Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Forensic Research of the Computer Tools and Systems in the Fight against Cybercrime

Serhii Drobotov *

*Corresponding Author, Department of criminal law policy and criminal law, Institute of Law Taras Shevchenko National University of Kyiv, Kyiv. E-mail: serhdrobotov@gmail.com

Roman Pertsev

Candidate of Juridical Scienses, practicing lawyer, Kiev, Ukraine. E-mail: romanpert sev82@gmail.com

Mariia Hrab

Attorney at law, partner of the bar association «Legal strategy». E-mail: grab-maria-00@ukr.net

Vasyl Fedytnyk

Department of Law, Institute of Lviv Interregional Academy of Personnel Management, Lviv, Ukraine. E-mail: Fedytnykvv@gmail.com

Svitlana Moroz

Department of Law Enforcement and Combating Corruption, National Research Institute of Law of Prince Volodymyr the Great, Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: s_moroz@gmail.com

Mariia Kikalishvili

Department of the State guard of Ukraine, Taras Shevchenko National University of Kiev, Kyiv, Ukraine. E-mail: balambon9@gmail.com

Abstract

The cybersecurity in the modern world has become global, and cyber attacks are becoming more complex and large-scale. In the system of civil and criminal justice, computer forensics helps to ensure the integrity of digital evidence presented in court cases. The purpose of this study is to develop scientifically sound proposals and recommendations for the implementation of tools for forensic research of computer tools and systems in the fight against cybercrime. The relevance of this study is due to the need to implement active ways to protect and combat cybercrime. To achieve the goal of the study, methodological principles

and approaches of legal science were used. It is proposed to use computer forensic methods more widely research in the fight against cybercrime.This study identifies the types of computer forensics: forensics database; electronic forensics; malware forensics; criminology of memory; mobile forensics; network forensics. The authors foundlack of a regulatory mechanism to regulate cybersecurity, capture and use of digital evidence and the regulatory framework for international cooperation. To brought need in strengthening international cooperation and in developing appropriate policies and legislative initiatives of security and network and information systems, improvement legislation in the field countering cybercrime.

Keywords: Forensic research; Computer tools and systems; Cybercrime.

Journal of Information Technology Management, 2023, Vol. 15, Issue 1, pp. 135-162
Published by University of Tehran, Faculty of Management
doi: https://doi.org/ 10.22059/jitm.2023.90741
Article Type: Research Paper

Received: September 19, 2021
Received in revised form: October 02, 2022
Accepted: December 23, 2022
Published online: January 21, 2023

Introduction

With the development of the Internet, the cybercrime is gaining momentum. The cybercrime has cost the world economy more than $ 1 trillion in 2020 - just over 1% of world GDP (New McAfee, 2020). Compared to 2018, this figure increased by more than 50%. The cybercrime gained a special volume during quarantine, when work, shopping, and meetings went online.

The results of the Microsoft IT Cloud Security Survey conducted by the analytical company IDC in Central and Eastern Europe, due to the forced transition of most companies to remote work, significantly the number of vulnerabilities and the formation of new risks has increased (Fig. 1).

Among those surveyed, the 79% of respondents named secure remote access to corporate networks as the main risk for companies. Only 42% of companies in Central and Eastern Europe have developed a comprehensive security strategy, with the vast majority of respondents (86%) saying they are satisfied with their organization's level of cybersecurity.

This may mean that some companies have a false sense of security. It is vital that the approach to cybersecurity is dynamic, providing protection against attacks that are becoming more sophisticated with each passing day.

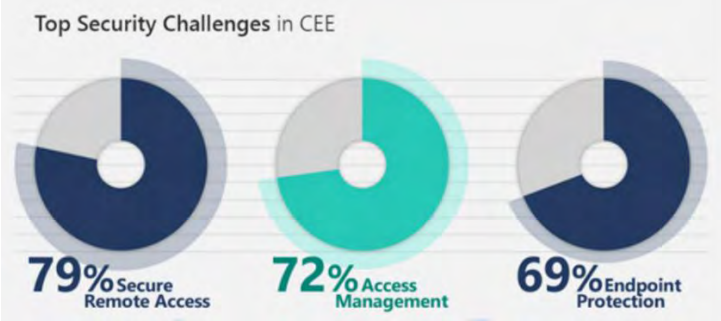

Figure 1. The key risks and vulnerabilities to cybercrime during a pandemic

By data FintechNews, the pandemic caused a surge of cyberattacks in August 2020. In particular, the number of attacks on banks increased by 238%, and 80% of companies in the world experienced an increase in the activity of criminals. According to researchers, international cyber infrastructures and data volumes are growing at an unprecedented rate, which creates difficulties for security experts and law enforcement agencies investigating cybercrime (Zawoad & Hasan, 2016; Ahmed et al, 2017; Albanian et al, 2018).

The cybercrime has already become a very lucrative type of business, which is not associated with high risk. After all, the proceeds of cybercrime can exceed millions of dollars. That is why today cybercrime is the number one problem in the world. Much attention is paid to its solution, programs of cooperation between special bodies of many countries are used (James, 2017). In this regard, it is necessary to implement active ways to protect and combat cybercrime. According to experts, one of the factors influencing the level of information security is cloud solutions: 54% of respondents said they plan to switch to cloud technology within two years (Barrett, 2020).

The cybercriminals use many methods - theft of personal data for profit and blackmail, data leakage, distributed denial of service and attacks by malware on medical devices and smart vehicles (Parker, 2007; Berghel, 2012; Gradon, 2013).

The cyberattacks can have a significant socio-economic impact on both global businesses and individuals. Therefore, the cybercriminals should be identified immediately, and high-quality evidence of attacks should be available in the courtroom (Gaggero et al, 2019). At the same time, cybercriminals are very difficult to identify, which constantly creates additional risks for business, is a significant problem that governments in many countries cannot solve (ACPO, 2012).

The forensic feature of cybercrimes is that their investigation and detection is impossible without the use and application of computer technology. There is a need for accurate, rapid response and search, recording, seizure and collection of evidence in electronic form, as well as operational and investigative measures (Oppliger et al, 2017). To prevent and combat

cybercrime, it is necessary to systematically train qualified specialists capable of protecting the interests of the state.

Due to the constant increase in cyber and digital crimes, the digital forensic investigation (DFI) has already become a profession and a scientific field of activity (Adu & Adjei, 2018). Although the field of digital forensics is now well established, its research community can be considered relatively new, compared to related fields of traditional forensics and computer science (Apau & Koranteng, 2019). DFI includes a variety of digital investigation processes, including the identification, storage, analysis, documentation, and presentation of digital evidence. These processes must be carried out reliably and legally in order to withstand the review of legal review in the courts. Around the world, many institutions rely on digital storage media (Baylon & Antwi-Boasiako, 2016). Information is now processed, stored and exchanged using these media. As the use of digital media for storage is rapidly expanding, there has been a corresponding increase in computer crime and cyber-fraud (Becker et al, 2010). This growth has exacerbated the challenges facing law enforcement and security forces around the world. The factors that affect the increase in threats in cyberspace are: an active establishment and building of opportunities for cyber influence by leading states; a development of organizational structures of these states, increase in the number of units and their composition involved in the cybersecurity system of the world. At the same time, non-state resources are actively involved in cybersecurity activities; an active development of cyber weapons and implementation with its use of certain actions in cyberspace; an increasing opportunities for covert execution of cyberattacks and cyber operations by opposing parties; an increased influence of states on the national information spaces of other states, network traffic by means of access to global information networks; an active development of information technologies on a global scale, including in the interests of cyber defense, cyber influence, execution of cyber operations in general.

