DOI: https://doi.org/10.34069/AI/2022.51.03.29

How to Cite:
Dumchikov, M., Fomenko, A., Yunin, O., Pakhomov, V., & Kabenok, Y. (2022). The essence and classification of cybercrime in the field of computer information. *Amazonia Investiga*, *11*(51), 291-299. https://doi.org/10.34069/AI/2022.51.03.29

The essence and classification of cybercrime in the field of computer information

Сутність та класифікація кіберзлочинів в сфері комп'ютерної інформації

Received: Janua ry 31, 2022 Accepted: March 10, 2022

Written by:
Mykhailo Dumchikov[110]
https://orcid.org/0000-0002-4244-2419
Web of Science researcher code: ABC-1338-2020
Andrii Fomenko[111]
https://orcid.org/0000-0003-3517-1638
Web of Science researcher code:AAP-2665-2021
Oleksandr Yunin[112]
https://orcid.org/0000-0003-4846-2573
Web of Science researcher code:AAP-5453-2021
Volodymyr Pakhomov[113]
https://orcid.org/0000-0002-0501-524X
Web of Science researcher code: AAC-7713-2022
Yuliia Kabenok[114]
https://orcid.org/0000-0001-9342-3835
Web of Science researcher code: AAM-2356-2021

Abstract

Cimes in the field of computer information have become pressing issue in society today. Its relevance is evidenced by news from around the world, criminal statistics, problematic issues in the science of criminal law, as well as problems in criminal proceedings. All this is due to the fact that as a phenomenon, crimes in the field of computer information belong to the very specific category that is constantly evolves technological progress.

The purpose of the article is to study the phenomenon of crimes in the field of computer information, to define the concept of crimes in the field of computer information and types of these crimes, to provide general characteristics of crimes in the field of computer information, as well as to identify their classification.

Various methods of scientific knowledge were used as a methodological basis for writing this article. In particular, comparison methods, analogies and generalization methods were used.

Анотація

Злочини в сфері комп'ютерної інформації сьогодні є дуже актуальною проблемою суспільства. Про її актуальність свідчать новини по всьому світу, кримінальна статистика, проблемні питання науці кримінального права, а також проблеми в кримінальному процесі. Все це пов'язано з тим, що як явище, злочини в сфері комп'ютерної інформації є дуже специфічною категорією, яка постійно розвивається паралельно з технічним прогресом.

Метою статті є дослідження феномену злочинів у сфері комп'ютерної інформації, визначення поняття злочинів в сфері комп'ютерної інформації та видів зазначених злочинів, надати загальну характеристику злочинам в сфері використання комп'ютерної інформації, а також визначити ознаки які притаманні зазначеному виду злочинів та зробити їх класифікацію.

[110] Senior lecture. Department of Criminal Legal Disciplines and Procedure, Sumy State University, Ukraine.
[111] Candidate of Juridical Sciences, Rector, Dnipropetrovsk State University of Internal Affairs, Ukraine.
[112] Docror of Juridical Sciences, Vice Rector, Dnipropetrovsk State University of Internal Affairs, Ukraine.
[113] Doctor of Juridical Sciences, Professor, Department of Administrative, Economic Law and Financial and Economic Security, Sumy State University, Ukraine.
[114] Ph.D in Law, Associate Professor, Associate Professor of the Department of International, Civil and Commercial Law Kyiv National University of Trade and Economics, Ukraine.

In our time, cybercrime has spiraled out of the control of one state's law enforcement agencies and has become a significant interstate and transnational problem.

Keywords: crimes in the field of computer information, information crimes, cybercrime, crimes in the field of payment systems, computer crimes, COVID-19.

Методологічною базою для написання даної статті було використано різні методи наукового пізнання. Зокрема було використано методи порівняння, аналогії та метод узагальнення.
В наш час кіберзлочинність вийшла з-під контролю правоохоронних органів однієї держави та стала значною міждержавною і транснаціональною проблемою.

Ключові слова: злочини в сфері комп'ютерної інформації, інформаційні злочини, кіберзлочинизлочини в сфері платіжних систем, комп'ютерні злочини, COVID-19.

Introduction

The active use of computer technology in almost all fields of public life has become an integral part of todays life. It can be emphasized that the 21st century is the century of digital and information technologies.

