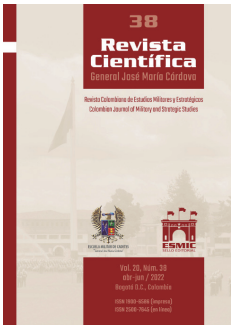




**Revista Científica General José María Córdova**
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

ISSN 1900-6586 (print), 2500-7645 (online)
**Journal homepage:** https://www.revistacientificaesmic.com

# Forensic and technical criminalistics support in cybercrime investigation: countering cyber threats in Ukraine

**Andrii Padalka**
https://orcid.org/0000-0003-1433-1030
andrii_padalka@edu.cn.ua
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

**How to cite in APA:** Padalka, A. (2022). Forensic and technical criminalistics support in cybercrime investigation: countering cyber threats in Ukraine. *Revista Científica General José María Córdova*, *20* (38), 407-423.
https://dx.doi.org/10.21830/19006586.901

**Published online:** April 1, 2022




Submit your article to this journal:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions


Miles Doctus

**Revista Científica General José María Córdova**
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 407-423
https://dx.doi.org/10.21830/19006586.901

# Forensic and technical criminalistics support in cybercrime investigation: countering cyber threats in Ukraine

## Apoyo criminalístico forense y técnico en la investigación de la ciberdelincuencia: la lucha contra las ciberamenazas en Ucrania

**Andrii Padalka**
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

**Abstract.** The issue of cyber security has become a key State objective in Ukraine. Cyber espionage and cyber-attacks by intelligence agencies (predominantly non-democratic countries) have become the most significant modern threat to automated systems, surpassing ordinary crimes seeking profit. Besides effective protection and immediate responses to counter cyber threats, cyber incident investigations are an important element that must be conducted by authorized law enforcement agencies and intelligence agencies when necessary. This article considers key aspects and issues to suggest practical recommendations to prepare and appoint forensic expertise in cybercrime investigations. Furthermore, it addresses the objects under examination, their removal's particularities, and the questions to ask telecommunications and technical computer experts.

**Keywords:** criminalistics; cyber-attack; cybercrime; cyber incident; cyber threat; forensic expertise; investigation; Ukraine

**Resumen.** La ciberseguridad se ha convertido en un objetivo clave del Estado en Ucrania. El ciberespionaje y los ciberataques de las agencias de inteligencia (predominantemente de países no democráticos) se han convertido en la amenaza moderna más importante para los sistemas automatizados, superando los delitos ordinarios con fines de lucro. Además de la protección efectiva y respuesta inmediata a las ciberamenazas, la investigación de los ciberincidentes es un elemento clave llevado a cabo por organismos policiales y de inteligencia autorizados cuando sea necesario. Este artículo considera aspectos y cuestiones clave para sugerir recomendaciones prácticas para la preparación y contratación de expertos forenses en estas investigaciones. Además, aborda los objetos examinados, las particularidades de su eliminación y las preguntas que deben formularse a los expertos en telecomunicaciones e informática.

**Palabras clave:** ciberamenaza; ciberataque; ciberdelincuencia; ciberincidente; criminalística; investigación; peritaje forense; Ucrania

Section: Dossier • Scientific and technological research article

Received: November 30, 2021 • Accepted: March 2, 2022

**Contact:** Andrii Padalka ✉ andrii_padalka@edu.cn.ua

## Introduction

Appointing forensic expertise is an important stage in investigating nearly every criminal offense. In *science-intensive*, *highly intelligent*, and *high-tech* crimes, appointing forensic expertise is crucial.

Legal knowledge alone will not enable an investigator to identify the traces of these crimes and their settings or perform further investigations that require reproducing the stages of these illegal acts; specialized knowledge must be involved. This requirement is fully applicable to the investigation of cybercrime. It requires a deep knowledge of modern information technology. Thus, the investigation of cybercrime without the appointment of computer or telecommunications expertise is inconceivable. The investigator must also be able to formulate the correct questions for the expert to obtain answers that can be effectively used in the process of evidencing the crime. Often, the initiator poses incorrect questions when appointing an examination. These may be issues that cannot legally be resolved by experts (Criminal Procedure Code of Ukraine, 2012c). Furthermore, replicating all the questions from the reference books, manuals, or departmental instructions on the appointment of forensic examinations (Ministry of Justice of Ukraine, 1998) would complicate and slow down an expert's work.

Thus, the preparation and appointment of forensic examinations during cybercrime investigations remain relevant objects of scientific research to develop scientifically substantiated recommendations for their implementation. According to the Criminal Procedure Code of Ukraine (2012c), an expert in criminal proceedings is a person with scientific, technical, or other specialized knowledge; the right to conduct an expert study, according to the Law of Ukraine (1994) *On Forensic Examination*; and the training to examine objects, phenomena, and processes concerning circumstantial information on the criminal offense and offer an opinion on issues that arise during the criminal proceedings according to the individual's scope of knowledge. An expert study is conducted by a professional expert organization or experts engaged by the parties to the criminal proceedings. In the cases provided in Article 244 of this Code, the investigating judge will seek expert support at the defense's request if specialized knowledge is required to clarify the circumstances relevant to the criminal proceedings. However, this expertise cannot be used to clarify legal issues (Security Service of Ukraine, 2015).

