Forensic Examination of Electronic Documents

Submitted: 30 November 2021
Revised: 13 January 2022
Accepted: 24 January 2022

Viktor S. Sezonov[*]
https://orcid.org/0000-0002-2580-2953
Mykhailo I. Fialka[**]
https://orcid.org/0000-0001-5599-3335
Eduard M. Poltavski[***]
https://orcid.org/0000-0002-7434-7061
Nataliia M. Prokopenko[****]
https://orcid.org/0000-0003-4985-937X
Maryna V. Fomenko[*****]
https://orcid.org/0000-0002-6606-5769

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v14i2.40965

Abstract

[Purpose] The purpose of the study is to reveal the concept and essence of forensic prevention of crimes of forgery of electronic documents, to identify problems in the use of information to establish a system of countering crime and document management.

[Methodology] The following approaches were used in the work: system-structural, dialectical, empirical. Forgery of electronic documents and their use is investigated not only within the framework of a single criminal case but also by a set of crimes committed depending on the mechanism that is the main one in the structure of criminal technologies.

[Findings] Lack of skills and knowledge about the latest forms of documents, methods of their forgery and use in the field of forensic investigations determine the reasons for the development of this condition. The analysis of investigative and judicial practice shows that cases of forgery of electronic documents are moved to separate proceedings due to the inability to fix the person who committed the crime. In some cases, court procedures are returned for additional investigation, since investigators cannot establish mechanisms for falsification tools and bring appropriate charges.

[Practical Implications] The practical significance lies in the formation of proposals for improving or making changes to the legislation, effectively improving the activities of law enforcement agencies involved in countering or combating the forgery of documents.

[*] Viktor S. Sezonov is a PhD in Law, Senior Forensic Expert at the Department of Automotive Research and Forensic Research of Vehicles, Kharkiv Research Forensic Center of the Ministry of Internal Affairs, Kharkiv, Ukraine. E-mail: v.sezonov7514-1@kpi.com.de.

[**] Mykhailo I. Fialka is a PhD in Law, Associate Professor at the Department of Criminal Law and Criminology, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.

[***] Eduard M. Poltavski is a PhD in Law, Deputy Head of the Department of Social and Humanitarian Disciplines, National Academy of the National Guard of Ukraine, Kharkiv, Ukraine.

[****] Nataliia M. Prokopenko is a PhD in Law, Senior Lecturer at the Department of Criminal Law and Criminology (Faculty No. 6), Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.

[*****] Maryna V. Fomenko is a Senior Lecturer at the Department of Criminal Law and Criminology, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.

Keywords: Forgery. Falsification. Law enforcement agencies. Countering a crime. Expertise.

INTRODUCTION

Bringing false documents to the market is a threat to the stability and integrity of the state's legal system. This process creates natural opportunities for the use of stolen data and forged documents, which acts as an extremely negative way to destabilize the legal system and the national economy, which leads to citizens' distrust of the state authorities. Forged documents are often used by attackers to commit other crimes, such as fraud, misappropriation or extortion of loans, acting as a tool aimed at destroying other traces of the crime committed. For the development of forensic technologies, it is extremely valuable to share information about progress in various fields of Science, which plays an important role in preventing and combating crime. Optimization of international cooperation in this aspect contributes to ensuring effective working methods, being both a preventive tool and a mechanism for collecting evidence and prosecuting crimes related to Information Systems and computer networks (SCHNEIDER and SEIDEL, 2014). Modern investigations should consider this relatively new area in proceedings related to the prevention and detection of computer and electronic crimes, which are closely related to data protection concepts and security policies in computer networks. They encourage the identification of prospects for the development of forensic methods using appropriate tools to uncover violations.