New forms of crime are a challenge to our society, but at the same time the variety of offenses are developing. Until a few decades ago, there were very few mentions of crimes in the field of computer information, but in a short period of time, these crimes began to pose not only a particular threat to individuals or society, but also to the state as a whole. Moreover, the problem of computer crime is the most acute, as the consequences of untimely response to such a threat are much more dangerous than in most other crimes.

At present, crimes in the field of computer information cover virtually all fields of society, from the banking sector to the national security of the state. The purpose of the article is to formulate a scientifically sound definition of the concept of "crimes in the field of computer information" and identify types of these crimes, as well as to identify specific features inherent in the rolled type of crime. and the use of computers, systems and computer and telecommunication networks. The subject of the study is the nature and classification of cybercrime in the field of computer information.

Theoretical Framework

Analyzing the legal aspect of crimes committed with the help of electronic computers, it should be noted that the concept of a crime in the field of computer information and a crime committed with the help of computer technology are not identical concepts. In our opinion, criminal offenses in the field of computer information should be considered as one of the subtypes of crimes using computer technology.

The public danger of crimes in the field of computer information is that illegal access to computer information can harm the activities of various public defense systems, the banking sector, municipal systems. Similarly, various types of actions to distort the accuracy of information can lead to problems of a national nature and harm the rights and interests of the individual.

The first concept of "crime in the field of computer information" was used in the 60s of the 20th century, when the first using computers crimes were discovered (Kurushin, 1998)

Today, there is no single definition for cybercrime. In particular, Bessonov V. under the definition of crime in the field of computer information means criminal, unlawful, culpable violation of other people's rights and interests in relation to automated data processing systems, full influence, subject to legal protection of property rights and interests, public and state security (Bessonov, 2000)

Smirnova T. under the definition of crime in the field of computer information means prohibited by criminal law socially dangerous intentional, guilty and illegal acts aimed at violating the inviolability of computer information protected by law and its material media, damaging the rights and interests of individuals and the state and public safety. (Smirnova, 1998)

Borovik V. defines crime in the field of computer information as intentionally socially dangerous acts that harm or threaten to harm public relations, regulating the safe production, storage,

use or dissemination of information or information resources (Borovukiv, 2015)

Begishev I. understands these crimes as a guilty, socially dangerous act committed for the purpose of violating the integrity, confidentiality, reliability and availability of digital information protected by law (Begishev, 2017)

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim (Aghatise, 2006)

Baturyn Y. believes that in the legal sense, crimes in the field of computer information as a special group of crimes do not exist, but emphasizes that many traditional types of crimes have improved as a result of raising funds for computer technology, and therefore we can only talk about computer aspects of crimes without allocating them to a separate group (Baturin, 1991)

Michael Aaron Dennis says that cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy (Michael, 2019)

Dobrovolsky D. under the concept of a crime in the field of computer information understands the criminal law guilty of socially dangerous acts aimed at violating the inviolability of legally protected electronic information and its media, carried out in the process of creating, using and disseminating electronic information, as well as aimed at disrupting computers, computer systems or their networks that harm the legitimate interests of owners or owners, life health, human and civil rights and freedoms, national security (Dobrovolsky, 2005)

We critically analyze the existing definitions, suggesting that crimes in the field of computer information are understood as intentional socially dangerous, illegal, culpable acts that encroach on and harm public relations, which regulate the storage, dissemination, use and protection of information.

Methodology

The basis of this study was using the variety of methods of scientific knowledge. In particular, the method of comparison and analogy was used to study the legal regulation of various types of crimes in the field of computer information, which is contained in the features and classification of crimes in the field of computer information.

The observation method was used to determine the main features of computer information crimes and to get acquainted with the essence of computer information crimes and the general specifics of this phenomenon, which is contained in the features and classification of crimes in the field of computer information.

The generalization method was used to study various types of information security crimes, the information is contained in the parts of crimes in the field of payment systems, fraud in the field of computer information and crimes in the field of information security.

The analytical method was used to study the specifics of the development of crimes in the field of computer information and determine their relationship with other types of crimes and scientific and technological progress.

Results and Discussion

Signs and classification of crimes in the field of computer information.

The 2001 Cybercrime Convention, that was ratified by Ukraine in 2005, identifies 4 types of crimes in the field of computer information based on their generic nature (Verjovna Rada de Ucrania, 2001).

1. Crimes against confidential information;
2. Crimes related to the use of computers;
3. Crimes related to the content of information contained on electronic media and the Internet;
4. Crimes related to infringement of copyright and related rights.

