**DOI: https://doi.org/10.32353/acfs.4.2021.01**
**UDC 343. 98**

**Nechyporuk Mykola**

**Mykola Nechyporuk,**
Doctor of Technology, Professor, Rector of Law Department of National Aerospace University – «Kharkiv Aviation Institute " NAU "KhAI", Chkalova Street, 17, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2723-6107
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57210558126
e-mail: khai@khai.edu

**Kliuiev Oleksandr**

**Oleksandr Kliuiev,**
Doctor of Law, Professor,
Honored Lawyer of Ukraine,
Director of the National Science Center «Hon. Prof. M.S. Bokarius Forensic Science Institute», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-8722-4781,
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57211296519,
e-mail: hniise@hniise.gov.ua

**Filipenko Nataliia**

**Nataliia Filipenko,**
PhD in Law, Docent, Associate Professor at the Law Department of National Aerospace University – "Kharkiv Aviation Institute " NAU "KhAI", Chkalova Street, 17, Kharki, Ukraine
ORCID: https://orcid.org/0000-0001-9469-3650
e-mail: n.filipenko@khai.edu

**Volodymyr Pavlikov,**
Doctor of Technology, Professor, Vice-Rector for Research of Law Department of National Aerospace University – "Kharkiv Aviation Institute " NAU "KhAI", Chkalova Street, 17, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-6370-1758
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=23397933100
e-mail: v.pavlikov@khai.edu

**Aleksandar Ivanović,**
Doctor of Law, Professor,
Director of Forensic Center Montenegro,
Danilovgrad, Montenegro

# Criminal Liability for Offenses in the Field of Information and Communication Technologies Use (Review Article)

The article analyzes scientific opinions on the content of studying peculiarities of criminal liability for offenses in the field of information and communication technologies use. An in-depth analysis of such scientific concepts as the crime object has been conducted. In particular, it is emphasized that information security can be both the *main* and *additional* object of a crime.

The article summarizes that crimes against security of information and telecommunication technologies are prohibited by criminal law socially dangerous acts encroaching on social relations that ensure the security of processes and methods of search, collection, storage, processing, provision, dissemination of information by means of electronic computing machines and information telecommunication networks.

**Keywords:** criminal liability, crime, crime object, information and communication technologies, systems and computer networks and telecommunication networks.

**Introduction.** The development of information and communication technologies conditioned by technological breakthrough and extensive use of innovations has become a determining factor of widespread introduction

and application of information and communication technologies in all areas of human lives, necessitating heightened requirements for addressing information security issues.

Real rates of development and dissemination of information-communication technologies in all areas of society activity are key elements that must considered while determining the main problems in the field of information security.

Currently, according to the findings of the Estonian e-Governance Academy, which annually publishes national cybersecurity indexes, Ukraine has the 25th National Cybersecurity Index; 78th Global Cybersecurity Index; 79th ICT Development Index and the 64th Networked Readiness Index[1].

At the same time, it should be emphasized that in inter-state relations there is an increased tendency for information pressure as an efficient mechanism of global competition. The use of different means of information propaganda and expansion of information have become an indispensable tool for resolving various social, economic and political conflicts. Certain countries of the world, which have the ability to monitor global dissemination of information, use its results to gain unilateral advantages in political, economic, military, environmental and other aspects of inter-state relations.

Extremist and terrorist organizations and groups are increasingly taking advantage of the potential of global information and communication networks to promote their ideology, recruitment and training of like-minded people, maintain communication and funding of various terrorist groups. As mentioned in professional researches, lack of operational and investigative information regarding persons who create a hacker group of criminal orientation; weakness of domestic anti-terrorist legislation containing many legal conflicts and contradictions; high level of secrecy and latency of cyber incidents, etc.[2]. A significant issue is prevalence of information crimes (cybercrime), including the activity of organized transnational criminal groups. Counteraction to information crimes requires law enforcement agencies and intelligence agencies to respond rapidly by performing joint coordinated actions with intelligence agencies and law enforcement agencies of foreign countries. The role and influence of global mass media and communication mechanisms in the development of economic, political and social situations in different countries of the world gain more importance. Radical changes having taken place over the recent years in ountries with different economic and political conditions point to the key role of new technologies in control over masses in these processes, including through the use of information and communication technologies: websites, social networks and mobile applications[3]. Therefore, it is not by chance that the issue of ensuring cybersecurity is included in all sections dedicated to pursuing strategic national priorities, a new version of the National Security Strategy of Ukraine[4]. The provisions outlined in the Strategy have been also

**Pavlikov Volodymyr**

**Ivanović Aleksandar**

**Funding**

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

**Disclaimer**

The funder had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

**Contributors**

The author contributed solely to the intellectual discussion underlying this paper, case-law exploration, writing and editing, and accept responsibility for the content and interpretation.

**Declaration of Competing Interest**

The author declare that they have no conflict of interest.

[1] Офіційний сайт Академії електронного управління Естонії. URL: https://ncsi.ega.ee/country/ua/

[2] Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206-220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). https://doi.org/10.1007/978-3-030-66717-7

[3] Спіцина Г. О., Філіпенко Н. Є. Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 188-191.

[4] Стратегія національної безпеки України. Указ Президента України №121/2021. URL: https://www.president.gov.ua/documents/3922020-35037

**М. В. Нечипорук, О. М. Клюєв, Н. Є. Філіпенко, В. В. Павліков, А. Іванович**

**КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**(оглядова стаття)**

У статті проаналізовано особливості кримінальної відповідальності за порушення у сфері використання інформаційно-комунікаційних технологій. Проведено грунтовний аналіз такого наукових понять, як об›єкти кримінального правопорушення. Зокрема зазначається, що інформаційна безпека може бути як основним, так і додатковим об›єктом кримінального правопорушення. Інформаційна безпека як додатковий об›єкт кримінального правопорушення наявна в значній кількості складів, відповідальність за які передбачена нормами Особливої частини Кримінального кодексу. Їх можна відносити до зазіхань на інформаційну безпеку з деякою часткою умовності. Отже, необхідно конкретизувати родовий об›єкт цієї групи кримінальних правопорушень як суспільних відносин, що забезпечують інформаційну безпеку.

Родовим об'єктом правопорушень, передбачених у розділі XVI Кримінального Кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп›ютерів), систем та комп›ютерних мереж і мереж електрозв›язку», є частина інформаційних відносин, які можна визначити як інформаційні відносини, засобом забезпечення яких є електронно-обчислювальні машини, системи, комп'ютерні мережі та мережі електрозв'язку. Інакше кажучи, кримінальні правопорушення, передбачені цим розділом, посягають на певну частину інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів, які широко відомі та досить добре розповсюдженні в наш час.

У статті зроблено висновок, що кримінальними правопорушеннями проти безпеки інформаційно-телекомунікаційних технологій є заборонені кримінальним законом суспільно небезпечні діяння, що посягають на суспільні відносини, які забезпечують

developed in the Strategy of Military Security of Ukraine[5]. These documents not only assess the current state of information security in Ukraine, but also provide a list of threats as well as a set of tools that can ensure a sufficient level of information security protection of the state.

