КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

UDC 343.532:004.056
DOI https://doi.org/10.32782/2521-6643-2025-1-69.13

Haborets O. A., PhD, Associate Professor, Associate Professor of the Department of Operational and Investigative Activities and Information Security, Faculty No. 3
Donetsk State University of Internal Affairs
ORCID: 0000-0001-7791-6795

Rybalchenko L. V., Ph.D, Associate Professor at the Department of Cyber Security and Information Technologies
University of Customs and Finance
ORCID: 0000-0003-0413-8296

TYPES, CHARACTERISTICS AND EXECUTION METHODS OF CYBER FRAUD

The article is dedicated to the study of cyber fraud characteristics and classification, methods of its execution. It examines key factors contributing to the rise of cybercrime, including the rapid digitalization of society, economic destabilization, the psycho-emotional vulnerability of the population, and the advancement of social engineering technologies.

In today's world, where technology has become an integral part of our daily lives, cyber fraud has become one of the biggest threats. With the growing use of the internet and mobile devices, cybercriminals are finding new ways to defraud people and organisations, causing them significant financial and reputational damage.

The process of cyber fraud often begins with fraudsters collecting information about their potential victims. This can be personal data, financial details, or even online behavioural history. Using this data, criminals create convincing fake platforms or messages.

The purpose of the article is to examine the current state of cyber fraud in the country and offer advice on protecting personal data and finances.

The main types of fraud are analyzed, including phishing, manipulative schemes in e-commerce, cryptocurrency fraud, and cyberbullying. Special attention is given to the specifics of fraudulent schemes in wartime conditions, including fake charitable initiatives and fraud involving disinformation.

Cyber fraud is a real threat that is growing every year, and protecting yourself from it requires care and caution. It is important not only to choose reliable online platforms, but also to have a strategic approach to online security. It is necessary to be vigilant and use modern protection methods to minimise risks and avoid them. Combating cyber fraud is one of the most important tasks for modern organisations and Internet users.

The study proposes approaches to combating cybercrime, which include improving digital security mechanisms, enhancing public cyber literacy, and implementing effective measures for detecting and counteracting fraudulent schemes.

Key words: *cybercrime, fraud, phishing, social engineering, cryptocurrency fraud, digital security, disinformation.*

Габорець О. А., Рибальченко Л. В. Види, характеристики та способи вчинення кібершахрайства

Стаття присвячена дослідженню шахрайств у кіберпросторі, їх особливостей, класифікації та методів здійснення. Розглянуто ключові фактори, що сприяють зростанню кіберзлочинності, зокрема, інтенсивну цифровізацію суспільства, економічну дестабілізацію, психоемоційну вразливість населення та розвиток технологій соціальної інженерії.

У сучасному світі, де технології стали невід'ємною частиною нашого повсякденного життя, кібершахрайство стало однією з найбільших загроз. Зі зростанням використання інтернету і мобільних пристроїв, кіберзлочинці знаходять нові способи обману людей та організацій, завдаючи їм значних фінансових та репутаційних збитків.

Процес кібершахрайства часто починається з того, що шахраї збирають інформацію про своїх потенційних жертв. Це можуть бути персональні дані, фінансові реквізити або навіть історія онлайн-поведінки. Використовуючи ці дані, злочинці створюють переконливі фальшиві платформи чи повідомлення.

Метою статті є дослідження сучасного стану кібершахрайства в країні та запропоновано поради щодо захисту особистих даних та фінансів.

Проаналізовано основні види шахрайства, включаючи фішинг, маніпулятивні схеми у сфері електронної комерції, криптовалютні шахрайства та кібербулінг.

Окрему увагу приділено специфіці шахрайських схем в умовах воєнного стану, включаючи фіктивні благодійні ініціативи та шахрайство з використанням дезінформації.

