UDC 004.9:330 DOI: 10.30929/1995-0519.2021.1.59-65

COMMERCIAL SECRET OF THE ENTERPRISE PROTECTION BASED ON STEGANOGRAPHIC ALGORITHMS

V. Kolenko, V. Nakonechna, Y. Anosova
Kherson polytechnic vocational college of the State university "Odesa polytechnic"
ORCID: 0000-0001-6376-1278; 0000-0001-6244-3585; 0000-0003-1465-3638

Purpose. The article proposes an approach to protection against unauthorized access to information about services, enterprise management, financial activities, business planning, marketing ideas, customer bases, technological strategies, production technology and recipes, other confidential information that is a commercial secret of the enterprise. This approach involves several IT tools usage, as electronic digital signature and steganographic algorithms. The electronic digital signature functionality is described. **Methodology.** The method of using an electronic digital signature is schematically shown. The connection between digital watermarks and the electronic digital signature is offered. The description of requirements to digital watermarks is executed. A method of authentication using an electronic digital signature is proposed, which allows proving the authorship during the examination. **Results.** The article describes a mathematical algorithm for embedding a digital watermark, using a secret key, timestamps, steganographic file system StegFS for Linux, hiding data in file formats unused areas, substituting characters in file names, text steganography. Using reserved fields of computer file formats - the essence of the method is that the part of the extension field that is not filled with information about the extension, by default is filled with zeros. **Originality.** The method of using special properties of format fields that are not displayed on the screen is based on special "invisible" fields to obtain footnotes, pointers. During the experimental verification of the simultaneous use of several technical security measures (digital watermark, electronic digital signature and timestamp), a significant result was obtained, which suggests an increase in the level of electronic document security in the system provided the organization and use of such protection. **Practical value.** Today's common steganographic methods of protecting raster images for embedding stable digital watermarks are mainly based on the statistical and physiological redundancy usage.

Key words: confidentiality, enterprise, stegonography, information, symbols, authentication.

ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПІДПРИЄМСТВА НА ОСНОВІ СТЕГОНОГРАФІЧНИХ АЛГОРИТМІВ

В. В. Коленко, В. І. Наконечна, Ю. П. Аносова
Херсонський політехнічний фаховий коледж Державного університету «Одеська політехніка»
ORCID: 0000-0001-6376-1278; 0000-0001-6244-3585; 0000-0003-1465-3638

Запропоновано підхід до захисту від несанкціонованого доступу до відомостей про послуги, управління підприємством, про фінансову діяльність, про планування діяльності, до маркетингових ідей, клієнтських баз, технологічних стратегій, до технології виробництва та рецептури та іншої конфіденційної інформації, що є комерційною таємницею підприємства. Даний підхід полягає в спільному використанні декількох інформаційно-технічних засобів захисту таких як електронний цифровий підпис та стегонографічні алгоритми. Опис функціоналу електронного цифрового підпису. Схематично відображено метод використання електронного цифрового підпису. Запропоновано зв'язок цифрових водяних знаків та електронного цифрового підпису. Виконано опис вимог до цифрових водяних знаків. Запропоновано метод аутентифікації з використанням електронного цифрового підпису, який дозволяє довести авторство при експертизі. Описано математичний алгоритм вбудови цифрового водяного знака, використання секретного ключа, поміток часу, стегонографічна файлова система StegFS для Linux, приховування даних в не використовуваних областях форматів файлів, підміна символів в назвах файлів, текстова стегонографія. Використання зарезервованих полів комп'ютерних форматів файлів — суть методу полягає в тому, що частина поля розширень, не заповнена інформацією про розширення, за замовчуванням заповнюється нулями. Метод використання особливих властивостей полів форматів, які не відображаються на екрані — цей метод ґрунтується на спеціальних «невидимих» полях для отримання виносок, покажчиків. В ході експериментальної перевірки використання одночасно декількох технічних заходів захисту (цифрового водяного знака, електронного цифрового підпису і мітки часу) значно був отриманий результат, який дозволяє припускати підвищення рівня захищеності електронного документа в системі за умови організації та використання такого захисту. Поширені на сьогодні стегонографічні методи захисту растрових зображень для вбудовування стійких цифрових водяних знаків в основному базуються на використанні статистичної та фізіологічної надлишковості інформації.

