DOI: 10.31648/sp.6569

Martin Mihók
Matej Bel University in Banská Bystrica, Slovakia
ORCID: 0000-0002-8981-4291
mihokmartin@gmail.com

Methodology of cybercrime investigation

Introduction

Computers are a part of our daily lives, it can be even said that sometimes they are a necessity. On the one hand, they represent a communication tool connecting the whole world with unbeatable speed, they represent an invaluable helper in the duties of everyday life, an ideal means of spending free time, or a common work tool. On the other hand, they can be a tool through which its user can harm another, for example by committing a crime; alternatively, the user can make already existing crime easier for himself/herself, which is simpler, more effective and more anonymous with the help of a computer (and the Internet)[1].

Cybercrime is now a common concept, which is analysed in many respects and it is possible to find several relevant sources of information that analyse this issue from a criminological, technical, legal, social, or general and summarizing point of view[2]. The beginnings of cybercrime (computer) crime date back to the 60s and 70s of the last century, taking into account the differences between contemporary computers and current computers. At present, it is one of the fastest growing types of crime and at the same time it is a highly sophisticated crime[3].

Cybercrime is causing increasing social and economic damage, which affects the fundamental rights of individuals and poses a threat to the rule of law and the stability of democratic societies in cyberspace, and is a growing problem in EU Member States. Cybercrime is gaining in intensity, complexity and scale, to the extent that in some EU countries it is more widespread than

[1] L. Klimek, *Základy trestného práva Európskej únie*, Bratislava 2017, p. 101.

[2] V. Porada a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání*, Plzeň 2019, p. 706.

[3] L. Klimek, op. cit., p. 101.

traditional forms of crime, extending to other areas of crime, such as trafficking in human beings. The use of encryption and anonymisation tools for criminal purposes and attacks through so-called ransomware are more common than the usual threats in the form of malware, such as Trojan horses. Malware (such as bank Trojan horses) is still at the centre of cyberattacks, but there has also been an increase in the number and consequences of attacks on industrial control systems and networks aimed at destroying critical infrastructure and economic structures, as well as destabilizing companies[4].

The concept of cybercrime, the classic personality traits of its perpetrators and the motives of the perpetrators

Cyber/computer crime (also known by the acronym "cybercrime") can be defined as the commission of a crime in which a computer interacts in some way as a collection of hardware and software, including data, or just some of its components, or a number of stand-alone computers or connected to a computer network, either as the subject of this criminal activity (with the exception of the criminal activity involving the described facilities as movable property) or as an instrument of a crime commission. From the forensic point of view, cybercrime also means a group of criminal offenses (anti-social behaviour) committed by means of computer technology in the conditions of electronic communications networks, ICT systems, software and databases in the means of computer technology[5].

The boundaries between cybercrime, cyber espionage, cyber warfare, cyber sabotage, and cyber terrorism are becoming increasingly blurred; as cybercrime can target individuals, public or private entities and can cover a wide range of crimes, including invasions of privacy, sexual abuse of children online, public incitement to violence or hatred, sabotage, espionage, financial crime and fraud, such as payment fraud, theft and identity theft, as well as illegal interference with the system. A significant number of cybercrime remain unprosecuted and unpunished[6].

It is precisely children who use the Internet at an ever younger age and are particularly vulnerable, so they can become victims of so-called grooming and other forms of sexual abuse on the Internet (cyberbullying, sexual abuse, sexual coercion and extortion), misuse of personal data, as well as dangerous challenges aimed at promoting various forms of self-harm (the case of Blue whale game) and therefore need special protection; as Internet perpetrators

[4] European Parliament Resolution No. 2017/2068 (INI) of 3 October 2017 on the fight against cybercrime.

[5] V. Porada a kol., op. cit., p. 960.

[6] European Parliament Resolution No. 2017/2068 (INI)…

can find and deceive victims more quickly through chat forums, e-mails, online games and social networks, and as hidden peer-to-peer (P2P) networks remain the main platforms for access, communication for child sex offenders, storing and exchanging material depicting the sexual exploitation of children and tracking new victims without being detected[7].