The internal factors that limit the state's ability to counter the negative impact in cyberspace are:

≠ an underdevelopment, moral and physical obsolescence, vulnerability to the illegal influence of the existing information infrastructure, information and telecommunication networks and systems;

≠ an active introduction and use in the state of information technologies (systems, products) of foreign origin, which do not guarantee the appropriate level of security of use and are difficult to control;

≠ the difficulty of distinguishing between military and civilian critical infrastructure of the state in cyberspace;

≠ the possibility of non-state actors and individual users to carry out illegal cyber influences in cyberspace and the difficulty of their detection;

≠ a violation of the procedure for the exchange of information with limited access in the field of defense established by national legislation;

≠ insufficient regulatory and legal regulation of the activities of the subjects of cyber security of the state;

≠ an insufficiency in view of the growing volume of tasks of both the quantitative and qualitative composition of the forces (units) of the subjects of cyber security of the state, and qualified specialists for staffing.

All the above requires the formation and implementation in the state of a single integrated approach to the further development and functioning of the national cybersecurity system, which should determine (specify) its purpose, principles, directions, main tasks, procedures for creating and operating the necessary organizational structures, training and management armed confrontation in cyberspace, other issues of the cyber security of the state. The purpose of the study is to develop scientifically sound proposals and recommendations for the introduction of tools for forensic research of computer tools and systems in the fight against cybercrime.

The object of study are public relations that arise in the implementation of information processes on the production, collection, processing, accumulation, storage, retrieval, transmission, distribution and consumption of computer information, as well as in other areas where computers are used, computer systems and networks. Subject of study - features of criminal offenses in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks and countermeasures against cybercrime.

One of the main issues is to consider the jurisdiction of cybercrime, as the digital world does not have clearly defined borders and geographical areas. For this reason, the principle of nationality is usually used to determine jurisdiction, for example, it may be related to the nationality of the offender (active personality principle) or the nationality of the victim (passive personality principle). What most countries have in common is that ISPs are required to store user data and provide it to investigators upon request. Some countries assign jurisdiction even for a crime committed in another state, if it has affected the interests and security of the country abroad (protective principle). The study examines the experience of Ukraine through the prism of world experience countering cybercrime.

Literature Review

The cybercrime involves a wide range of illegal activities, from fraud and threats to the individual, to crimes resulting from hatred and drug trafficking (Boateng et al, 2011).

Table 1 presents the main terms and categories of the research question.

The cybercriminals use computer technology to access personal information and trade secrets, and use the Internet for operational or malicious purposes. Different types of criminals can also use computers to communicate, along with storing documents or data. The common forms of cybercrime include theft of online banking data, identity theft, cybercrime, and unauthorized access to a computer, along with serious and even bigger problems such as cyberterrorism.

Table 1. The terms and categories of issues of combating cybercrime

Terms and categories	**Definition**	**Source**
Cyberspace	a set of interconnected information resources, software, databases and data banks processed in computer networks and related infrastructure, together with the objects that fall under their control and management	Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.
Cybersecurity	protection of vital interests of man and citizen, society and state during the use of cyberspace, which ensures sustainable development of information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to national security of Ukraine in cyberspace	Draft of the Cybersecurity Strategy of Ukraine (2021-2025)
Cybersecurity system	interconnected by common goals and objectives for the realization of national interests in cyberspace, a set of bodies, which as a result of joint, agreed on the principles and methods of activity achieve common results using the inherent forms and methods of subject competence defined in law	Law of Ukraine "On Basic Principles of Cyber Security of Ukraine"
Organizational providing a cybersecurity system	characterized by the place and role of special entities (relevant government agencies and their specialized units), their functions, powers, as well as the grounds, conditions and directions of their interaction in the implementation of security measures in cyberspace	Draft of the Cybersecurity Strategy of Ukraine (2021-2025)
Cybersecurity	a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detection and protection against cyber attacks, elimination of their consequences, restoration of sustainability and reliability of communication, technological systems	Law of Ukraine "On Basic Principles of Cyber Security of Ukraine"
Cybercrime (computer crime)	socially dangerous criminal act in cyberspace and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine	

From the point of view of fundamental legal doctrine, cybercrime consists of criminal acts committed with the help of electronic information and communication means.

In other words, the cybercrime can be any traditional offline crime (such as theft, fraud, money laundering), but committed on the Internet. Some researchers also single out "hybrid"

or "cyber-driven" crimes and cyber-dependent crimes, which have become possible only through the development of the Internet and related digital technologies (Dolliver et al, 2017).

In Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" the cybersecurity is defined asprotection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace. At the same time, the cybersecurity is a set of organizational, legal, engineering and technical measures, as well as cryptographic and technical information protection measures aimed at preventing cyber incidents, detecting and protecting against cyberattacks, eliminating their consequences, restoring the stability and reliability of communication and technological systems. The cybercrime (computer crime) - a socially dangerous criminal act in cyberspace and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine. Conventionally, cybercrime is divided into:

≠ traditional, carried out with the help of computer technology and the Internet (computer fraud, illegal collection of information constituting a trade secret, through unauthorized access to computer information);

≠ new crimes that have become possible thanks to the latest computer technology (crimes under Section XVI of the Criminal Code of Ukraine).

The main types of cybercrime are presented in Figure 2.

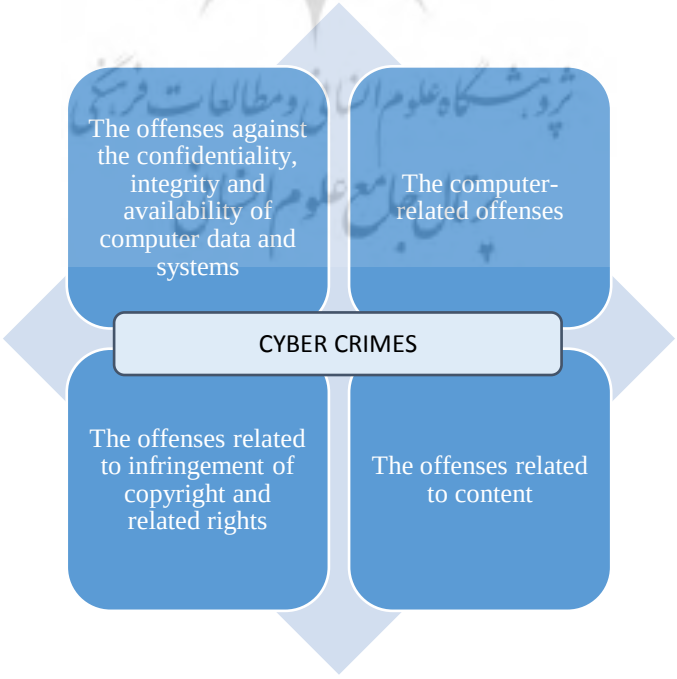

Figure 2. Types of cybercrime

There are four main types of cybercrime:

≠ • the offenses against the confidentiality, integrity and availability of computer data and systems - illegal access, illegal interception, data interference, system interference, device abuse;

≠ • the computer-related offenses - computer-related counterfeiting, computer-related fraud;

≠ • the offenses related to content - offenses related to child pornography;

≠ • the offenses related to copyright and related rights infringement.

≠ The section XVI of the Criminal Code of Ukraine classifies cybercrimes into:

≠ Part 3 of Art. 190 (fraud committed through illegal transactions using electronic computers);

≠ Art. 200 (use of counterfeit electronic means of access to bank accounts);

≠ Part 4 of Art. 301 (sale and distribution of pornographic items using computer technology).

≠ The following traditional crimes are most often committed using computers and the Internet:

≠ infringement of copyright and related rights (Article 176);

≠ fraud (Article 190);

≠ illegal actions with documents for transfer, payment cards and other means of access to bank accounts, equipment for their production (Article 200);

≠ evasion of taxes, fees and mandatory payments (Article 212);

≠ import, production, sale and distribution of pornographic items (Article 301);

≠ illegal collection for the purpose of use or use of information constituting a commercial or banking secret (Article 231).

