UDC 343.1
DOI https://doi.org/10.32849/2663-5313/2022.7.19

Oleh Tarasenko,
Doctor of Law, Associate Professor, Professor at the Department of Operational and Investigative Activities, National Academy of Internal Affairs, 1, Solomianska square, Kyiv, Ukraine, postal code 03035, o.s.tarasenko@gmail.com
ORCID: *orcid.org/0000-0002-3179-0143*

Tarasenko, Oleh (2022). Actors of detection of criminal offenses related to illegal content on the internet and the scope of their search activities. *Entrepreneurship, Economy and Law*, 7, 124–130, doi

ACTORS OF DETECTION OF CRIMINAL OFFENSES RELATED TO ILLEGAL CONTENT ON THE INTERNET AND THE SCOPE OF THEIR SEARCH ACTIVITIES

Abstract. ***Purpose.*** The purpose of the article is to identify the actors of detection of criminal offenses related to illegal content on the Internet and the scope of their search activities. ***Results.*** The structure of the multilevel system of actors responsible for preventing criminal offenses related to illegal content on the Internet is determined, which is a totality of state bodies whose activities are fully or partially related to the prevention of using the Internet for unlawful purposes. The actors of the detection system are identified depending on the functions performed by them in the detection process: operational units, functions thereof include response to criminal offenses in the field of computer technology; operational units involved in the implementation of priority measures in the commission of criminal offenses related to illegal content on the Internet; confidants who perform "blocking" of objects where criminal intentions can be realised; employees of other law enforcement units who can receive primary information about the commission of criminal offenses related to illegal content on the Internet; state control bodies, functions thereof include ensuring cybersecurity of the state, and counteracting criminal offenses related to illegal content on the Internet (State Centre for Cyber Defence and Counteraction to Cyber Threats of the State Service of Special Communications and Information Protection of Ukraine). ***Conclusions.*** The scope of search activities during the detection of signs of placement and/or dissemination of illegal content is distinguished enabling to conclude that they have significant differences from the "classical" scope of search, due to the fact that the electronic environment in which the search for factual data is carried out is formed by a totality of information carriers, software and hardware for automated information processing and telecommunication networks (material media, electric fields and signals, means of their processing, communication channels, etc.)

Key words: illegal content on the Internet, criminal offenses, detection, actors, scope of search activities.

1. Introduction

The development of the information society gives new impetus to traditional threats and creates fundamentally new challenges for combating cybercrime. In such context, it is of particular importance to find new opportunities for active counteraction, timely detection of signs of criminal offenses in cyberspace, including the commission of criminal offenses related to illegal content on the Internet. Although Ukraine began to enter the information space only in the early 1990s, this caused a sharp surge in computer crime, which requires to develop appropriate legal tools, adapting them to new technologies, to define the actors who will use them and to identify the scope of their search activities The relevancy of this problem is also determined by the rapid development of a new type of illegal activities – transnational computer crimes, a sharp increase in criminal computer professionalism, active migration of criminals and organisation of their actions, international nature, which significantly complicates the criminogenic situation (Borysova, 2007, p. 17) and necessitates close consolidation of these actors with foreign and international bodies that perform identical functions in their own countries. The search for signs of these criminal actions is carried out within the organisational and tactical system

of detection of criminal offenses related to illegal content on the Internet. One of the main elements of this system is its actors, since their list determined, the functions and scope of application of search competence established are a prerequisite for identifying persons who commit (prepare to commit) criminal offenses related to illegal content on the Internet, establishing the circumstances related to the preparation for the commission of criminal offenses, as well as the place and time of its commission (Tarasenko, 2021, p. 266).