While some criminal offenses can be successfully investigated without the appointment of forensic expertise, others may require specific knowledge. A forensic expert possesses specialized knowledge in fields including science, technology, art, and craft that other participants of the criminal proceeding do not. For example, forensic expertise is essential in *high-tech* crimes, given the intense development of computer technologies

that require new technical solutions almost on a daily basis. Fittingly, criminals *hack* these technologies or methods to commit illegal acts. Although legal knowledge is fundamental for the investigator, prosecutor, and judge, they usually lack technical knowledge in information technology, making cybercrime investigation without expert help impossible (Yaroshenko et al., 2018).

The expertise typically required in criminal investigations can be referred to as *general*. However, we will refer to the expertise required in the crimes addressed here as *specialized*. In the investigation of cybercrime, the first group of *specialized* expertise includes those necessary to study the mechanisms and means of conducting cyberattacks. Specialized knowledge in information technology, namely computer technology and telecommunications, is vital in these crimes.

It should be noted that depending on the subject under study, certain computer and technical examinations can be attributed to *general* expertise categories. These include examining a suspect's signature in documents and examining photos or video surveillance camera recordings to identify a suspect's laptop or establish its brand and model. For example, the examination of email history can be considered *general* expertise, as it does not presuppose studying the mechanisms and means of cyberattacks. The need to investigate correspondence may arise in investigating many crimes, including theft and corruption. However, if this correspondence contains a description of a cyberattack, this description should be provided to the expert to meticulously examine the attack's mechanism, making it *specialized* expertise.

Specialized expertise implies a more detailed examination of items containing information on a cyberattack. These include:

- Items containing information regarding a possible a cyberattack;
- Items evidencing a consummated cyberattack (or its individual stages) or information on the consequences.

It should be noted that large-scale cyberattacks, especially Advanced Persistent Threat (APT), which are complex cyberattacks to gain unauthorized access to the victim's information systems for control or future use (Daly, 2009), are usually implemented in several stages. Each stage, including the preparation stage, can be a separate cyberattack. Traces of these stages can be considered a plan for a cyberattack, whose final stage is the actual attack. These individual stages –considered cyberattacks in themselves– are a chain of attacks, components of a large-scale cyberattack.

Usually, before appointing an expert, investigative actions are carried out to seize material evidence, which is subsequently submitted for expert examination. For example, when inspecting the attacked system, the following items are seized and submitted for expert examination:

- Media, their clones, or bitmaps;
- RAM dumps;
- Log files of services and applications;
- Login settings;
- Diagnostic report files;
- Diagnostic utility setups;
- Schemes for building automated systems and their integration into clusters and networks;
- Schemes of internal networks (LAN, Local Area Network) and connection to the global network (WAN, Wide Area Network);
- Network equipment setups;
- Software configuration (system, server, and user) of the automated system, particularly remote access configurations; and
- Email correspondence, primarily emails containing attachments (potential malware) or external links (potential sources of malware downloads).

Each cyberattack has its own characteristics; therefore, an exhaustive list of recommendations to extract each specific item is impossible. To find and extract the evidence correctly, the investigator must involve a knowledgeable person in the investigative action and a technical and forensic support unit specialist in the investigation actions. This specialist's knowledge should be in the middle ground between the investigator and the forensic expert (Kozlovskyi et al., 2019).

Prior to the 2016 internal affairs bodies reform, the expert service of the Ministry of Internal Affairs was part of the police. The experts were police officers that, in addition to performing forensic examinations, also provided technical and forensic support for investigative actions. After the reform, the Ministry of Internal Affairs' expert service was no longer part of the Ukrainian National Police's structure; forensic examinations remained the core function of external experts. However, the National Police introduced positions for technical and forensic support of investigative actions for forensic inspectors.

The experience, however, revealed that the quality of site inspections by forensic inspectors was much worse than by forensic experts (Guliyeva et al., 2018). The outcome was not surprising. Unlike the forensic inspectors, the experts are not only knowledgeable in finding and collecting material evidence, but they also know how to analyze this evidence further during the expert examination. Moreover, an expert can assess the identified material evidence better in terms of its further suitability for examination, including recording, extracting, and storing the evidence better, ensuring its proper preservation.

## Literature Review

Expert units in the Security Service of Ukraine simultaneously perform the functions of forensic support of justice and technical and forensic support of investigative actions, counterintelligence, and operational and investigative measures. Therefore, forensic activity in Ukraine is considered here in more detail.

The Law of Ukraine (1994), *On forensic examination*, regulates the basic principles of forensic activity in Ukraine. It defines a forensic examination as a study of objects, phenomena, and processes based on specialized knowledge in science, technology, art, and craft, among others, to provide an opinion on issues that are or will be the subject of litigation. Therefore, persons can be forensic experts if they possess the necessary knowledge to provide an opinion on the issues under investigation.