The Criminal Code of Ukraine provides for criminal liability for:

≠ Unauthorized sale or distribution of restricted information stored in computers, automated systems, computer networks or on such media (art. 361);

≠ creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale (Article 361-1);

≠ Unauthorized sale or dissemination of restricted information stored in computers, automated systems, computer networks or on media such information created and protected in accordance with applicable law (Articles 361-2);

≠ unauthorized actions with information that is processed in computers (computer), automated systems, computer networks or stored on media of such information, committed

by a person who has the right to access it (Article 362);

≠ violation of the rules of operation of electronic computers, automated systems, computer networks or telecommunication networks or the order or rules of protection of information processed in them (Article 363);

≠ interfering with the work of electronic computers (computers), automated systems, computer networks or telecommunication networks by mass dissemination of telecommunication messages (Article 363-1).

Thus, in the forensic aspect, cybercrime (computer crime) is a socially dangerous criminal act in cyberspace and / or with its use, liability for which is provided by the Law of Ukraine on Criminal Liability and / or which is recognized as a crime by international treaties of Ukraine (On the basic principles of cybersecurity of Ukraine: the Law of Ukraine of October 5, 2017 № 2163-VIII).

The object of cybercrime, defined in the Criminal Code of Ukraine, is part of the information relationship, which can be defined as information relations, the means of which are computers, systems, computer networks and telecommunications networks. Thus, cybercrimes affect information relations with the use of special technical means. The current criminal law today lists four types of such means:

≠ the computer - a functional device consisting of one or more interconnected CPUs and peripherals and can perform calculations without human intervention;

≠ the automated system - an organizational and technical system consisting of means of automation of a certain type (or several types) of activities of people and personnel performing these activities;

≠ the computer network - a set of geographically dispersed data processing systems, means and (or) systems of communication and data transmission, which provides users with remote access to its resources and the collective use of these resources;

≠ the telecommunication network - a set of technical means of telecommunications and facilities designed for routing, switching, transmission and / or reception of signs, signals, written text, images and sounds or messages of any kind by radio, wired, optical or other electromagnetic systems between the terminal equipment.

Depending on these means, information relations are of the following types: with the use of computers; computer systems; computer networks; means of communication - telecommunication networks.

The terms "digital forensics" and "cybercriminal", "cybercrime", "crimes in the field of IT technologies", "high-tech crimes", "internet crimes", "computer crimes", "crime in the field of high technologies", "e- crimes " are often used as synonyms for computer forensics.

The computer forensics is essentially the recovery of data by means of law enforcement instructions to make information acceptable in court. At the heart of computer forensics - the use of methods of investigation and analysis to collect and store evidence from a particular computer device in a way that is suitable for presentation in court. The purpose of computer forensics is to conduct a structured investigation and support documented chains of evidence in order to find out exactly what happened on the computer and who was responsible for it (Babenko et al., 2021).

The digital forensics begins with gathering information in a way that maintains its integrity. The investigators then analyze the data or system to determine if it has changed, how it has changed, and who made the change.

The use of computer forensics is not always associated with crime. A forensic process is also used as part of data recovery processes to collect data from an emergency server, a failed drive, a reformatted operating system, or another situation where the system has suddenly stopped working.

Therefore, the main challenges in combating cybercrime are the following:

≠ changes in the paradigms of modern legal sciences, which requires the development of proposals for,,implementation of the best,,practices of the regulatory framework of the advanced countries of the world, interaction and interaction of international, integrative and national legal orders to ensurecountering cybercrime;

≠ the need to strengthen law enforcement activities that update the application, as appropriate, of existing provisions of domestic law and international law on crimes committed online;

≠ issues of continuous improvement of domestic legislation - in order to criminalize cybercrime acts and provide law enforcement agencies with procedural powers to investigate alleged crimes in compliance with appropriate procedural guarantees, principles of privacy, civil liberties and human rights;

≠ request for the development of internal procedural law - in accordance with the development of technology, providing law enforcement agencies with appropriate equipment to combat cybercrime;

≠ the need to develop public-private partnership mechanisms in the fight against cybercrime, including through legislation and channels for dialogue, to promote cooperation between law enforcement, communications service providers and academia in order to deepen knowledge and increase the effectiveness of measures to combat cybercrime;

≠ the need to build capacity (technical, intellectual, personnel, communication, etc.) in order to increase the effectiveness of investigations, improve understanding of cybercrime and available technical means and technologies to combat it;

≠ compliance with the needs of the time to create the conditions for prosecutors, judges and central national authorities to properly prosecute and adjudicate in cases involving such crimes.

Methodology

The basis of this study was methodological principles and approaches of legal science, which were used to solve the tasks.

The dialectical method was used in the work, as a general scientific method of cognition of social and legal phenomena in their contradictions - to determine the peculiarities of the criminal-legal qualification of crimes in the use of electronic computers, systems and computer networks and telecommunications networks. The logical-semantic method was used to study the main features of the criminal law qualification of cybercrime.

The system-structural method allowed to identify problematic research issues. The statistical method was used in the process of generalization, grouping and analysis of empirical material and evaluation of quantitative and qualitative indicators of the current state of crime in Ukraine. The application of the comparative method made it possible to study the experience of foreign countries in the fight against cybercrime.

Empirical basis the research consists of statistical data of the General Prosecutor's Office of Ukraine, the Ministry of Internal Affairs of Ukraine, the State Statistics Service of Ukraine for the period 2010-2020; selective analysis of materials of criminal proceedings (cases) for the period 2010-2020 under articles 361-363-1 Of the Criminal Code of Ukraine.

Results

Current trends in cybercrime: the situation in Ukraine, world experience

According to experts in the field of information technology, the situation with cybercrime in the world is deteriorating. The cybersecurity in the modern world has become global. The cyberattacks are becoming more complex and large-scale. The EU Cyber Security Agency (ENISA) has published a report on cyber incidents for the period 2019-2020. It follows that the geography of cyber attacks is constantly expanding, they are becoming more sophisticated, targeted, widespread, it is becoming increasingly difficult to identify customers. Cybercrime has increased dramatically with the introduction of artificial intelligence and machine learning technologies.

The cybercriminals infiltrate target systems using AI and ML (Machine Learning) in their malware. That is, cybercriminals will use artificial intelligence to carry out their intentions in the same way as in any sector, enhancing its ability to find and exploit vulnerabilities.

Deepfeak technology is becoming even more sophisticated and realistic, which could potentially call into question the results of video surveillance. The development of cybercrime also extends to proven methods, such as phishing lures, that will be harder to spot. As a result, company employees become even more vulnerable to these types of attacks. Among them will need to be constantly trained and reminded of the techniques developed in the field of cybersecurity.

The cybercrime statistics are deteriorating. The leader in the number of cyber attacks is the United States - 35.4% of the global cybercrime rate. In second place is South Korea - 12.8%; followed by China - 6.9%; Germany - 6.7%; France - 4%, Great Britain - 2.2% of the total cyberattack rate.

The most common types of cyberattacks in the world are: software viruses, computer viruses, self-replicating and other forms of software code failures. That is, the highest level of cybercrime are countries with the highest level of technological development, as it has the largest number of users (Budhijanto, 2019).

Regarding the state of cybercrime in Ukraine, c*accordi*ng *to the statistics of the Prosecutor General's Office of Ukraine,* during 2010-2018 we have a tendency to increase.

For example, in 2018, 2,301 the criminal offenses in the field of the use of electronic computers, systems and computer networks and telecommunication networks were registered, 1,330 CP for such offenses were sent to court with an indictment (Fig. 3).