Several scientists have studied this issue. For example, D.S. Kosinova, K.I. Ivchuk, O.V. Cherniavskyi considered the issue of regulating the procedures for identifying the facts of threats in the field of cybersecurity in the context of implementing cybersecurity policy in the EU and Ukraine (Kosinova, Ivchuk, Cherniavskyi, 2021); T.V. Stanislavskyi made scientifically based proposals to increase Ukraine's ability to adequately counter cybersecurity threats and develop a national cybersecurity system, including by creating a system for their detection (Stanislavskyi, 2020). Several scholars argue that the detection of criminal offenses is the prerogative of all law enforcement bodies. For example, M. Borchakovskyi consistently builds a system of detection of criminal offenses and defines: areas and places of detection of latent criminal offenses (Borchakovskyi, 2016, pp. 17–19). Other scholars consider in detail certain elements of search activities not related to the commission of cybercrime (places of search for criminal offenses (Iermakov, 2019, pp. 241–246), areas and places of search activities (Shapovalov, 2018, pp. 304–314)); accordingly, they do not extrapolate them to the state system for detecting these criminal offenses. Therefore, in fact, the issues of identification of actors of search activities and their search full powers in this field remain unexplored.

The purpose of the article is to identify the actors of detection of criminal offenses related to illegal content on the Internet and the scope of their search activities.

2. Specificities of detection of criminal offenses in the field of computer technology

One of the elements of the detection system is its actors. Formally, the detection of criminal offenses in the field of computer technology, communication networks, etc., belongs to the functions of response units to cybercrime, but given the specifics of criminal offenses related to illegal content on the Internet, and that their consequences (material damage) can also be reflected in the performance of other units, then, in our opinion, other operational units can also be attributed to the actors (not in full, but in terms of certain functions performed to counter these offenses). The actors are identified depending on the functions performed by them in the detection process:

1) operational units, functions thereof include response to criminal offenses in the field of computer technology;

2) operational units involved in the implementation of priority measures in the commission of criminal offenses related to illegal content on the Internet;

3) confidants who perform "blocking" of objects where criminal intentions can be realised.

The analysis of scientists' opinions allows to attribute to the actors of detection also other law enforcement officers who can receive primary information about the commission of criminal offenses related to illegal content on the Internet.

It should be noted that the scope of these criminal offenses allows a number. of state control bodies, functions thereof include ensuring cybersecurity of the state, and counteracting criminal offenses committed in the field of computer technology, to be listed as the actors of detection:

Decree of the President of Ukraine No. 242/2016 of June 7, 2016 approved the Regulation on the National Coordination Centre for Cyber Security (Decree of the President of Ukraine On the National Coordination Centre for Cyber Security, 2016) (headed by the Secretary of the National Security and Defence Council, and composed of almost all heads of law enforcement bodies or their deputies). The competence of the National Coordination Centre for Cybersecurity is provided for by Part 2 of Article 5 of the Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine", in particular, the Centre coordinates and controls the activities of the security and defence sector entities that ensure cybersecurity, submits proposals to the President of Ukraine on the formation and clarification of the Cybersecurity Strategy of Ukraine (Law of Ukraine On Basic Principles of Cyber Security of Ukraine, 2017).

The task of performing all procedures, including regulatory ones, is entrusted to the State Service of Special Communications and Information Protection of Ukraine (Law of Ukraine On the State Service of Special Communications and Information Protection of Ukraine, 2006), functions thereof include: accumulation and analysis of data on the commission and/or attempts to commit unauthorised actions against information resources in information and telecommunication systems, as well as their effects, informing law enforcement bodies to take measures to prevent and deter criminal offenses in this field; support