**Analysis of publications where this problem solution is initiated.** Issues of information security of the state and criminal liability for violations of legislation in the field of information and communication technologies have not yet been covered widely today. Particular aspects of criminal liability for offenses while the use of electronic computing machines (computers), systems and computer networks and telecommunication networks have been studied by such scholars as Yu. M. Baturin, K. V. Basin, P. D. Bilenchuk, A. B. Venherov, V. S. Venediktov, V. V. Vertuzaiev, M. V. Viekhov, O. H. Volievodz, O. A. Havrylov, V. V. Holina, V. V. Holubiev, P. A. Dubrov, O. V. Ivanenko, A. M. Zhodzyshskyi, M. A. Zuban, R. A. Kaliuzhnyi, M. V. Karchevskyi, M. M. Kovalenko, V. K. Kolpakov, A. T. Komziuk, O. V. Kokhanovska, V. V. Kuznietsov, T. V. Mikhailina, M. V. Nechyporuk, M. I. Panov, V. V. Pyvovarov, M. S. Polievoi, V. A. Severyn, S. I. Semylietov, V. V. Sydorenko, K. S. Skoromnikov, F. P. Tarasenko, L. K. Tereshchenko, T. I. Tarakhonych, B. S. Ukraintsev, N. Ie. Filipenko, V. S. Frolov, A. V. Chernykh, S. V. Yasechko and others[6]. The authors refer to various perspectives of legal liability for violating legislation in the field of information and communication technologies use, both within the framework of experimental developments and applied researches. But many aspects of this complex problem still need to be addressed immediately.

At the current stage, legal means of ensuring information security of Ukraine include the need to prepare and adopt new regulations as well as clarify existing conceptual and doctrine documents that would sufficiently reflect national interests of Ukraine, including in the field of information and communication technologies use, and contributed to the fulfillment of tasks on ensuring the country information security, based upon the dynamics of modern threats.

**Aim.** The aim of the article is to study peculiarities of criminal liability for offenses in the field of information and communication technologies use.

**Results and discussion.** Criminal liability is one of the types of legal liability and is, by its content, the most severe of them. Criminal liability is a statutory restriction of rights and freedoms of a person who has committed a crime, consisting of his official condemnation, possible punishment and confession by the convicted.

Peculiarities of criminal liability: a type of legal responsibility (coexists with its other types, in particular, administrative, civil, etc.); applicable to a

[5] Стратегія воєнної безпеки України. Указ Президента України № 392/2020. URL: https://www.president.gov.ua/documents/1212021-37661

[6] E. g., Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206-220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). https://doi.org/10.1007/978-3-030-66717-7; Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206-220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). https://doi.org/10.1007/978-3-030-66717-7; Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Белякова. Київ: КВІЦ, 2019.; Спіцина Г. О., Філіпенко Н. Є. 2019 Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС. С. 188-191.; Карчевський В. М. 2002. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп›ютерних мереж: Монографія / МВС України, Луг. акад. внутр. справ ім. 10-річчя незалежності України; Наук. ред. Л. М. Кривоченко. Луганськ; Швачич Г. Г. & Толстой, В. В. & Петречук, Л. М. & Іващенко, Ю. С. & Гуляєва, О. А. & Соболенко, О. В. 2017 Сучасні інформаційно-комунікаційні технології: Навчальний посібник. Дніпро: НМетАУ. 230 с. та ін.

person who committed a crime; characterized by adverse effects stipulated by the law on criminal liability (condemnation (conviction), punishment, criminal records, testing); is to restrict rights and freedoms of a person.

It should be emphasized that information relations have become the object of criminal encroachment and have received certain criminal law protection in the current Criminal Code of Ukraine. It is confirmed by criminal law norms included by the legislator in many sections of the Code. We fully agree with the opinion of scholars that a separate, special criterion fundamentally changing the vision of criminal law on the possibility of committing criminal offenses in the field of information and communication technologies use is commission of acts by means of remote communications. In fact, remote is considered to be a communication realized between remote subjects with the use of IT. The technologies owing to which a person has the opportunity to instantly exchange information at a distance is a peculiarity of relations in the information society, progress of the XXI century, which, undoubtedly, contributes to the effectiveness of globalization processes[7].

Therefore, if we apply an adequate modern view to crimes outlined in the Criminal Code, namely the possibility of committing an act by means of remote communications; committing acts in relation to virtual objects; committing acts with the use of virtual means of influence, to acts that encroach on resources belonging to the area of information relations; large groups of traditional crimes can be fully attributed accordingly to the sections of the Criminal Code.

For example, Article 114 of the Criminal Code of Ukraine: *Espionage*, which is defined as transfer or collection for transfer to a foreign state, foreign organization or their representatives of information constituting a state secret, if these acts are committed by a foreigner or a stateless person[8]. One of the current features of the present is such a criminal phenomenon as *cyber spying*. In general, it should be understood as illegal collection, theft, transfer or storage of information in information and telecommunications networks owned by a foreign state, in case when they are not publicly available. Cyber spying is not always implemented in relation to information constituting a state secret. Thus, for example, the National Counterintelligence Directorate has submitted a report to the US Congress entitled: *Foreign Spies Steal American Economic Secrets in Cyberspace*[9] stating that China and Russia are using cyber spying to steal US trade and technology secrets. The authors of the report believe that in this way these countries are growing their own economies, resulting in a significant threat to the prosperity and security of the United States. A report by US counterintelligence also states that Chinese hackers alone have been able to obtain maximum access to the computer networks of numerous US energy, oil and military companies over the past two years. Cybersecurity experts have published a report on one of the largest cyber spying operations: *Red October*. The attack was aimed at various government agencies, diplomatic organizations and companies in different countries of the world. Red October is also capable of collecting data from mobile devices; collect information from network equipment; collect files from USB drives; copy mailbox databases from the local storage of the email client or from a remote mail transfer agent, and also extract files from local servers in the network. Therefore, the object of cyber spying can be any other information with limited access (information that constitutes bank secrecy; personal data, etc.). At the same time, the very fact of illegal interference, regardless of consequences, must be criminally punished.

And there are many such examples. First of all, the Criminal Code traditionally stipulates liability for acts that encroach on the essence of

[7] Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Белякова. Київ: КВІЦ, 2019. С 207.

[8] Кримінальний кодекс України. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=комп#w1_11

[9] Кібершпигуни з Китаю та Росії атакують компанії США – доповідь. https://news.obozrevatel.com/ukr/abroad/60549-kibershpiguni-z-kitayu-ta-rosii-atakuyut-kompanii-ssha-dopovid.htm

безпеку процесів і методів пошуку, збору, зберігання, обробки, надання, поширення інформації за допомогою засобів обчислювальної техніки та інформаційно-телекомунікаційних мереж.

Ключові слова: кримінальна відповідальність, кримінальне правопорушення, об›єкт кримінального правопорушення, інформаційно-комунікаційні технології, системи та комп›ютерні мереж і мережі електрозв›язку.

**Mykola Nechyporuk, Oleksandr Kliuiev, Nataliia Filipenko, Volodymyr Pavlikov, Aleksandar Ivanović**

**CRIMINAL LIABILITY FOR OFFENSES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES USE**

**Review Article**

The article analyzes peculiarities of criminal liability for offenses in the field of information and communication technologies use. An in-depth analysis of such scientific concepts as the crime object has been performed. In particular, it is stressed that information security can be both the main and additional crime object. Information security as an additional object of a crime exists in a significant number of corpora deliciti, the responsibility for which is stipulated by norms of the Special Part of the Criminal Code. They can be attributed to encroachments on information security with a certain conventionality. Therefore, it seems necessary to specify the generic object of this group of crimes as social relations ensuring information security.

The generic object of crimes provided for in Section XVI of the Criminal Code of Ukraine: *Criminal offenses related to the use of electronic computing maschines (computers), systems and computer networks and telecommunication networks* is part of information relations that can be defined as information relations, means of ensuring which are electronic computers, systems, computer networks and telecommunication networks. In other words, crimes stipulated in this section encroach on a certain part of information relations: information relations related to the use of special technical means that are widely known and quite common today

The article summarizes that crimes against security of information and telecommunication technologies

are prohibited by criminal law socially dangerous acts encroaching on social relations that ensure the security of processes and methods of search, collection, storage, processing, provision, dissemination of information by means of electronic computing machines and information telecommunication networks.