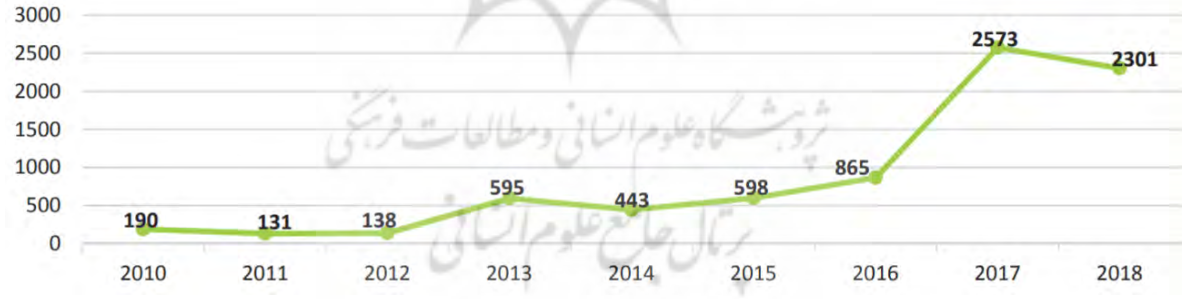

Figure 3. The number of reported criminal offenses in the field of cybercrime

The share of recorded criminal offenses in the use of electronic computers (computers), systems and computer networks and telecommunications networks from the total number of recorded criminal offenses also tends to increase (Fig. 4).

Figure 4. The share of recorded criminal offenses in the field of cybercrime in the total number of recorded criminal offenses

The analysis of the data of the official statistical reporting showed that the overwhelming majority in the structure of the investigated cybercrimes are those crimes for which the responsibility under Art. 362 of the Criminal Code of Ukraine (46.5%). In second place - the crimes under Art. 361 of the Criminal Code of Ukraine (44.5%). In third place - the crimes under Art. 361-1 of the Criminal Code of Ukraine (5.8%). On the fourth - the crimes provided by Art. 361-2 of the Criminal Code of Ukraine (2.3%). All other crimes in the field of use of electronic computers, systems and computer networks and telecommunication networks account for 0.5%. According to the Cyberpolice Department of the National Police of Ukraine, in 2018 the spread of 4 mass cyberattacks on the territory of Ukraine was prevented. In 2017, a number of cyber operations were carried out against Ukraine, the main of which were: BugDrop; "WannaCry" (known as "WannaCwt"); "NotPetya" (also known as "Petya. A", "Petya"). In 2019, the 32156 criminal cases of fraud were registered. The fight against Internet piracy continues: in 2018, more than 40 pirate sites were shut down. Within the framework of international cooperation, 8 transnational hacker groups were exposed and more than 30 international operations took part. During the period from January to November 2020, the 42563 criminal proceedings were registered on the facts of fraud. Such data indicate an overall increase in these offenses compared to 2019.

According to industry research, in 2020, 99% of organizations in the world survived attacks using mobile viruses due to the spread of remote control during the COVID pandemic.

According to calculations OpenDataBot, over the years the number of information crimes increased what at least 2.5 times. During the development of the new Cyber Security Strategy of Ukraine, an analytical study was conducted using an online survey of key cybersecurity actors, critical infrastructure facilities, enterprises of the real sector of the economy, financial sector, services, etc. (Assessment of the state of development of the national cybersecurity system, 2021; Gontareva et al., 2020).

An assessment of the readiness of organizations for modern cyberattacks. To do this, respondents on a scale of 1 to 10 assessed the level of readiness in different areas. Grades from 1 to 4 were defined as low, from 5 to 7 as average, from 8 to 10 as high.

The generalized results are shown in fig. 5.

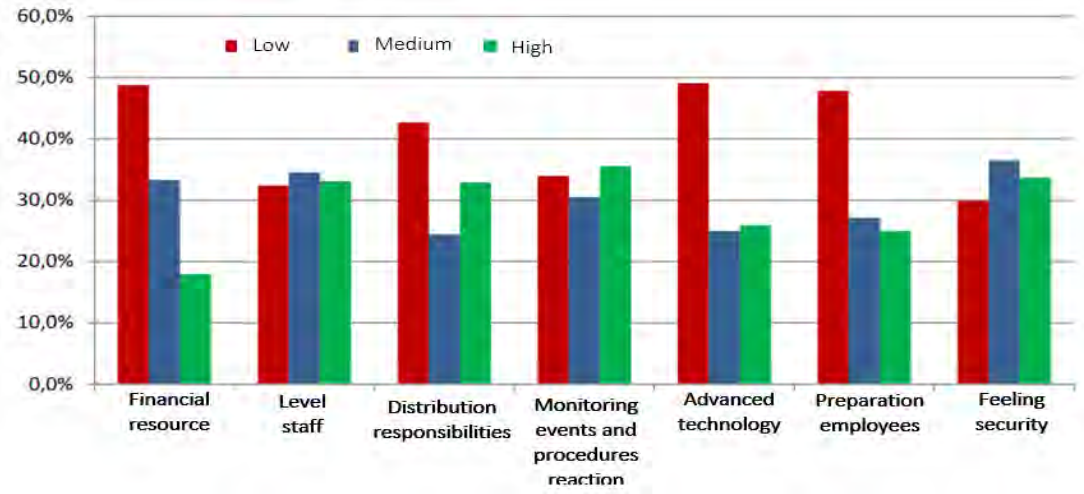

Figure 5. Assessments of readiness of organizations for modern cyberattacks, Ukraine, 2021

The lowest level of readiness of organizations is observed in terms of the introduction of advanced technologies in the field of cybersecurity, adequacy of financial resources and efforts of organizations to improve the skills of employees in the field of cybersecurity (Vovk et al., 2020). Despite the high level of competencies of information security and cybersecurity specialists of the surveyed organizations, most respondents feel safe. At the same time, the most organizations monitor security events and define procedures for responding to cyber incidents.

However, as the results of the analysis showed, in most organizations there is no formalized division and the functions of information security and information technology units are not fixed in the administrative documents.

The generalized assessment of the level of readiness of organizations (by forms of ownership) to modern cyberattacks (in different directions) presented in Figure 6.

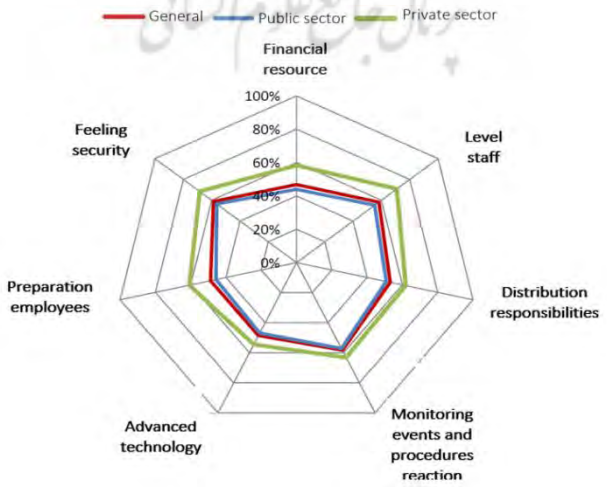

Figure 6. Assessment of the readiness of organizations (by form of ownership) to of modern cyberattacks, Ukraine, 2021

The generalized assessment of the level of readiness for modern cyberattacks of organizations in Ukraine is 53%, in the public sector - 51%, in the private sector - 63%. The businesses are not yet ready to fully meet the new challenges in the field of information security: more than half of companies (58%) do not have a comprehensive cybersecurity strategy.

The ability of organizations to counter cyberattacks in various areas was assessed on a scale from 1 to 10. The ratings from 1 to 4 were defined as low, from 5 to 7 - as medium, from 8 to 10 - as high. The generalized results are shown in fig. 7.

According to the results of the study, the ability of organizations to counter cyber threats is low in almost all areas. Only the ability to install updates and configure hardware to address identified vulnerabilities is considered high. Of course, the capacity of private organizations is higher (62%) than public sector organizations (45%), with an overall assessment of all respondents at 55%.