The legal procedure for appointing an expert and using the expert's opinion as a source of evidence is regulated by the relevant procedural codes. These are the Criminal Procedural Code of Ukraine (2012a), Civil Procedural Code of Ukraine (2004), Commercial Procedure Code of Ukraine (1991), and the Code of Administrative Procedure of Ukraine (2005).

Article 7 of the Law of Ukraine (1994), *On forensic examination*, defines the system of forensic institutions in Ukraine. These specialized agencies operate within the systems of the Ministry of Justice, Ministry of Internal Affairs, Ministry of Health, Ministry of Defense, the Security Service of Ukraine, and the State Border Guard Service of Ukraine.

It should be noted that expert profiling (computer-technical and telecommunication) in cyber-attack-related cybercrime investigations is not performed in all the forensic institutions listed above. It is only performed in expert institutions of the Ministry of Justice, Ministry of Internal Affairs, and the Security Service of Ukraine.

The Ministry of Justice's system of forensic institutions consists of the Scientific Research Institutes of Forensic Expertise (NDISE) and the Research Center for Forensic Examination on Intellectual Property. Currently, there are six NDISE in Ukraine located in Dnipro, Donetsk (temporarily moved to Slovyansk due to the partial occupation of some territories of the Donetsk region), Kyiv, Lviv, Odesa, and Kharkiv, with regional offices in other regions.

The Ministry of Justice's Department of Expert Support of Justice directs and controls the activities of forensic science and research institutions belonging to this Ministry and forensic experts that are not employees of state specialized institutions. The Ministry of Justice has established and operates an interdepartmental Coordination Council for Forensic Problems and a Central Expert Qualification Commission, as well as the Scientific Advisory and Methodological Council on the Issues of Forensic Examination.

## Analysis of Expert Services

### Expert services in Ukraine

The forensic institutions of Ukraine's Ministry of Justice annually conduct more than 100 thousand examinations (about 83 thousand are in criminal proceedings) and support the activities of the courts of all levels. They also support the National Anti-Corruption Bureau of Ukraine (NABU), the Specialized Anti-Corruption Prosecutor's Office (SAPO), the investigative bodies of the Ministry of Internal Affairs, Ukraine's Security Service (SSU), prosecutor's offices, customs service, and other institutions (Ministry of Justice of Ukraine, 2021).

In addition to providing a wide range of forensic expertise, these institutions also provide expertise in scientific forensic theoretical and practical principles, new methods of expert research, and forensic expert training and certification in these areas of research. The Kyiv NDISE (KNDISE) is the Ministry of Justice's largest forensic institution in Ukraine. It has five multidisciplinary laboratories and two departments that are directly involved in forensic science. The KNDISE has seven additional regional departments in Vinnytsia, Zhytomyr, Kropyvnytskyi, Ternopil, Khmelnytsky, Cherkasy, and Chernihiv.

The National Scientific Center, "Hon. Prof. M. S. Bokarius Forensic Science Institute" (NSCFSI), is one of the Ministry of Justice's leading scientific and research institutions. The Institute offers more than thirty types of expertise, including criminalistic, chemical forensic, biologic, physical, automotive forensic, construction, technical and commodity, and forensic accounting. The NSCFSI has a forensic theory department with an information and computing center that develops automated data banks and information retrieval systems. The NSCFSI also includes the Poltava and Sumy regional branches. It offers a postgraduate and doctoral program in specialty 081, Law, and forensic profiling to train highly qualified scientific and scientific-pedagogical staff.

In terms of its number and its tasks, the Expert Service of the Ministry of Internal Affairs of Ukraine is the largest. It includes the State Scientific Research Forensic Center (SSRFC) and the Ministry of Internal Affairs of Ukraine, the main institution of the service. It provides the service's organizational, managerial, and scientific-methodological management, with territorial research forensic centers (SRFC) located in the regions of Ukraine.

The main tasks of this expert service include forensic activities, involving employees in pre-trial investigation and trial, certification and other tests, property assessment, ensuring the functioning of accounting for instruments of criminal offenses, information retrieval systems, training, retraining, and advanced training of employees as forensic experts.

The Security Service of Ukraine's system of expert institutions includes the Ukrainian Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine (ISSEE SSU) and separate expert units in the regional bodies of the SSU. Some of the main forensic expertise classes conducted by divisions include criminalistic, special technical means of information interception, forensic biological, explosive technical, and computer and telecommunications. Its functions are entrusted to the ISSEE SSU.

The ISSEE SSU consists of five centers, three separate departments, and six separate sectors. The Center for Forensic and Special Expertise (CFSE) performs the functions of forensic support of justice, forensic support of investigative actions, and operational search activities carried out by the SSU's investigative and operational units and other law enforcement agencies. The CFSE is the ISEE SSU's only structural unit with a proper name in addition to a number (other units have only numbers), indicating the extreme importance of its responsibilities.