Crimes of forgery pose a threat to the proper functioning and development of individual individuals or legal entities, as well as to the country as a whole. The rapid increase in crime and attempts to reduce it undoubtedly affect progress in the field of criminology. Falsification of documents is often a preparatory step for committing further illegal actions (BAKER, 1956; CIARDHUAIN, 2004). Offences of this type pose a serious threat to economic stability and the correctness of the actions of state bodies since the scale of forged documents is very large today. The developing trend of modern technologies and free access to them contributes to the dynamic growth of financial and economic activities and various types of advanced technologies with a low level of security. This led to some threats to public administration bodies and the sphere of business operations. Counterfeiting violations have not changed; they evolve and develop only the tools used for data carriers. Here you should take into account such classic storage media as physical and electronic documents, with a special emphasis on digital technology. In this context, innovative technologies are used to fake or modify information, payment means, credit cards, and identity cards (KENT et al., 2006; KERNIAKEVYCH-TANASIICHUK et al., 2021).

When analysing cases, the culprit often changes documents in an unauthorised way to create the appearance of the correct action or hide it. This processing can apply to all types of documents: contracts, resumes, bank guarantees, balance sheets, invoices, reports, and websites. Changes made to them may be the following: physical - the document can be physically changed by deleting entries or links, handwriting information; intellectual – the content does not correspond to reality, false description of the services provided, false signatures. Signatures are the main form of authentication and give legal meaning to documents (KERNIAKEVYCH-TANASIICHUK et al., 2021). For this reason, they are subject to numerous fakes. Knowledge of graphology and signature forgery techniques can be an effective tool in the hands of a criminal. Depending on how the signature is falsified, the process can be divided into five groups: signatures created by technical reflection or copying; signatures that are more or less similar to authentic ones, imitating them; signatures that sign the data of another person but made without an original template; signatures made without trying to adapt their graphic visuals to the original sample; signatures called Auto-forgery, which consist in falsifying their signature, then interrogating its authenticity (KAM et al., 1994).

The purpose of the study is to reveal the concept and essence of forensic prevention of crimes of forgery of electronic documents, to identify problems in the use of information to establish a system of countering crime and document management.

MATERIALS AND METHODS

The theoretical and methodological basis of the research consists of the following approaches: system-structural, dialectical, empirical. The system-structural approach provided for the study of individual elements of forgery of electronic documents and the scope of their use. The tools of the elements made it possible to detail the composition of the criminalistics process for further decomposition of each functional factor, aimed at considering the influence of external and internal factors of committing an offence in the form of falsification of an electronic document. The correlation of industry concepts takes into account their broad nature of social origin, existing in the law enforcement system, as well as the regulatory structure, which ensures the construction of system norms of interrelations, forming an integral structure for organising investigations and examinations on forgery of electronic documents in various sources of modern technologies.

The dialectical paradigm considers the forensic investigation of electronic documents as a controversial process that seeks to move and develop at the latest stage of law enforcement. Its materialism dictates the ideology of class struggle

to create a claim as a mechanism of separate structural processes of legal reality caused by contradictory opposites to distinguish the socio-legal realities of the material legal canon. The categorical dialectical potential of Criminalistics properties exists in the general objective reality, stating the theoretical foundation of the criminal's consciousness in the process of violating the law. The dialectic method has revealed modern and improved means of countering or combating the forgery of documents by putting forward factual legal hypotheses and materials to carry out specific theoretical checks and generalisations. Such justifications and properties contribute to predicting and proving explanations and legal phenomena that determine the facts of Forensic Crime Prevention and document management while requiring establishing a relationship between the ways of finding out the subordination and content of the entity.

The empirical approach analysed the main generalisations of concepts and systematised descriptions of specific research data aimed at supporting the issues of countering and combating document forgery, which occurs based on observations, comparisons and measurements. Practical aspects formed the results of observations and legal laws to improve the activities of the system of law enforcement agencies existing in the general system of a criminal structure. Theoretical conceptual schemes served as postulates of reality for identifying the facts of a deep understanding of the falsification of electronic documents. The information base was:

– resolutions of the plenum of the Supreme Court;

– laws and acts of Ukraine that regulate document flow and establish criminal liability for forgery and use of electronic documents, as well as the activities of law enforcement and regulatory bodies;

– criminal cases under certain articles;

– forensic examinations of research institutes and institutions of the Ministry of internal affairs of Ukraine;

– materials of the judicial and investigative practice of world countries;

– the work of Ukrainian and international scientists in the field of criminal activity.