Кібершахрайство – це реальна загроза, яка зростає з кожним роком, і захист від нього вимагає уважності та обережності. Важливо не тільки обирати надійні онлайн-платформи, а й мати стратегічний підхід до безпеки в інтернеті. Необхідно бути пильними і використовувати сучасні методи захисту для мінімізації ризиків та їх уникнення. Протидія кібершахрайству є однією з найважливіших задач для сучасних організацій та користувачів Інтернету.

Запропоновано підходи до боротьби з кіберзлочинністю, що включають вдосконалення механізмів цифрової безпеки, підвищення кіберграмотності населення та впровадження ефективних заходів з виявлення та протидії шахрайським схемам.

Ключові слова: *кіберзлочинність, шахрайство, фішинг, соціальна інженерія, криптовалютні шахрайства, цифрова безпека, дезінформація.*

Problem Raising. Execution of cyber fraud has become particularly relevant in the context of global challenges such as the COVID-19 pandemic and the war waged by Russia against Ukraine. Criminal activities in cyberspace are driven by the unique nature of the digital environment and its ability to adapt to socio-economic changes, creating new opportunities for manipulation and illicit financial gain.

One of the key factors contributing to the spread of cybercrime is the intensive digitalization of society. The increased use of the Internet, prompted by quarantine restrictions, martial law, and the transition of a significant part of socio-economic activities to digital formats, has substantially expanded the volume of online interactions among citizens. The widespread adoption of remote work, e-commerce, and digital communication platforms has acted as a catalyst for the development of fraudulent schemes aimed at exploiting users' trust and stealing their personal data.

Another crucial factor is the psycho-emotional vulnerability of the population, which has been exacerbated by both the pandemic and wartime conditions. Mass fears, anxiety, and a general sense of instability have become tools actively used by fraudsters for manipulative purposes. For instance, they create fraudulent charitable initiatives, offer pseudo-medical services or fake protective measures against the virus, enabling them to gain unlawful access to citizens' financial resources.

Economic destabilization also plays a significant role in the rise of cybercrime, as financial hardships have affected a considerable portion of the population. Cybercriminals exploit this context by offering fraudulent job vacancies, false promises of quick earnings, or fake "financial assistance" programs. These methods are particularly prevalent due to their ability to take advantage of individuals' financial needs during crises.

Disinformation serves as another powerful tool for cyber fraud. During armed conflicts and information warfare, the spread of fake news, chain messages, and other forms of misleading content has become a key method of gaining access to personal data and financial resources. Fraudsters use disinformation to create an atmosphere of distrust and chaos, making it more difficult to identify real threats.

A significant transformation in user behavior online has also contributed to the proliferation of cyber fraud. The mass shift to e-commerce, the growing popularity of online services, and increased social media engagement have substantially heightened the risks of falling victim to fraudulent websites. Cybercriminals create phishing websites that mimic legitimate platforms or use social engineering techniques to gain unauthorized access to users' confidential information.

Thus, cyber fraud is a multifaceted phenomenon influenced by social, psychological, and economic factors. Criminal activities in the digital space are characterized by a high degree of adaptability, the use of advanced information technologies, and the capacity to target a vast audience of potential victims. All of these aspects underscore the urgent need for the development of scientifically grounded approaches to detecting and combating cyber fraud, taking into account the specific methods used by cybercriminals and the scale of their impact on society.

Analysis of recent research and publications. The problems of frauds committed in cyberspace in Ukraine have been paid attention to by such national scholars as O. V. Byshevets, O. S. Belytskyi, T. S. Vaida, V. V. Vynnyk, V.M. Galunko, L.P. Hrynko, N.O. Dumanskyi, O.M. Dzhuzha, L.M. Ivashko, O.V. Klyuvak, T.V. Korshykova, O.I. Kryvenko, A.B. Mizerak, L.M. Prudka, D.V. Perepelytsia, T.V. Romanenko, Y.P. Rudenko, V.P. Sabadash, O.A. Samoilenko, I.V. Sabadash, N.V. Smetanina, I.A. Fedchak, I.M. Chekmariova, S.S. Cherniavskyi, S.V. Shapochka, O.M. Yurchenko and others. In their studies, they considered general aspects of crimes committed in cyberspace, in particular, Internet fraud in peacetime. The study of frauds committed on the Internet under martial law was carried out by such scholars as O. M. Bryskovska, M. O. Helemey, Y. V. Levkivska, M. E. Sobachenko and V. H. Teliychuk.