**Key words:** criminal liability, crime, crime object, information and communication technologies, systems and computer networks and telecommunication networks.

**Н. В. Нечипорук, А. Н. Клюев, Н. Е. Филипенко, В. В. Павликов, А. Иванович**

**УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

**Обзорная статья**

В статье проанализированы особенности уголовной ответственности за нарушения в сфере использования информационно-коммуникационных технологий. Проведен анализ таких научных понятий, как объект уголовного правонарушения. В частности, отмечается, что информационная безопасность может выступать как основным, так и дополнительным объектом уголовного правонарушения. Информационная безопасность в качестве дополнительного объекта уголовного правонарушения присутствует в большом количестве составов, ответственность за которые предусмотрена нормами Особенной части Уголовного кодекса. Их можно отнести к посягательствам на информационную безопасность с некоторой долей условности. Таким образом, представляется необходимым конкретизировать родовой объект данной группы уголовных правонарушений как общественных отношений, обеспечивающих информационную безопасность.

Родовым объектом правонарушения, предусмотренных разделом XVI Уголовного Кодекса Украины «Уголовные правонарушения в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи», являющихся частью информационных отношений, можно определить как информационные отношения, средством обеспечения которых

"relations in the information field", i.e. those that are committed in relation to information, or its circulation or security (including – for disruption of access to it). Such acts are contained in almost every section of the Special Part of the Criminal Code, and, at the same time, at the level of dispositions such acts are set out in such a way that, for the most part, information in them is either an object or a tool (means of committing an act). The list of them ranges from "Actions aimed at forceful change or overthrow of the constitutional order or take-over of government" through calls for such actions, including through mass media (Parts 2, 3 of Article 109), or *High treason* (Article 111) to *Illegal use of symbols of Red Cross, Red Crescent, Red Crystal* (Article 445). And in the modern world, almost all of them can be committed with the use of remote communications, due to which all social relations become both exploitative and vulnerable, and which subjects have been digitalized[10*].

Unfortunately, the volume of scientific paper prevents us from analyzing them all, so we will focus in greater detail on crimes which directly indicate the responsibility for violations in legislation in the field of information and communication technologies use (Section XVI: *Criminal offenses related to the use of electronic computing maschines (computers), systems and computer networks and telecommunication networks*)[11].

But before we consider in detail criminal and legal characteristics of these offenses, we want to dwell on general theoretical concepts which include the category: *crime object*.

Criminal offenses in the field of information and communication technologies use should include prohibited by law socially dangerous acts encroaching on public relations and ensuring the security of processes and methods of search, collection, storage, processing, provision, dissemination of information by means of electronic computing machines (computers), systems and information-telecommunication networks. With regard to criminal law, any object of a crime is a system of social relations protected by law.

However, such understanding of the crime object is not shared by all scholars. For example, opinions of 19th century scholars varied significantly. The first group of experts, transforming the ideas of the German criminalist A. Feuerbach, viewed the understanding of the crime object as part of the subjective right of a person. Thus, V. D. Spasovich viewed a crime as encroachment on someone's right which is protected by the state through punishment[12]. After analyzing this statement, it is possible to draw some weighty conclusions. According to his opinion, the bearers (owners or subjects of rights) can only be a person (one or a few), so the encroachment can be aimed only at a specific person. In addition, such a violation is excluded from the category of criminal offenses if the state will not protect the subjective right. Supporters of these views can be considered I. Ia. Foinytskyi, L. S. Belohrits-Kotliarevskyi and others. The second group of scholars shared the opinion that the object of crime is a certain equivalent of *legal good*, which is based on the postulate of protection of a specific vital interest by law. Moreover, there were known approaches to understanding the crime object as vital interests protected by norms of law (F. Liszt), as legal good (H. Welzel), as values that are conditions for a healthy existence of society (K. Binding), etc.

One of the first experts in the theory of criminal law who introduced a modern approach to the essence of the category *object*, was a pre-revolutionary researcher M. S. Tahantsev[13], who noted that criminally punishable is an act that encroach on a legal norm in its real existence …

[10] Докладніше про ці кримінальні правопорушення див.: Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О.П. Дзьобань та ін.; за заг. ред. проф. К. І. Белякова. Київ: КВІЦ, 2019. 344 с.

[11] Кримінальний кодекс України. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=комп#w1_11

[12] Спасович В. Д. Учебник уголовного права. Часть Общая. С.-Пб., 1863. С. 94.

[13] Таганцев М. С. Юридична енциклопедія : у 6 т. / ред. кол. Ю. С. Шемшученко (відп. ред.) та ін.. К. : Українська енциклопедія ім. М. П. Бажана, 2004. Т. 6 : Т- Я. С. 8. ISBN 966-7492-06-0.

acts encroaching on such legally protected interests of life which in this country, this time, are recognized as significant... and the state, due to the lack of other protection measures, threatens those who encroach on them with punishment[14]. Based on the above definition, it can be seen that the scientist saw not only the legal norm as the crime object, but also interests / benefits that it covers. Criticizing the theory of understanding the object as a subjective right, as well as normative theory, S. V. Poznyshev noted that crime objects are those specific relations, things and states of persons or things that are protected by law in fear of punishment[15]. At the beginning of the 20th century, the classical notion of the crime object as a set of social relations was introduced into the theory of criminal law by a number of distinguished scholars, in particular A. A. Piontkovskyi, M. Y. Korzhanskyi, M. I. Bazhanov. However, as rightly noted by V. Ia. Tatsii, it should be emphasized that one of the trends of modern theory of criminal law is the attempt of researchers to step away from understanding the crime object as social relations, since such an understanding of the crime object, according to their opinion, is based on abstract speculative ideological postulates artificially introduced into reality[16].

In this regard, we agree entirely with the conclusion of V. Ia. Tatsii that to date it has not yet been possible to create a perfect theory of the crime object. Undoubtedly, many current scientific approaches to determining the crime object have a right to exist. Furthermore, some of them seem to be quite convincing when studying a specific corpus delicti[17]. However, at the same time they contain a scope for justified criticism. In particular, if we consider most of these theories through the prism of social relations structure, it could be established that they mainly boil down to some structural element of social relations: their subject, subjects or social connection constituting the content of these relations. Thus, social values theory, despite its indisputable positive aspect as compliance with the Constitution of Ukraine (Article 3), which recognizes the highest social value human being, his or her life and health, honor and dignity, inviolability and security, is not without flaws. In particular, axiological approach to determination of the crime object does not provide sufficient grounds for automatic and unquestionable shift of the *social values* concept to criminal law.

The fact that the legislator points to such supreme values as human and citizen rights and freedoms in Article 1 of the Criminal Code of Ukraine does not indicate that they are protected by criminal law outside social relations, as it is known that the value of human life and health, property, etc. is ensured through their existence in society; outside of it, any regulation and protection in general make little sense. And therefore the legal construction of Article 1 of the Criminal Code of Ukraine is only a kind of legislative technique enabling to emphasize the importance of protecting social relations that ensure mentioned social values. In addition, social values, in our opinion, is an umbrella term that encompasses various subject matters of social relations (goods, interests, subjective rights, etc.) ensuring them. It is proof of the fact that social values theory narrows down the concept of the crime object to such an element of social relations as their subject. It should be stressed that this approach does not sufficiently take into account historical traditions, specific nature of the criminal law field and its separate institutions. A similar conclusion can be made regarding the position of recognizing a certain good as the crime object, which concept is even narrower than social values[18]. It seems necessary to agree with the opinion expressed in the literature that the category of *good* cannot encompass all realities of reality, which are protected

[14] Материалы для пересмотра нашего уголовного законодательства. Сборник дополнительных узаконений к французскому и германскому уголовным уложениям. Т. 7: Вып. 1-2 / Сост.: Г. Г. Савич; Под ред.: Н. С. Таганцев. С.-Пб. Тип. Правит. Сената, 1883. 786 с.