for the functioning of the governmental computer emergencies response team of Ukraine CERT-UA, created as teams of experts engaged in collecting information about cyber incidents, their classification and neutralisation); coordination of cybersecurity entities' activities on cyber defence; implementation of the organisational and technical model of cybersecurity, implementation of organisational and technical measures to prevent, detect and respond to cyber incidents and cyber-attacks and eliminate their effects; informing about cyber threats and appropriate methods against them; ensuring the implementation of an information security audit system at critical infrastructure facilities, establishing requirements for information security auditors, their certification (recertification); coordination, organisation and conducting of vulnerability audits of communication and technological systems of critical infrastructure facilities; ensuring the functioning of the State Centre for Cyber Defence (clauses 85-92 of the Law (Law of Ukraine On the State Service of Special Communications and Information Protection of Ukraine, 2006), Cyber Centre UA 30 (The National Security and Defence Council has adopted a strategy for the development of cybersecurity in Ukraine for 5 years, 2021)). In case of detection of cyber incidents and cyber-attacks that may pose a threat to the national security or defence capability of the state, the State Centre for Cyber Defence and Counteraction to Cyber Threats of the State Service of Special Communications and Information Protection of Ukraine informs the National Coordination Centre for Cybersecurity in the prescribed manner, as well as provides the necessary information from the State Register of Critical Infrastructure Objects, to form (adjust) the Cybersecurity Strategy of Ukraine and other strategic decisions in this field (Stanislavskyi, 2020, pp. 69-70). Regarding the participation in the detection of criminal offenses, the Administration of the State Special Communications Service of Ukraine proposed the Protocol of joint actions of the main actors of cybersecurity, cyber defence and owners (managers) of critical information infrastructure and during the prevention, detection, elimination of cyberattacks and cyber incidents, as well as in eliminating their effects (June 2019) (Order of the State Special Communications Administration On Approval of the Procedure for Coordination of Activities of Public Authorities, Local Self-Government Bodies, Military Formations, Enterprises, Institutions and Organisations Regardless of Forms of Ownership on Prevention, Detection and Elimination of Unauthorised Actions on State Information Resources-Telecommunication systems, 2008), according to which information is exchanged when taking measures to respond to cyber incidents and cyber-attacks (Draft Order of the Administration On Approval of the Protocol of Joint Actions of Major Cyber Security Entities, Cyber Security Entities and Owners (Managers) of Critical Information Infrastructure Facilities and in Preventing, Detecting, Terminating Cyber Attacks and Cyber Incidents, and in Eliminating Their Consequences, 2021). According to this procedure, in case of detection of an attempt to commit and/or commission of unauthorised actions in relation to information and telecommunication systems, the said entities shall perform the following actions: measures to immediately inform the State Service of Special Communications by sending an appropriate electronic message in the form established by this Procedure; the security administrator of the information and telecommunications system in respect of which attempts or unauthorised actions have been detected, shall take measures to inform CERT, which performs the functions of coordinator within the State Service of Special Communications, within 24 hours; owners/managers of information and telecommunication systems shall take measures to preserve (fix) the signs of unauthorised actions and implement, among other things, the recommendations of the coordinator, as well as physical access of his representatives to take measures to block and localise the negative effects of unauthorised actions and restore the system's performance.

Although the Protocol shall logically apply to both key actors of cybersecurity, actors of cyber defence and owners (managers) of critical information infrastructure, but the justification for its development (Analysis of the regulatory impact of the draft resolution of the Cabinet of Ministers of Ukraine on approval of the Protocol on joint actions of key actors of cybersecurity, actors of cyber defence and owners (managers) of critical information infrastructure during prevention, detection, cessation of cyberattacks and cyber incidents their consequences, 2021) states that its norms do not apply to cyber incidents that are not related to unauthorised actions against state information resources. Similarly, the Law (Law of Ukraine On Basic Principles of Cyber Security of Ukraine, 2017) does not apply to internal (local) computer networks that do not interact (are not connected to global computer networks). The relations that develop when using social networks, as well as "private" information electronic resources (apparently, non-state resources), are not regulated by the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" under certain conditions,

such as the absence of information, which protection is established by law (Dovhan, Doronin, 2017, p. 97).