Ключові слова: конфіденційність, підприємство, стегонографія, інформація, символи, аутентифікація.

PROBLEM STATEMENT. At the present stage of the whole information system development, and its security tools development either, we need to apply reliable cryptographic and steganographic methods of the information protection. Of course, today there are some data hiding technologies. However, many approaches of solving the problems of steganography are based on a common theoretical basis with cryptography.

Analyzing the process of the computer steganography development, we can say that in the coming years the interest in the development of its methods will greatly increase. The relevance of the information security problem is constantly growing and stimulates the search for new methods of information protection. On the other hand, the rapid development of information technology provides an opportunity to implement these new meth-

ods of protection. Steganographic methods, along with cryptographic, occupy an important place among the methods of information protection.

But if the presence of an encrypted message in itself attracts attention to malefactor in cryptography, the hidden connection remains invisible, in steganography which makes the organization of this process relevant. A common feature of steganographic methods is that the hidden message, or additional information, is embedded in some harmless, unnoticed object or container, resulting in a stegan message, which is then openly transported to the recipient via the communication channel or stored in this form.

Today, economic entities, regardless of size, face very fierce competition in the market of goods and services. Information is an important corporate asset in the modern world. Today, the issue of the enterprise economic security and its provision directly within the organization is very important. The economic security of the enterprise is a complex, multilevel system, one of the elements of which is the commercial secrets' protection organization [1, p. 20].

The concept of a commercial secret is given in Art. 505 of the Civil Code of Ukraine, according to which a commercial secret is a piece of information that is secret in the sense that it is in the whole or in some form and the totality of its components is unknown and is not easily accessible to persons who normally deal with the type of information, to which it belongs, is therefore of commercial value and has been the subject of adequate measures to maintain its secrecy by the person lawfully in control of the information [2].

Due to the importance of each organization to maintain a market position, make a profit and be competitive, the need to protect trade secrets is increasing. The system of protection of trade secrets implies a thorough approach on the part of management and departments to ensure its safety, as deficiencies or even small omissions can easily lead to information leakage and disclosure. Due to the fact that technology does not stand still and is constantly evolving, we can assume that the system of trade secrets' protection at the enterprise must be constantly refined and ensure security at the current level.

The reasons why the state of economic security of the enterprise may not be stable are divided into two groups [1, p. 45]:

1) Subjective, arise due to inefficient work of management and the enterprise as a whole, as well as from the actions of various bodies and organizations, including government and international organizations and competitors.

2) Objective, arise in addition to the will and without the participation of the company, its employees and the actions of the manager, these reasons are regardless of the decisions made by the manager - the state of the financial market, its conjuncture, force majeure, innovation, etc. Factors of economic security of the enterprise are a set of conditions that affect the parameters of economic security.

To achieve the highest level of economic security of the enterprise it is necessary to ensure a high security level of the main functional components of the enterprise economic security system. Functional components of the enterprise economic security are a set of the basic directions of its economic safety having essential differences from each other on the maintenance. It is accepted to allocate the following functional components of the enterprise economic safety [3, p. 140]:

1) financial;
2) intellectual and personnel;
3) technical and technological;
4) political and legal;
5) ecological;
6) information;
7) power.

An approach to protecting the reliability of commercial information of an enterprise is proposed, which consists in the joint use of several information and technical protection measures. In this paper, it is proposed to use electronic digital signatures and digital watermarks.

Enterprises require the signature of the responsible persons and the seal at a commercial enterprise, any paper documentation on financial transactions, contracts with suppliers and intermediary enterprises, other documents related to internal document flow. The main requirement is the accuracy of the documents.

An analogue is an electronic document signed by an electronic digital signature (EDS) [4, p. 256].