In turn, the Criminal Code of Ukraine contains a slightly different classification of crimes in the field of computer information. In particular, section 16 criminal offenses in the field of computer use (computers), systems and computer networks and telecommunication networks includes 6 types of crimes in the field of computer information (Law № 2341-III, 2001)

1. Unauthorized interference in the operation of computers, automated systems, computer networks or telecommunication networks.
2. Creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale.

3. Unauthorized sale or dissemination of information with limited access, which is stored in computers, automated systems, computer networks or media of such information.
4. Unauthorized actions with information processed in electronic computers (computer), automated systems, computer networks or stored on the media of such information, committed by a person who has the right to access it.
5. Violation of the rules of operation of electronic computers (computers), automated systems, computer networks or telecommunication networks or the order or rules of protection of information processed in them.
6. Interference with the operation of electronic computers (computer), automated systems, computer networks or telecommunication networks through the mass dissemination of telecommunication messages.

It should be noted that the list of crimes in the field of computer information contained in the Criminal Code of Ukraine does not cover the full range of criminal acts committed in cyberspace. In our opinion, crimes in the field of computer information should also include fraud committed in cyberspace, theft committed in cyberspace.

According to the report of the Cyber Police Department of Ukraine for 2018, 11131 crimes in the field of computer information were committed, and only 25% of them were solved. According to statistics, the largest number of crimes was committed in the field of payment systems and banking, respectively. In second place are crimes in the field of e-commerce and directly in the field of cybersecurity (Cyber police in Ukraine, 2018)

It is worth noting that under the quarantine restrictions associated with COVID-19, the number of computer information crimes has increased dramatically. This trend is primarily due to the fact that people increasingly prefer online services (billing, delivery, buying and selling goods, communication). In our opinion, it is necessary to identify the main features of crimes in the field of computer information that would emphasize their social danger, such as:

1. The latency of such crimes. Computer information crime is currently the most latent type of crime of all. First of all, this is primarily due to the fact that persons who have become victims of such crimes do not apply to law enforcement agencies, which are responsible for investigating crimes in the field of computer information. Secondly, a large number of victims of such crimes do not even realize that they have fallen into the trap of criminals. Third, a large proportion of victims of computer information crimes at the same time wanted to buy illicit goods, services, documents or information from an attacker, thus also committing an illegal act, but were deceived. Banks, credit institutions, online services and shops often do not report crimes against themselves in order to protect their reputation.
2. The distance of crimes in the field of computer information. Intruders with expert knowledge of computer networks can steal millions from the banking sector, deploy a satellite 180 degrees, turn off a patient's life support system in a hospital, and remain unnoticed anywhere in the world (Lyadskiy, 2014)
3. The transnational nature of crimes in the field of computer information. The place of commission of these crimes is cyberspace, namely the environment created by an organized set of information processes based on the common principles and rules of information, telecommunications and information and telecommunications systems, regardless of ownership.
4. The availability of materials necessary for committing crimes in the field of computer information. Currently, there are a large number of forums where both paid and free information on how to commit certain crimes in the field of computer information (carding, phishing, scamming). In addition, such resources provide information on the creation of separate software for further criminal activity.
5. The reduced age of persons committing crimes in the field of computer information. It is worth noting that due to the fact that crimes in the field of computer information, firstly, a very lucrative form of employment, and secondly, information on the commission of such crimes is freely available, there is a reduced age of such crimes.
6. The use of social engineering skills. Many computer crime crimes are committed with the help of social engineering skills. Social engineering is a type of attack that is based on human interaction and is often accompanied by manipulation of these people in violation of normal security procedures and is a best practice to gain access to systems, networks or for financial gain (Voitko, Marchenko, Antonov, 2020)

We would like to propose the following classification of crimes in the field of computer information:

1. Crimes in the field of payment systems:

– Skimming
– Carding
– Enroll
– Cash - trapping

2. Computer information fraud.

– Fishing
– Fraud in the field of online auctions
– Use of fictitious e-commerce entities

3. Crimes in the field of intellectual property

– Internet piracy
– Cardsharing

4. Crimes in the field of information security

– Forgery of computer information
– Creating malware
– Malware distribution
– Selling malware
– Damage to computer data or computer program data
– Change computer data or computer program data
– Computer espionage
– Illegal use of protected information.