[15] Познышев С. В. Основные начала науки уголовного права. Общая часть уголовного права. М., 1912. С. 133.

[16] Тацій В.Я. Об'єкт злочину. Вісник Асоціації кримінального права України, 2013, № 1(1). С. 126-143.

[17] Там само. С. 129.

[18] Тацій В.Я. Об'єкт злочину. Вісник Асоціації кримінального права України, 2013, № 1(1). С. 130.

является электронно-вычислительные машины, системы, компьютерные сети и сети электросвязи. Иначе говоря, уголовные правонарушения, предусмотренные этим разделом, посягают на определенную часть информационных отношений – информационные отношения, связанные с применением специальных технических средств.

В статье сделан вывод, что уголовные правонарушения против безопасности информационно-телекоммуникационных технологий – это запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации с помощью средств вычислительной техники и информационно-телекоммуникационных сетей.

Ключевые слова: уголовная ответственность, уголовное преступление, объект уголовного преступления, информационно-коммуникационные технологии, системы и компьютерные сети и сети электросвязи.

**Mykola Nechyporuk, Oleksandr Kliuiev, Nataliia Filipenko, Volodymyr Pavlikov, Aleksandar Ivanović**

**RESPONSABILITÉ PÉNALE POUR LES VIOLATIONS DANS LE DOMAINE D'APPLICATION DE LA TECHNOLOGIE DE L'INFORMATION (TI)**

Article de revue

L'article analyse les caractéristiques de la responsabilité pénale pour les violations dans l'utilisation des technologies de l'information. L'analyse de concepts scientifiques tels que l'objet d'une infraction pénale est effectué. En particulier, il est noté que la sécurité de l'information peut être à la fois l'objet principal et l'objet supplémentaire d'une infraction pénale. La sécurité de l'information en tant qu'objet supplémentaire d'une infraction pénale est présente dans un grand nombre de structures dont la responsabilité est prévue par les normes de la partie spéciale du code pénal. Elles peuvent être qualifiées d'infractions à la sécurité de l'information avec un certain degré de convention. Ainsi, il semble nécessaire de concrétiser l'objet générique de ce groupe d'infractions pénales comme des relations

sociales qui assurent la sécurité de l'information.

L'objet générique de l'infraction prévue à la section XVI du Code pénal de l'Ukraine « Infractions pénales liées à l'utilisation d'ordinateurs, de systèmes et de réseaux informatiques et de réseaux de télécommunication » qui font partie des relations d'information, peut être défini comme relations d'information dont les moyens sont les calculateurs électroniques, les systèmes, les réseaux informatiques et les réseaux de télécommunication. En d'autres termes, les infractions pénales prévues dans cet article empiètent sur une certaine partie des relations d'information: les relations d'information associées à l'application de moyens techniques particuliers.

L'article conclut que les infractions pénales contre la sécurité des technologies de l'information sont des actes socialement dangereux interdits par le droit pénal, portant atteinte aux relations publiques, garantissant la sécurité des processus et des méthodes de recherche, de collecte, de stockage, de traitement, de fourniture, de diffusion d'informations à l'aide d'ordinateurs, la technologie et les réseaux d'information.

Mots-clés: responsabilité pénale, infraction pénale, objet délictueux, technologies de l'information, systèmes et réseaux informatiques et réseaux de télécommunication.

**Mykola Nechyporuk, Oleksandr Kliuiev, Nataliia Filipenko, Volodymyr Pavlikov, Aleksandar Ivanović**

**STRAFRECHTLICHE VERANTWORTUNG FÜR VERFEHLUNGEN BEI DER BENUTZUNG VON INFORMATIONS- UND KOMMUNIKATIONS-TECHNOLOGIEN**

Übersichtsartikel

Der Artikel analysiert die Besonderheiten der strafrechtlichen Verantwortlichkeit für Verfehlungen bei der Verwendung von Informations- und Kommunikationstechnologien. Eine gründliche Analyse solcher wissenschaftlichen Konzepte als Gegenstand einer Straftat wurde durchgeführt. Insbesondere wird darauf hingewiesen, dass Informationssicherheit sowohl Haupt- als auch zusätzlicher Gegenstand einer Straftat sein kann. Informationssicherheit als zusätzlicher Gegenstand einer Straftat ist in einer erheblichen

by the law on criminal liability. If classification to the category of *good* of such realities of reality as life, health, freedom, dignity, human security, property and social status, is not in doubt, it cannot be stated, for example, about the activities of the penitentiary system which is a forced attribute of state power and can hardly be called *good* for man and humanity. Fascist and other totalitarian political regimes are labeled good by its instigators and perceived as such by one part of the country's population, but are not perceived as good by another part of the country's population and all democratic states, and vice versa are considered as evil to be destroyed. It is impossible to disregard situations when the legislation on criminal liability continues to protect those categories and conditions of reality that have long been inconsistent with the idea of good, serve only as a brake on social development and require fast change and decriminalization[19].

We adhere to the understanding of the crime object as social relations protected by law, agreeing on the fact that recognition of social relations as the crime object is the result of some kind of abstraction. At the heart of any social relations, including those protected by criminal law, are certain interests (individual, society or state) or legal goods, that is the same interests protected by law.

Therefore, the object of crime in the field of information and communication technologies use is an open dynamic system of social relations. Openness of this system is due to the fact that it cannot be of permanent, enduring nature (at least because new types of offenses occur over time, and such acts are criminalized, or vice versa, decriminalized). As an object of criminal law protection, information security is an open dynamic system of social relations ensuring fulfillment of interests of the individual, society and the state in the information field. The structure of information security as an object of criminal law protection cannot be defined linearly. Nonlinear classification of information security structure is conditioned by the complexity of the information field itself.

The Doctrine of Information Security of Ukraine[20] states that national interests of Ukraine in the information field are:

1) vital interests of a person: ensuring constitutional rights and freedoms of a human to collect, store, use and disseminate information; ensuring constitutional rights of a human for protection of privacy; protection from devastating information and psychological influences;

2) vital interests of society and the state: protection of Ukrainian society from aggressive influence of destructive propaganda, particularly from the Russian Federation; protection of Ukrainian society from the aggressive information influence of the Russian Federation aimed at propaganda of war, incitement of national and religious discord, change of the constitutional order by force or violation of the sovereignty and territorial integrity of Ukraine; comprehensive provision of needs of citizens, enterprises, institutions and organizations of all forms of ownership in access to reliable and impartial information; ensuring free circulation of information, except for cases provided by law; development and protection of national information infrastructure; preservation and increase of spiritual, cultural and moral values of the Ukrainian people; ensuring a full development and functioning of the Ukrainian language in all areas of social life across Ukraine; free development, use and protection of national minority languages and promotion of the study of international communication languages; strengthening information ties with the Ukrainian diaspora, promotion of the preservation of its ethnocultural identity; development of media culture of society and socially responsible media environment; creation of an effective legal system to protect the individual, society and the state from destructive propaganda influences; formation of a system and mechanisms

[19] Емельянов, В. П. Концептуальные аспекты исследования объекта преступления. Право и политика. 2002. № 10. С. 65–66.