RESULTS AND DISCUSSION

The evolution of crimes related to the forgery of electronic documents and means of payment is unfavourable for the safety of citizens and public order. Disregarding the law and legal protection bodies contributes to the expansion of the sense of threat to their security in society. In the bodies responsible for the state of security of citizens and order, they are obliged to take specific responsibility to deter a falsified crime (YARASKAVITCH et al., 2008). Despite a significant increase in crime, traditional schemes of struggle are still used. Such factors seriously undermine the effectiveness of counteraction, including non-

compliance of organizational structures of law enforcement agencies and the judiciary with the requirements of productivity of actions. The science whose main task is to work out optimal and modern methods of resisting crime is criminalistics. With the help of scientific methods of Criminalistics, it is possible to use skills actively for intelligence, detection, proof and preventive activities in the process of combating forgery of electronic documents. It constantly improves the tactics of means and forms of its activities, using the achievements of Technical Sciences, develops forensic medical technologies. The tightness of organised systems and their solidarity show the limited effectiveness of counteraction, which requires, first, serious involvement of budgetary resources, as well as well-trained and comprehensively trained law enforcement and judicial authorities.

In the modern world, electronic crime is a serious social problem. Forensic tactics play a major role in this regard. Its task is to analyse in-depth the main issues that are constant in the course of the fight, ranging from identifying threats, identifying crimes and their perpetrators, collecting evidence and preventing violations. Such knowledge is necessary to perform the daily activities of employees considering criminal cases of forgery of electronic documents. Criminalistics of electronic documents reveals the mechanisms of criminal activity and develops tactical and technical measures for detection, proof and resistance (BAKER, 1956; BAXENDALE and RENSHAW, 2019). The attacker is responsible for committing the established act, and the judicial authorities provide certain evidence of its commission. Otherwise, the process of impunity spreads, which leads to the next criminal act. In the fight against such offences, one should take into account the fact that laws and the best training of the judiciary in the field of knowledge of regulations will not determine the effectiveness of such a phenomenon. Only the cooperation of qualified specialists, prosecutors and, properly trained judges who consider criminal cases and the public can significantly contribute to increasing the number of solved crimes and reducing them in the future.

Criminalistics of combating forgery of electronic documents is gradually developing due to the demand of law enforcement agencies and the judiciary for such a universal and effective set of methods and tools that will allow us to rationally identify offenders and prove their guilt in the context of the growth of this type of crime. The practice of forensic medical examination is carried out in the activities of identifying those responsible for acts. It serves as the basis for the formation of justice in the disclosure of violations of electronic document management. The concept of criminal law realities refers to the dynamic development of dangerous phenomena for the internal and external security of the state, including those that require the implementation of long-term strategic

actions to contain and neutralize them. The strategy of Criminalistics of electronic documents is based on the analysis of determining the forecast of the course of the phenomenon, followed by the development of methods for its prevention and the use of a set of resources for future struggle. Such examples are scientifically established personalities of linear samples of human fingerprints, handwriting or voice features that allow for identification tests. At this stage, operational activities are legally defined and confidential within the framework of countering falsification of document flow (MICHAEL and BARRETT, 2011; FIALKA, 2019).

Cases of fraud with documents, including electronic ones, remain one of the biggest problems, as forgery is often a key element for committing other criminal acts. Expertise is becoming an important aspect of combating these crimes due to the rapid development and improvement of falsification methods. Despite increased security measures, criminals are using new methods that include obtaining authentic documents under false pretenses. These mechanisms make it difficult for the relevant authorities to detect violations. To strengthen the role of combating document fraud, it is important to provoke the development of a specific system of tasks aimed at supporting and addressing threats related to facilitating the recognition of false documents. It is necessary to conduct expert training on the detection of forgery of electronic documents, take an active part in the development of analytical reports, workshops and textbooks, sharing knowledge and skills on the issues of this criminalistics. The action plan focuses on identifying and identifying the perpetrator of the offence, as well as addressing any gaps through close cooperation between the state and the relevant institutions.