It is man who is the one who can most endanger the security of himself/herself or others in cyberspace, and that is by acting or failing to act. The basic technical causes of cybercrime, such as obsolescence and non-updating of the software used, non-use of anti-virus programs, insufficient security settings, relative availability of sophisticated technical means that can be used for attacks and the like, must also be adequately taken into account. Smartphones, for example, are relatively easy to exploit, and users often have no idea about them. It is clear that the human factor plays a key role in committing cybercrime; the human factor is undoubtedly generally considered to be the greatest safety risk[8].

The typical perpetrator of computer crimes is most often an employee of the injured organization. Literature sources indicate that, for example, in the United States, only 6% of offenders were employees of other companies, 24% of offenders were directly employed in the computer centre of the injured company, and 70% were recruited from end users of the injured company's computers. The situation in the Slovak Republic and the Czech Republic seems to be similar[9].

The perpetrator's personality is dominated by more than a high IQ, greed or desire for power, perseverance and ruthlessness. Many perpetrators are neurotics who are clumsy in social contacts, often with sexual problems. Perpetrators of cybercrime often do not feel guilty and do not see anything wrong with their actions. Of importance is the specific position of the typical perpetrator of this illegal activity, which may be that:

– is authorized to perform certain computer operations,

– is familiar with the sequence of operations required, including details of the behaviour of the automated system,

– is able to misuse his/her knowledge without the risk of immediately signalling the system to the unauthorized operation of the operation, or without the risk of recording the operation in a "log" or "audit trail" type, etc.,

– knows in detail the functions of individual programs,

– has access to the workplace software,

– has access to files intended for the transmission of data to the headquarters or to other organizations,

[7] Ibidem.

[8] V. Porada a kol., *Bezpečnostní vědy,* Plzeň 2019, p. 161.

[9] Idem, *Kriminalistika. Technické, forenzní a kybernetické aspekty…*, p. 965.

– can create or abuse non-standard situations that are handled operationally without standardized procedures[10].

The most common motives of these perpetrators are in particular greedy motives, motives arising from conflicts in interpersonal relationships, desire to gain power or sovereignty, desire to demonstrate their intellectual superiority, desire to overcome the feeling of underestimation of their abilities, cover motives to conceal the pursuit of another criminal activities, political motives and others.

Knowing the motive of a computer crime is significantly important, especially for identifying the probable perpetrator of a crime from a predefined circle of suspects - mostly current or former employees of the injured company. Finding out the motive is closely linked to resolving the question of who benefits or can benefit from the consequences of an anti-social act. Last but not least, it is important to know the motive for the correct criminal qualification of the unlawful conduct and for determining the degree of social harm of this proceeding.

Knowing the motive of a computer crime is significantly important, especially for identifying the probable perpetrator of a crime from a predefined circle of suspects – mostly current or former employees of the injured company. Finding out the motive is closely linked to resolving the question of who benefits or can benefit from the consequences of an anti-social act. Last but not least, it is important to know the motive for the correct criminal qualification of the unlawful conduct and for determining the degree of social harm of this behaviour[11].

Characteristic methods of cybercrime commission and corresponding crimes in the Slovak Republic, stages of unlawful conduct

The methods of cybercrime commission are, like other methods of commission, a system of operational elements of crime and related activities. The operational elements of cybercrime commission are not only the method of abuse of computer technology or electronic communications network, but also the method of the perpetrator´s actions before its abuse, as well as the method of perpetrator´s actions during and after the implementation of this abuse. The determining operational element is always the method of abuse of computer

[10] Ibidem.

[11] Ibidem.

technology, due to its specific properties and the dominant position among the material components of the method of commission[12].

Typical method of cybercrime commission can be as follows:

– *unauthorized interference with input data* (e.g. input data for bank accounts),

– *unauthorized changes to stored data* (e.g. change to stored data in accounts and various records),

– *unauthorized instructions for computer operations* (e.g. unauthorized transfer of money from a foreign bank account to one's own),

– *unauthorized intrusion into computer systems and their databases* (e.g. individual operations via the Internet in order to obtain information of various kinds from databases and their use, or abuse),

– *attack on a foreign computer, its software and databases* (computer viruses, malicious programs – malware, etc.),

– *information crime* (access and dissemination of harmful content via Internet networks, unauthorized handling of personal data, classified data, etc.)[13].

