European Journal of Sustainable Development (2021), **10**, 3, 420-431 ISSN: 2239-5938
Doi: 10.14207/ejsd.2021.v10n1p420

Peculiarities of The Economic Crimes Committed with the Use of Information Technologies

By Serhii Cherniavskyi[1], Viktoria Babanina[2], Inna Vartyletska[3], Oleksandr Mykytchyk[4]

ABSTRACT
The article looks into peculiarities of the economic crimes committed using information technologies. Different approaches to the concept of the economic crime are analyzed to reveal types of economic crimes, which can be committed with the use of information technologies. It is stated that mostly two types of economic crimes could be committed using information technologies – online fraud and forgery. Subjects and objects of a forgery committed with the use of information technologies are analyzed. Close attention is paid to the online fraud and its specific features. The classification of types of the Internet fraud is made. Some specific characteristics of certain types of the Internet fraud are given in the article. Such types of the Internet fraud as spam, carding, phishing, fraud in online games are described.
The main method used in the investigation is the method of comparative analysis, which was used to reveal differences between traditional economic crimes and economic crimes committed with the use if information technologies. The general conclusion was made that economic crimes committed with help of information technologies have a number of differences compared to traditional ones. These differences determine the features of the investigation of such crimes. In particular, such features are manifested in the implementation of operational and investigative measures and investigative actions.

Keywords: economic crime, fraud, forgery, Internet, carding, phishing.

1. Introduction

High rates of development of information technologies, active implementation of the created information and telecommunication systems and technical means in all spheres of life of a society, as well as the current characteristics of systems for the protection of information have created objective preconditions of emergence of a new kind of crimes - crimes in the field of high technologies. The spread of such crimes inevitably puts law enforcement officers in need of a detailed study of the technical capabilities of existing computer systems, their use in the fight against crime in this area.

Thus, modern computer systems are used in almost all areas of science, social structure and, especially, economics. The relative availability of information resources, high speed of database processing, the formation of global cyberspace - all this contributes to the

[1]Vice-Rector of National Academy of Internal Affairs, Doctor of Law, Professor, Kyiv, Ukraine.
[2]Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine.
[3]Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine.
[4]Professor of Criminal Law Department of the National Academy of Internal Affairs, PhD in Law, Associate Professor, Kyiv, Ukraine.

integration of information technology into human life. Despite the huge number of positive opportunities that have come into everyone's life with the transfer of social relations to cyberspace, there are still some negative ones - this is cybercrime, which is developing at the same frantic pace as cyberspace itself.

In this regard, the fight against crime in cyberspace is one of the pressing problems of law enforcement not only in Ukraine but also in each developed country in the world.

Among the crimes committed on the Internet, which are known today, economic crimes are of particular danger. Due to their high latency, as well as the difficulties of detection and investigation, these crimes require a comprehensive scientific study and justification of the possibility of counteraction. The growing number of online stores and online auctions, the creation of banking systems in the global network, the development of payment systems contributes to the fact that more and more people trust and use payments online, forgetting that even in virtual economies can be committed a big number of crimes

The current state of scientific development of methods of investigation and counteraction to economic crimes on the Internet is characterized by insufficient interest in a particular type of crime compared in comparison to cyberterrorism, distribution of pornographic products or information security. At the same time, there is great theoretical and practical significance of the study of crimes committed on the Internet to combat them.

Despite the large number of publications devoted to the investigation of crimes related to the use of computer technology, which have appeared recently, the question of the methodology of investigation of economic crimes in cyberspace has not been considered. This determines the relevance of the study of economic crimes committed with the use of information technology.

2. The concept and general characteristics of economic crimes committed with the use of information technology

Before moving on to economic crimes committed with the use of information technology, it is necessary to define the category of "economic crimes".

Scientific interest in the concept of economic crime is caused by the fact that scholars have a differentiated approach to the definition of crimes in the field of economics. A variety of interpretations of this phenomenon is found in the research of many scientists, in particular, they distinguish "crimes in the field of economics", "economic crimes", "shadow economy", "criminal economy", "economic crime" and others. These concepts are often identified, but there are attempts to prove the different nature of these phenomena.