When assessing the ability to implement a cybersecurity strategy in Ukraine, it was found that a significant obstacle is the low level of interagency cooperation - only 41%, the implementation of organizational measures to comply with regulations in the field of cybersecurity is assessed (52%). 59% of companies that participated in Cisco's Future of Secure Remote Work survey acknowledged that they were hampered by a lack of employee awareness about cybersecurity. In such circumstances, even updating cybersecurity policies is difficult, as employees simply do not know how or do not follow the instructions correctly.

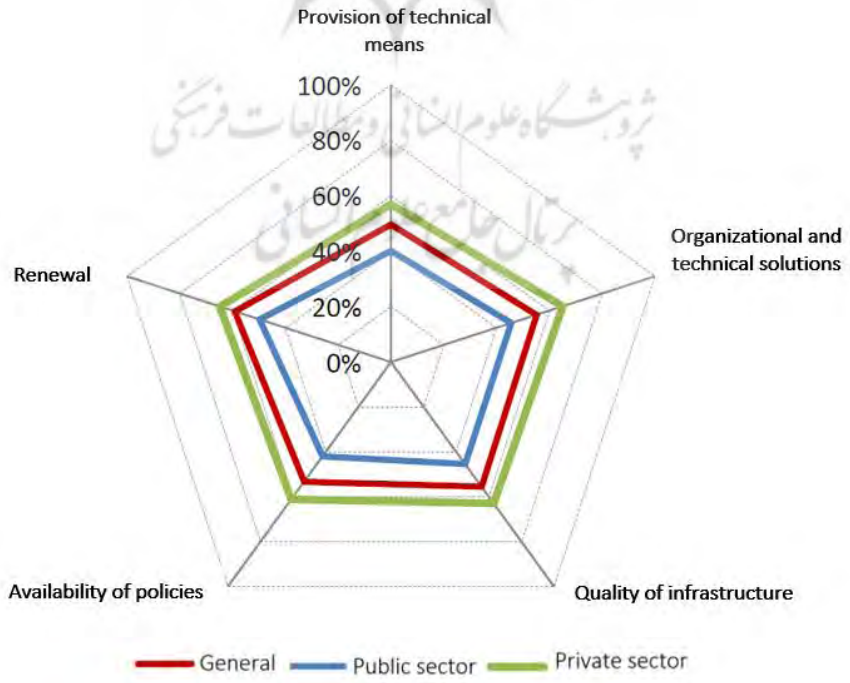

Figure 7. Assessment of the level of ability of organizations (by form of ownership) to counter cyberattacks

The low values in the public sector primarily indicate a low level of incident detection. On average, organizations spent 60.5 hours solving one incident, with a maximum of about 3 months. Some respondents said that the incident could not be resolved. A total of 128 organizations that answered the question about the time spent on resolving the incident spent more than 7,700 hours.

This state of affairs is a negative phenomenon that does not contribute to the implementation of effective measures to combat cybercrime, and, of course, requires special attention from the state.

Organized crime is increasingly using the Internet to cover up its activities. For example, the Darknet network was created as a black market platform for the sale of drugs, weapons, stolen goods and more. The technology provides network anonymity, so the Internet is uncontrolled and therefore secure for the activities of various criminal groups. According to the National Police of Ukraine, the number of organized groups and criminal organizations that commit criminal offenses using high information technology has increased by 36% over the last year.

The most common types of cybercrime are presented in table 2.

The most common types of cybercrime are: camcording; cardsharing; fake online auctions; mailing (spam); online gambling (with a deposit of money); creation of viruses; theft of personal data and personal information.The most common type of crime is fraud.

Fraud is the taking of another's property or the acquisition of property rights by deception or abuse of trust.

Table 2. The types of cybercrime

See	Characteristic
Carding	credit card fraud (credit card details) not approved by the cardholder
Phishing: SMS phishing Internet phishing	fraudulent actions aimed at extorting card details from its holder.
Viching	the attackers use card calls to extract card details
Skimming	copying payment card data using a special device (skimmer)
Shimming	Scammers use an almost invisible device that is placed inside the card reader to copy credit card data
Online fraud	fake online auctions, online stores, websites and telecommunications
Piracy	illegal distribution of intellectual property on the Internet.
Malware	creation and spread of viruses and malware.
Illegal content	content that promotes extremism, terrorism, drug addiction, pornography, the cult of cruelty and violence.
Refilling	illegal substitution of telephone traffic.
Theft of cryptocurrency	fraudulent schemes where the owner of an e-wallet gives fraudsters access to their accounts and they transfer tens of thousands of dollars to another wallet

The payment card fraud, theft of money from bank accounts, the spread of computer viruses, the theft of personal data by hackers, online drug trafficking, the fight against piracy

and the distribution of illegal content are far from the complete tasks of the Cyberpolice. In total, more than 5,000 cybercrimes were registered last year, in which 106 people involved in criminal proceedings were promptly detained, including 13 pedophiles. With regard to quarantine fraud schemes, the Cyberpolice Department notes that in December 2020 received a number of appeals from citizens about the misappropriation of money by criminals, under the guise of compensation payments to entrepreneurs.

According to the press service, the most common schemes of Internet scammers in 2020 were:

≠ sale of non-existent goods on advertising platforms;

≠ the telephone fraud. For example, an attacker under the guise of a bank employee calls a potential victim and asks for confidential information;

≠ creation of phishing resources for personal data collection.

In recent years, Ukraine has a high degree of latency of cybercrime due to industrial cyber espionage, which is ignored, as it is difficult to detect the leakage of confidential information such as personal data, information that constitutes banking or trade secrets, and so on.

The number of spam and targeted attacks on social media platforms is also increasing. In December in 2020, hackers attacked the European Medicines Agency and gained access to Pfizer / BioNTech vaccine documents stored on the Agency's server.

Cybercrime is cross-border in nature, ie the offender and the object of the crime can be located in one country or in different ones. However, the investigation of traces of cybercrime committed from other countries in relation to critical infrastructure is not allowed without the permission of the local authorities of the country from which such a crime was committed, so it is important to establish international cooperation.

Thus, attention should be paid to the lack of a legal mechanism to regulate cybersecurity, the recording and use of digital evidence and the regulatory framework for international cooperation, as some countries may not recognize acts as cybercrime and prohibit investigations on their territory.

This situation significantly increases the need for the European Union to strengthen cooperation with international partners.

The international cooperation, cyberdialogues focus more on the exchange of information on the institutional structure and powers of cyberspace authorities, on the latest developments in the development of relevant policies and legislative initiatives, including the update of the EU Network and Information Systems Directive (ISD), and partners in the development of cybersecurity policies and legislation in line with the EU legal and institutional framework.

The particular attention is paid to coordination and cooperation within international organizations to strengthen cyber resilience and ensure responsible behavior of states in cyberspace.

The legal bases countering cybercrime

The experience of the European Union

The scientists note the existence of a lag in regulatory regulation from the development of technology, which significantly contributes to the development and spread of cybercrime.

Some crimes, such as terrorism, human trafficking, sexual abuse of children and drug trafficking, have largely moved to the digital world or been controlled from the Internet. Due to this, the investigation of criminal cases in most of such criminal offenses has a digital component.

The EU has focused its efforts on the above types of cybercrime, and the Council of Europe Convention on Cybercrime has led to the emergence of the following acts:

≠ the Directive on Combating Sexual Exploitation of Children on the Internet and Child Pornography – 2011;

≠ the Directive on attacks on information systems – 2013;

≠ the regulatory proposals and directives promoting cross-border access to electronic evidence for criminal investigations – 2018;

≠ Non-cash fraud directive – 2019;

≠ Proposal on temporary regulation of the processing of personal and other data in order to combat sexual violence against children – 2020;

The Europol has also established and operates as a key body in the fight against cybercrime in the EU - the European Cybercrime Center. Its aim is to bring together European cybercrime expertise to support cybercrime investigations in the Member States.