Crimes in the use of payment systems.

In the criminal legislation of Ukraine, as well as in the scientific literature, there is no concept of crimes in the use of payment systems, most scholars consider such crimes as crimes in the financial and banking fields, or crimes in the field of financial and banking information (Vakulyk et al, 2019) Computer information crime in the use of payment systems is a type of cybercrime. In Ukraine, this type of fraud is gradually becoming widespread. In particular, one such crime is skimming.

Skimming - theft of card data using a special device - a skimmer (Dictionary of banking terms, 2022)

In general, skimming should be divided into 2 types:

– Physical skimming. Attackers copy all information from the card's magnetic stripe (card name, card number, expiration date, CVV and CVC code), you can find out the PIN code using a mini-camera or keyboard pads installed on ATMs . You can become a victim of skimming not only by withdrawing cash, but also by paying for purchases at outlets. Waiters, cashiers, and hotel employees use portable skimmers or devices attached to the terminal to copy the data.
– Software skimming. It involves the installation by attackers of certain malicious software that will copy the magnetic stripe of the card, the code and date of the card, and then send such data to the servers of attackers.

Privat Bank of Ukraine emphasizes that so-called anti-skimming pads are currently used, which significantly reduce the risk of installing skimmers on ATMs. In addition, specialists of the cybersecurity department of a private bank recommend the use of chip cards, which have a much higher level of protection, because the information contained in the chip has cryptographic protection that prevents it from being compromised (Privat Bank, 2022).

Another type of crime in the field of payment systems is carding. Carding is illegal financial transactions using payment cards and electronic payment systems that have not been confirmed or initiated by the cardholder or e-wallet holder. Payment card details are usually taken from various darknet services. The cost of e-wallet or plastic card varies from 2 to 300 dollars, depending on the country of the card or e-wallet holder, the amount of money on them, the type of card (business, corporate, gold), the bank that issued the card.

An attacker with a card or e-wallet can use the funds, for e-commerce products on the Internet, top up the phone number and then transfer it in cash, buy equipment in online stores with their subsequent sale. The most popular way to use such cards is to buy goods at various marketplaces yourself, this method, unlike others, allows you to use the entire balance of the card, first without intermediaries, and secondly without a commission for resale of purchased goods.

Similar to carding is another crime in the field of payment systems, Enroll can be called a predicate crime in some areas of carding, namely Enroll is a procedure by which an attacker obtains or creates new access to online banking

of the victim. After gaining access to the victim's online banking, the attacker significantly simplifies the procedure for confirming a transaction (even a very suspicious one) because the confirmation can be done in the online banking itself.

Cash - trapping is the theft of cash from an ATM by installing a special retaining pad on the ATM tent.

To commit such a criminal act, criminals close the hole for the issuance of money in the ATM with a special overlay (bar) with adhesive tape on the other side. Thus, when citizens carry out cash withdrawal operations, banknotes are seized - the money sticks to the tape, which prevents them from being issued to the legal cardholder. In most cases, the user of the ATM, without receiving money decides that transaction has failed or ran out of cash and is unaware of the fact of fraud. After that, the fraudsters come and take the cash (Yurchuk, 2017)

Computer information fraud.

Fishing is an innovative type of fraud in the Internet, which aims to obtain personal data, bank details, details of electronic payment systems and crypto wallets and data from e-accounts of online stores, with the subsequent sale of such data or using such data at its discretion.

It is worth noting that fishing websites are very difficult to recognize for their originality. Fishing websites completely copy the original websites, the only difference being the domain name address, which does not attract the attention of an untrained person due to a slight difference in letters or numbers. As an example, the crypto website MyEtherWallet.com, cybercriminals used a phishing site to steal about $ 700,000 in a few days. The attackers copied the original website and gave it the domain name myetherwallet.com, thus stealing the private keys responsible for accessing the ETH and ETC addresses.

The social danger of Fishing is the direct financial damage and the creation of a crisis of confidence in financial transactions carried out on the Internet. Because of the costs of fishing attacks, many financial and banking institutions refuse to pay and place all responsibility on the customer. In a broad sense, phishing undermines the marketing image of a company or financial institution and strongly affects its overall image, dealing a severe blow to e-commerce (Klochko, Kulish, Reznik, 2016)

It can be difficult for the average Internet user to detect a fishing attack because of their gullibility and poor knowledge of constantly changing phishing methods and tactics (spam is increasingly combined with malicious software) (Kumar, Chatterjee, Díaz, 2020).