In the Encyclopedia of modern Ukraine, economic crimes are considered as a kind of crimes committed in the course of professional activity within and under the guise of lawful economic activity with the use of legal economic institutions (rules, forms, procedures). Economic crime is the basis of the shadow economy and is aimed at property and production relations, economic rights of citizens, legal entities, municipalities and state entities (Baranovskyi, 2009).

N. Kozak considers economic crime as a property and mercenary crime, as well as a crime in the economy, the author notes that economic crime is characterized by a set of mercenary encroachments on property, the order of management of the economy committed by persons occupying certain social positions in the structure of economy (Kozak N., 2018).

According to S. Kravchuk, all these concepts have a different spectrum of illegal acts. Thus, crimes in the field of economics, according to the author, are mainly economic crimes committed in various fields; economic crime is the commission of crimes in the sphere of economic activity, including the use of official position. S. Kravchuk classifies acts related to causing material damage or obtaining material benefit as crimes of an economic nature (Kravchuk, 2009).

We fully agree with the latter opinion, as we also believe that the concept of "economic crime" should have a broader interpretation and include not only crimes in the field of economic activity, which are allocated to the current Criminal Code of Ukraine in a separate section, but also other property crimes.

Given this broad interpretation, it should be noted that criminal law contains a large group of rules that determine the criminality of acts in the field of economic activity and legal responsibility for their commission. They are grouped into separate sections "Crimes in the sphere of economic activity" and "Crimes against property".

However, despite the huge number of articles in the Criminal Code of Ukraine with a criminal economic orientation, only Art. 190 in Part 3 provides for criminal liability for fraud committed on a large scale, or through illegal transactions using electronic computers, as well as Art. 200 of the Criminal Code of Ukraine, which criminalizes illegal actions with documents for transfer, payment cards and other means of access to bank accounts, electronic money, equipment for their manufacture. That is, there are only two types of economic crimes that can be committed in cyberspace.

3. Types of economic crimes that can be committed with the use of information technology

The current Criminal Code of Ukraine defines fraud as the acquisition of another's property or the acquisition of the right to property by deception or abuse of trust. In other words, the essence of the criminal act has not changed from the previous edition, only what until 2001 was treated as personal property of citizens now has a more concise and broader form - someone else's property. Similarly, this property can already be understood as the property of citizens, foreign citizens or stateless persons, and, importantly, legal entities or the state. That is, with the change in the wording of the Criminal Code of Ukraine, the sphere of potential victims of fraud has significantly expanded.

Fraud and abuse of trust as means of fraud are perceived as the achievement of certain intermediate results before the final receipt of another's property or obtaining the right to it, namely misleading the property owner so that the offender later received the property from the victim. Otherwise, it will not be a fraud, but a kind of theft committed using special methods (Bilous, 2002).

In recent years, fraud on the Internet has been actively developed. Of course, the main difference between this type of crime and traditional fraud is the special circumstances of criminal encroachment.

Internet fraud, which, on the one hand, is the result of the evolution of traditional fraud, as some of its types occur on the Internet without any major changes in the methodology of criminal intent; on the other hand, it is a qualitatively new group of crimes, because with the similarity of implementation methods, specific methods have significant differences (Juravl, 2006). This type of crime, like many other computer crimes, is characterized by high latency, firstly, due to the complexity of the investigation, and secondly, due to the specifics of the implementation of fraudulent schemes on the Internet.

As in traditional fraud, the bulk of the attacks are aimed at an indefinite range of potential victims. One of the features of this type of crime is that some methods of Internet fraud are characterized by the presence of additional requirements for the identity of the offender. Most often it is about the presence of special knowledge in a particular field - the field of information technology (Areshonkov, 2013).

Of course, in the case of Internet fraud, encroachment occurs exclusively on the right to property, as the Internet is rather a certain environment capable of transmitting only information. Such an environment can be considered material only conditionally, because it does not have all the signs of materiality. In our opinion, in this case it is appropriate to talk about the virtual world and the virtual environment, which, being the object of the material world, however, is intangible (Belskyi, 2014).