This problem has already been considered in a slightly different context by scientists who argue that in general, the problem of developing and implementing organisational and legal mechanisms for strategic management of the development of cyber security of these objects is especially relevant in ensuring the cyber protection of critical infrastructure (Stanislavskyi, 2020, p. 54). However, the issue of ensuring interaction between the National Coordination Centre for Cybersecurity, the State Centre for Cybersecurity (Cyber Centre UA 30 (The National Security and Defence Council has adopted a strategy for the development of cybersecurity in Ukraine for 5 years, 2021)), Governmental Computer Emergency Response Team of Ukraine (CERT-UA) and other computer emergency response teams, as well as their interaction with international cyber defence centres remains uncertain. In our opinion, the effective implementation of the search function requires the staff of critical infrastructure facilities to involve a person who has the functions of countering cyber threats and interacting with the State Centre for Cyber Defence, and the central authorities that control the areas containing critical infrastructure facilities, shall have tasks defined in the regulatory documents (which regulate their activities) to provide information about such objects to the State Centre for Cyber Defence (indicating the critical state of such objects, a list of possible threats, actions during the implementation of such a threat for each of the possible situations and the ability to provide cyber defence on their own).

3. Specificities of the competence of the actors of the system of detection of criminal offenses related to illegal content on the Internet

Considering the competence of the actors, the issue of applying their search functions to certain areas should be under the focus, since it is the precise distribution of their full powers by places of search that ensures its effectiveness (areas where signs of criminal offenses can be detected, the main places where it is possible to obtain information about the commission of these criminal offenses or preparation for them). For these criminal offenses, these places are specific that the signs of the use of illegal content can be detected not only by the actors of search activities (or law enforcement activities), both in electronic form and in the form of material traces arising in the case of a criminal offense with the use of illegal content posted on the Internet. Accordingly, the primary information comes to operational units already in processed (distorted) form, and may not come at all (if the actors are not interested in providing such information to law enforcement bodies). A significant factor influencing the positioning of certain places as search areas is a difference between the concept of "criminal acts committed through the placement and dissemination of illegal content on the Internet" and the concept of "criminal offenses related to illegal content on the Internet", because in the second case the search areas can be unlimited and not subject to definition. Therefore, we consider not the scope of search for signs of criminal offenses related to illegal content on the Internet, but the places where actors can detect signs (facts) of placement and/or dissemination of illegal content.

The scope of search during detection of signs of placement and/or dissemination of illegal content has significant differences from the "classical" scope of search, and the place of direct commission of an illegal act with the use of computer technologies (primarily network technologies) (the place where the actions of the objective side of the criminal offense were committed) and the place of harmful consequences (the place where the result of the illegal act occurred) do not coincide (Holubiev, 2003, p. 143). In order to identify the signs of placement and/or dissemination of illegal content, it is necessary to link the information to specific technical means of its storage, transmission, reception and processing, that is, to specify the places of possible commission of a criminal offense.

In our opinion, such places are:

1) computer, which is a set of technical means and system software, enabling automated processing of information and obtaining the result in the required form;

2) automated systems processing data such as technical means, their processing (means of computing and communication), as well as methods and procedures, software;

3) computer (information) networks, which are a totality of geographically dispersed data processing systems, means and/or systems of communication and data transmission, which provides users with remote access to its resources and collective use of these resources;

4) telecommunication networks (telecommunication networks), which are a complex of technical means of telecommunications and facilities designed for routing, switching, transmitting and/or receiving signs, signals, written text, images and sounds or messages of any kind by radio, wire, optical or other electromagnetic systems between end equipment (Law of Ukraine on Telecommunications, 2003). The places of search do not include all of them, but only those that can be identified on

the basis of already available data (the victim's computer system; the victim's provider's server; the offender's computer system; the provider's servers and computer systems of third parties used by the offender (both without their knowledge and with their knowledge); other places of the network used by the offenders) (Spyropulos, 2013, p. 17);

5) places where malicious programs are created (directly at one of the workplaces of the automated information system in the organisation; at the place of residence of a person on his/her personal computer, etc;