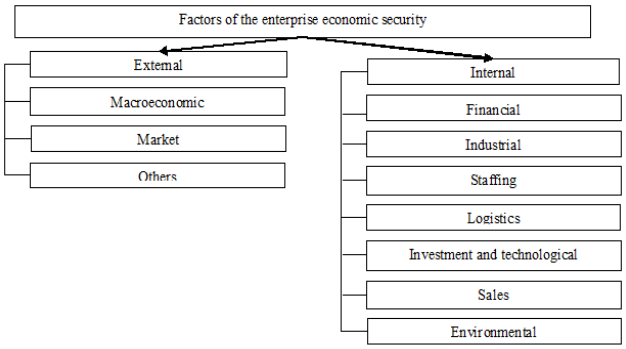

Figure 1 – Factors of the enterprise economic security

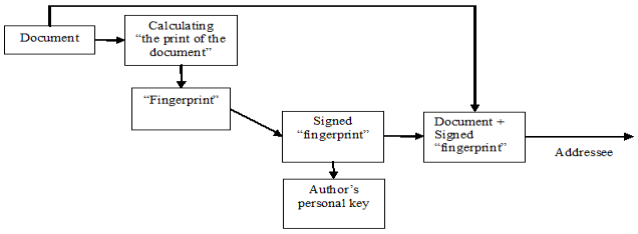

Figure 2 – An approach to protecting the authenticity of commercial information of an enterprise

According to Ukrainian law, electronic digital signature is the requisite of an electronic document designed to protect the electronic document from counterfeiting and allowing to identify the author of the document, as well as establish the absence of information distortion in an electronic document [5, p. 543].

MATERIAL AND RESULTS. Electronic digital signature protects the document from distortion, data substitution. However, this is not enough to control

access to the information contained in the document; additional methods are required.

There are a lot of existing methods of classification of steganographic methods. So, if analyzing the classification of Tarasov D. [11], the division of steganography into technological and informational is proposed.

In modern researches, four areas of steganography are often proposed [12]:

1. Classic.
2. Digital.
3. Linguistic.
4. Quantum.

The daily transmission of information through open communication channels opens up many opportunities for hidden communication. Secret messages can be embedded not only in ordinary open messages, as in traditional steganography, but also in the control elements of communication protocols and in the results of changes in the logic of the protocol.

Analyzing the literature [12], we can confidently identify another separate area of steganography - network steganography, where the network protocols of the reference model OSI are used as the carriers of confidential data.

The methods of technological steganography, namely classical, include methods that are based on the use of chemical or physical properties of various material information carriers.

Chemical methods of steganography are practically reduced to the use of organic liquids and sympathetic chemicals.

Physical methods include microspots, holograms, various types of storage and camouflage methods.

Information steganography includes methods of linguistic, computer, network and quantum steganography.

Linguistic methods of steganography are divided into two main categories: conditional letters; semagrams.

There are three types of conditional letter: slang code, blank code and geometric system.

In the slang code, the seemingly innocent word has a completely different real meaning, and the text is composed so that it looks as innocent and believable as possible. When using an empty code in the text, only certain letters or words are important. Blank codes usually look even more artificial than slang code. The third type of conditional letter is a geometric shape. When using it, the words located on the page in certain places or at the points of the geometric figure intersection of a given size have meanings.

The second category of linguistic methods are semagrams - secret messages in which the cipher symbols are any symbols except letters and numbers. These messages can be transmitted, for example, in a figure containing dots and dashes for reading by the Morse code.

Network steganography already covers a wide range of methods, so it can be distinguished as a separate independent area of steganography. Network steganography is a type of steganography where network protocols of the OSI reference model are used as the carriers of the confidential data.

The transmission of hidden data in network steganography is carried out through the hidden channels. A hidden channel can exist in any open channel in which there is some redundancy.

In general, network steganography is a subspecies of digital steganography, but recently methods have become popular when hidden information is transmitted over computer networks using the features of data transmission protocols. Such methods are called "network steganography". Typical methods of network steganography include changes in the properties of one of the network protocols. In addition, interconnection between two or more different protocols can be used to transfer a secret message more securely.

