating and researching them. In connection with the foregoing, there is a need for further research of the criminal procedural properties of the Internet and the introduction of its results into the practical activities of law enforcement agencies.

Literature

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII: станом на 17 серп. 2022 р. URL: https://zakon.rada. gov.ua/laws/show/2163-19#Text (дата звернення: 31.10.2022)
2. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. С. 304–307. URL: http://pgp-journal.kiev.ua/archive/2019/5/57.pdf (дата звернення: 28.10.2022)
3. Білоус В.В., Шепітько В.Ю. Роль сучасних інформаційних технологій у встановленні особи злочинця. Сучасні проблеми криміналістики. Вип. 14. 2014. С. 5−11.
4. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб / В.М. Бутузов, В.Д. Гавловський, Л.П. Скалозуб та ін. Київ: Нац. акад. СБУ України, 2011. 404 с.

УДК 343.01(043.2)

Ющик О.І., к.ю.н.,
Чернівецький національний університет імені Юрія Федьковича,
м. Чернівці, Україна

КРИМІНАЛЬНИЙ ПРОСТУПОК: НЕОБХІДНІСТЬ ЗАКОНОДАВЧОГО ЗАКРІПЛЕННЯ

Адаптація законодавства України до законодавства ЄС, прагнення України стати демократичною, правовою державою вимагає певних змін правової системи в цілому і, відповідно, адміністративного та кримінального права як її складової. Реформування адміністративного та кримінального законодавства необхідно здійснювати на основі положень Конституції України при комплексному підході до реформування інших галузей законодавства (цивільного, трудового, фінансового тощо). Необхідно передбачити динаміку розвитку адміністративного та кримінального права, пов’язану з поступовими змінами розвитку суспільства, визначити пріоритетні напрямки становлення вказаних галузей законодавства на майбутнє, послідовність прийняття законів, виходячи з необхідності забезпечення прав та свобод громадян інтересів держави і суспільства в цілому, з урахуванням розвитку економіки, соціальної та політичної сфер.

Існування проступку в більшості держав східної групи континентальної правової сім’ї та в дореволюційному законодавстві обумовлено системою матеріально-формальних ознак, притаманних для певної категорії складів злочинів та неуправлінських деліктів. Матеріальні ознаки кримінального проступку обумовлені поглинанням багатьох