[20] Доктрина інформаційної безпеки України. Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

of protection against negative external information and psychological influences considering norms of international law, specifically propaganda; development of information society, in particular its technological infrastructure; safe functioning and development of the national information space and its integration into the European and world information space; development of the system of strategic communications of Ukraine; effective interaction of public authorities and civil society institutions during the formation and implementation of state policy in the information field; ensuring the development of information and communication technologies and information resources of Ukraine; security of state secrets and other information which security requirements are established by law; formation of a positive image of Ukraine in the world, communication of timely, reliable and objective information on events in Ukraine to the international community; development of Ukrainian international broadcasting system and ensuring the availability of a foreign-language Ukrainian channel in cable networks and in satellite broadcasting outside Ukraine[21].

The indicated social relations are also included in the list of relations protected by current criminal legislation of Ukraine. Hence, the structure of information security includes: social relations ensuring exercise of the right to information and protection of information from illegal interference; social relations ensuring information resources security; social relations ensuring security in the use of information and communication technologies.

It should be emphasized that information security as an object of criminal law protection is of certain complexity. This is due to the fact that information technologies have entered into all areas of life of a person, society and the state. Information security, in turn, actively influences the state of political, economic, defense and other components of Ukraine's security. The state of other components of national security of the state depends on the level of its protection, allowing to talk about the information aspect of political, economic, environmental and other types of security.

As for criminal law theory, the above enables us to hypothesize that information security can be both the *main* and *additional* object of a crime. Information security as an additional object of a crime is available in a significant number of corpora deliciti, the responsibility for which is provided by the norms of the Special Part of the Criminal Code. They can be attributed to encroachments on information security with some conventionality. Thus, it seems necessary to specify the generic object of this group of crimes as social relations that provide information security.

The generic object of crime stipulated in Section XVI of the Criminal Code of Ukraine: *Criminal offenses related to the use of electronic computing machines (computers), systems and computer networks and telecommunication networks* is part of information relations that can be defined as information relations, means of ensuring which are electronic computing machines, systems, computer networks and telecommunication networks[22]. In other words, criminal offenses stipulated in this section encroach on a certain part of information relations: information relations related to the use of special technical means that are widely known and quite common today[23].

There is a problem with definition of the generic object of crimes in the field of the use of electronic computing machines, systems, computer networks and telecommunication networks: a problem of naming crimes encroaching on this object. The law defines these acts as "criminal offenses in the use of electronic computing machines, systems and computer networks and telecommunications networks". The term: *cyber crime* is increasingly used in literature. It seems that a fairly common understanding of computer

Anzahl von Tatbeständen vorhanden, deren Verantwortlichkeit die Bestimmungen des Besonderen Teils des Strafgesetzbuches vorsehen. Man kann sie mit einiger Formalität auf Eingriffe in die Informationssicherheit zurückführen. Daher erscheint es notwendig, den allgemeinen Gegenstand dieser Gruppe von Straftaten als Öffentlichkeitsbeziehungen zu konkretisieren, die Informationssicherheit bieten.

Der allgemeine Gegenstand der in Abschnitt XVI des Strafgesetzbuches der Ukraine «Straftaten bei der Benutzung von Computertechniken (Computern), Systemen und Computernetzen und Telekommunikationsnetzen» vorgesehenen Straftaten ist ein Teil der Informationsbeziehungen, die als Informationsbeziehungen definiert werden können, deren Versorgungsmittel elektronische Computer, Systeme, Computernetze und Telekommunikationsnetze sind. Anders gesagt verüben die in diesem Abschnitt vorgesehenen Straftaten einen Anschlag auf einen bestimmten Teil der Informationsbeziehungen – Informationsbeziehungen im Zusammenhang mit dem Einsatz spezieller technischer Mittel, die heute allgemein bekannt und recht verbreitet sind.

Der Artikel kommt zum Schluss, dass Straftaten gegen die Sicherheit von Informations- und Telekommunikationstechnologien sind sozial gefährliche Handlungen, die strafrechtlich verboten sind und auf Öffentlichkeitsbeziehungen einen Anschlag verüben, die die Sicherheit von Verfahren und Methoden der Suche, Sammlung, Speicherung, Verarbeitung, Verschaffung, Verbreitung von Informationen durch Computertechniken und Informations- und Telekommunikationsnetze gewährleisten.

Schlüsselwörter: strafrechtlichen Verantwortlichkeit, Straftat, Gegenstand einer Straftat, Informations- und Kommunikationstechnologien, Systeme und Computernetze und Telekommunikationsnetze.

[21] Доктрина інформаційної безпеки України. Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

[22] Кримінальний кодекс України. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=комп#w1_11

[23] Буга Я. **Загальна характеристика комп'ютерних злочинів**. URL: http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iii-konferentsii/78-buga-ya

offenses as those committed with the use of computer technology or regarding computer information is improper, such that it does not reflect their nature, specific character and distinguish from other crimes where a computer is only a tool, means or subject. When analyzing this issue, we should first distinguish between the terms computer crimes and crimes related to computer technology.

The criminal law lists four types of such special technical means:

- automated electronic computing machines (computers, AECM), including personal: a set of electronic technical means created on the basis of microprocessors and intended for automatic processing of information while solving computational and information tasks[24]. In addition, particular provisions of the current Ukrainian legislation include in this group display devices: electronic means for displaying any graphic or alphanumeric information (on the basis of a cathode-ray tube, liquid-crystal, plasma, projection, organic LED monitors and other latest developments in the field of information technologies) [25];

- automated system (in information technology) is a system implementing information technology for performing set functions with the help of staff and a set of automation tools[26]. When synthesizing judicial practice on this type of crimes, automated system is also viewed as an organizational and technical system consisting of means of automation of a particular type (or several types) of people/staff activities performing this activity. In particular, such systems should be considered a set of ECMs, means of communication and programs through which document circulation is performed, databases are created, updated and used, information is accumulated and processed. Since processing of certain data is possible as a result of single computer operation, automated system is a single computer with its software[27].

- computer network is a set of geographically distributed data processing systems, means and (or) systems of communication and data transmission, which provides users with remote access to its resources and collaborative use of these resources[28]. In legislative acts, the term: *The Internet* is used. It is a global electronic communications network intended for data transmission and comprising of physically and logically interconnected individual electronic communications networks, which interaction is based on the use of a single address space and the use of the Internet protocols determined by international standards[29];

- telecommunication network is a set of technical means of telecommunications and structures intended for routing, switching, transmission and/or reception of signs, signals, written text, images and sounds or messages of any kind by radio, wired, optical or other electromagnetic systems between the terminal equipment [30](the Law will

---

[24] Узагальнення судової практики розгляду Бориспільським міськрайонним судом кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI Особливої частини Кримінального кодексу України) за 2012-2014 роки. URL: https://court.gov.ua/userfiles/file/bor111/eom.pdf

[25] Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. Наказ Міністерства соціальної політики України від 14. 02. 2018, № 207. URL: https://zakon.rada.gov.ua/laws/show/z0508-18#Text

[26] ДСТУ 2938-94. Системи оброблення інформації. Основні положення. Терміни та визначення. 01.01.96. С. 3

[27] Узагальнення судової практики розгляду Бориспільським міськрайонним судом кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI Особливої частини Кримінального кодексу України) за 2012-2014 роки. URL: https://court.gov.ua/userfiles/file/bor111/eom.pdf

[28] ДСТУ 2938-94. Системи оброблення інформації. Основні положення. Терміни та визначення. 01.01.96. С. 7.