Hidden data is called a steganogram. They are located in a specific carrier. In network steganography, the role of the carrier is performed by the packet transmitted over the network.

The main parameters of network steganography are the bandwidth of the hidden channel, the probability of detection and steganographic cost. Bandwidth - the amount of classified data that can be sent per time unit.

The probability of detection is determined by the possibility of detecting the steganogram in a particular carrier. The most popular way to detect a steganogram is to analyze the statistical properties of the obtained data and compare them with the typical values for this medium. Steganographic value characterizes the modification degree of the carrier after exposure to the steganographic method.

Methods of network steganography can be divided into three groups:

1. Methods, the essence of which is to change the data in the header fields of network protocols and in the payload fields of packages;
2. Methods in which the structure of the package transmission changes, for example, changing the sequence of the package transmission or intentional introduction of the package losses during their transmission;
3. Mixed (hybrid) methods, the application of which changes the content of the packages, delivery times of the packages and the order of their transmission.

Each of these methods is divided into several groups. Package modification methods contain three different methods:

1. Methods of changing data in the fields of protocol headers: they are based on the fields modifications of IP, TCP, SCTP headers, and so on;
2. Methods of the payload modification of the package; in this case, algorithms of watermarks, language codecs and other steganographic techniques for hiding data are used;
3. Methods of mixed techniques.

Methods of modifying the package transmission structure include:

1. Methods in which the order of the package sequence changes;
2. Methods that change the delay between package;
3. Methods, the essence of which is to introduce intentional loss of package by skipping the serial numbers of the sender.

Mixed (hybrid) steganography methods use two approaches:

1. Methods of loss of audio packages (LACK)

2. Package retransmission (RSTEG).

Quantum steganography, similar to traditional methods, aims to increase the level of secrecy by hiding the very fact of information transfer. Like classical digital steganography, it is hidden in quantum information by embedding a message in an excess of the coating medium (container). Quantum steganography has not yet reached the level of practical implementation, but quite often theoretical models of stegosystems using the properties of quantum states are proposed. This direction is a synthesis of classical and quantum informatics and is based on the joint use of the laws of quantum physics and classical information theory.

Currently, three main methods of quantum steganography are proposed:

1. Concealment in quantum noise;

2. Concealment with the use of quantum noise-tolerant codes;

3. Hiding in data formats, protocols.

Within the framework of computer steganography, issues related to the concealment of information stored on media or transmitted over telecommunications networks, the organization of hidden channels in computer systems and networks with digital watermark technologies and fingerprints is considered.

On the one hand, there are some differences between digital watermark and fingerprint technologies and, on the other hand, there is the actual steganographic technology of hiding classified information for further transmission or storage. The main difference is that digital watermarks and fingerprints are intended to protect the digital object itself (programs, images, music files) where they are embedded, and to provide proof of ownership of this object.

The digital signature is not tied strictly to the author. The private key for creating a digital signature can be used by anyone who has access to it. A digital signature can be compared to digital printing, as it is usually tied to an enterprise, department, which are so-called shared resources. Of course, access is granted only to legitimate users after appropriate authorization, and all actions are logged.

1. A digital signature should have the properties of a regular signature and at the same time should be a chain of data that can be transmitted;

2. Documents that are transmitted over the network are authenticated with a digital signature. Digital signature solves the problem of possible contradictions between the sender and the recipient;

3. The digital signature must be unique, i.e. no one except the author can create the same signature, including persons who verify its authenticity;

4. Each network user, legal or not, at any time, including the initial one, can verify the truth of the digital signature;

5. The one who signed can not refuse the message, document, etc. certified by his digital signature.

To satisfy all the above requirements, a digital signature, in contrast to a “paper” one, must depend on all message bits and change even when one bit of a signed message is changed [6, p. 453].

There are two main directions of computer steganography methods development:

- the usage of special properties computer formats;
- the redundancy of audio and visual information.