The ISEE SSU also has 15 separate expert units in SSU Departments in Donetsk, Luhansk, Odesa, Lviv, Kharkiv, Dnipropetrovsk, Chernihiv, Rivne, Volyn, Zakarpattia, Ivano-Frankivsk, Ternopil, Chernivtsi, Kirovohrad, Poltava, and the Zhytomyr region. Some of these separate units are zonal; they provide services to several regions (Ukraine Security Service, 2020). The responsibilities of the ISEE SSU include:

- Development of the latest forensic tools, technologies, forensic expertise methods, and the preparation of practice manuals and their implementation in practical activity;
- Scientific, methodological, and informational support of expert activity, analysis of expert practice, development of practice manuals, and other methodological support of the forensic activity.

In this regard, the Institute develops forensic examination methods and organizes their certification and state registration according to the procedure prescribed by the Cabinet of Ministers of Ukraine.

The ISSEE SSU has a Scientific and Methodological Council for Forensic Expertise (SMC), whose main task is to review the Institute's forensic expertise staff's scientific works. The SMC's chairman is the Institute's director. Its first deputy chairman is the deputy director supervising the activities of the CFSE and the head of the center. The other members of the Council are elected by CFSE staff by secret ballot.

It should be noted that forensic institutions must have ISO / IEC 17025 accreditation to guarantee their compliance with the international standard requirements recognized worldwide, ensuring the quality of their forensic activities. Similarly, certain issues related to forensic expertise also require ISO / IEC accreditation regulating international sectoral standards. The ISSEE SSU, for example, is currently developing the

Ukrainian Scientific Research and Training Center for Standardization, Certification, and Quality Problems (DSTU) using a direct translation of the ISO / IEC 27042: 2015 Information technology –Security techniques– Guidelines for the analysis and interpretation of digital evidence. The introduction of international standards in expert institutions not only ensures the use of best practices in forensic activities; it standardizes approaches to these activities. Regardless of whether the examination is conducted in Germany, France, or Ukraine, the basic principles of the examination will be the same (Parfilo & Nizovtsev, 2020).

The ISSEE SSU is the only state forensic institution in Ukraine. Besides being an expert institution, it has research and development units and certain production facilities. As part of improving forensic activities, it develops and implements specialized forensic equipment (specialized software and hardware, means for search and retrieval of forensic evidence, among others) and improves existing ones in close cooperation with experts.

According to part two of Article 8 of the Law of Ukraine, *On the basic principles of cybersecurity in Ukraine*, the main subjects of the national cyber security system are the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and General Headquarters of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine (Law of Ukraine, 2017). The task of ensuring the implementation of the Cybersecurity Strategy Implementation Plan of Ukraine is entrusted to Ukraine's Security Service, its cabinet of Ministers, and the Foreign Intelligence Service (President of Ukraine, 2021).

Each agency forms and develops its expert institutions according to its needs. Among them, only the Security Service of Ukraine has forensic units in its structure. Out of all the expert institutions (Ministry of Justice, Ministry of Internal Affairs, and the Security Service of Ukraine [SSU]), only the SSU's forensic experts are servicemen; in fact, more than half of its experts are service members, some with access to secret State information in the prescribed form (Abrhám et al., 2018).

Because of the peculiarities of the special services' operational and service activities, experts must often conduct forensic examinations and expert studies on materials considered State secrets. In addition, because some SSU experts are servicemen, their involvement effectively supports technical and forensic investigative and operational actions (counterintelligence and operational search), including covert operations or those conducted in combat areas (Joint Forces Operation). Finally, when required, the experts can also perform urgent expertise or expert analyses around the clock; this is especially relevant, for example, when investigating the preparation of a terrorist act to prevent it.

## Types of expertise

The types of expert investigations conducted by the Institute are also influenced by the profile of the Service's activity. For example, only SSU experts can conduct expert inquiries regarding special technical information interception because the responsibility of its investigative units includes crimes related to these specific technical means, including illicit trafficking and espionage. Considerable attention is also focused on computer-technical and telecommunication expertise, particularly the relevant expert unit's proper technical equipment. In this case, special attention is paid to the technical means of obtaining forensic information while preserving the original condition of the objects, avoiding their destruction or damage.

Thus, hardware write blockers are used to avoid making changes to the information content of the examined storage media. These include the EPOS WriteProtector (2021c), a hardware protector designed to prevent accidental or intentional changes to the data on the Hard Drive Disk (HDD) when investigating computer incidents and crimes; the EPOS BadDrive Adapter, a specialized recording blocker used in the recovery process of hard disks with defective and unstable sectors (EPOS, 2021a); the EPOS BadDrive Adapter USB, a specialized hardware recording blocker for removing and recovering information on USB-drives with defective sectors (EPOS, 2021b); the Tableau T6es-B, a compact write-blocker for hard drives with SAS interface (Guidance Software, 2020a); the Tableau T3458is, which is a universal hardware recording blocker that supports several interfaces, including IDE, SATA, SCSI, and USB (Guidance Software, 2021b); the CRU WiebeTech Forensic UltraDock Fudv5.5 Drive Write Blocker, a universal hardware write-blocker that supports several interfaces, including eSATA, USB 3.0, PATA/IDE/EIDE, FireWire 800, SATA II, USB 2.0, SATA III, SATA I, and FireWire 400 (WiebeTech, 2021a); and the CRU WiebeTech USB 3.0 WriteBlocker compact hardware (WiebeTech, 2021b).