In our opinion, there are 3 main types of fishing

- Mass fishing. This type of phishing involves the use of spam emails, websites, fake advertising banners and push messages that are addressed to a large number of people. As a rule, the victims of this type of fishing are bank customers and so on. The main feature of this type of fishing is that it does not involve the identification of specific victims in advance, as the recipients of a fishing attack are taken from randomly obtained databases.
- Target fishing. The most dangerous type of fishing is targeted fishing, which is aimed at the target audience, about which information is specially collected to make the message addressed to it more convincing. This type of fishing is characterized by the following stages: planning, preparation, attack, collection, fraud, completion stage. At the planning stage, the attacker conducts some research on the victim or group of victims, selects vulnerabilities and analyzes them.

The preparation stage is characterized by compiling a phishing letter, or creating a phishing website and developing means of attack. At the stage of the attack, the attacker sends a fishing e-mail or malware. The next stage is the collection of information by malicious software and the subsequent analysis of the collected information. The stage of fraud is characterized by the sale of collected information, blackmail. In the final stage, the attacker eliminates the evidence and sweeps away the traces.

- Corporate fishing. It is characterized by the creation of websites that look like a complete copy of the original but have a different domain address. Such websites narrowly define the class of victims of fishermen. The main purpose of the fishermen is to make the victim perceive the fake website as legal and provide information about personal data. The purpose of the scammer is either to gain access to the protected site, or to disguise his

real identity. In this case, the scammer can steal the victim's address, falsifying information about the routing of the message, so that it seems that it came from the victim's account instead of his own (Rusch, 2005)

Fraud in the field of online auctions. Of all the types of online fraud in the field of computer information, online auctions come first. Mostly mythical lots are exhibited at online auctions, when a non-existent thing is behind the picture and description on the monitor screen. With the help of online auctions, gullible buyers are willing to spend thousands of dollars for a fictitious lot. The procedure of fraudulent actions is that the goods are exhibited at a lower price than the common kind of goods, but not so much that the victim is suspicious.

Use of fictitious e-commerce entities. Quite a common type of fraud, represented by one-page websites with a unique price offer for any product. As a rule, fictitious online stores operate on a partial or 100% prepayment. Accordingly, the victim, having transferred funds, does not receive the necessary goods. Then the site is blocked, and then "moves" to another hosting or changes the domain name and continues its illegal activities. Such a site can be filled with a lot of fake reviews in order to create the image of a bona fide online store and mislead potential victims. This type of fraud is one of the simplest methods of criminal activity on the Internet and causes great damage to the financial capacity of vulnerable and ignorant citizens, given their low level of information literacy (Sergeev, Lyubimenko, Savvateeva, 2020).

Crimes in the field of intellectual property

Internet piracy. The U.S. Copyright Act defines Internet piracy as the use of the Internet to illegally copy and / or distribute software (Copyright Law of the United States, 1999) The main purpose of Internet piracy is to profit from such activities. On the Internet, Internet pirates can make a profit from providing paid access to materials that are in private access or are paid at a price much lower than the price offered by the author. Internet pirates can also provide access to copyrighted materials for free, and make a profit by advertising on the resource where the pirated materials are posted, or even integrate advertising directly into pirated materials. In the worst case, pirated files may contain virus programs as a result of obtaining personal data that an attacker may use at its discretion. In our opinion, Internet piracy is the use of Internet space for illegal copying, hacking and distribution of video content, audio content, literary works, software and other types of digital products that are placed on the Internet for further distribution on both paid and free basis.

One of the types of crimes in the field of intellectual property is card sharing. Cardsharing is the provision of illegal access to satellite and cable TV.

Crimes in the field of information security.

The following features are characteristic of crimes in the field of information security: heterogeneity of the object of encroachment (in practice we have that the object of crimes in the field of information security is not only computer information but also national security, public safety, economic sphere) , the use of computers as both the subject and method of committing a crime, the use of computer information as a means of committing a crime and as an object of crime.

The creation, distribution and sale of malicious software are usually combined with this type of crime in the field of computer information. It is, first of all, the conscious creation and use of such software, which allows: blocking, destruction, modification of computer information, copying of protected data.