The following methods of cybercrime commission constitute predominantly the following criminal offenses within the legal system of the Slovak Republic:

– unauthorized access to the computer system (Section 247 of the Criminal Code),

– unauthorized interference with the computer system (Section 247a of the Criminal Code),

– unauthorized interference with computer data (Section 247b of the Criminal Code),

– unauthorized capture of computer data (Section 247c of the Criminal Code),

– production and possession of an access device, password to a computer system or other data (Section 247d of the Criminal Code),

– drug addiction spreading (Section 174 of the Criminal Code),

– sexual abuse (Section 201a of the Criminal Code),

– dangerous stalking (Section 360a of the Criminal Code),

– dissemination of child pornography (Section 369 of the Criminal Code),

– possession of child pornography (Section 370 of the Criminal Code),

– endangering morality (Section 371 of the Criminal Code),

– defamation (Section 373 of the Criminal Code),

[12] V. Smejkal, *Kybernetická kriminalita*, 2. vyd., Plzeň 2018, p. 520.

[13] P. Polák, J. Kubala, *Repetitórium kriminalistiky*, druhé, prepracované a doplnené (aktualizované) vydanie, Bratislava 2017, p. 121; Bližšie pozri aj V. Porada a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty…*, pp. 963–964.

– unauthorized handling of personal data (Section 374 of the Criminal Code),

– infringement of one´s rights (Section 376 of the Criminal Code).

In the indicated context, it is not possible to omit the fact that in “cyberspace” it is also possible to commit the so-called extremist crimes, especially the offense of establishing, supporting and promoting movements aimed at suppressing fundamental rights and freedoms (section 421 and section 422 of the Criminal Code), the offense of defamation of nation, race and belief (section 423 of the Criminal Code), the offense of incitement to racial and ethnic hatred (Section 424 of the Criminal Code), the offense of producing extremist materials (Section 422a of the Criminal Code), the offense of disseminating extremist materials (Section 422b of the Criminal Code), the offense of possessing extremist materials (Section 422c of the Criminal Code) and the offense of denial and approval of the Holocaust and crimes of political regimes and crimes against humanity (Section 422d of the Criminal Code).

In connection with the unlawful conduct of a cybercrime perpetrator, we distinguish the following stages:

– *preparation of the attack by the perpetrator*,

– *perpetrator’s attack itself*,

– *detection of an attack* (mostly by the injured party),

– *elimination of the consequences of the attack* (by the injured),

– *eradication of traces after the attack* (by the perpetrator),

– *finding out information leading to the detection of the perpetrator* (by the criminal law enforcement authorities with the cooperation of the injured party, or with other persons – the operator of the facility or information system),

– *collection of evidence* (by the criminal law enforcement authorities),

– *in case of identification and apprehension of the perpetrator – criminal proceeding itself* (criminal law enforcement authorities, defence, court),

– *implementation of measures to reduce the risk of further attack* (by the injured party, the person authorized by him, etc.)[14].

Specific forensic traces, initial acts and measures

In the process of investigating cybercrime, a number of forensic traces can be encountered, some of which are typical of cybercrime. The number, variety and distribution of traces depends on the specific circumstances of the case. We find both traces of material and other forensic evidence, as well as memory traces[15].

[14] V. Porada a kol., *Bezpečnostní vědy…*, p. 178.

[15] V. Porada a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty…*, p. 966.

Thus, forensic traces can be distinguished into:

– *Material traces* (dactyloscopic, biological, trasological traces),

– *Digital traces* (traces found in computer systems and on data carriers, which are created in such a way that each technological device that acquires, processes, sells or stores data leaves reflections – records of its activities; a digital trace is in fact a physical interpretation - a record of intangible information that is encoded in digital format,

– *Documentary and factual evidence* (proving the offender's criminal activity in connection with the preparation and commission of a cyber illegal activity),

– *Computer traces* (information or changes in material carrier created in connection with a criminal offense; in particular:

● traces of computer technology, including unauthorized interference with technology,

● traces on recording media and information stored on them,

● traces of organizational and office equipment that allow the recording and storage of digital information – e.g. telephones with memory, fax, dictaphones, scanners, printers, security and camera systems, attendance systems, etc.),

– *Memory traces* – this includes:

● memory trace of the perpetrator,

● memory traces of associates, partners, co-workers, family members of persons suspected or accused of committing a crime,

● memory traces of employees of the injured organization[16].