6) separate premises or their complex, where automated systems with the corresponding technical complex of their activity support are located;

7) electronic media that ensure its safety;

8) organisations that assign addresses on the Internet, which during registration of a network on the Internet, are given a network identifier depending on the class (further identification of nodes in subnets of the network is carried out by the organisation-owner, and when a person connects to the Internet, his/her computer becomes part of the network and is assigned an IP address (which can be dynamic or static);

9) state regulatory authorities in the field of communications;

10) telecommunications operators, telecommunications providers;

11) manufacturers and suppliers of equipment, materials and means in the field of communications and informatisation, television and radio broadcasting equipment;

12) enterprises, institutions and organisations that use information or telecommunication technologies in their economic or business activities.

4. Conclusions

Therefore, the actors of the detection system are identified depending on the functions performed by them in the process of search activities: operational units, functions thereof include response to criminal offenses in the field of computer technology; operational units involved in the implementation of priority measures in the commission of criminal offenses related to illegal content on the Internet; confidants who perform "blocking" of objects where criminal intentions can be realised; employees of other law enforcement units who can receive primary information about the commission of criminal offenses related to illegal content on the Internet; state control bodies, functions thereof include ensuring cybersecurity of the state, and counteracting criminal offenses related to illegal content on the Internet (State Centre for Cyber Defence and Counteraction to Cyber Threats of the State Service of Special Communications and Information Protection of Ukraine). The scope of search activities during the detection of signs of placement and/or dissemination of illegal content is distinguished enabling to conclude that they have significant differences from the "classical" scope of search, due to the fact that the electronic environment in which the search for factual data is carried out is formed by a totality of information carriers, software and hardware for automated information processing and telecommunication networks (material media, electric fields and signals, means of their processing, communication channels, etc.)

References:

Borysova, L.V. (2007). Transnatsionalni kompiuterni zlochyny yak obiekt kryminalistychnoho doslidzhennia [Transnational computer crime as a subject of forensic investigation]. *Candidate's thesis.* Kyiv (in Ukrainian).

Tarasenko, O.S. (2021). *Teoriia ta praktyka protydii kryminalnym pravoporushenniam, poviazanym z obihom protypravnoho kontentu v merezhi Internet [Theory and practice of combating criminal offenses related to illegal content on the Internet].* Kyiv: Natsionalna akademiia vnutrishnikh sprav (in Ukrainian).

Kosinova, D.S., Ivchuk, K.I., Cherniavskyi, O.V. (2021). Pravovyi analiz suchasnoho stanu ta tendentsii rozvytku zakonodavstva YeS ta Ukrainy u sferi kiberbezpeky [Legal analysis of the current state and trends in the development of EU and Ukrainian legislation in the field of cybersecurity]. *Міжнародний науковий журнал "Інтернаука" – International Scientific Journal «Internauka», 4* (in Ukrainian).

Stanislavskyi, T.V. (2020). Rozvytok mekhanizmiv publichnoho upravlinnia u sferi kiberbezpeky [Development of public administration mechanisms in the field of cybersecurity]. *Candidate's thesis.* Kyiv (in Ukrainian).

Borchakovskyi, M.B. (2016). Sfery ta mistsia vyiavlennia latentnykh kryminalnykh pravoporushen [Areas and places of detection of latent criminal offenses]. *Stanovlennia ta rozvytok naukovykh doslidzhen – Formation and development of scientific research, 1*, 17-19 (in Ukrainian).

Iermakov, Yu.O. (2019). Mistsia poshukovoi diialnosti kryminalnykh pravoporushen, shcho vchyniuiutsia u sferi vykorystannia ta okhorony nadr [Places of search activity of criminal offenses committed in the field of subsoil use and protection]. *Yurydychna nauka – Legal science, 12,* 241-246 (in Ukrainian).