The first EU Cyber Security Strategy, adopted in 2013, set out strategic goals and concrete actions to achieve cyber resilience, reduce cybercrime, develop cyber defense capabilities, develop technological resources and establish a coherent international cyberspace policy for the EU.

One of the foundations of the EU regulatory framework was Directive 2016/1148 on the security of network and information systems, adopted in 2016.

In the same year, the EU Global Strategy for Foreign and Security Policy was presented. The "Cybersecurity" section states that the strategic goal for the EU remains to strengthen the

institutional capacity of the EU institutions and Member States to combat cyber threats, while maintaining open, free and secure cyberspace.

The European Commission has also adopted the Cyber Security Package, which aims to achieve the following goals: to take measures to ensure cyber resilience, to develop mechanisms for cyber deterrence and cyber defense. The importance of creating effective criminal liability for cybercrime is emphasized, for which international cooperation should be developed.

In 2018, the European Parliament adopted a resolution "Fighting Cybercrime", which states that Russia and China through governmental and non-governmental institutions are planning and implementing cyber attacks on critical infrastructure of EU member states.

In May 2019, the EU Council decided to impose restrictive measures against individuals and organizations that carry out cyber attacks. Thus was born a new sanctions regime, which first worked in 2020.

Last July, the EU Council decided to impose sanctions on cyber attacks and other malicious activity on the Internet. Russian individuals were found involved in cyber attacks on OPCW resources (The Hague, the Netherlands) in April 2018. They have been banned from entering the EU and their assets have been frozen.

The Main Center for Special Technologies of the Main Directorate of the General Staff of the Ministry of Defense of the Russian Federation is recognized as involved in the implementation of cyber attacks NotPetya and EternalPetya. It is established that this center plays a key role in the cyber activities of the Sandworm branch, which carried out a cyber attack on the Ukrainian power system. In October 2020, the EU Council decided to impose sanctions on two individuals and one Russian legal entity involved in a cyber attack on the German federal parliament.

A number of countries have developed special laws aimed at combating cybercrime. For example, Germany, Japan and China have amended the relevant provisions of their criminal codes to describe and combat cybercrime.

Some countries, instead of dividing cybercrime into separate criminal acts, have simply added specific clauses to their national legislation and codes to criminalize the illicit use of digital technology to commit any crime. This approach has resulted in the offender being charged with two crimes at the same time.

The legal support of the fight against cybercrime in Ukraine

The legal basis of information security of Ukraine is:

≠ The Constitution of Ukraine;

≠ The Criminal codex of Ukraine;

≠ The Laws of Ukraine "On Basic Principles of Cyber Security of Ukraine", "About information", "On information protection in information and telecommunication systems", "On the national security of Ukraine" and other laws;

≠ The Doctrine of information security of Ukraine, the Council of Europe Convention on Cybercrimeand other international agreements, the binding nature of which has been approved by the Verkhovna Rada of Ukraine;

≠ The Cybersecurity strategyOf Ukraine for the years 2021-2025.

The cybersecurity is identified as one of the priorities in Ukraine's national security system.

In March 2021, the National Security and Defense Council approved a draft of the new Cyber Security Strategy of Ukraine for 2021-2025, which will significantly strengthen the existing institutional capacity to combat cyber threats.

The cybersecurity or cybersecurity units have been established in the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the Ministry of Internal Affairs, the National Bank, the Ministry of Infrastructure, and the Ministry of Defense (Armed Forces of Ukraine).

A new powerful actor has appeared - the Ministry of Digital Transformation, the National Telecommunication Network is being developed, secure data processing centers (data centers) are functioning, and a system for detecting vulnerabilities and responding to cyber incidents and cyberattacks has been launched.

To improve the coordination of the activities of cyber security entities, a working body of the National Security and Defense Council of Ukraine was established - the National Coordination Center for Cyber Security, whose decisions allow solving the most difficult problems in this area.

In February 2021, the Cabinet of Ministers of Ukraine launched the National Center for Reservation of State Information Resources as a pilot project.

The cyberdialogues with foreign partners have become common practice, but dialogues with the European Union have become the first format to involve one of the world's most powerful intergovernmental associations.

The computer tools and systems in the fight against cybercrime

In the system of civil and criminal justice, computer forensics helps to ensure the integrity of digital evidence presented in court cases. The computers and other data collection devices are used more often in every aspect of life. Therefore, the digital evidence and the trial used to collect, preserve and investigate it are becoming increasingly important in the detection of crimes and other legal issues.

With the digitalization of all spheres of human activity, the role of information is growing, which may be critical in resolving a legal case or crime. The computer forensics often plays a role in identifying and storing this information. The digital evidence is useful not only for detecting crimes in the digital world, such as data theft, network intrusion, and illegal online transactions. The digital evidence is also used to uncover crimes in the physical world, such as theft, assault, accident and murder. The businesses often use multi-layered data management, and network security strategies to protect their own information. Having well-managed and secure data can help streamline litigation if this data is ever investigated.

The companies also use computer forensics to track information related to system or network compromise that can be used to detect and prosecute cyber criminals. The businesses can also use digital forensics and processes to help them recover data in the event of a system or network failure caused by a natural disaster or other circumstances (Ramazanov et al., 2020).

The specialists in computer forensic research, the police are widely used computer forensic methods to keep up with the growing rates of cybercrime.

There are different types of computer forensics.

Everyone is dealing with a certain aspect of information technology (Fig. 8).

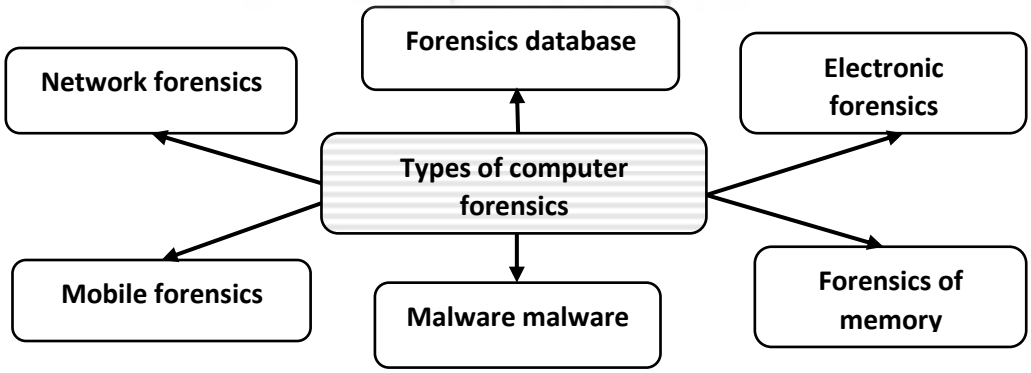

Figure 8. The types of computer forensics

Some of the main types include the following:

≠ The forensics database. Checking the information contained in databases, both data and relevant metadata.

≠ The electronic forensics. Recovery and analysis of e-mails and other information contained on e-mail platforms, such as schedules and contacts.

≠ The malware criminology. Screen code to identify possible malware and analyze their payload. Such programs may include Trojan horses, ransomware, or various viruses.

≠ The forensics of memory. Collect information stored in computer RAM and cache.

≠ The mobile forensics. Examination of mobile devices to obtain and analyze the information they contain, including contacts, incoming and outgoing text messages, images and video files.

≠ The network forensics. Find evidence by monitoring network traffic using tools such as a firewall or intrusion detection system.

The forensic investigators typically follow standard procedures, which vary depending on the context of the trial, the device under investigation, or the information that investigators are looking for. The stages of the criminological investigation are presented in Figure 9.