Due to the nature of typical computer traces and other evidence of cybercrime, taking into account the nature of the crime (economic or financial crime, theft, organized crime), the initial operational and investigative and investigative actions may differ. Cybercrime investigations need to be swift but prudent from the outset, as perpetrators of this crime are generally highly qualified and knowledgeable in computer operations, which usually go beyond the knowledge of investigators and police authorities; therefore, it is necessary for police authorities to cooperate with computer experts from the outset[17].

In investigating this modern crime, a priority is to prevent the erasure of data, also important is the recovery of erased data and information, or the prevention of the spread of viruses. The initial and urgent actions in the initial phase of a cybercrime investigation include in particular:

– *receiving a criminal complaint*,

– *requesting the necessary explanations*,

– *surrender and seizure of items relevant to criminal proceedings*,

– *crime scene inspection, home search and search of other premises*,

[16] V. Smejkal, op. cit., p. 643.

[17] V. Porada a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty…*, pp. 971–972.

– *requesting expertise in the field of computer technology, accounting and carrying out collection and seizure operations for that expertise*,

– *search for computer (electronic) traces and evidence*,

– an assessment of the possible extent of the provision of information to the media and the public[18].

The initial actions and measures taken by investigative bodies in investigating cybercrime may include in particular:

– *crime scene inspection*,

– *home and personal searches, searches of other areas where traces of cybercrime may be found.*

Given technical developments and the exploitation of its results in relation to crime commission, computer data are a valuable source of evidence for bodies active in criminal procedure and the courts. The commission of crimes by means of computer systems, the transmission of information on planned, committed or already committed criminal offenses through them and the storage of information relevant to criminal proceedings by means of computer systems require that these bodies have a legitimate impact on computer data, whether in order to obtain evidence or removal of computer data with defective content from the computer system. Criminal law at both international and national levels had to respond to this need and technical progress[19].

From a practical point of view, in investigating cybercrime by bodies active in criminal procedure, relatively effectively are used for example, institutes of storage and issuance of computer data (Section 90 of the Criminal Procedure Code) and the discovery and reporting of data on telecommunications operation performed (Section 116 of the Criminal Procedure Code), which are subject to telecommunications secret[20], or covered by the protection of personal data which are necessary to clarify facts relevant to criminal procedure. The criminally relevant facts thus established may subsequently serve as evidence in criminal proceedings.

In the application practice of bodies active in criminal procedure, there were doubts as to whether the procedure pursuant to Section 90 of the Criminal Procedure Code could also be applied in relation to data stored in mobile phones. It can be said that within the procedure of bodies active in criminal

[18] Ibidem, p. 972.

[19] R. Kubička, O. Kubička, *Počítačové údaje v trestnom konaní*, [in:] *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*, Akadémia Policajného zboru v Bratislave, Bratislava 2018, p. 83.

[20] Pursuant to Section 63 para. 1 of Act no. 351/211 Coll. on electronic communications, subject to telecommunication secrecy is *a) the content of transmitted messages, b) related data of communicating parties, which are the telephone number, business name and registered office of a legal entity, or business name and place of business of a natural person - entrepreneur or personal data name, surname, title and address of permanent residence; the subject of telecommunication secret is not the data published in the telephone directory, c) operational data and d) location data.*

procedure, the prevailing opinion was that computer data stored in the so-called smartphones represent computer data pursuant to Section 90 of the Criminal Procedure Code. A smartphone can be defined as a "mobile phone with an operating system". The most used systems are Google Android, Apple iOS and Microsoft Windows, which allow the device to be equipped with a rich basic set of applications (functions) and later expanded by others. There are also operating systems that are hardly used anymore – Symbian or PalmOS. The smartphone is mainly used for communication, GPS, access to the Internet via mobile and WiFi networks and the use of various other applications that can be installed on the smartphone via the Internet directly from a mobile phone, for games, work, mobile office and entertainment[21].

The legal regulation of the institute of storage and issuance of computer data contained in section 90 of the Criminal Procedure Code responds to the Council of Europe Convention on Cybercrime, which was adopted by the member states of the Council of Europe on 23 November 2001 in Budapest[22] (hereinafter the "Convention on Cybercrime").

Given the continuity of the legislation of the institute of the retention and surrender of computer data to the Convention on Cybercrime, and when answering the question whether the data stored via mobile phones constitute computer data stored via a computer system (and thus whether we can apply the procedure under section 90 of the Criminal Procedure Code in respect to them), it is appropriate to proceed from the interpretation of terms used in the Convention on Cybercrime and compare the technical characteristics of the mobile phone and data stored via the mobile phone with the definition of relevant terms in the Convention[23].