Thus, if a criminal, having committed a fraud against an indefinite large group of people, stole their money, transferring it to his secret bank account, then, in our opinion, this will not be the theft of money (Voronov, 2010). On the contrary, it should be considered as obtaining the right to them, including the right to receive this money in material form (for example, to transfer cash through an ATM).

Online fraud (or the fraud committed on the Internet) has the following characteristics:

1. The main elements of the forensic characteristics of fraud on the Internet are as follows:

1) the circumstances of the crime, including place and time;

2) the method of committing the crime (method of preparation, method of direct commission and method of concealment of the offense);

3) the object and subject of encroachment;

4) general characteristics of the personality of the offender;

5) general characteristics of the victim.

2. Deception and abuse of trust as a means of fraud is the achievement of certain intermediate results before the final receipt of another's property or obtaining the right to it, namely misleading the owner so that the offender later received the property from the victim. Otherwise, it will not be a fraud, but a kind of theft committed using special methods.

3. In the case of an Internet fraud, the right to property is infringed, as the Internet is rather an environment capable of transmitting only information. Such an environment can be considered material only conditionally, because it does not have all the signs of materiality. In this case, it is appropriate to talk about the virtual world and the virtual environment, which, being the object of the material world, however, is intangible.

4. In most cases, the direct subject of fraud is money, which, due to its special status, is of the greatest interest to fraudsters. The rest of the items, for the most part, can

also be tentatively equated to money, as, ultimately, after the theft or acquisition of the right to them, this property is then resold.

5. As the Criminal Code of Ukraine does not contain detailed information on what is to be understood by the right to property in the context of its articles, the question may arise as to whether the crime is considered complete from the moment of full ownership of the property, or only some authority (possession, use or disposal).

Of course, this issue must be addressed in each case. Since the rights to property are enshrined in the relevant documents, in cases where the subject of criminal encroachment is the right to another's property, the crime should be considered completed from the moment when the offender is endowed with the rights to which the victim was granted.

6. In recent years, there has been a clear trend of "merging" the real criminal world and the so-called virtual (Nekit, Kolodin & Fedorov, 2020). In the context of the study of fraud on the Internet, we can say that this trend will ultimately allow us to build more complex fraudulent schemes. As a result, the complexity of detecting and investigating such crimes is growing significantly.

7. Victims of Internet fraud may be a natural person who has caused physical, property, moral damage, and a legal entity, if the damage to his property or business reputation. Of course, however, that the bulk of these crimes committed against individuals.

Analyzing the second type of economic crimes that can be committed in cyberspace, consider Art. 200 of the Criminal Code of Ukraine, which states that forgery of documents for transfer, payment cards or other means of access to bank accounts, as well as the purchase, storage, transportation, forwarding for sale of forged documents for transfer or payment cards or their use or sale - shall be punishable by a fine of 500 to 1,000 tax-free minimum incomes or imprisonment for a term up to three years. Transfer documents here are understood as a paper or electronic document used by banks or their clients to transfer orders or information for the transfer of funds between the subjects of the transfer of funds (settlement documents, documents for the transfer of cash, as well as those that used for interbank transfer and payment notification, others) (Verkhovna Rada, 2001).

The object of this crime is the established procedure for the production, use and circulation of documents for transfer, payment cards or other means of access to bank accounts, which ensures the proper functioning of the banking system of Ukraine. The subject of the crime are: 1) documents for the transfer of funds; 2) payment cards; 3) other means of access to bank accounts (Ahtyrska & Antoshyuk, 2018).

The concept of documents for transfer is given in the note to Art. 200 of the Criminal Code of Ukraine. Such documents, in particular, are:

a) settlement documents, which are a payment order, settlement check, payment request and settlement documents of other types, established by the National Bank of Ukraine;

b) interbank settlement documents, i.e. transfer documents formed by the bank on the basis of settlement documents submitted by clients, documents for cash transfer, as well as orders for contractual write-off provided for in agreements concluded between clients and their servicing banks;

c) documents for cash transfer, details and features of registration of which are also established by the National Bank of Ukraine;

d) clearing requirements;

e) other documents used in payment systems to initiate the transfer.