Examples of such projects are locker viruses, Trojan viruses, clipper viruses, styler viruses, keylogger viruses. Locker viruses, or malware as they are called, are viruses that completely block the system when you get on your computer or phone. However, even after paying the attacker money and receiving a password to unlock, the victim's device system is completely destroyed.

Clipper viruses are a type of virus that replaces a victim's card or electronic account with an attacker's account, and when transferring funds, the victim actually transfers money to the attacker.

Virus stylists are a type of virus that steals information from your browser and makes an imprint of the victim's browser on the attacker's server. With such data, the attacker can easily use the full range of information contained in the victim's browser, from actions on social networks to buying goods at the expense of the victim.

Forgery of computer information. Creation, alteration, destruction, concealment of computer

data or computer programs or other interference with the processing of data in various ways, or the creation of conditions which, under national law, would constitute an offense such as forgery in the traditional sense.

Damage to computer data or computer program data. Unauthorized destruction, damage, or deterioration of computer data or computer programs.

Modification of computer data or computer program data Unauthorized modification of computer data or computer programs.

Computer espionage. Acquisition by illegal means or by unauthorized disclosure, transfer or use of a trade or commercial secret for the purpose of causing economic harm to a person entitled to the secret or gaining an illegal economic advantage for himself or a third party.

Illegal use of protected information.

Use a legally protected computer program without permission or illegally reproduce it for economic gain for yourself or a third party, or with the intent to harm the lawful owner of the program (Bolgov, Gladun, 2015).

Conclusions

Summarizing the above, it should be emphasized that crimes in the field of computer information are one of the most dangerous cybercrimes of our time, which is primarilo cause financial harm to individual users and organizations, and can pose a threat to national and international security. The public danger of crimes in the field of computer information is due to their main features, namely: latency, transnational nature, remoteness and reduced age of criminal liability.

According to the purpose of the study, the definition of the concept of crime in the field of computer information, namely, we propose to understand them as intentional socially dangerous, illegal, culpable acts that encroach on and harm public relations governing the storage, dissemination, use of information and their protection. We also highlighted the main specific features of computer information crimes, namely latency, remoteness, transnationality, reduced age of criminal responsibility and the use of social engineering skills. We have also proposed a classification of crimes in the field of computer information, we consider the following classification urgent: crimes in the field of payment systems, fraud in the field of computer information, crimes in the field of intellectual property, crimes in the field of information security.

It is worth noting that due to the complex and specific nature of crimes in the field of computer information, there is no single universal model for identifying all possible categories of threats and directly investigating this type of crime, as evidenced by disappointing statistics.

The current state of cybercrime is dynamically transforming and adapting to the realities and needs of today, and therefore society and the state face new and new challenges that require immediate legal, organizational intervention to protect financial institutions, the banking sector and cyberspace in general. In today's world, the problem of computer information crime cannot be solved without legal countermeasures and norms of international cooperation.

Bibliographic references

Aghatise, E.J. (2008) Cybercrime Definition. Computer Research Center, Retrived from https://www.researchgate.net/publication/265350281_Cybercrime_definition#:~:text=Cybercrime%20is%20defined%20as%20crimes,murder%20or%20theft%20need%20not

Baturin, Y.M. (1991). Computer crime and computer security. M.: Legal Literature. Recovered from: https://ua1lib.org/book/3215802/04b963

Begishev, I. R. (2017). Concept and types of crimes in the sphere of digital information circulation. (PHD thesis). Kazan (Volga Region) Federal University. Recovered from: https://www.prlib.ru/item/1156241

Bessonov, V.A. (2000). Victimological aspects of crime prevention in the field of computer information. (Doctoral thesis). Nizhny Novgorod Law. Inst. of the Ministry of Internal Affairs of the Russian Federation. Recovered from: https://rusneb.ru/catalog/000200_000018_RU_NLR_bibl_294121/

Bolgov, V.M., & Gladun, O.Z. (2015). The competence of the National Securities and Stock Market Commission in countering the legalization (laundering) of obtained incomes by criminal ways. Revision of the National Institute of Justice, 2(33). Recovered from: https://ibn.idsi.md/sites/default/files/imag_file/28_32_Kompetentsiya%20Natsionalnoy%20komissii%20po%20tsennyim%20bumagam%20i%20fondovomu%20ryinku%20v%20sfere%20protivodeystviya%20legalizatsii%20%28otmyivaniyu%29%20dohodov_poluchennyih%20prestupnyim%20putem.pdf