[29] Про електронні комунікації. Закон України від 01.01.2022. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

[30] Про телекомунікації. Закон України від 18.11.2003. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text

expire on 01.01.2022). In the new Law: *On Electronic Communications* (will enter into force on 01.01.2022) the electronic communications network is interpreted as a set of technical means of electronic communications and structures aimed at provision of electronic communications services. In turn, electronic communication (telecommunications) is transmission and/or reception of information, regardless of its type or kind in the form of electromagnetic signals using technical means of electronic communications[31].

Depending on these means, information relations (the generic object of investigated crimes) can be divided into four types:

1) information relations, means of ensuring which are computers;
2) information relations, means of ensuring which are computer systems;
3) information relations, means of ensuring which are computer networks;
4) information relations, means of ensuring which are telecommunication networks;

The first type of these information relations is the simplest form of using computer technology for working with information. The subjects of such relations use computer technology to perform relatively simple operations, such as preparing documents, performing engineering calculations, organizing and working with databases. Let's note that the electronic computing machine is understood not only as computers in their "classic", we can say usual form, that is *system unit – monitor – keyboard – printer*, but also as other equipment that comprises of a processor and can perform calculations without human interference.

The use of computer systems relates to more sophisticated information relations. Automated systems are used to perform a wide range of tasks: enterprise management, technological preparation of production, control and testing of industrial products, management of vital services of an enterprise, etc.

The third type of information relations that form the studied generic object refers to the use of computer networks, there are two types: local, uniting computers within one organization, and global, ensuring communication between various organizations, legal entities and persons. The most famous and widespread global computer network is the Internet which is used predominately for such types of information handling: e-mail; file transfer; remote access: the ability to connect to a remote computer and work with it in on-line mode.

Information relations, means of ensuring which are telecommunication networks, consist in provision and receipt of telecommunication services, i.e. in the use of telecommunication networks for transmission or reception of information. In relation to the definition of the content of these social relations, the question of their separation from information relations is of a certain interest, means of ensuring which are computer networks.

Analysis of current legislation in the field of telecommunications suggests that existence of the term: *telecommunications network* along with the other: *computer network* actually leads to understanding of telecommunications network as all telecommunication networks, except for computer (networks of city, long-distance and international telephone communication, mobile communication, cable radio broadcasting, terrestrial TV and radio broadcasting, etc.). Thus, information relations, means of ensuring which are telecommunication networks, should be understood as social relations in the field of use of telecommunication networks excluding computer networks[32].

Therefore, the generic object of these crimes: information security, the direct: a proper functioning of electronic computing machines (computers), automated systems, computer networks, computer information and telecommunication networks.

The subject of crimes:

---

[31] Про електронні комунікації. Закон України від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

[32] Про Національну програму інформатизації. Закон України. Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181.

1) electronic computing machines (computer);
2) automated systems (AS);
3) computer networks (ECM network);
4) telecommunication networks;
5) information transmitted through telecommunication networks is any information provided in the form of signals, signs, sounds, images or in other way (telephone messages, radio and television broadcasts, etc.), including by computer if it is transmitted over telecommunications network.
6) computer information. It is textual, digital, graphic or other information (data, information) about persons, objects, events, phenomena that exists in electronic format and is kept in an ECM, AS or computer network, and also stored in corresponding electronic media which include floppy disks (diskettes), hard disks (HDD), cassette tapes (streamers), drum memories, magnetic cards, etc. Media information can be used, processed or modified by ECMs (computers)[33].

Opinions on the range of crime subjects stipulated by Section XVI of the Criminal Code of Ukraine vary significantly. At the same time, it should be stressed that a certain group of experts does not single out computer information as the crime subject under Article 361 of the Criminal Code, which is clearly laid down in this norm as an object subjected to distortion or destruction by the offender[34]. We fully agree with findings of scholars[35] who believe that non-recognition of computer information as a subject of crime is due to the materialistic approach of the classical theory of criminal law to defining the crime subject as a certain material having an obligatory physical feature. Scholars who see this category as the crime subject under Articles 361-363 of the Criminal Code view computer information itself differently. The former consider it as a material object of the objective world and accordingly automatically recognized it as the crime subject specified by articles of Section XVI of the Criminal Code of Ukraine. Thus, D. S. Azarov notes that the only possible crime subject is computer information which he attributes to "material formations"[36], objects of the material world. While agreeing with the doctrinal concept of such a definition regarding the need to define computer information as the crime subject in general, we cannot agree with the scientist's assumptions that it is the only subject of indicated crimes. The second group of experts identify computer information with a physical medium in which it can be stored. For example, V. M. Karchevskyi stresses that a physical feature of computer information as the crime subject is its medium, the one that is usually understood as an object, thing which properties are used to transmit, store and process information[37]. That is, physical feature of computer information, according to his findings, is the existence of its medium which is included in the system of social relations. However, we believe that computer information is a digital reflection of the material world and may exist in some way individually from its media. At the same time, computer information cannot be equated with its medium, since firstly, it can be recorded on different types of media and not always the ownership of such media coincides with the ownership of computer

[33] Кримінальне право України: Особлива частина : підручник / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін. ; за ред. В. В. Сташиса, В. Я. Тація. 4-те вид., переробл. і допов. Х. : Право, 2010. 608 с. URL: http://library.nlu.edu.ua/POLN_TEXT/KNIGI-2010/UgolovPravoOsob.pdf

[34] E.g., Див., наприклад: Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника. М. І. Хавронюка. К., 2001. С. 902; Науково-практичний коментар до Кримінального кодексу України / Під загальною редакцією Потебенька М.О., Гончаренка В.Г. К., 2001., у 2-х ч. Особлива частина. С. 721.

[35] Мазуренко О., Розенфельд Н. Комп›ютерна інформація як предмет злочинів, передбачених Розділом XVI КК України. ПРАВО УКРАЇНИ, 2004, № 6. С. 80-83. ISSN 0132-1331. URL: https://www.savinova.info/sites/default/files/all/articles/2004_01s.pdf

[36] Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп›ютерної інформації. Автореф. дис. ... канд. юрид. наук. Київ, 2003. С. 9.

[37] Карчевський В. М. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп›ютерних мереж: Монографія / МВС України, Луг. акад. внутр. справ ім. 10-річчя незалежності України; Наук. ред. Л.М.Кривоченко. Луганськ, 2002. С. 56.

information itself; and secondly, computer information can be transmitted through communication channels where socially dangerous encroachment on it (e.g., theft, destruction)[38] may be implemented. The third group of researchers defines computer information as one of alternative subjects of a crime[39]. We accept these ideas because computer information is directly specified in the criminal law as a subject influenced by a person who commits analyzed crimes.

The following commentary will also be relevant: if a material object is understood as any specific material phenomenon perceived by senses[40] (so to speak, a tangible object of the material world)[41], then a virtual object is an object "conditional, physically absent", but which can acquire external representation "using available special methods"[42]. In other words, we understand a virtual object as an object that has no external representation but can acquire it through the use of special tools and methods. Therefore, computer information is a virtual object, since it has no external representation in itself but can acquire it through the use of special tools and methods: computer systems providing it with a form suitable for perception and processing.

Such terms as *digital information* and *data* are used in legislation of foreign countries. In turn, *data* is a wider concept than *digital information*. The Ukrainian legislator distinguishes *data* as a separate concept (viewing them as information presented in a form suitable for its processing by electronic means)[43]. It is believed to be necessary to replace the *computer information* concept with the concept: *electronic information*. The term: *electronic* is not new to domestic law. The Law of Ukraine: *On Electronic Documents and Electronic Documents Circulation* (Article 5) provides the following definition for this category: electronic document is a document in which information is recorded as electronic data, including mandatory particulars of a document[44].