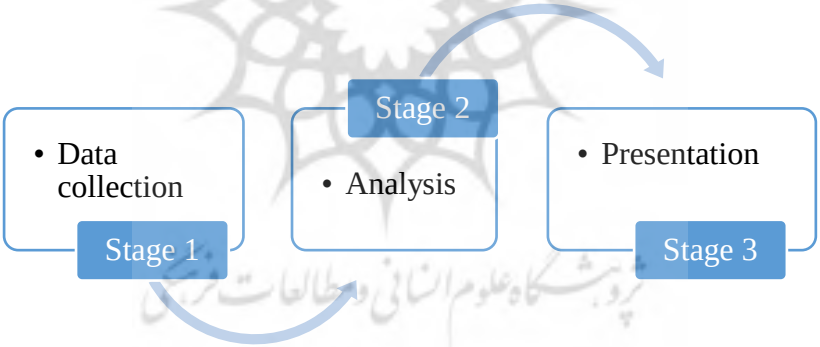

Figure 9. The stages of criminological investigation

In general, these procedures include the following three steps:

1. Data collection. Information stored electronically must be collected in such a way as to maintain its integrity. This often involves physically isolating the device under test to ensure that it cannot be accidentally contaminated or tampered with. Experts make a digital copy of the storage medium, also called forensic, and store the original device in a safe or other secure space to preserve its original condition. The investigation is conducted on a digital copy. In other cases, publicly available information may be used for forensic purposes, such as posting on Facebook or publicly accusing Venmo of purchasing illegal products or services displayed on the Vicemo website.

2. Analysis. Investigators are analyzing digital copies of media in sterile conditions to gather information for the case. The various tools are used to help with this process, including a Basis Technology autopsy to examine the hard drive and a Wireshark network protocol analyzer. The mouse jiggle is useful when scanning your computer so that it does not fall asleep or lose volatile memory data that is lost when the computer goes to sleep or loses power.

3. Presentation. The judicial investigators present their findings during court proceedings, where a judge or jury uses them to help determine the outcome of a lawsuit. In a situation of data recovery, forensic investigators represent what they were able to recover from a broken system.

The computer tools are often used in computer forensic investigations to test the results they produce. The investigators use a variety of techniques and their own forensic programs to examine a copy they made of a broken device. They search the hidden folders and unallocated disk space for copies of deleted, encrypted, or corrupted files. Any evidence found on a digital copy shall be carefully documented in the report of the findings and verified by the original device in preparation for the trial, which involves the discovery, storage or actual trial.

The computer forensic investigations use a combination of methods and expertise. Some common methods include the following:

≠ Reverse steganography. The steganography is a common tactic used to hide data in any type of digital file, message, or data stream. The computer forensic experts will cancel the steganography attempt by analyzing the hashing of the data contained in the corresponding file. If a cybercriminal hides important information inside an image or other digital file, it may look unrealized before and after to the untrained eye, but the basic hash or data string representing the image will change.

≠ Stochastic criminology. Here, investigators analyze and reconstruct digital activities without the use of digital artifacts. The artifacts are unintentional changes to data that occur as a result of digital processes. The artifacts include clues related to digital crime, such as changing file attributes during data theft. The stochastic forensics is often used to investigate data breaches, where an attacker is considered an insider who cannot leave behind digital artifacts.

≠ Cross-analysis. This technique correlates and intersects information found on many computer disks to search, analyze, and store information that is relevant to the investigation. Suspicious events are compared with information on other disks to find similarities and provide context.

This is also known as anomaly detection.

≠ Live analysis. With this technique, the computer is analyzed from the OS while the computer or device is running using system tools on the computer. The analysis looks at unstable data that is often stored in cache or RAM. Many of the tools used to obtain unstable data require the computer to be in a forensic lab to maintain the legitimacy of the chain of evidence.

≠ Recover deleted files. This technique involves searching the computer system and memory for fragments of files that have been partially deleted in one place, but leave traces in other places on the machine. This is sometimes called a file thread or data thread.

The computer forensics has become an independent field of scientific experience. According to Salary.com, the average annual salary of a computer forensic analyst is about $ 65,000. Some examples of cyber forensic career paths include the following:

≠ Forensic engineer. These specialists are engaged in the stage of collecting a computer forensic process, collecting data and preparing them for analysis. They help determine how the device has failed.

≠ Forensic accountant. This post covers crimes related to money laundering and other transactions carried out to cover up illegal activities.

≠ Cybersecurity analyst. This item applies to the analysis of data after its collection and analysis, which can then be used to improve the organization's cybersecurity strategy.

A bachelor's degree - and sometimes a master's degree - in computer science, cybersecurity or a related field is required of forensic experts. Several certificates are available in this field, including the following:

≠ Forensic analyst at the Institute of Cyber Security. This account is intended for security professionals with at least two years of experience. Testing scenarios are based on real cases.

≠ International Association of Computer Specialists. This program focuses primarily on testing the skills needed to support a business in accordance with established forensic guidelines.

≠ Forensic Investigator of the Council of the EU. This certification assesses the applicant's ability to identify perpetrators and gather evidence that can be used in court. It covers the search for and seizure of information systems, working with digital evidence and other skills in cyber forensics.

≠ Certified Computer Expert of the International Society of Forensic Computer Experts (ISFCE). This forensic program requires training at an authorized bootcamp training center, and applicants must sign the ISFCE Code of Ethics and Professional Responsibility.

Conclusion

This study examines the main aspects introduction of tools for forensic research of computer tools and systems in the fight against cybercrime. It is proved that the investigation of criminal cases in most criminal offenses has a digital component. The analysis shows that currently the ability of organizations to counter cyber threats is low in almost all areas. A significant obstacle is the low level of interagency cooperation, and the implementation of enhanced cybersecurity measures in most cases is hindered by the lack of awareness of employees on these issues.

It is proposed to use computer forensic research methods more widely in order to keep up with the growing rates of cybercrime. The following types of computer forensic examinations are distinguished: criminology of the database; electronic forensics; malware forensics; criminology of memory; mobile forensics; network forensics. A combination of special methods and expertise is used in the process of computer forensic investigations.

Therefore, there is a need strengthening minternationaloh cooperationand in developing appropriate policies and legislative initiatives of securityand network and information systems, improvement legislation in the field countering cybercrime.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Adu, K.K. & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana, Foresight, 20(2), 150-161, https://doi.org/10.1108/FS-08-2017-0043.

Ahmed, I., Obermeier, S., Sudhakaran, S. & Roussev, V. (2017). Programmable Logic Controller Forensics. IEEE Security & Privacy, 15(6), 18-24. doi: 10.1109/MSP.2017.4251102.

Albanese, M., Jajodia, S. & Venkatesan, S. (2018). Defending from Stealthy Botnets Using Moving Target Defenses. IEEE Security & Privacy, 16(1), 92-97, doi: 10.1109/MSP.2018.1331034.

Apau, R. & Koranteng, F.N. (2019). Impact of cybercrime and trust on the use of Ecommerce Technologies : an application of the theory of planned behavior, J. Cyber Criminol. 13, 228-254, https://doi.org/10.5281/zenodo.3697886.

Assessment of the state of development of the national cybersecurity system. (2021). https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/analityka_1.pdf. (Accessed 25.07.2021).

Association of Chief Police Officers (ACPO), Good practice guide for computer based electronic evidence (2012). https://www.digital-detective.net/digital-forensicsdocuments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, (Accessed 25.07.2021).

Babenko, V., Demyanenko, O., Lyba, V., Feoktystova, O. (2021). Assessment the Cost-effectiveness of Information Support for the Business Processes of a Virtual Machine-building Enterprise in the Framework of Industry 4.0. *International Journal of Engineering, Transactions A: Basics*, 34(1), 171-176. http://dx.doi.org/10.5829/IJE.2021.34.01A.19

Barrett, D. (2020). Cloud based evidence acquisitions in digital forensic education. Inf. Syst. Electron. J., 18 (6), 46-56.