Although forgery of electronic documents is a general term, it covers many different methods. There are several forms of atrocities that pose a threat: full reproduction of the document, but in practice this form does not go unnoticed, since the display of the original is often poorly performed; modification of one or more elements based on authentic information; clean documents stolen for personalisation; completely created by an attacker. Therefore, the risk of falsification today is very high and is an important issue, because offenders use more and more complex techniques and do not hesitate to achieve their goals regularly. Criminals are becoming stronger and more diverse, increasingly resorting to forms of cooperation aimed at facilitating their activities. The specificity of the forms depends on the tendency of important innate or socially determined permanent features of the criminal, while situational factors that characterise the criminal act are underestimated. Therefore, it is necessary to apply specific measures and solutions that can be adapted to the legal system, procedures, social, political and economic characteristics of the state. The implementation of these programs is a complex and time-consuming process, and

their effectiveness at the present stage of Criminalistics development is quite limited (ZHANG et al., 2019).

The phenomenon of forgery of electronic documents puts criminal activity at a higher level of development, which is facilitated by the dynamic growth of the economic sphere and access to financial types of advanced low-security technologies. Because of various payment forms, a new category of crimes has appeared which is carried out using electronic storage media and payment cards. There is also an active development of this type of violation of the law due to the widespread use of Cards. On the other hand, standard electronic documents, such as contracts, invoices, and others, play a role, with the help of which a large number of different types of atrocities can be committed. The most common is the illegal use of a stolen ID or the processing of personal electronic media by third parties. Therefore, measures to prevent forged electronic documents depend on the methods of technical expertise and the social degree of legal development of technical conditions and society as a whole. Increasing the detail of certain characteristics of a document counteracts fraud, because the greater their readability and appearance, the more difficult it is to implement the falsification process. Electronic proof is personalized visually and electronically during its issuance process. Visual personalisation can be done if the proof of security is confirmed.

The Electronic Document Security system should be based on a trade-off between simplicity and efficiency. Modern technologies make it possible to turn a huge electronic component into a complete service and service function. The number of these functions should be limited to minimise the risk of unforeseen events that may harm the interests of the subject (FERREIRA et al., 2020). The important thing of checking electronic documents often goes to another level due to the human factor, so developing the habit of checking them minimises the risk of forgery. Taking advantage of these advantages of modern technologies, you should pay attention to safety standards that provide proper protection against falsification. Forgery of identity documents is now widely used in the form of fraud. This involves making changes to the existing identity document. Unlike a complete forgery, where the document is fully reproduced, it is only about making changes that can be simple or very complex. Therefore, it is not always easy to detect them. Significant interpretations can lead to a complete modification of the identity of the original document. This type of disruption often occurs when establishing long-distance relationships. The criminal will use another person to use a service that they do not have access to.

References to individual, environmental, social and macroeconomic determinants of crime are the starting point for thinking about the theory and practice of preventing falsifications. Special emphasis is placed on combating

electronic crime by changing the situation itself. Prevention and counteraction programs are aimed at neutralising social phenomena recognised as the causes of crimes, or at changing certain features of the offender. Dissatisfaction with the philosophy of crime prevention based on an etiological approach led to a more detailed analysis of the circumstances of its commission, physical conditions and motivation resulting from it. Proponents of the situational direction in criminology believe that the potential of a criminal, as a rule, does not act on the impulse to a greater or lesser extent, consciously analysing the situation before committing a crime and making a decision on how to commit it. The emergence of a situational trend to prevent violations should not mean the rejection of prevention methods that take into account certain social factors that refer to the conditions of resistance to the forgery of electronic documents. The two-dimensional typology of the crime prevention program is aimed at the general public and social risk groups, coming into conflict with the law or becoming a victim of a crime (BERGMAN, 2001; CASEY, 2011).