A payment card is a special means of payment in the form of a plastic or other type of card issued in the manner prescribed by law, used to initiate the transfer of money from the payer's account or from the relevant bank account to pay for goods and services, transfer money from their accounts to other accounts persons, receiving money in cash at the cash desks of banks, foreign exchange offices of authorized banks and through ATMs, as well as other operations provided for in the relevant agreement.

Other means of access to bank accounts should be considered any, other than transfer documents and payment cards, documents or items with which a person can access to a particular bank account and the ability to carry out transactions with funds in such account. Such another means, in particular, is a bank identification card (identification card) - an identification means in the form of a plastic or other type of card containing the details specified by the bank, which identify the client and his bank accounts.

When committing this crime by purchasing, storing, transporting, forwarding for sale, use or sale, its subject is only forged documents for transfer or forged payment cards.

The objective side of the crime may be expressed in the commission of any illegal act under Part 1 of Art. 200 of the Criminal Code of Ukraine:

a) in the forgery of transfer documents, payment cards or other means of access to bank accounts, electronic money;

b) in the acquisition, storage, transportation, forwarding, use or sale of forged documents for transfer or payment cards;

c) in the illegal issuance or use of electronic money.

Forgery of transfer documents, payment cards or other means of access to bank accounts, electronic money is the creation of a completely falsified item or partial falsification of a real item.

4. Features of fraud committed on the Internet

Characterizing the place of online fraud, it should be emphasized that in contrast to traditional types of fraud, in this case the perpetrator and the potential victim, from the beginning of the crime and ending with the onset of socially dangerous consequences, can be at a considerable distance from each other.

When committing crimes in the field of computer information using new technologies and telecommunications, the place of commission of a socially dangerous act, as a rule, does not coincide with the place of actual occurrence of socially dangerous consequences. There may be several such places. They can be at a considerable distance from each other, be in vehicles, various institutions, in areas, including in different countries and on continents. Therefore, the place of commission of a crime is most appropriate to consider a vehicle, the area or territory of the institution, organization, state, where socially dangerous acts were committed, regardless of the place of occurrence of criminal consequences (Fris & Savinova, 2013).

Of course, this approach to understanding the crime scene is the most acceptable when it comes to computer crimes and, in particular, cyber fraud. Given that now the Internet can be accessed almost anywhere, in our opinion, it would be unreasonable to consider

the place of the crime to be the place of occurrence of socially dangerous consequences. Otherwise, it can lead to an absurd situation, when, for example, socially dangerous consequences will occur in a city park, where the victim, sitting on a bench with a laptop, worked on the Internet (Hrynchak, 2015).

Of course, sometimes there are situations in which the place of the crime may also be the place of occurrence of socially dangerous consequences. However, in such cases, the perpetrator and the victim are likely to be slightly distant from each other.

Internet fraud has significant differences from both conventional and high-tech fraud (excluding the Internet). These differences are due primarily to the Internet itself. The fact is that the Network in the encroachments considered in this paper performs two main functions simultaneously:

1) gives more opportunities to increase and maintain maximum anonymity of the scammer;

2) in skilled hands is an effective tool that allows you to successfully deceive potential victims.

It is also necessary to take into account the fact that actions committed on the Internet (for example, agreements) lose the sign of territoriality (Litvinov, 2017). As a result, settling disputes over these actions is difficult for any particular country.

Thus, the probability of exposing the fraudster is reduced, and if the fact of fraud is still revealed, the possibilities of bringing the perpetrators to justice are quite limited. This situation can be illustrated by the following example.

The organization sells erotic and / or pornographic photo and video materials through its own website on the Internet. To access the materials, visitors need to register by filling out a questionnaire, the content of which includes credit card details. After registration, the victim is offered a free tour of the site, but in the process of viewing the content of the site from the user's account small amounts are deducted.

This example shows quite well the potential of Internet fraudsters, because in this case, the amount written off may be small enough for the victim to pay attention to it. And if the victim finds out about the fraud, it will be difficult to prove the guilt of the perpetrators, because despite the fact that there was a fact of deception of the user (free tour was paid), in the end, the image service was provided. Because the Internet provides more opportunities to remain anonymous, fraudsters may well deceive the victim.