Borovukiv, V.B. (2015). Criminal Law. Kharkiv: Odyssey. Recovered from: https://stud.com.ua/53996/pravo/zagalna_chastina

Copyright (1999). Copyright Law of the United States Title 17. Recovered from: https://www.copyright.gov/title17/

Cyber police in Ukraine. (2018). Official Web site. Recovered from: https://cyberpolice.gov.ua/results/2018/

Dobrovolsky, D.V. (2005). Actual problems of combating computer crime: Criminal-legal and criminological problems. (PHD thesis). Modern HUmanitarian Academy, Moscow. Recovered from: http://www.dslib.net/kriminal-pravo/aktualnye-problemy-borby-s-kompjuternoj-prestupnostju-ugolovno-pravovye-i.html

Dictionary of banking terms. (2022). Banki. Recovered from: https://www.banki.ru/wikibank/skimming/

Klochko, A.N., Kulish, A.N., & Reznik, O.N. (2016). The social basis of criminal law protection of banking in Ukraine. Russian Journal of Criminology, 10(4), pp. 790–800. Recovered from: https://essuir.sumdu.edu.ua/handle/123456789/49217

Kumar, A., Chatterjee, J.M., & Díaz, V.G. (2020). A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. International Journal of Electrical and Computer Engineering (IJECE), 10(1), 486–493. doi: 10.11591/ijece.v10i1.

Kurushin, V. D. (1998). Computer crimes and information security. M.: New lawyer. Recovered from: https://www.twirpx.com/file/587744/

Lyadskiy, V.V. (2014). Crimes in the field of computer information. Electronic Bulletin of the Rostov Socio-Economic Institute, № 6. Recovered from: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii

Law № 2341-III. Criminal Code of Ukraine. Information of the Verkhovna Rada of Ukraine, № 25-26, 2001. Recovered from: https://zakon.rada.gov.ua/laws/show/2341-14

Michael, A.D. (2019). Cybercrime: Facts & Related Content. The Information Architects of Encyclopaedia Britannica. Recovered from: https://www.britannica.com/facts/cybercrime

Privat Bank (2022) Official site. Recovered from: https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva#:~:text=3.,4.

Rusch, J. (2005). The compleat cyber-angler: A guide to phishing. Computer Fraud & Security, (1), 4-6. doi: 10.1016/S1361-3723(05)00145-4.

Sergeev, D.R., Lyubimenko, O.A., & Savvateeva, O.V. (2020). Fraud on the internet as threat to economic security States. Theoretical Economics, 3, 76-84. Recovered from: https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kak-ugroza-ekonomicheskoy-bezopasnosti-gosudarstva/viewer

Smirnova, T. G. (1998). Criminal law fight against crimes in the field of computer information. (PHD thesis). Academy of Management of the Ministry of Internal Affairs of Russia. Recovered from: http://www.dslib.net/kriminal-pravo/ugolovno-pravovaja-borba-s-prestuplenijami-v-sfere-kompjuternoj-informacii.html

Vakulyk, O.O., Andriichenko, N.S., Reznik, O.M., Volik, V.V., & Yanishevska, K.D. (2019). International aspect of a legal regulation in the field of financial crime counteraction by the example of special services of Ukraine and the CIS countries. Journal of Legal, Ethical and Regulatory Issues, 22(1). Recovered from: https://www.abacademies.org/articles/international-aspect-of-a-legal-regulation-in-the-field-of-financial-crime-counteraction-by-the-example-of-special-services-of-ukr-7870.html

Verjovna Rada de Ucrania (2001). Cybercrime Convention: Convention, International document Voice of Ukraine from № 9-10. Recovered https://zakon.rada.gov.ua/laws/show/994_575#Text

Voitko, B.S., Marchenko, M.M., & Antonov, Yu. S. (2020). Social engineering as a tool for penetration into the information system of enterprise. Applied aspects of the use of information systems, 1. Recovered from: https://jait.donnu.edu.ua/article/view/9023

Yurchuk, A.M. (April, 2017). Types of cybercrime. In Korsun Yaroslav Petrovich (Presidency), VII regional interuniversity student scientific "practical conference" problems of ukrainian society: cyber crime. Separate structural subdivision "Rivne College of the National University of Life and Environmental Sciences", Rivne. Recovered from: http://prog-rdak.16mb.com/wp-content/uploads/2017/04/kiberzlochunu.pdf