Forgery of electronic documents is quite common in judicial practice. For offenders, it is enough to get access to a computer that stores an electronic signature in the form of a digital file. By copying the signature, attackers get the opportunity to conclude various kinds of transactions on behalf of the victim. In this way, they can gain access to an electronic wallet and easily withdraw money from an electronic account, while using a fake signature. The results of the study of criminal cases pointed to the imperfection of the current legislation, which creates errors in the qualification of the crime committed by the investigation and the court. Experts face difficulties in classifying certain documents as official, due to the lack of clear criteria and a single concept of this phenomenon. Analysis of judicial errors indicates that they are not always associated with ignorance of the norms of substantive law. Although some attention is paid to the problems of forgery of electronic documents in the theory of criminal law, the degree of its development remains insufficient, since the technical sphere of life of the population has changed significantly since the adoption of the relevant codes. Individuals and legal entities have rights, bear obligations, and can create them by signing relevant decisions or acts. The signature confirms that the person specified in the document manages the rights or obligations.

The problem of signature forgery for criminal imitation of someone else's will has a long history. The issue of using an electronic signature in modern conditions does not cause a public outcry until cases of electronic fraud of documents where someone else's electronic signature was used have become widely popular. The technology of manufacturing electronic signature keys according to Ukrainian algorithms is very reliable, there are no ways of its mathematical forgery, so trust in certified electronic signature tools, and as a

result, in authentication mechanisms using them, is quite high. Another important condition for legal turnover is trust in the information entered in the electronic signature certificate, which is determined by the confidence of the identification procedure of the person receiving the certificate. Because the procedure and conditions for identification are not sufficiently described in the current legislation, there are primary prerequisites for violating the law. The current legislation contains a whole range of measures that regulate the requirements of many innovations, but still do not pay enough attention to identification procedures. It is important to avoid excessive restriction of the possibility of using an electronic signature (STOLC et al., 2017).

Monopolization of the issue of Electronic Signature Certificates by the state carries the risk of reducing the convenience and potential economically favourable conditions, without solving the problem at the root of its occurrence - at the level of recognition of the certificate holder and entering relevant information in the electronic signature. Considering proposals to tighten the requirements for the current legislation, it should be noted that currently there is no information about proven cases of direct damage caused because of falsification activities, and assumptions about systemic violations are not confirmed by judicial practice. This indirectly indicates the insufficiency of organizational measures taken to ensure the responsibility of intruders. At the same time, based on the analysis of violations, it can be seen that they are mainly associated with an insufficient level of identification of persons, which initiates the development of gaps in the regulation of procedures for checking electronic documents. The reason for the occurrence of such atrocities can be considered a relatively accessible possibility of implementing criminal plans through the illegal acquisition and use of electronic information, as well as signatures. Illegal actions lead to crimes where the material carrier of an electronic signature is the instrument of committing a violation in the hands of the perpetrator.

Investigating the crimes of forgery of electronic documents requires special skills and serious efforts from law enforcement agencies. It is important to prevent such crimes by modifying the legal framework in the sphere of circulation of electronic media and information in general. There are two direct ways to improve the legislation: regulating the procedure and conditions for identifying a person when introducing his materials into circulation, as well as ensuring comprehensive responsibility of participants in relationships in this area, including preventive - at the early stages of electronic signature turnover (POWERS, 2011). According to the processes of Electronic Document Management, the secure role of security tools is not sufficiently developed. This stage can be automated as much as possible, if the formats for creating and exchanging information materials are standardised. The difficulty of establishing

compatibility both at the level of national legislation and at the level of electronic document standards leads to the fact that free space is not established due to the appropriate level of legal support and standardisation. Within the framework of the electronic order, it is necessary to introduce an element for the development of communication in the digital world. Problems with not achieving these goals lie in the difference in national approaches and the inertia of legislative changes.