Pursuant to Art. 1 (a) of the Convention on Cybercrime "computer system" means a device or group of interconnected or related devices, one or more of which is an automated data processing machine on a program basis. Pursuant to Art. 1 (b) of the Convention on Cybercrime "computer data" means the recording of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of causing a computer system to perform a certain activity.

A mobile phone is a device that performs automated data processing on the basis of a program, i.e., a list of commands or instructions used to solve tasks on this device. Such a program used in a mobile phone may be, for example, a text editor, a program for storing and sorting contacts, clients´ e-mails into groups, and the like. Following the above, we are of the opinion that the mobile phone meets the conceptual features of the computer system under Art. 1 (a) of the Convention on Cybercrime, as it represents a device performing

[21] R. Kubička, O. Kubička, op. cit., pp. 83–84.

[22] Explanatory memorandum to Act No. 301/2005 Coll. Criminal Procedure Code.

[23] R. Kubička, O. Kubička, op. cit., p. 84.

automated data processing on the basis of a program. Following this and taking into account Art. 1 (b) of the Convention on Cybercrime, we consider data stored via a mobile phone, representing a record of facts, information or concepts in a form that is suitable for processing in a computer system (i.e., also suitable for processing in the mobile phone itself) as the computer data stored via a computer system, to which the procedure pursuant to Section 90 of the Criminal Procedure Code may be applied[24].

Investigation versions and subsequent investigation stages

Cybercrime, including its organized form, is a very diverse activity; this fact determines the current possibilities of using typical versions, which represent a generalized experience. At the beginning of the clarification of the case or at the beginning of the operational elaboration, a typical version on the nature of the crime will, as a rule, be formulated. In this way, a version can be determined that a) the event is a cybercrime without signs of organized crime or with signs of organized crime, or b) the event is caused by a technical failure, administrative error or mistake in manipulating computer, systems, software or databases. These versions must be thoroughly verified in the further process[25].

The method of committing cybercrime is not always fully known at first, so after performing all the initial and urgent actions, it is possible to determine typical versions of the method of committing cybercrime and the implementation of the values obtained by crime:

– *a version on the abuse of a computer and its means of communication to commit crime* (it aims in particular to specify, for example, computer fraud, theft committed by unauthorized transfer of funds from account to account of the perpetrator, etc.),

– *version on unauthorized spread of computer viruses and logical bombs* (aimed at concretizing the fact that the perpetrator exploits features - weaknesses of the computer system, which under certain conditions activates programs and performs certain activities that result in erasing memory, blocking computer operation, performing logical attacks to a program, file, etc.),

– *version on unauthorized tampering with software, databases and communication equipment* (specified on the basis of changes to the program and data, etc.),

– *version on unauthorized access to data by the offender* (specified in case of intrusion into the computer system as well as intrusion into its databases and information),

– *version on the perpetrator of cybercrime* (it is about determining the number of perpetrators, the degree of their organization, tasks, degree of re-

[24] Ibidem, pp. 84–85.

[25] V. Porada a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty…*, p. 973.

sponsibility, motives, knowledge, access to information carriers, computers, telecommunications networks, etc.)[26].

After carrying out the initial actions and measures and after determining the relevant investigative versions, the next stage of the investigation follows, which is characterized in particular by forensic digital expertise.

Forensic digital expertise focuses mainly on the study of computer and communication technology, or technical and other means directly related to this technology, including information carriers in clarification and taking of evidence in criminal proceedings. The technical properties (parameters) of the given technology are determined and the information stored on the recording media is examined[27].

In the case of expert examinations on data carriers, no change or loss of information must take place during the expertise; in order to prevent these situations, all information from the secured media is transmitted to another data carrier, which serves as a data standard, i.e., as an exact bit image, if possible[28].

In the investigation of criminal activity committed in the form of cybercrime, the results of the examination within the framework of computer expertise are very important and in most cases also a decisive source of evidentiary information. They are also necessary and decisive for the further procedural procedure and other procedural acts in the case.

Procedural acts depending on the results of computer expertise, implemented in the next process, are in particular:

- questioning of the accused,
- questioning of witnesses,
- investigative test and reconstruction of a crime,
- recognition and confrontation.