The purpose of the article. The purpose of the study is to systematise and analyse frauds in cyberspace, their types, features and methods of commission, and to identify the key factors contributing to their spread. Particular attention is paid to frauds that have arisen or intensified as a result of socio-economic crises, the COVID-19 pandemic and martial law in Ukraine. Based on the analysis of existing fraudulent schemes, the author proposes effective mechanisms for their prevention and counteraction, including legal, technological and educational measures.

Summary of the main material. Fraud is one of the most common types of criminal offences against property in many criminal law systems, including in Ukraine. Given the trend towards an increase in the number of cases of

property encroachments through fraudulent actions, combating these offences remains one of the key tasks of law enforcement agencies. The commission of such crimes not only threatens the property rights of individuals, but also harms the stability of the state's economic system, jeopardising its effective functioning.

According to Article 190 of the Criminal Code of Ukraine, fraud is defined as the misappropriation of another's property or the acquisition of rights to it by deception or breach of trust [1]. This criminal offence is characterised by a special focus, which may relate to both material assets and rights to such assets. An important feature of fraud is the presence of direct intent, which implies that the perpetrator is aware of the unlawfulness of his or her actions, and a mercenary motive aimed at obtaining an unlawful benefit.

The development of digital technologies and the widespread use of the Internet in Ukraine have created new conditions for committing fraud. Due to the accessibility of the Internet for citizens of different age groups, criminals have received new tools to implement their illegal intentions. The peculiarity of Internet fraud is the absence of direct contact between the offender and the victim, which not only facilitates concealment of the offender's identity but also encourages him to develop more complex and sophisticated schemes for seizing other people's property or financial resources.

Frauds committed in cyberspace include numerous types of crimes that use digital technologies to manipulate, deceive and illegally obtain benefits. According to the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" [3] (hereinafter – the Law), "cyberspace" is defined as an environment (virtual space) that provides opportunities for communication and implementation of social relations, formed through the functioning of interconnected communication systems and electronic communications using the Internet and/or other global data networks.

The main subcategory observed in this context is the non-delivery of orders placed through online resources. This phenomenon includes transactions for the purchase and sale of goods on digital trading platforms, placement of advertisements for the provision of certain services and receipt of advance partial or full payment for such services or goods. Such cases pose a significant threat to e-commerce and pose risks to the financial security of users, as unfair practices may be accompanied by intentional fraudulent schemes and breach of contractual obligations. The growth in the activity of such schemes is due to the large-scale transition of business entities to online platforms. This format allows optimising operating costs, in particular, eliminating the need to lease physical commercial premises, which, in turn, contributes to more affordable and competitive prices for goods and services, increasing their attractiveness to end users.

Among the most common methods of cybercrime, along with the failure to deliver goods or services, a special place is occupied by social engineering techniques used to manipulate the minds of users. One of the most dangerous manifestations of such techniques is phishing, which allows attackers to access victims' confidential information through deception. This type of fraud has become particularly popular due to the growing use of digital platforms and the lack of cyber literacy among the population.

Phishing is a type of fraud based on manipulative techniques that allow users to obtain personal data, such as passwords, bank card numbers, account logins, etc. Phishing attacks are based on misleading the user into voluntarily handing over their data to the attackers. Phishing can be implemented in various forms and targets both individuals and organisations.