The growing dependence of the Information Society on technological tools of electronic document management makes the sphere of law enforcement agencies constantly interested in the digital world due to the expansion and increase of the criminal structure in this space. Defining the principles of liability for forgery of electronic documents, the legislator recognizes that preparatory activities for this type of falsification are also punishable. Communication with another person to commit a crime is an example of preparatory measures as well as drawing up an action plan, collecting tools or other means necessary to commit a prohibited act. The directions of innovative technologies in the development of Criminalistics will determine trends. These multidimensional technological phenomena make it necessary to consider issues of different jurisdictions related to forensic expertise. The problem of an overabundance of devices that require simultaneous use to analyse increased mobility and portability hinders the process of improving electronic security. With the use of cryptographic mechanisms, the freedom to conduct forensic research and analysis is restricted. Their main challenge, of course, is to support and use research methods and processes to counteract the forgery of electronic documents in the period of the rapid evolution of the unpredictable digital world. Such challenges for forensic surveillance can successfully activate the structure of productive prosecution of crimes in the electronic aspect (BAEZA-YATES and RIBEIRO-NETO, 1999; CHRISTLEIN et al., 2012).

Identification of those responsible for crimes of falsification of electronic documents is based not only on conducting specific investigative actions, but also requires special knowledge of the motives of the criminal and the circumstances of the commission of atrocities. Criminal liability is imposed not only on the perpetrator of a false document but also on any person who uses it. The condition of a criminal record is, of course, that the prosecutor demonstrates that the person using such a document knew that it was forged. Usually, the fact of such awareness is obvious. Due to the growing importance of forensic methods achieved using new technologies, including research conducted on digital platforms, crime detection usually involves some complex measures that reveal the facts of the crime. Knowledge and skills of verifying the authenticity of an electronic document and processing monitoring data collected during the period of committing an offence help to assess the effectiveness of evidence. During the

implementation of investigative actions, some algorithms are carried out aimed at identifying and confirming the identity of the perpetrator. Well-known methods of activity need to be modernised because the classic frequently used mechanisms in the fight against forgery of documents are impossible and ineffective. The growing role of forensic methods for the effectiveness of investigations creates a demand in the labour market for special knowledge on the technique and tactics of effective investigation in this area (KANUNGO et al., 1993).

The development of technology undoubtedly supports and increases the efficiency of experts' work. The use of modern programs and devices, in many cases, provides increased accuracy, reliability and efficiency of identification and isolation of a person who has committed forgery of electronic documents. Replacing manual work not only speeds up the work of specialists but also improves the preparation of materials with greater accuracy. Although the specific form of an electronic document is not important from the point of view of criminal legislation, it is undoubtedly of a material nature, since it is a specific object or carrier of information. Therefore, whether the document is official or private, the provisions of the legislation should still regulate a variety of issues related to crimes against forgery of electronic document management. When the risk of realizing the signs of this offence is significant, it provides for the obligation to submit and submit, at the request of the court, all types of documents related to these facts and relevant for resolving the case. Everyone may be obliged to submit an electronic document or certain information that is available and is proof of the fact of committing a crime by a court decision at a certain time and place (BANDURKA and LITVINOV, 2016; FIALKA, 2018; KERNIAKEVYCH-TANASIICHUK et al., 2021).

CONCLUSIONS

Thus, the rapid scale of technology sets the pace of the spread of such a type of crime as forgery of electronic documents. The widespread use of innovative technologies in Ukraine has led to the formation of new mechanisms for electronic automated document management based on modern platforms. The number of offenses in the field of computer technology is constantly increasing, which is associated with insufficiently developed methods of forensic activity and a high level of latency, which interfere with effective crime detection and timely response. To counteract these crimes, Ukraine has adopted some normative legal legislative acts, among which the most important are the Criminal Code of Ukraine, resolutions of the Cabinet of Ministers of Ukraine, the Criminal Procedure Code of Ukraine, which relate to the activities and regulation of electronic and magnetic documents. After all, these concepts are quite vulnerable compared to paper materials and are directly dependent on the hardware, which

forms the specifics of logical and physical structures that do not coincide with traditional ideas. Therefore, the further development of Forensic Science in this aspect is inextricably linked with the modernisation of organisational and legal support.

In the structure of Forensic Research, through the use of an effective set of specialised knowledge of forensic technical and computer expertise of Electronic Document Management, a certain system of signs of the manufacturing method and their forgery is formed, which help to implement productive identification. So, the use of innovative technologies in the forgery of electronic documents sets some tasks for forensic expertise, among which the main ones are: improving existing and creating new expert methods to combat this activity, legal regulation of their use, development of hardware, technical and methodological support, training of qualified specialists, improving the current legislative framework.