In addition, modern forensic software provides the direction of computer and technical expertise in expert units. X-Ways Forensics software, for example, provides support for file systems of various types (FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3 ®, CDFS / ISO9660 / Joliet, and UDF). It detects and accesses alternative NTFS (ADS) data streams, providing the built-in interpretation of JBOD, RAID 0, RAID 5, RAID 5EE, and RAID 6 systems; software RAID implementations in Linux and Windows operating systems and LVM2 dynamic disks; and the ability to read partitions and file system structures from RAW images (.dd), as well as ISO, VHD, and VMDK, among others (X-Ways, 2021). Running X-Ways Forensics without installation allows running it on third-party computers during investigations. Although X-Ways Forensics has effective capabilities for detecting and recovering deleted files, the powerful R-STUDIO Network Technician tool is also used to recover deleted information.

Another powerful software package is the Magnet AXIOM, developed by Magnet Forensics, which is used to examine different media (Magnet Forensics, 2021). This software package enables automated and manual searches for digital evidence in media images and mobile devices running on iOS, Android, Windows Phone, Blackberry, and Windows Mobile. It allows extracting, decrypting, and decoding the structure of mobile file systems devices manufactured by Apple, Blackberry, and Android-based devices. It also allows processing images in E01, DD, and DMG formats, virtual hard disks and virtual machine disks, memory dumps, and physical and logical copies of mobile devices supporting file systems such as NTFS, FAT / ExFAT / TFAT, Ext2-Ext4, ReiserFS, UFS / UFS2, HFS / HFS +, Next3, CDFS, ISO9660, Joliet, and UDF. The Magnet AXIOM complex can also be used to examine (analyze and recover) data in RAM dumps.

Cellebrite UFED Touch 2 software and hardware are used to examine mobile devices, such as mobile phones, smartphones, tablets, and GPS navigators, providing full access to physical, logical, and file system data. Software functions include extracting, decoding, analyzing the information obtained, and compiling a practical report for other participants in the criminal process. The complex's compact format and convenient, intuitive interface help create information content dumps of mobile devices outside the forensic institution (Cellebrite, 2021).

The Center for Forensic and Special Expertise experts use the XRY software and hardware complex to examine mobile devices. Although XRY is usually sold as a software product, the developers produced a unique software and hardware complex based on a moisture-resistant tablet at the request of experts. This technical solution has enabled the effective use of XRY in investigative (search) activities outside the expert unit (MSAB, 2021).

The examination of mobile devices, including outside the unit, is conducted using a software and hardware complex based on the specialized forensic software, MOBILedit Forensic Express PRO (MOBILedit, 2021), and a compact and powerful ultrabook-transformer.

In 2018, the ISSEE SSU received accreditation according to the ISO / IEC 17025 international standard in computer and technical examinations. The Institute is also actively involved in implementing international standards for the investigation of cyber incidents within the Ukrainian regulatory framework, particularly the international ISO-IEC 27042-2016 standard. However, despite the significant efforts in managing expert institutions to successfully provide forensic support in investigating cybercrimes and countering cyber threats in Ukraine, several problematic issues remain unresolved. They are discussed in more detail below.

One of these problematic points is the insufficient scientific and methodological base. According to Russetskiy (2018), the analysis of scientific developments in recent

years shows that the difficulty in generalizing empirical material is that methods for detecting cyberattacks using malicious software (malware) are sealed and mainly carried out by the relevant units of the SSU.

Given its prevalence in cyberattacks and the potential destructive power of malware –a software specially designed or modified for these purposes– performing high-quality investigations of cyber incidents involving the illegal use of such software is becoming increasingly important. However, although approved by the Ministry of Justice of Ukraine, the document, *Methods of computer and technical research in cases related to the establishment of facts of interference in the work of automated systems*[1], did not provide clear answers on how to investigate potential malware nor on the general criteria for deeming a program malicious.

With this in mind, between 2014 and 2018, the ISSEE SSU developed a guideline called the "Forensic examination of malicious software" (Nizovtsev, 2018). It consists of six sections. The first one discusses the subject of malicious software, defining the concept and the task of forensic expertise in this regard. The other sections include the classification of malicious software, some examples of malicious software, the requirements for materials provided for examination, the methods of malicious software examination, and the stages of expert examination. In addition, it provides a list of abbreviations and references. In 2020, these guidelines were completed, and the techniques for malware detection were expanded (Nizovtsev, 2018). Earlier, in 2016, the ISSEE SSU developed guidelines for forensic examination of signs of remote Denial-of-Service attacks, which constitute a significant share of the cyberattacks (Nizovtsev, 2016).