This example also serves as a good illustration of why some victims of fraud do not turn to law enforcement.

Ultimately, the main features of fraud on the Internet depend on the scheme chosen by the attacker, the type of fraud, as well as the sphere of life in which the offender is going to act. This choice determines the method of realization of criminal intentions, as well as the form in which the ultimate benefit will be obtained: money, goods, services or information.

Of course, all types of fraud on the Internet can be grouped into the following groups:

1. based primarily on the use of e-mail and / or other means of messaging as the main tools to influence the victim;

2. fraud, in the schemes of which the central place is given to the use of sites.

The criterion of this classification is the individual preferences in the choice of tactics of the scammer, which are due to the level of his special training, personal

preferences, the circumstances of the objective situation, as well as some other circumstances.

It should be noted that such a distribution is conditional, because today there are infrequent fraudulent schemes in which criminals use only one thing. As an example, we can cite some fraudulent schemes, which are based on the cloning of a site owned by any organization. In this case, the attacker creates the most accurate copy of the original site (up to the consonant Internet address), but specifies other details for calculations. Here, the scammer usually works only with the site. In most other cases, the implementation of a scheme of fraud involves the active use of all possible electronic resources. Of course, such activities are associated with a high risk of exposure, as more traces will remain.

5. Characteristics of certain types of the Internet fraud

The first type of fraud committed on the Internet are crimes in which the object is encroached upon mainly by e-mail and / or other means of messaging. This group includes those types of fraud in which the main tool for implementing a criminal plan is the Instant Messaging Service (IMS). Included in this group of crimes are characterized by the fact that almost all work with the victim takes the form of correspondence, and in some cases for a successful outcome for the fraudster a single letter may be enough.

Regardless of which method of messaging is chosen, in the vast majority of cases, the main thing that the scammer focuses on is the mass sending of certain messages - spam. This increased attention is due to the fact that the purpose of spam is to attract the attention of as many potential victims as possible. This is especially true when spam is part of the preparatory phase for a crime and is aimed at collecting personal financial and other confidential information about victims by secretly introducing malicious software (such as spyware) into their computers, as well as in other ways, for example, by sending letters with a proposal to fill out a questionnaire. Therefore, when planning a crime, special attention is paid not only to the number of messages sent, but also to the quality of their compilation (Romashov & Bryleva, 2019).

The message sent by an attacker must meet three main parameters:

1) relatively small size;

2) maximum persuasiveness (the situation is somewhat facilitated in cases where the victim receives a message from a person on the list of friends, which is relevant for fraud on social networks);

3) ensuring the lowest possible probability of disclosure of fraud and self-detection.

The second type of fraud committed on the Internet would be fraud in social networks. This type of deception has become widespread in recent years. As in other cases, the standard tactics of sending spam were initially used (creating a large number of accounts and then sending messages to as many other users as possible), but it quickly proved ineffective. Therefore, after some time there was a qualitatively new way to deceive users of social networks. It consisted of hacking and gaining short-term full access to users' accounts and sending special text messages on their behalf to people on the "hacked" user's friends list (Shulzhenko & Romashkin, 2020).

The peculiarity of this method of fraud is that the user still has the opportunity to use their account, so potential victims are more likely to come as the fraudster wants (for example, download the program specified in the message link and install it on your computer, and in fact such program is malicious).

Currently, a similar method of sending messages is realized with help of instant messaging services. If a successful outcome is achieved, malicious software is installed on the victim's computer in most cases, the purpose of which is to steal personal information, such as credit card data (Kvartsova, 2014).

It is very common for such programs to be detected in a timely manner by special means, as companies producing anti-virus and other security programs do not always have time to detect new malware in time. Of course, in such cases, the security of the user's computer and the information available on it will largely depend on the computer literacy of the user, i.e. the possession of sufficient information about the Internet and the ability to use this knowledge.