Shapovalov, O.O. (2018). Sfery ta mistsia poshukovoi diialnosti operatyvnykh pidrozdiliv [Areas and places of search activities of operational units]. *Yurydychnyi chasopys – Law Journal, 1*, 304-314 (in Ukrainian).

Ukaz Prezydenta Ukrainy Pro natsionalnyi koordynatsiinyi tsentr kiberbezpeky: vid 7 cherv. 2016 № 242 [Decree of the President of Ukraine On the National Coordination Centre for Cyber Security: June 7, 2016

№ 242]. (2016). *president.gov.ua*. Retrieved from https://www.president.gov.ua/documents/2422016-20141 (in Ukrainian).

Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : vid 05 lystop. 2017 roku [Law of Ukraine On Basic Principles of Cyber Security of Ukraine: dated November 5, 2017]. (2017). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

Zakon Ukrainy Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy: vid 23 liut. 2006 roku № 3475-IV [Law of Ukraine On the State Service of Special Communications and Information Protection of Ukraine from February 23, 2006 № 3475-IV]. (2006). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text (in Ukrainian).

RNBO ukhvalyla stratehiiu rozvytku kiberbezpeky Ukrainy na 5 rokiv [The National Security and Defence Council has adopted a strategy for the development of cybersecurity in Ukraine for 5 years]. (2021). *pravda.com.ua*. Retrieved from https://www.pravda.com.ua/news/2021/05/14/7293553/ (in Ukrainian).

Nakaz Administratsii Derzhspetszviazku Pro zatverdzhennia Poriadku koordynatsii diialnosti orhaniv derzhavnoi vlady, orhaniv mistsevoho samovriaduvannia, viiskovykh formuvan, pidpryiemstv, ustanov i orhanizatsii nezalezhno vid form vlasnosti z pytan zapobihannia, vyiavlennia ta usunennia naslidkiv nesanktsionovanykh dii shchodo derzhavnykh informatsiinykh resursiv v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh: vid 10 cherv. 2008 roku № 94 [Order of the State Special **Communications Administration On Approval of the Procedure for Coordination of Activities of Public Authorities, Local Self-Government Bodies, Military Formations, Enterprises, Institutions and Organisations Regardless of Forms of Ownership on Prevention, Detection and Elimination of Unauthorised Actions on State Information Resources-Telecommunication systems from June 10, 2008 № 94]**. (2008). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/z0603-08 (in Ukrainian).

Proekt nakazu Administratsii Pro zatverdzhennia protokolu spilnykh dii osnovnykh subiektiv zabezpechennia kiberbezpeky, subiektiv kiberzakhystu ta vlasnykiv (rozporiadnykiv) obiektiv krytychnoi informatsiinoi infrastruktury ta pid chas poperedzhennia, vyiavlennia, prypynennia kiberatak ta kiberintsydentiv, a takozh pry usunenni yikhnikh naslidkiv [Draft Order of the Administration On Approval of the Protocol of Joint Actions of Major Cyber Security Entities, Cyber Security Entities and Owners (Managers) of Critical Information Infrastructure Facilities and in Preventing, Detecting, Cessating Cyber Attacks and Cyber Incidents, and in Eliminating Their Consequences]. (2021). *dsszzi.gov.ua*. Retrieved from URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=308016&cat_id=38837&ctime=1559743156921 (in Ukrainian).

Analiz rehuliatornoho vplyvu proektu postanovy Kabinetu Ministriv Ukrainy Pro zatverdzhennia Protokolu spilnykh dii osnovnykh subiektiv zabezpechennia kiberbezpeky, subiektiv kiberzakhystu ta vlasnykiv (rozporiadnykiv) obiektiv krytychnoi informatsiinoi infrastruktury pid chas poperedzhennia, vyiavlennia, prypynennia kiberatak ta kiberintsydentiv, a takozh pry usunenni yikh naslidkiv [Analysis of the regulatory impact of the draft resolution of the Cabinet of Ministers of Ukraine on approval of the Protocol on joint actions of key actors of cybersecurity, actors of cyber defence and owners (managers) of critical information infrastructure during prevention, detection, cessation of cyberattacks and cyber incidents their consequences]. (2021). *dsszzi.gov.ua*. Retrieved from http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=43C2F32D FABF17DB4B178168DDF198F3.app1?showHidden=1&art_id=308043&cat_id=38837&ctime=1559743813443 (in Ukrainian).