Another significant problem is the lack of highly qualified experts, especially those specialized in telecommunications systems (equipment) examinations and tools. As most cyberattacks are carried out via the Internet or local area networks, experts must have in-depth knowledge of network technologies, including network types, data transmission protocols, and network addressing methods, to conduct examinations. Unfortunately, as of October 2021, only 34 out of 61 forensic experts certified in this specialty nationwide were authorized, a critically low number. The main reason is not the quality of education, as many higher education institutions in Ukraine train highly qualified IT specialists. However, government agencies and even expert institutions cannot offer these specialists competitive wages. Therefore, graduates prefer private companies that can offer much higher salaries.

Expanding on the issue of the definition of malicious software (malware) according to Ukrainian legislation, Article 361-1 of the Criminal Code of Ukraine (2001) defines it as malicious software intended for unauthorized interference involving electronic com-

1 Method registration number 10.9.12, registered on January 29, 2016.

puters, automated systems, computer networks, or telecommunications networks Article 361 provides for liability for unauthorized interference involving electronic computers, automated systems, computer networks, or telecommunications networks leading to leakage, loss, forgery, and blocking of information, distortion of the processing of information, or violating the established procedure for its routing (Criminal Code of Ukraine, 2001). Thus, Ukrainian legislation provides a concordant definition and liability for the mentioned actions.

However, investigators typically appoint forensic expertise during malicious software crime investigations to obtain an expert opinion on whether the program is, in fact, malicious software, and establishing the program's *harmfulness* is beyond the expert's competence. Several technical and legal factors hinder the expert's right to determine whether the program is malicious software, negating the expert's opportunity to do so. The following are among the legal factors.

First, classifying the program as malicious software implies deeming it *unauthorized*. This feature is a legal concept, and the solution of legal issues through expertise is prohibited by Art. 242 of the Criminal Procedure Code of Ukraine (Criminal Procedural Code of Ukraine, 2012b). Secondly, an investigation must take place to determine the designed program's exact purpose and the program developer's (or customer's) intent behind its creation (including unauthorized interventions). In this regard, several problem issues arise, which are discussed below.

*Intention* is a form of guilt, which is an element of the crime. Establishing the corpus delicti –or *legal qualification of the corpus delicti*– is the main object of proof. However, under Ukrainian law, the burden of proof lies with the investigator and prosecutor, not the expert. *Proof* involves the collection of evidence, but the law prohibits an expert from gathering evidence on his or her own. Lastly, the intent is not reflected in the program code (although it may be reflected in some way in the technical documentation); thus, the gathering of evidence is unavoidable.

The following should be noted regarding the technical factors preventing forensic experts from classifying the program as malicious software.

1. There are no purely malicious functionalities. Any function can be inherent in useful programs (for example, deleting a file can be both useful and malicious).
2. There is no one-size-fits-all link between a program's functionality and its purpose; the same function can be used for different purposes.
3. Programs with the same purpose can have significant differences in functionality and the basic principles of operation. Conversely, programs with different uses may have similar functionality.
4. A useful program can be used for harmful purposes and vice versa, depending on the user's intention.

5. Technical failures, like *bugs* or vulnerabilities, in a useful program can perform malicious actions. However, this does not imply that the program is malicious.
6. A useful program can perform malicious actions when run with the wrong settings (the user makes a mistake).

## Discussion

Thus, an expert cannot classify a particular program as harmful upon examination. Instead, the expert can examine the program's functionality to determine whether it can, for example, be used to perform certain (harmful) actions, function in a specific automated information system, and copy itself to removable media (flash carrier). Therefore, when appointing forensic expertise, the correct wording of the questions to the expert is essential. The *Scientific and methodological recommendations for the preparation and appointment of forensic expertise and expert examinations* by the Ministry of Justice of Ukraine (1998) provide a significant amount of information on the functions of certain types of expertise. Similarly, common questions that may be posed to the expert can be found in the Security Service of Ukraine's (2015) document, *On the approval of the Instruction on appointment and conduct of forensic examinations and expert research in the system of the Security Service of Ukraine*, and directories. In addition, examples of questions concerning scientific and methodological materials, specifically, are provided in the sources mentioned above.

The following are general exemplary issues that can be raised for forensic expertise in investigating cybercrime and countering cyber threats.

1. Are there any signs of interference in the telecommunications system?
2. Do the log files submitted for examination (indicate which ones) or the diagnostic utilities report files (indicate which ones) contain evidence of a cyberattack? If so, what cyberattack evidence do the log files or diagnostic utilities report files provided for examination contain?

It should be explained why this last question concerns evidence of a cyberattack and not establishing the fact. Firstly, a cyber incident may be caused by a technical failure, and it is not always possible to positively establish that a technical failure has occurred, especially if the failure occurred outside the affected system. For example, if a computer user visited a web page on the affected system and the computer's browser began to refresh the page indefinitely due to an F5 sticky key, in effect, performing a remote denial-of-service attack. Of course, this can also result from conscious user actions; it is enough to simply press the "F5" key with an object. Technically, the identical thing happened in both cases (Inshyn et al., 2021). However, in the first case, it is a technical failure without any user intention; meanwhile, the second one involves intentional illegal actions by the user. The

log files of the affected automated system will not show the reason for pressing the "F5" key on the user's computer; only information regarding numerous requests of a specific Internet page from a specific computer is recorded. Thus, we are referring only to the signs of a cyberattack. Initial data may not be enough to establish the fact of a cyberattack.