Electronic evidence and cross – border seizure of electronic evidence

More and more activities are taking place in the digital world. Almost every aspect of human life takes on an electronic form - most of the population of the developed countries of the world has at least an established electronic address and also uses a mobile phone, mostly a smartphone. Just as it is possible to identify the date of sending, saving or receiving a document, content information and even the presence of fingerprints, using special techniques, from a classic letter mail, so receiving or sending an e-mail leaves a certain

[26] Ibidem, pp. 973–974.
[27] Ibidem, p. 974.
[28] Ibidem, p. 975.

trace in the virtual world. A trace – that is not so obvious and noticeable at first glance compared to the physical ones. Communication within interpersonal relationships is disappearing more and more into the online space[29].

A certain milestone in the development of electronic evidence is the Convention on Cybercrime, which was one of the first documents to predict the collection of evidence of crime in electronic form. By electronic evidence we therefore mean any information with probative value relevant to criminal proceedings, which is transmitted or stored in digital form[30] and which has been lawfully obtained. We consider cloud storage, computer technology, including computers, technical media (USB keys, external disks), as well as portable electronic devices, i.e., mobile phones, tablets and smart watches, to be the sources of electronic evidence in the broadest sense. All these electronic devices have one and the same feature, and that is that they have built-in memory, which is the very essence of the data source, as this is where all the information is stored. The information may then be volatile or persistent in nature, depending on whether it is stored on the device's hard disks or in operational memory. Electronic means of proof can be understood as the taking of evidence in various ways, for example by e-mail or profile from a social network, i.e., its conversion, interpretation into human-perceptible form, as data are only a cluster of mathematical operations, which in this original form have no informative value for a lay person[31].

During the investigation, criminal law enforcement authorities often encounter the problem that the data of interest is stored on foreign servers. Another equally fundamental problem is the reluctance of cooperation on the part of organizations authorized to store this data and providers of electronic communications services. However, the process of obtaining electronic evidence is complicated and significantly prolonged by confusing legislation[32].

Effective judicial cooperation and mutual legal assistance between states is a prerequisite for obtaining evidence of any nature in a cross-border manner. At European Union level, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters was adopted (Official Journal of the EU, L 130, 1 May 2014, p. 1), reflecting the Europeanisation of criminal law. It has introduced a new instrument in the European Union - the European Investigation Order, which is based on the principle of mutual recognition of judicial decisions and which establishes a uniform regime for obtaining evidence; by the nature of the case,

[29] P. Dražová, *Zákonnosť a prípustnosť elektronických dôkazov*, [in:] *Zákonnosť a prípustnosť dôkazov v trestnom konaní. Zborník príspevkov z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2019*, Bratislava 2019, p. 168.

[30] R. Polčák, a kol., *Elektronické důkazy v trestním řízení*, 1. vyd., Brno 2015, p. 91.

[31] P. Dražová, op. cit., p. 169.

[32] Ibidem, p. 170.

its territorial scope is limited to the Member States of the European Union. It is the institute of the European Investigation Order that is currently fully usable for the cross-border acquisition of electronic evidence within the European Union.

Conclusion

Forensics is an independent scientific discipline that examines and clarifies the laws of origin, extinction, search, seizure, investigation and use of forensic traces, other forensic evidence and forensically relevant information. On this basis, it develops methods, means, procedures, operations and recommendations for forensic practical activities, regardless of the formal conditions of their use in the practice of various police forces[33].

Since its inception, forensics has been classified (together with criminology, penology, criminal science and various forensic sciences) into a group of scientific disciplines dealing with the negative social phenomenon – crime[34].

Cybercrime can also be described as one of the modern types of crime, which, no doubt, is also dealt with by forensics. Its origins date back to the 60s and 70s of the last century and it is currently one of the fastest growing types of crime and at the same time it is a highly sophisticated crime. The theory, but also practice, distinguishes several methods of committing this so-called computer crime, whether it is unauthorized interference with input data, unauthorized changes in stored data, unauthorized intrusion into computer systems and their databases and the like, and these methods of cybercrime can constitute certain offences stipulated by the Criminal Code.