An electronic document can be created, sent, stored and converted electronically into a visual form. The visual form of electronic document submission is display of data it contains, by electronic means or on paper, in a form suitable for human content. Based on the text of the Regulations on operation of individual subsystems (modules) of the Unified Judicial Information and Telecommunication System, an electronic document is a document in which information is recorded as electronic data, containing mandatory particulars of a document, which legal status is certified by a qualified electronic signature of an author and "electronic copy of a paper document" is a document in electronic format containing a visual representation of a paper document obtained by scanning (photographing) a paper document. Conformity to the original and legal status of the electronic

---

[38] Мазуренко О., Розенфельд Н. Комп›ютерна інформація як предмет злочинів, передбачених Розділом XVI КК України. ПРАВО УКРАЇНИ, 2004, № 6. С. 80-83. ISSN 0132-1331. URL: https://www.savinova.info/sites/default/files/all/articles/2004_01s.pdf

[39] Кримінальне право України: Особлива частина: Підруч. для студ. вищ. навч. закл. освіти / М. І. Бажанов, В. Я. Тацій, В. В. Сташис, І. О. Зінченко та ін. / За ред. професорів М. І. Бажанова, В. В. Сташиса, В. Я.Тація. К.: Юрінком Інтер. Х.: Право, 2001. С. 363.

[40] Академічний тлумачний словник української мови в 11 томах. URL: http://sum.in.ua/s/predmet

[41] Yuriy Khodyko The concept of things in the context of determining the object of the property relationship. URL:ttps://www.researchgate.net/publication/321892948_The_concept_of_things_in_the_context_of_determining_the_object_of_the_property_relationship

[42] ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Видання офіційне. Київ: Держстандарт України, 1994.

[43] [Про електронні документи та електронний документообіг. Закон України. Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

[44] Про електронні документи та електронний документообіг. Закон України. Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

copy of a paper document shall be certified by a qualified electronic signature of a person who created such a copy[45].

The concept of *electronic signature* is enshrined in the Law of Ukraine: *On Electronic Trust Services* as electronic data that are added by the signatory to other electronic data or logically linked to them and used by him as a signature[46].

**Conclusions.** To conclude, crimes against the security of information and telecommunication technologies are prohibited by criminal law socially dangerous acts encroaching on social relations that ensure the security of processes and methods of search, collection, storage, processing, provision, dissemination of information by means of electronic computing machines and information telecommunication networks.

## References

Akademichnyy tlumachnyy slovnyk ukrayinskoyi movy v 11 tomakh [Academic Explanatory Dictionary of the Ukrainian Language in 11 volumes]. URL: http://sum.in.ua/s/predmet. [in Ukrainian].

Avtomatyzovani systemy. Terminy ta vyznachennya. DSTU 2226-93 [ДСТУ 2226-93. Automated systems. Terms and definitions]. Vydannya ofitsiyne. Kyyiv: Derzhstandart Ukrayiny, 1994. [in Ukrainian].

Azarov, D. S. 2003. Kryminalna vidpovidalnist za zlochyny u sferi komp'yuternoyi informatsiyi [Criminal liability for crimes in the field of computer information]. Avtoref. dys. ... kand. yuryd. nauk. Kyyiv, 2003. [in Ukrainian].

Buha, YA. 2021. Zahalna kharakterystyka kompyuternykh zlochyniv [General characteristic of computer crimes]. URL: http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iii-konferentsii/78-buga-ya [in Ukrainian].

Doktryna informatsiynoyi bezpeky Ukrayiny [Doctrine of Information Security of Ukraine]. Ukaz Prezydenta Ukrayiny vid 25 lyutoho 2017 roku № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 [in Ukrainian].

Emelyanov, V. P. 2002. Kontseptualnye aspekty yssledovanyya obekta prestuplenyya [Conceptual aspects of crime object study]. Pravo y polytyka. № 10. S. 65–66. [in Russian].

Karchevskyy, V. M. 2002. Kryminalna vidpovidalnist za nezakonne vtruchannya v robotu elektronno-obchyslyuvalnykh mashyn, system ta komp'yuternykh merezh [Criminal liability for illegal interference in the work of electronic computing machines, systems and computer networks]: Monohrafiya / MVS Ukrayiny, Luh. akad. vnutr. sprav im. 10-richchya nezalezhnosti Ukrayiny; Nauk. red. L. M. Kryvochenko. Luhansk [in Ukrainian].

Kibershpyhuny z Kytayu ta Rosiyi atakuyut kompaniyi SSHA – dopovid [Cyber spies from China and Russia are attacking US companies]. URL: https://news.obozrevatel.com/ukr/abroad/60549-kibershpiguni-z-kitayu-ta-rosii-atakuyut-kompanii-ssha-dopovid.htm [in Ukrainian].

Klymanska, L. D. 2005 Komunikatyvni tekhnolohiyi modelyuvannya politychnoho prostoru v demokratychnomu suspilstvi. URL: www.democracy.kiev.ua/publications/collections/conference_2005. [in Ukrainian].

Kochubey, L. Osoblyvosti suchasnykh informatsiyno-komunikatyvnykh tekhnolohiy v Ukrayini. Naukovi zapysky IPiEND im. I.F. Kurasa NAN Ukrayiny. Vypusk 3(89). S. 44-70. [in Ukrainian].

Kryminalne pravo Ukrayiny: Osoblyva chastyna [Criminal law of Ukraine: Special Part] : pidruchnyk / YU. V. Baulin, V. I. Borysov, V. I. Tyutyuhin ta in. ; za red. V. V. Stashysa, V. YA. Tatsiya. 4-te vyd., pererobl. i dopov. Kh.: Pravo, 2010. 608 s. URL: http://library.nlu.edu.ua/POLN_TEXT/KNIGI-2010/UgolovPravoOsob.pdf [in Ukrainian].

[45] Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи. Рішення Вищої ради правосуддя від 17 серпня 2021 року № 1845/0/15-21.

[46] Про електронні довірчі послуги. Закон України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.400. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534

Kryminalne pravo Ukrayiny: Osoblyva chastyna [Criminal law of Ukraine: Special Part] : Pidruch. dlya stud. vyshch. navch. zakl. osvity / M.I. Bazhanov, V.YA.T atsiy, V.V. Stashys, I.O. Zinchenko ta in. / Za red. profesoriv M.I.Bazhanova, V.V.Stashysa, V.YA.Tatsiya. K.: Yurinkom Inter. Kh.: Pravo, 2001 [in Ukrainian].

Kryminalnyy kodeks Ukrayiny [Criminal Code of Ukraine]. Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 2001, № 25-26, st.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=komp#w1_11 [in Ukrainian].

Materyaly dlya peresmotra nasheho uholovnoho zakonodatelstva [Materials for review of our criminal legislation]. Sbornyk dopolnytelnykh uzakonenyy k frantsuzskomu y hermanskomu uholovnym ulozhenyyam. T. 7: Vyp. 1-2 / Sost.: H. H. Savych; Pod red.: N. S. Tahantseva. S.-Pb. Typ. Pravyt. Senata, 1883. 786 s. [in Russian].

Mazurenko, O. & Rozenfeld, N. 2004 Komp'yuterna informatsiya yak predmet zlochyniv, peredbachenykh Rozdilom XVI KK Ukrayiny [Computer information as the crime subject under Section XVI of the Criminal Code of Ukraine]. PRAVO UKRAYINY, 2004, № 6. S. 80-83. ISSN 0132-1331. URL: https://www.savinova.info/sites/default/files/all/articles/2004_01s.pdf [in Ukrainian].

Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko 2020 Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206-220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). https://doi.org/10.1007/978-3-030-66717-7 [in English].

Naukovo-praktychnyy komentar do Kryminalnoho kodeksu Ukrayiny [Scientific-practical commentary of the Criminal Code of Ukraine] / Pid zahalnoyu redaktsiyeyu Potebenka M.O., Honcharenka V.H. K., 2001., u 2-kh ch. Osoblyva chastyna [in Ukrainian].

Naukovo-praktychnyy komentar Kryminalnoho kodeksu Ukrayiny [Scientific-practical commentary of the Criminal Code of Ukraine]/ Za red. M.I. Melnyka, M.I. Khavronyuka. K., 2001. [in Ukrainian].

Navchalni materialy z informatyky. Informatsiya i svit. Informatsiyni y komunikatsiyni tekhnolohiyi. URL: https://www.ua5.org/svit/281-nformacjjn-jj-komunkacjjn-tekhnolog.htm [in Ukrainian].

Ofitsiynyy sayt Akademiyi elektronnoho upravlinnya Estoniyi [Official website of the Estonian e-Governance Academy]. URL: https://ncsi.ega.ee/country/ua/ [in English].

Polozhennya pro poryadok funktsionuvannya okremykh pidsystem (moduliv) Yedynoyi sudovoyi informatsiyno-telekomunikatsiynoyi systemy [Regulations on Single judicial information and telecommunication system and/or by the provisions determining procedure for functioning of its separate subsystems (modules)]. Rishennya Vyshchoyi rady pravosuddya vid 17 serpnya 2021 roku № 1845/0/15-21 [in Ukrainian].

Poznyshev, S. V. 1912 Osnovnye nachala nauky uholovnoho prava [Fundamentals of criminal law science. The general part of criminal law]. Obshchaya chast uholovnoho prava. M. [in Russian].

Pro elektronni dovirchi posluhy [On Electronic Trust Services]. Zakon Ukrayiny. Vidomosti Verkhovnoyi Rady (VVR), 2017, № 45, st.400. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534 [in Ukrainian].

Pro elektronni dokumenty ta elektronnyy dokumentoobih [On Electronic Documents and Electronic Documents Circulation]. Zakon Ukrayiny. Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 2003, № 36, st.275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

Pro elektronni komunikatsiyi [On Electronic Communications]. Zakon Ukrayiny vid 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text [in Ukrainian].

Pro Natsionalnu prohramu informatyzatsiyi. Zakon Ukrayiny [About the National Informatization Program]. Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 1998, № 27-28, st.181. [in Ukrainian].

Pro telekomunikatsiyi [On telecommunications]. Zakon Ukrayiny vid 18.11.2003. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text [in Ukrainian].

Shvachych, H. H. & Tolstoy, V. V. & Petrechuk, L. M. & Ivashchenko, YU. S. & Hulyayeva, O. A. & Sobolenko, O. V. 2017. Suchasni informatsiyno-komunikatsiyni tekhnolohiyi [Modern information and communication technologies]: Navchalnyy posibnyk. Dnipro: NMetAU. 230 s.

Spasovych, V. D. 1863 Uchebnyk uholovnoho prava [Criminal law textbook]. Chast Obshchaya. S.-Pb. [in Russian].

Spitsyna, H. O., Filipenko, N. Ye. 2019. Terorystychna diyalnist: kryminalno-pravova polityka protydiyi [Official website of the Estonian e-Governance Academy] // Kryminalno-pravovi ta kryminolohichni zasoby protydiyi zlochynam proty hromadskoyi bezpeky ta publichnoho poryadku : zb. tez dop. mizhnar. nauk.-prakt. konf. do 25-richchya KHNUVS (18 kvit. 2019 r., m. Kharkiv) / MVS Ukrayiny, Kharkiv. nats. un-t vnutr. sprav ; Kryminol. asots. Ukrayiny. Kharkiv : KHNUVS. S. 188-191. [in Ukrainian].

Stratehiya natsionalnoyi bezpeky Ukrayiny [National Security Strategy of Ukraine.]. Ukaz Prezydenta Ukrayiny №121/2021. URL: https://www.president.gov.ua/documents/3922020-35037 [in Ukrainian].

Stratehiya voyennoyi bezpeky Ukrayiny [Strategy of Military Security of Ukraine.]. Ukaz Prezydenta Ukrayiny № 392/2020. URL: https://www.president.gov.ua/documents/1212021-37661 [in Ukrainian].

Systemy obroblennya informatsiyi. Osnovni polozhennya. Terminy ta vyznachennya. DSTU 2938-94. 01.01.1996. [ДСТУ 2938-94. Information processing systems. Main provisions.] [in Ukrainian].

Tahantsev, M. S. 2004. Yurydychna entsyklopediya [Legal Encyclopedia] : u 6 t. / red. kol. YU. S. Shemshuchenko (vidp. red.) ta in.. K. : Ukrayinska entsyklopediya im. M. P. Bazhana. T. 6 : T-YA. S. 8. ISBN 966-7492-06-0. [in Ukrainian].

Tatsyy, V.Ya. 2013. Obyekt zlochynu [The crime object]. Visnyk Asotsiatsiyi kryminalnoho prava Ukrayiny. № 1(1). S. 126-143. [in Ukrainian].

Uzahalnennya sudovoyi praktyky roz·hlyadu Boryspilskym miskrayonnym sudom kryminalnykh provadzhen pro zlochyny u sferi vykorystannya elektronno-obchyslyuvalnykh mashyn (kompyuteriv), system ta kompyuternykh merezh i merezh elektrozvyazku (rozdil XVI Osoblyvoyi chastyny Kryminalnoho kodeksu Ukrayiny) za 2012-2014 roky [Overview of judicial practice of criminal proceedings consideration on crimes in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks by the Boryspil City District Court]. URL: https://court.gov.ua/userfiles/file/bor111/eom.pdf [in Ukrainian].

Vymohy shchodo bezpeky ta zakhystu zdorovya pratsivnykiv pid chas roboty z ekrannymy prystroyamy [Safety and health requirements for workers when working with display devices]. Nakaz Ministerstva sotsialnoyi polityky Ukrayiny vid 14.02.2018 № 207. URL: https://zakon.rada.gov.ua/laws/show/z0508-18#Text [in Ukrainian].

Yuriy Khodyko, 2021. The concept of things in the context of determining the object of the property relationship. URL: https://www.researchgate.net/publication/321892948_The_concept_of_things_in_the_context_of_determining_the_object_of_the_property_relationship [in English].

Yurydychna vidpovidalnist za pravoporushennya v informatsiyniy sferi ta osnovy informatsiynoyi deliktolohiyi [Legal liability for offenses in the field of information and the basics of information delictology] : monohrafiya / I. V. Aristova, O. A.Baranov, O. P. Dzoban ta in.; za zah. red. prof. K. I. Byelyakova. Kyiv: KVITS, 2019. 344 s. [in Ukrainian].

Received by Editorial Board: 16.09.2021

**Suggested Citation:**

Nechyporuk, M., Kliuiev, O., Filipenko, N., Pavlikov, V., Ivanović A. (2021). Criminal Liability for Offenses in the Field of Information and Communication Technologies Use (Review Article). Archives of Criminology and Forensic Sciences. 2(4). 20-34 DOI: https://doi.org/10.32353/acfs.4.2021.01