The next type of fraud committed on the Internet are crimes in which the encroachment on the object is carried out mainly using the capabilities of Internet sites (Scarcella, 2020). This group is the majority of encroachments, the distinguishing feature of which is the use of sites as the main tool of influence. In our opinion, among the activities of fraudsters in this group will be the following:

1) investment schemes;
2) earnings;
3) "magic wallets";
4) auctions and online trade;
5) carding;
6) online casinos and lotteries;
7) cloning sites.

Of course, the biggest dangers today are online commerce (rarely, auctions), carding, lotteries and site cloning. Consider some of these types of fraud in more detail.

The activities of auctions and online stores have a lot in common, namely: the goods that a potential buyer intends to buy, are not sent at all, or a parcel arrives, but its content is completely different; the fee for the specified product is asked to be transferred before the desired item reaches the recipient.

One of the most common types of online fraud remains credit card fraud - carding.The term "carding" is used to denote a type of fraud in which an operation is performed using a bank card or its details, which is not initiated or confirmed by its owner. Criminals usually receive payment card details from hacked servers of online stores and payment systems (WebMoney, PayPal, etc.), as well as from personal computers (either directly or through remote access programs, by implementing malicious software security).

Carding has many schemes that provide a variety of implementations. In any case, credit card fraud can be considered a crime in the field of high technology, as it can take the form of ordinary fraud, and crimes on the Internet, and mixed, when, for example, in an organized crime group, some accomplices work via the Internet (spam, theft of information, etc.), and the other part carries out criminal activities in the real world (creation of fake credit cards based on the information obtained, cash transfer through ATMs etc.).

It is necessary to note such a type of Internet fraud as phishing. To date, it is the most common method of stealing payment card numbers. Phishing consists in creation of a fraudulent site that will enjoy the trust of the user, for example - a site similar to the bank's site, through which payment card details are stolen. It can be implemented through messaging services, sites, cellular or telephone communications, both individually and in combination (McClure, Scambray & Kurtz, 2003).

Phishing, as a type of fraud, is characterized primarily by the desire to obtain identification data for further embezzlement of funds as the main purpose of the activity (for example, bank account details or credit cards). Mailing is also used in phishing. Distinctive features of such mailings are the following:

1) messages are sent, as a rule, on behalf of a known name (for example, on behalf of a bank or payment system);

2) very often the letter contains a link to a site that is either an exact copy of the original, or redirects the user to the desired page of the offender. The purpose of this site is to "fish out" the necessary confidential information from the victim.

Soon, the so-called fraud in online games will become widespread. In the last 3-5 years, massive multiplayer online games have become increasingly popular. Over the years, the audience of this type of entertainment has grown significantly, as well as the number of games presented by developers. In this regard, the activity of fraudsters and malware developers has also increased significantly.

The gameplay of the vast majority of online games is built in such a way that the player needs to spend a lot of time in the game and make a lot of effort to achieve some success, which is expressed in a high degree of game character development, high-level game items and a large amount of game currency (Butuzov, Ostapets & Shelomentsev, 2005). Therefore, given that the age of the gaming audience has virtually no restrictions, it would be logical to conclude that there is a category of people who do not have too much free time, but have sufficient earnings. This category is a circle of potential victims of fraud in online games. Since there are people who are willing to pay real money for game values, there will always be those who are willing to offer these values.

Experts from Kaspersky Lab point out that there are several main methods for stealing gaming confidential information, which can later be used for fraudulent purposes:

1) the use of social engineering in the form of phishing messages.

2) the use of software vulnerabilities of game servers in order to gain unauthorized access to user databases, which allows you to steal passwords from player accounts.

3) the use of malicious programs (Butuzov, 2010).

Conclusions

1. Economic crimes committed with help of information technologies have a number of differences compared to traditional ones. These differences determine the features of the investigation of such crimes. In particular, such features are manifested in the implementation of operational and investigative measures and investigative actions.

2. The situation of Internet fraud is a system of interdependent and interconnected elements, in the spatial and temporal boundaries of which there is interaction between criminals and their victims, as well as the circumstances of the objective environment that

took place at the time of investigation and influenced the formation of traces crime, its detection and investigation.