Baylon, C. & Antwi-Boasiako, A. (2016). Increasing internet connectivity while combatting cybercrime: Ghana as a case study: https://www.cigionline.org/publications/increasing-internet-connectivity-whilecombatting-cybercrime-ghana-case-study. (Accessed 6.06.2021).

Baylon, C. & Antwi-Boasiako A. (2016). Increasing internet connectivity while combatting cybercrime: Ghana as a case study. https://www.cigionline.org/publications/increasing-internet-connectivity-while-combatting-cybercrime-ghana-case-study. (Accessed 6.06.2021).

Becker, W.S., Dale, W.M. & Pavur, E.J. Jr. (2010). Forensic science in transition: critical leadership challenges. Forensic Sci. Pol. Manag., 1, 214-223.

Berghel, H. (2012). Breaking the Fourth Wall of Electronic Crime: Blame It on the Thespians. Computer, 45(5), 86-88, doi: 10.1109/MC.2012.161.

Blyznyuk, A., Melnyk, I., Hrinchenko, Y., Solomko, A., Lernyk, S., Moshak, O. (2021). Formation the Project Maturity of Public Administration in implementation of Digital Transformation Projects. Journal of Information Technology Management, Special Issue, 163-187.

Boateng, R., Isabalija, R.S., Olumide, L. & Budu, J. (2011). Sakawa - Cybercrime and Criminality in Ghana. Journal of Information Technology Impact, 11(2), 85-100.

Bondarenko, S., Halachenko, O., Shmorgun, L., Volokhova, I., Khomutenko, A. & Krainov, V. (2021). The Effectiveness of Network Systems in Providing Project Maturity of Public Management. TEM Journal, 10(1), 358- 367.

Bondarenko, S., Tkach, I., Drobotov, S., Mysyk, A., Plutytska, K. (2021). National Resilience as a Determinant of National Security of Ukraine. Journal of Optimization in Industrial Engineering, 14(1), 111–117

Budhijanto, D. (2019). The Virtual Jurisdiction to Combating Cyberterrorism in Indonesia. Central European Journal of International and Security Studies, 12(4), 61-80.

Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. https://www.official-document/cm76/7642/7642.pdf (Accessed 24.05.2021).

Dolliver, D.S., Collins, C. & Sams B. (2017). Hybrid approaches to digital forensic investigations: a comparative analysis in an institutional context. Digital Investigation, 23, 124-137.

Draft of the Cybersecurity Strategy of Ukraine (2021-2025) (Unofficial English translation). https://www.rnbo.gov.ua/ua/Diialnist/4838.html (Accessed 25.07.2021).

Gaggero, M., Paola D. Di, Petitti, A. & Caviglione, L. (2019). When Time Matters: Predictive Mission Planning in Cyber-Physical Scenarios, IEEE Access, 7, 11246-11257.

Gradon, K. (2013). Crime Science and the Internet Battlefield: Securing the Analog World from Digital Crime. IEEE Security & Privacy, 11(5), 93-95, doi: 10.1109/MSP.2013.112.

Gumennykova, T., Pankovets, V., Liapa, M., Miziuk, V., Gramatyk, N. & Drahiieva L. (2020). Applying Instructional Design Methods to Improve the Effectiveness of Blended-Learning, International Journal of Management, 11 (5), pp. 31-42.

Half a thousand YouControl users about fraud 2020. https://youcontrol.com.ua/data-research/pivtysiachi-korystuvachiv-youcontrol-pro-shakhraystva-2020/ (Accessed 18.04.2021).

Hubanova, T., Shchokin, R., Hubanov, O., Antonov, V., Slobodianiuk, P. & Podolyaka, S. (2021). Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine. Journal of Information Technology Management, Special Issue, 75-90.

Ivashchenko, A., Kovalenko, Yu., Hubanov, O., Hubanova, T., Lutsenko, I. & Fialkovska A. (2021). Digital Tools inCcross-Cultural Analysis of SME Financial State Support in the Conditions of Pandemic Crisis. Journal of Information Technology Management, Special Issue, 142-162.

James, J. (2017). How Businesses Can Speed Up International Cybercrime Investigation. IEEE Security & Privacy, 15(2), 102-106, doi: 10.1109/MSP.2017.40.

Khomutenko A., Mishchenko, A., Ripenko, A., Liulchak, Z., Hrozovskyi R. (2019). Tools of the neuro-fuzzy model of information risk management in national security. International Journal of Engineering and Advanced Technology, 8 (6). 4526-4530.

Klochan, V., Piliaiev, I., Sydorenko, T., Khomutenko, V., Solomko, A. & Tkachuk A. (2021). Digital Platforms as a tool for the transformation of strategic Consulting in Public Administration. Journal of Information Technology Management, Special Issue, 42-61.

Kovalenko, Y, (2015) Financial sector development and economic factors of its support in Ukraine Economic Annals-XXI, 5-6, 77–81.

Mavlutova, I., Babenko, V., Dykan, V., Prokopenko, N., Kalinichenko, S., Tokmakova, I. (2021). Business Restructuring as a Method of Strengtening Company's Financial Position. Journal of Optimization in Industrial Engineering, 14(1), 129-139. http://dx.doi.org/10.22094/JOIE.2020.677839

New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion (2020). https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629 (Accessed 28.07.2021).

On the basic principles of cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII (2017). https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed 26.07.2021).

Oppliger, R., Pernul, G. & Katsikas, S. (2017). New Frontiers: Assessing and Managing Security Risks. Computer, 50(4), 48-51, doi: 10.1109/MC.2017.93.

Parker, D. (2007). The Dark Side of Computing: SRI International and the Study of Computer Crime. IEEE Annals of the History of Computing, 29(1), 3-15, doi: 10.1109/MAHC.2007.15.

Perevozova, I., Daliak, N., Babenko, V. (2019). Modeling of Financial Support for the Competitiveness of Employees in the Mining Industry. CEUR Workshop Proceedings, vol. 2422, pp. 444-454. URL: http://ceur-ws.org/Vol-2422/paper36.pdf

Ramazanov, S., Babenko, V., Honcharenko, O., Moisieieva, N., Dykan, V. (2020). Integrated intelligent information and analytical system of management of a life cycle of products of transport companies. *Journal of Information Technology Management*, 2020, 12(3), 26-33. https://doi.org/10.22059/jitm.2020.76291

Romanenko, Y. O., & Chaplay, I. V. (2016). Marketing communication system within public administration mechanisms. Actual Problems of Economics, 178(4), 69-78.

Sagan, O., Yakovleva, S., Anisimova, E., Balokha, A., & Yeremenko, H. (2020). Digital didactics as a new model in the theory of education. Revista Inclusiones, 7 num Especial, 193-204.

Vovk, V, Zhezherun, Y, Bilovodska, O, Babenko, V, Biriukova, A. (2020). Financial Monitoring in the Bank as a Market Instrument in the Conditions of Innovative Development and Digitalization of Economy: Management and Legal Aspects of the Risk-Based Approach. *IJIEPR*. 31 (4), 559-570. https://doi.org/10.22068/ijiepr.31.4.559

Zavhorodnii, A., Ohiienko, M., Biletska, Y., Bondarenko, S., Duiunova, T. & Bodenchuk, L. (2021). Digitization of agribusiness in the development of foreign economic relations of the region. Journal of Information Technology Management, Special Issue, 123-141. doi: 10.22059/JITM.2021.82613

Zawoad, S. & Hasan, R. (2016). Trustworthy Digital Forensics in the Cloud. Computer, 49(3), 78-81, doi: 10.1109/MC.2016.89/

Bibliographic information of this paper for citing:

Drobotov, S.; Pertsev, R.; Hrab, M.; Fedytnyk, V.; Moroz, S. & Kikalishvili, M. (2023). Forensic Research of the Computer Tools and Systems in the Fight Against Cybercrime. *Journal of Information Technology Management*, 15 (1), 135-162. https://doi.org/ 10.22059/jitm.2023.90741