The main types of phishing attacks:

1. Email Phishing.

Email phishing attacks are the most common type of cybercrime used for both mass and targeted attacks. The basic scheme involves sending fake emails on behalf of banks, government agencies, online services or social networks. Such emails may contain:

Fake links that lead to fake web pages that look like genuine banking sites or authorisation platforms;

Malicious attachments (.pdf,.docx,.xls files) that contain viruses, spyware or macros for data theft;

Phishing forms that mimic user account login pages, but send the entered data to the attackers.

The most dangerous attacks are Spear Phishing, which targets specific individuals (company executives, government officials, journalists, etc.). Such emails contain personalised information, which increases their credibility and effectiveness.

2. Smishing.

Smishing is SMS and messenger phishing, where fraudsters use text messages to get the victim to perform certain actions. Attackers send messages on behalf of banks, delivery services, mobile operators, or even government agencies with a demand:

Click on a fraudulent link to confirm a transaction, update an account, or view an 'important message';

Provide confidential information in response to the message (e.g. a verification code for financial transactions);

Download a fake application that is actually malware.

Modern spear phishing attacks actively use fake messages about problems with bank accounts, blocked cards, or winnings in promotions. The victim, panicking, is more likely to act in favour of the attackers without checking the authenticity of the information.

3. Vishing.

Vishing is a method of fraud through telephone calls, during which attackers pretend to be representatives of banks, law enforcement agencies, tax authorities or technical support. The main scenarios of such attacks include:

Imitation of bank employees who inform the victim of "suspicious activity" on the account and could block the card, forcing the owner to hand over passwords or one-time access codes;

Fraudulent calls on behalf of law enforcement agencies, which scare the victim that their account is being "checked for financial crimes", demanding that they transfer funds to a 'safe account';

Tech support-related vishing, where attackers tell the user that a virus has been 'detected' on their device and offer to install 'security' software that is actually a Trojan.

Some vishing attacks are based on collecting public information about the victim (e.g. from social media), which allows fraudsters to be more convincing and use personalised details during the conversation.

4. Social media phishing

On social media, fraudsters create fake accounts or hack into the accounts of real people, using them to commit fraud. The main schemes include:

Sending personal messages asking for money (on behalf of a hacked friend or relative);

Fake sweepstakes and contests that require the victim to click on a link and enter bank card details to "claim the prize";

Fraudulent job offers, where criminals pretending to be HR managers promise easy money by demanding an advance payment or transfer of personal data.

Given the popularity of social media, this method of phishing is particularly dangerous, as people trust messages from friends more than emails or calls.

5. Web Phishing.

Phishing websites are created to imitate legitimate resources in order to collect personal data from users. They can look like:

Fake login pages (banks, postal services, online stores, social networks);

Fake payment systems that steal credit card data.

Phishing remains one of the most serious cyber threats nowadays, requiring comprehensive protection measures and continuous improvement of defensive tactics.

It is also worth paying attention to malware, which is often an integral tool for phishing attacks. Malware is one of the most common threats used to achieve various criminal goals, such as stealing confidential information, disrupting systems or blackmailing. Typically, PUPs are distributed via phishing links or attachments that masquerade as legitimate files or programs. When combined with personalised phishing messages created with the help of artificial intelligence, PUP becomes particularly dangerous as it can infiltrate the systems of even experienced users.

According to the statistics of the Prosecutor General's Office of Ukraine, in 2024, the number of criminal proceedings opened under Article 190 of the Criminal Code of Ukraine 'Fraud' was 64,978. Compared to 2022, this is 2.7 times more, but 21% less than in 2023 (82,609 cases). Almost every fourth case goes to court: in 2023 – 14838 cases, in 2024 – 15607 cases [6].