Dovhan, O.D., Doronin, I.M. (2017). *Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense]*. Kyiv: Vydavnychyi dim «ArtEk» (in Ukrainian).

Holubiev, V.O. (2003). *Informatsiina bezpeka: problemy borotby z kiberzlochynnistiu [Information security: problems of combating cybercrime]*. Zaporizhzhia: ZIDMU (in Ukrainian).

Zakon Ukrainy Pro telekomunikatsii: vid 18 lystop. 2003 roku № 1280-IV [Law of Ukraine on Telecommunications from November 18, 2003 № 1280-IV]. (2003). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

Spyropulos, D. (2013). *Bor'ba s prestuplenijami, sovershaemymi v virtual'nom prostranstve: rukovodstvo dlja sotrudnikov pravoohranitel'nyh organov po prestuplenijam [[Fighting Cyber Crime: A Law Enforcement Guide to Crime]*. Moskva (in Russian).

Олег Тарасенко,
доктор юридичних наук, доцент, професор кафедри оперативно-розшукової діяльності, Національна академія внутрішніх справ, площа Солом'янська, 1, Київ, Україна, індекс 03035, o.s.tarasenko@gmail.com
ORCID: *orcid.org/0000-0002-3179-0143*

СУБ'ЄКТИ ВИЯВЛЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ ТА СФЕРИ ЇХ ПОШУКОВОЇ ДІЯЛЬНОСТІ

Анотація. ***Мета.*** Мета статті полягає у виокремленні суб'єктів виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, та сфери їх пошукової діяльності. ***Результати.*** Визначено структуру багаторівневої системи суб'єктів, які уповноважені запобігати кримінальним правопорушенням, пов'язаним з обігом протиправного контенту в мережі Інтернет, що становить собою сукупність державних органів, діяльність яких повністю або в певній її частині пов'язана із недопущенням використання мережі Інтернет у протиправних цілях. Суб'єктів системи виявлення визначено залежно від функцій, що виконуються ними в процесі пошукової діяльності: оперативні підрозділи, до функцій яких відноситься протидія кримінальним правопорушенням у сфері комп'ютерних технологій; оперативні підрозділи, які беруть участь у проведенні першочергових заходів при вчиненні кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет; конфіденти, які здійснюють «перекриття» об'єктів, де можуть бути реалізовані злочинні задуми; працівники інших підрозділів правоохоронних органів, які можуть отримати первинну інформацію про вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет; державні контролюючі органи, до функцій яких віднесено забезпечення кібербезпеки держави, а, відповідно, і протидію кримінальним правопорушенням, пов'язаним з обігом протиправного контенту в мережі Інтернет (Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України). ***Висновки.*** Виокремлено сфери пошукової діяльності під час виявлення ознак розміщення та/або обігу протиправного контенту та зроблено висновок, що вони мають суттєві відмінності від «класичної» сфери пошуку, що пояснюється тим, що електронне середовище, в якому здійснюється пошук фактичних даних, утворюється сукупністю носіїв інформації, програмно-технічних засобів автоматизованої обробки інформації та телекомунікаційними мережами (матеріальними носіями інформації, електричними полями та сигналами, засобами їх оброблення, каналами зв'язку тощо).

Ключові слова: протиправний контент в мережі Інтернет, кримінальні правопорушення, виявлення, суб'єкти, сфери пошукової діяльності.

The article was submitted 19.07.2022
The article was revised 09.08.2022
The article was accepted 30.08.2022