REFERENCES

BAEZA-YATES, R. A., & RIBEIRO-NETO, B. (1999). *Modern information retrieval*. London: Addison Wesley.

BAKER, J. N. (1956). Law of disputed and forged documents. *Michigan Law Review*, 54(5), 730-732.

BANDURKA, O. M., & LITVINOV, O. M. (2016). The concept and content of special criminological crime prevention. *Bulletin of the Criminological Association of Ukraine*, 2(13), 98-108.

BAXENDALE, D., & RENSHAW, I. D. (2019). The large-scale searching of handwriting samples. *Journal of the Forensic Science Society*, 19(4), 245-251.

BERGMAN, M. (2001). The Deep web: surfacing hidden value. *Journal of Electronic Publishing*, 7(1). https://doi.org/10.3998/3336451.0007.104.

CASEY, E. (2011). *Digital evidence and computer crime*. London: Elsevier Academic Press.

CHRISTLEIN, V., RIESS, C., JORDAN, J., & RIESS, C. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on Information Forensics and Security*, 7(6), 1841-1854.

CIARDHUAIN, S. O. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, 3(1), 1-22.

FERREIRA, L., HUANG, J., & CAI, R. (2020). A Copy-proof scheme based on the spectral and spatial barcoding channel models. *IEEE Transactions on Information Forensics and Security, Tampere*, 15, 1056-1071.

FIALKA, M. I. (2018). Forgery of documents as a way to evade military service (criminal law analysis). *Bulletin of the Criminological Association of Ukraine*, 2(19), 77-86.

FIALKA, M. I. (2019). The mechanism of individual criminal behaviour is associated with the falsification of documents. *Legal Scientific Electronic Journal*, 5, 266-270.

KAM, M., WESTEIN, J., & CONN, R. (1994). Proficiency of professional document examiners in writer identification. *Journal of Forensic Sciences*, 39(1), 5-14.

KANUNGO, T., HARALICK, R., & Phillips, I. (1993). *Global and local document degradation models.* In: *Proceedings of the Second International Conference* (pp. 5-13). London: IEEE.

KENT, K., CHEVALIER, S., GRANCE, T., & DANG, H. (2006). *Guide to integrating forensic techniques into incident response.* Gaithersburg: National Institute of Standards and Technology.

KERNIAKEVYCH-TANASIICHUK, Y. V., SEZONOV, V. S., NYCHYTAILO, I. M., SAVCHUK, M. A., & TSAREVA, I. V. (2021). Problems of forensic identification of handwriting in forensic examination. *Journal of the National Academy of Legal Sciences of Ukraine*, 28(1), 195-204.

MICHAEL, G., & BARRETT, D. (2011). *Computer forensics jump start.* Medway: Sybex.

POWERS, D. (2011). Evaluation: From precision, recall and f-measure to roc. *International Journal of Machine Learning Technology*, 2(1), 37-63.

SCHNEIDER, U., & SEIDEL, U. (2014). *Current aspects in machine authentication of security documents. Part I: Do we need optical document security?* Retrieved from: https://www.semanticscholar.org/paper/Current-aspects-in-machine-authentication-of-Part-1-Seidel/8b05a8dcbf458d0717b4c88e2e50369c3eb93c02. Access date: 04 August 2021.

STOLC, S., WILD, P., & VALENTIN, K. (2017). *On interoperability of security document reading devices*. In: Proceedings – 2016 European Intelligence and Security Informatics Conference, EISIC 2016 (pp. 9-15). Uppsala: IEEE Computer Society.

YARASKAVITCH, L., GRAYDON, M., & TOBIN, T. (2008). Controlled electrostatic methodology for imaging indentations in documents. *Forensic Science International*, 177(2-3), 97-104.

ZHANG, L., CHEN, C., & MOW, W. H. (2019). Accurate modeling and efficient estimation of the print-capture channel with application in barcoding. *IEEE Transactions on Image Processing, Tampere,* 28(1), 464-478.