3. Was there evidence of access to the telecommunication system; how was it done?

This question concerns obtaining remote control of the affected automated system. This control is possible with the help of regular operating system tools, usually if the attackers know the relevant authorization data. Also, third-party applications are often used for remote administration, including TeamViewer, Radmin, and Ammyy Admin, again, provided that the attackers have authorization data. However, attackers often use specially designed malicious software to penetrate automated systems –the so-called backdoors.

4. Was there evidence of information transmission (receipt) in the telecommunication system; in what way?

Cybercriminals often download additional files to the affected system (usually specific additional modules of malicious software) or download specific files from this system (for example, keylogger logs).

5. In which operating system is the program provided for examination able to function? (Specify which one is the file name, folders, etc.)
6. Can the program submitted for examination (specify which one) function in the following conditions: (specify the architecture and composition of the computer, the name and version of the operating system, and the presence or absence of certain libraries.)?
7. Is it possible to perform certain actions (specify which ones) with the help of the examined program (specify which one)?

These last questions concern the potential malware's functionality.

Only the most common questions that can be posed to a forensic expert in the investigation of cybercrime and countering cyber threats in Ukraine have been listed. Consideration of all issues and disclosure of their essence is beyond the scope of this publication.

## Conclusion

There are several departmental expert services and institutions in Ukraine. The largest is the expert service of the Ministry of Internal Affairs of Ukraine and expert institutions subordinated to the Ministry of Justice of Ukraine. Although the smallest in employee

numbers, the expert service of the Security Service of Ukraine plays a significant role in supporting forensic, technical, and criminalistic cybercrime investigation and countering cyber threats in Ukraine, given its tasks. The institution is accredited in computer and technical expertise under the ISO / IEC 17025 international standard. It actively participates in the implementation of international standards for cyber incident investigations in the Ukrainian regulatory framework and develops scientific and methodological materials for expert assessments in cybercrime investigations.

The most effective measures directly aimed at combating cybercrime include:

- Increasing the number of scheduled and unscheduled inspections.
- Establishing strict control over the circulation of technical means prohibited or restricted in free civil circulation.
- Adopting the experiences in this area of law enforcement agencies abroad.
- Cooperating with relevant authorities in other countries on detecting, investigating, and preventing crimes in the analyzed area.
- Exchanging experiences in law enforcement; and
- Identifying persons prone to committing crimes in the analyzed area.

However, these measures require further research developments to create effective tools to counter the modern challenges of cybercrime.

Despite considerable efforts to increase the capacity of expert institutions in performing computer and telecommunications expert investigations in cybercrime, there are still significant challenges in this area. They include insufficient scientific and methodological base, lack of highly qualified personnel, and inadequate legislation.

## Disclaimer

The authors declare no potential conflict of interest related to the article.

## Funding

The authors do not report sources of funding for this article.

## About the authors

***Andrii Padalka*** is a Ph.D. in Legal Science, Deputy Director of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, and Associate Professor at the Department of Financial Investigations of the University of the State Fiscal Service of Ukraine.

https://orcid.org/0000-0003-1433-1030 - Contact: andrii_padalka@edu.cn.ua

## References

Abrhám, J., Britchenko, I., Jankovic, M., & Garškaite-Milvydiene, K. (2018). Energy security issues in contemporary Europe. *Journal of Security and Sustainability Issues, 7*(3), 387-398. https://doi.org/10.9770/jssi.2018.7.3(1)

Cellebrite. (2021). *UFED Touch 2*. https://www.cellebrite.com/en/ufed/

Civil Procedural Code of Ukraine. (2004). Law No. 1618-IV. Base "Legislation of Ukraine." March 18, 2004. https://zakon.rada.gov.ua/laws/show/1618-15#Text

Code of Administrative Procedure of Ukraine. (2005). Law No. 2747-IV. Base "Legislation of Ukraine." July 6, 2005. https://zakon.rada.gov.ua/laws/show/2747-15#Text

Commercial Procedural Code of Ukraine. (1991). Law No. 1798-XII. Base "Legislation of Ukraine." November 6, 1991. https://zakon.rada.gov.ua/laws/show/1798-12#Text

Criminal Code of Ukraine. (2001). Law of Ukraine No. 2341-III. Article 361-1. https://zakon.rada.gov.ua/laws/show/2341-14#Text

Criminal Procedural Code of Ukraine. (2012a) Law of Ukraine No. 4651-VI. Article 4651-VI. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Criminal Procedural Code of Ukraine. (2012b). Law of Ukraine No. 4651-VI. Base "Legislation of Ukraine." April 13, 2012. https://zakon.rada.gov.ua/laws/show/4651-17#Text

Criminal Procedural Code of Ukraine. (2012c). Law of Ukraine No. 4651-VI. Code of Ukraine. May 20, 2012. https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Daly, M.K. (2009). *The Advanced Persistent Threat (or Informationized Force Operations)*. USENIX. https://static.usenix.org/event/lisa09/tech/slides/daly.pdf