By the end of 2024, 62% of Ukrainians had become victims of cyber fraud, while at the beginning of 2024, there were about 21% of such cases. 30% of Ukrainians have not encountered such fraudsters but have heard of such cases, and only 8% have neither encountered nor heard of such cases. Since the beginning of 2025, almost 40% of Ukrainians have become the most aware and informed about cases of fraud and have a better understanding of how to protect their data from cybercriminals. The most common cases involve the purchase and sale of goods when the seller, having received money for the goods, does not provide certain services, i.e. failure to deliver online orders by pseudo-sellers. The second most common type is phishing, where social engineering and software tools are used to create malicious links for users to steal their personal data, accounts, etc. In third place are 'bank calls', when fraudsters pose as bank representatives and obtain the necessary information for abuse.

In 2025, cybercriminals have become even more inventive, using new methods of data theft and fake bank websites that ask you to click on a link and provide your card details. Phone fraudsters use AI-generated voices of relatives or bank employees to steal data. Scammers create fake, fake photos and extort money. Therefore, it is necessary to follow safety rules, protect yourself and your finances, take your time to trust strangers and always check the information.

Cyberbullying is a complex social phenomenon that has arisen as a result of the rapid development of information and communication technologies and the growing integration of digital platforms into everyday life. It is a form of aggressive behaviour that is implemented through the online environment with the aim of psychological pressure, humiliation or discrediting a person.

This form of aggression is manifested through the use of digital platforms to intimidate, humiliate, blackmail or discredit a person. The characteristic features of cyberbullying are its systematic nature, public nature and the possibility of anonymity of offenders, which creates additional challenges for detecting and preventing this phenomenon.

Its consequences can be profound and have a serious impact on the victim, including emotional exhaustion, social isolation and reduced self-esteem. Factors that contribute to the spread of cyberbullying include the growing availability of digital technologies, low awareness of cybersecurity basics, and the lack of effective legal mechanisms to combat such phenomena.

There are several key types of fraudulent schemes in the cryptocurrency sector. First, it is deception through social media, where attackers create fake accounts imitating famous people or companies to convince users to invest in fraudulent projects. Secondly, social engineering is widely used, when criminals manipulate the emotions of victims to force them to transfer access to their cryptocurrency wallets.

Manipulations with initial coin offerings (ICOs) are particularly noteworthy. Attackers create fictitious projects promising high profits but disappear as soon as the funds are raised. In addition, under the guise of crypto investment funds, fraudsters promise users a guaranteed profit, which is often part of pyramid schemes.

Cloud mining fraud also poses a serious threat when, under the pretext of providing cryptocurrency mining services through cloud platforms, criminals obtain users' funds without performing any real operations. All these schemes require special attention and improved cybersecurity methods to protect crypto assets.

In the context of military conflict, criminals actively exploit the vulnerabilities of society to implement specific fraudulent schemes that have become widespread due to the current circumstances. Such schemes include fictitious fundraising for the army, manipulation of reports of missing or captured persons, and distribution of fake evacuation notices requiring advance payment or "financial assistance".

These fraudulent activities are aimed at exploiting the emotional state of victims caused by fear, anxiety or a desire to help in a crisis. Criminals are actively adapting their methods to current realities, using social platforms, mobile applications and other digital communication tools to achieve their goals. Fraud is often based on social engineering techniques, such as creating trusting situations or influencing a sense of responsibility that forces citizens to transfer funds or personal data.

The key tools used by fraudsters are computers, mobile devices, bank accounts registered in the names of front men, and specialised software. In addition, online platforms are actively used to implement such schemes, allowing for the rapid dissemination of disinformation, fake websites and ads. The effectiveness of fraud is often reinforced by the high level of technological equipment of criminals, which allows them to adapt their actions to changing conditions and remain invisible to law enforcement agencies.

Thus, fraud in wartime acquires unique features due to the specifics of the socio-economic situation and the scale of digital technologies. This underscores the need to improve the mechanisms for protecting citizens, in particular by increasing the level of digital literacy, introducing stricter regulations and developing effective monitoring and counteraction tools [4].