In the process of investigating cybercrime, it is possible to encounter a number of forensic traces, some of which are typical for cybercrime, especially material traces, digital, computer traces, documents and factual evidence, and memory traces. Given these highly specific forensic traces, the investigating authority must adapt not only the process of securing these traces, but also the process of cybercrime investigation itself so that the individual evidence is legally secured so that the perpetrators of the crime can be identified and fairly punished in the subsequent process. However, the fight against cybercrime should be primarily about protecting and strengthening critical infrastructure and other network facilities, and not just about taking repressive measures[35].

[33] J. Musil, *Kriminalistika, vybrané problémy teorie a metodologie*, Praha 2001, p. 18.

[34] V. Porada a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty…*, p. 29.

[35] European Parliament Resolution No. 2017/2068 (INI)…

References

Dražová P., *Zákonnosť a prípustnosť elektronických dôkazov*, [in:] *Zákonnosť a prípustnosť dôkazov v trestnom konaní. Zborník príspevkov z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2019*, Univerzita Komenského v Bratislave, Právnická fakulta, Bratislava 2019.

Klimek L., *Základy trestného práva Európskej únie*, Wolters Kluwer, Bratislava 2017.

Kubička R., Kubička O., *Počítačové údaje v trestnom konaní*, [in:] *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*, Akadémia Policajného zboru v Bratislave, Bratislava 2018.

Musil J., *Kriminalistika, vybrané problémy teorie a metodologie,* PA ČR, Praha 2001.

Polák P., Kubala J., *Repetitórium kriminalistiky*, druhé, prepracované a doplnené (aktualizované) vydanie, Wolters Kluwer, Bratislava 2017.

Polčák R. a kol., *Elektronické důkazy v trestním řízení*, 1. vyd., Masarykova univerzita, Právnická fakulta, Brno 2015.

Porada V. a kol., *Bezpečnostní vědy*, Aleš Čeněk, Plzeň 2019.

Porada V. a kol., *Kriminalistika. Technické, forenzní a kybernetické aspekty*, 2. aktualizované a rozšířené vydání, Aleš Čeněk s.r.o., Plzeň 2019.

Smejkal V., *Kybernetická kriminalita*, 2. vyd., Aleš Čeněk, Plzeň 2018.

Summary

Methodology of cybercrime investigation

Key words: forensics, cybercrime, perpetrator, methods of cybercrime, forensic traces, electronic evidence.

The aim of the article is to analyse the phenomenon of cybercrime focusing mainly on the methodology of investigation. Cybercrime can be described as one of the modern types of crime, which, no doubt, is also dealt with by forensics. Its origins date back to the 60s and 70s of the last century and it is currently one of the fastest growing types of crime and at the same time it is a highly sophisticated crime. In the process of investigating cybercrime, it is possible to encounter a number of forensic traces, some of which are typical for cybercrime, especially material traces, digital, computer traces, documents and factual evidence, and memory traces. Given these highly specific forensic traces, the investigating authority must adapt not only the process of securing these traces, but also the process of cybercrime investigation itself so that the individual evidence is legally secured so that the perpetrators of the crime can be identified and fairly punished in the subsequent process.

Streszczenie

Metodologia dochodzeń w sprawie cyberprzestępczości

Słowa kluczowe: kryminalistyka, cyberprzestępczość, sprawca, metody cyberprzestępczości, ślady kryminalistyczne, dowody elektroniczne.

Celem artykułu jest analiza zjawiska cyberprzestępczości, ze szczególnym uwzględnieniem metodologii śledztwa. Cyberprzestępczość można określić jako jeden ze współczesnych rodzajów przestępstw, którym bez wątpienia zajmuje się również kryminalistyka. Jej początki sięgają lat 60. i 70. ubiegłego wieku i jest to obecnie jeden z najszybciej rozwijających się rodzajów przestępstw, a jednocześnie bardzo wyrafinowany. W trakcie badania cyberprzestępczości, można napotkać szereg śladów kryminalistycznych, z których część jest typowa dla cyberprzestępczości, zwłaszcza ślady materialne, cyfrowe, komputerowe, dokumenty i dowody rzeczowe oraz ślady pamięci. Biorąc pod uwagę te bardzo szczegółowe ślady kryminalistyczne, organ prowadzący dochodzenie musi dostosować nie tylko proces zabezpieczania tych śladów, ale także sam proces dochodzenia w sprawie cyberprzestępczości, tak aby poszczególne dowody były prawnie zabezpieczone, a sprawcy przestępstwa mogli zostać zidentyfikowani i sprawiedliwie ukarani w kolejnym procesie.