EPOS. (2021a). *EPOS BadDrive Adapter* https://www.epos.ua/view.php/ua/products_epos_baddrive_adapter

EPOS. (2021b). *EPOS BadDrive Adapter USB* https://www.epos.ua/view.php/products_epos_baddrive_usb

EPOS. (2021c). *EPOS WriteProtector*. https://www.epos.ua/view.php/en/products_epos_write_protector

Guidance Software (2020a). *Tableau T6es SAS Forensic Bridge.* https://tableau.guidancesoftware.com/pdf/en/Tableau_T6es_Product_Brief.pdf

Guidance Software (2021b). *Tableau Hardware T3458is*. https://tableau.guidancesoftware.com/index.php?pageid=specs&xml=spec_t3458is.xml&model=T3458is

Guliyeva, A., Britchenko, I., & Rzayeva, U. (2018). Global security and economic asymmetry: A comparison of developed and developing countries. *Journal of Security and Sustainability Issues, 7*(4), 707-717. https://doi.org/10.9770/jssi.2018.7.4(8)

Inshyn, M., Vakhonieva, T., Korotkikh, A., Denysenko, A., & Dzhura, K. (2021). Transformation of labor legislation in the digital economy. *InterEULawEast, 8*(1), 39-56. https://doi.org/10.22598/iele.2021.8.1.3

Kozlovskyi, S., Butyrskyi, A., Poliakov, B., Bobkova, A., Lavrov, R., & Ivanyuta, N. (2019). Management and comprehensive assessment of the probability of bankruptcy of Ukrainian enterprises based on the methods of fuzzy sets theory. *Problems and Perspectives in Management, 17*(3), 370-381. https://doi.org/10.21511/ppm.17(3).2019.30

Law of Ukraine (1994). *On forensic examination*. No. 4038-XII. Article 7. February 25, 1994. https://zakon.rada.gov.ua/laws/show/4038-12#Text

Law of Ukraine. (2017) No. 2163-VIII. *On the basic principles of cybersecurity in Ukraine*. Article 8, part 2. https://zakon.rada.gov.ua/laws/show/2163-19#Text

Magnet Forensics. (2021). MAGNET AXIOM. https://www.magnetforensics.com/products/magnet-axiom/

Ministry of Justice of Ukraine. (1998). Instruction No. 53/5. *Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert studies*. https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

Ministry of Justice of Ukraine. (2021). *Transition Book: Mission and Responsibilities*. https://www.pravojustice.eu/storage/app/uploads/public/5d7/f77/c88/5d7f77c88c23b147881339.pdf

MOBILedit. (2021). *MOBILedit Forensic Express PRO*. https://www.mobiledit.com/online-store/forensic-express

MSAB. (2021). *XRY Mobile Forensics and Data Recovery Software*. https://www.msab.com/product/xry-extract/

Nizovtsev, Yu.Yu. (2016). *Forensic examination of signs of interference in the work of information and telecommunications systems by remote attacks on denial of service: guidelines.* Kyiv: ArTek Publishing House.

Nizovtsev, Yu.Yu. (2018). *Forensic examination of malicious software: guidelines*. Kyiv: ArTek Publishing House.

President of Ukraine. (2021). Presidential Decree No. 447/2021. *On the Cyber Security Strategy of Ukraine*. Decision of the National Security and Defense Council of Ukraine. August 26, 2021. https://www.president.gov.ua/documents/4472021-40013

Russetskiy, A. A. (2018). Place of Forensic Science in the Cyberthreats Prevention System in Field of a Ukrainian Information Security. *Theory and Practice of Forensic Science and Criminalistics*, *18*, 263-271. https://doi.org/10.32353/khrife.2018.29

Security Service of Ukraine. (2015). Request No. 371. *On the Approval of the Instruction on Appointment and Conduct of Court Appraisals and Expert Surveys in the System of the Ukrainian Security Service.* https://zakon.rada.gov.ua/laws/show/z0738-15

Ukraine Security Service, Order of the Central Department. (2020). Request No. 80. *On approval of Amendments to the Regulation on the Security Service of Ukraine Expert-Qualification Commission and Certification of Court Experts*. https://zakon.rada.gov.ua/laws/show/z0310-20#Text

WiebeTech. (2021a). *Forensic UltraDock FUDv5.5 by* CRU. https://www.cru-inc.com/products/wiebetech/forensic-ultradock-v5-5/

WiebeTech. (2021b). *USB 3.0 WriteBlocker by CRU*. https://www.cru-inc.com/products/wiebetech/usb-3-0-writeblocker/

X-Ways. (2021). *X-Ways Forensics: Integrated Computer Forensics Software*. http://www.x-ways.net/forensics/

Yaroshenko, O. M., Vapnyarchuk, N. M., Lozovoi, S. V., Yakovleva, G. O., & Yakovlyev, O. A. (2018). General-compulsory medical insurance: World experience. *Journal of Advanced Research in Law and Economics, 9*(5), 1829-1838. https://doi.org/10.14505//jarle.v9.5(35).38