Conclusions. Summarising the above, we can conclude that effective counteraction to fraud in cyberspace, especially in wartime, requires a systematic approach. The key methods of combating fraud are to increase the digital literacy of citizens, introduce modern technologies for monitoring and detecting fraudulent schemes, and improve legal mechanisms aimed at regulating online activities. Special attention should be paid to developing information campaigns to raise public awareness of the threats posed by cybercrime and the need for responsible behaviour in the digital environment. Only through the integrated efforts of the state, civil society and technological platforms can effective protection against threats in cyberspace be ensured.

Thus, countering cyber fraud in Ukraine is a difficult but important task that requires efforts from the state, business and society. Raising awareness, improving legislation and investing in technology can significantly reduce risks and protect citizens from fraudulent activity. Only by working together can we create a safe digital environment for all.

Further research in cybersecurity should focus not only on identifying fraudulent schemes but also on developing innovative mechanisms for their prevention and neutralisation. An interdisciplinary approach that combines legal, technological, psychological and economic aspects is important, as only comprehensive measures can ensure effective counteraction to modern threats in cyberspace.

Bibliography:

1. Кримінальний процесуальний кодексу України від 13 квітня 2012 року № 4651-VI. Дата оновлення: 21 листопада 2024 року. Вебпортал Верховної Ради України. Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

2. Організація розкриття шахрайств, учинених в кіберпросторі / Шевчишен А. В., Романов М. Ю., Волобоєв А. О., Лунгол О. М., Габорець О. А., Головкін С. В.; за заг. ред С. С. Вітвіцького. Київ : Алерта, 2023. – 200 с.

3. Про основні засади забезпечення кібербезпеки України : закон України від 17.08.2022 № 2163-VIII. Вебпортал Верховної Ради України. Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Haborets O. The impact of cyber threats on community and citizen security: analysis and perspectives on resolution. Взаємодія державних органів та громадськості у сфері протидії кримінальним правопорушенням

у центральних регіонах України : матеріали круглого столу (17 квітня 2024 року, м. Кропивницький). Кропивницький : ДонДУВС, 2024. С. 36–37. Режим доступу: URL: https://surl.li/nzkzfl

5. Rybalchenko L. Ensuring economic security of enterprises taking into account the peculiarities of information security / L. Rybalchenko, A. Kosychenko, I. Klinytskyi // Philosophy, Economics and Law Review. – 2022. – Volume 2, no. 1. – P. 96-107. https://doi.org/10.31733/2786-491X-2022-1-96-107

6. Опендатабот. Шахрайство. Режим доступу: URL: https://opendatabot.ua/analytics/fraud-2024-12

References:

1. Criminal Procedural Code of Ukraine (2012, April 13). (№ 4651-VI). Updated on November 21, 2024. Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

2. Shevchyshen, A. V., Romanov, M. Yu., Voloboyev, A. O., Lungol, O. M., Haborets, O. A., & Golovkin, S. V. (2023). Orhanizatsiia rozkryttia shakhraistv, uchinenykh v kiberprostori [Organization of investigating fraud committed in cyberspace] (S. S. Vitvitskyi, Ed.). Kyiv: Alerta.

3. On the Basic Principles of Ensuring Cybersecurity of Ukraine (2022, August 17). (№ 2163-VIII). Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Haborets, O. A. (2024). The impact of cyber threats on community and citizen security: Analysis and perspectives on resolution. In Interaction between state bodies and the public in counteracting criminal offenses in the central regions of Ukraine: Roundtable materials (April 17, 2024, Kropyvnytskyi) (pp. 36–37). Kropyvnytskyi: DonDUVS. Access mode: https://surl.li/nzkzfl

5. Rybalchenko, L., Kosychenko, A., & Klinytskyi, I. (2022). Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review, 2*(1), 96–107. https://doi.org/10.31733/2786-491X-2022-1-96-107

6. Opendatabot. Fraud. Access mode: URL: https://opendatabot.ua/analytics/fraud-2024-12