3. The time of committing fraud on the Internet is the time of completion of a socially dangerous act, regardless of the time of occurrence of socially dangerous consequences. The specific time of this crime is calculated by periods of time, the duration of which depends on various factors relevant to the activities of the victims.

4. In contrast to traditional types of fraud, in the case of Internet fraud, the offender and the potential victim, from the beginning of the crime and ending with the onset of socially dangerous consequences, may be at a considerable distance from each other.

5. The use of specialized knowledge in the investigation of cybercrime also requires the investigator's knowledge of high information technology to determine the necessary specialization, which must have an expert and a specialist, as well as for the most productive interaction with these individuals at all stages of pre-trial investigation of Internet fraud.

References

Baranovskyi O. (2014). *Economic crimes. In: Encyclopedia of modern Ukraine.* [online] Retrieved from http://esu.com.ua/search_articles.php?id=18798

Kozak N. (2018). Definition of crimes in the sphere of taxation committed with the use of computer technologies. Actual issues of reforming the legal system of Ukraine, 18, pp. 484-485.

Kravchuk S. (2009). Economic crime in Ukraine. Kyiv: Kondor, 282 p.

Bilous V. (2005). Coordination of the fight against economic crime. Irpin: Academy of State Tax Service of Ukraine, 449 p.

Juravl V. (2006). Forensic prevention of economic crimes. Kharkiv: "Kharkiv Legal", 236 p.

Verkhovna Rada of Ukraine. (2001). *Criminal Code of Ukraine: Law of Ukraine of April 5, 2001.* Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text

Fris P. & Saviniva N. (2013). *Criminal-legal policy in the field of combating cybercrime in Ukraine: efficiency and prospects of development. Fight against Internet crime: materials of the international scientific-practical conf.* Donetsk: Donetsk juridical institute, 172 p.

McClure S., Scambray J. & Kurtz G. (2003). *Hacking Exposed*: *Network Security Secrets* and *Solutions*. N.-Y.: McGraw-Hill, 312 p.

Kvartsova M (2014). Factors determining cybercrime in modern criminological theory. Legal scientific electronic journal, 5, pp. 113-118.

Butuzov V. (2005). Crimes in the field of use of electronic computers, systems and computer networks and telecommunication networks. Kyiv: Ministry of Internal Affairs of Ukraine, 86 p.

Butuzov V. (2010). Counteraction to computer crime in Ukraine (system-structural analysis). Kyiv: KIT, 405 p.

Areshonkov V. (2013). Some international legal problems in the fight against cybercrime in the context of globalization. Bulletin of the State University of internal affairs of Luhansk, 5. pp. 173-176.

Akhtyrska N. & Antoshuk V. (2018). Computer crime in Ukraine through the prism of judicial practice. Bulletin of the prosecutor's office, 3, pp. 84-95.

Belskyi Yu. (2014). On the definition of cybercrime. Legal Bulletin, 6, pp. 414-418.

Voronov I. (2010). Organization of counteraction to crimes in the sphere of using payment cards and other means of access to bank accounts. Pivdennoukrainskyi pravnychy chasopys, 1, pp. 26-29.

Hrynchak I. (2015). Cybercrime as a crime of international character. Scientific Information Bulletin of Ivano-Frankivsk University of Law named after King Danylo Halytsky, 12, pp. 93-98.

Litvinov M. (2017). World and Ukrainian practice of combating cybercrime. Law and Security, 1, pp. 85-89.

Nekit K., Kolodin D. & Fedorov V. (2020). *Personal data protection and liability for damage in the field of the Internet of Things.* Juridical Tribune, 10(1), pp. 80-93.

Scarcella L. (2020). *E-commerce and effective VAT/GST enforcement: Can online platforms play a valuable role?* Computer law & security review, 36, pp. 105-137

Romashov R. & Bryleva E. (2019). *Urgent Problems in the Investigation of Computer Crimes at the Modern Stage.* Ubiquitous computing and the Internet of Things: prerequisites for the development of ICT, 826, pp. 411-417.

Shulzhenko N. & Romashkin S. (2020). *Internet fraud and transnational organized crime.* Juridical Tribune, 10(1), pp. 162-172