Special format properties are selected taking into consideration the protection of the hidden message from direct listening, viewing or reading.

However, methods based on the usage of redundant audio and visual information are used more widely. Digital photos, digital music, digital video are a matrix of numbers, which encode intensity at discrete moments in space and / or time. Digital photography is matrix of numbers representing intensity light at a certain point in time. Digital audio is a matrix of numbers that represents intensity of the sound signal in successively tracking moments of time. Junior digits of digital readings contain very little useful information about the exact parameters of sound and visual image. Their filling does not significantly affect the quality of perception, which allows for additional information concealment.

Graphic color files with an RGB blending scheme encode by three bytes each point of the image.

Each such point consists of additive components: red, green and blue. Changing each of the three least significant bits changes less than 1% of the intensity of a given point. This allows you to hide in standard 800 KB graphic image capacity about 100 KB of information that is not visible when viewing the image.

This approach is quite simple and clear, however, it misses many important points when choosing the necessary way to hide the data.

So, the methods of computer steganography can be divided according to certain criteria. Let us look at some of them:

- By the method of container selection:
  - surrogates (ersatzmethody);
  - selective (methods of rejection);
  - constructing (simulation methods).
- By the way of access to information:
  - streaming;
  - fixed.
- By the way of container organization:
  - systematic;
  - unsystematic.
- By the message retrieval method:
  - of the original;
  - without the original container;
  - on a fragment of the original container.
- By the principle of concealment:
  - direct replacement;
  - spectral.
- By the container format:
  - text;
  - audio;
  - graphic;
  - video.
- By purpose:
  - protection of confidential data;
  - copyright protection;
  - data authentication.

Analyzing the existing methods of steganographic methods classification, it should be noted that they all only partially reflect the situation that has developed with the rapid development of steganography as a science. The complete reflection of all the features you need to take into consideration as for the effective usage of covert messaging following the main provisions of modern steganography doesn't exist:

1. Concealment methods must ensure the authenticity and integrity of the file.

2. It is assumed that the violator knows all possible steganographic methods.

3. The safety of methods is based on preservation the steganographic transformation of the main properties of an open file.

4. Even if the fact of concealing the message became known to the attacker, the isolation of the most secret message is a complex computational task.

The main determinative moment in steganography is steganographic transformation. Not so long ago steganography, as a science, mainly studied some methods of hiding information and ways of their technical implementation. The variety of principles which laid down in steganographic methods, in fact, inhibited the development of steganography as a separate scientific discipline and did not allow it to form the modern science with its theoretical provisions and a single conceptual system that would provide formal receipt of qualitative and quantitative assessments of steganomethods.

The modern interest in steganography, as a set of concealing information methods, has arisen due to intensive implementation and wide-ranging spread of computer technology in all human activity areas.

Quite wide opportunities for prompt exchange of various information appeared within computer networks between any participants of network sessions regardless of their location. They were in the form of texts, programs, sound, images. This allows you the active appliance of all the benefits that give steganographic methods of protection.

Steganography is increasingly used in the defense and commercial spheres due to the easy adaptability in solving information security tasks, as well as the absence of the obvious signs of protection means, the usage of which may be restricted or prohibited (such as cryptographic means of protection).

After analyzing the existing secure data transmission methods at this stage, we can propose a new approach to the classification of computer steganography methods. Ading and combining all the methods discussed above, we can group them by features:

- container selection,
- purpose,
- key availability,
- hiding data.

Results. System security must be fully determined by the security of the key. This means that the intruder can fully know all the algorithms of the stegosystem and the statistical characteristics of the sets of messages and containers, and this will not give him any additional information about the presence or absence of a message in this container [7].

A filled container should be visually indistinguishable from an empty one. To satisfy this requirement, it would seem necessary to embed a hidden message in visually insignificant areas of the signal. However, the same areas use compression algorithms. Therefore, if the image will be further compressed, the hidden message may be destroyed. Therefore, bits must be embedded in visually significant areas, and relative invisibility can be achieved by using special methods, for example, the combination of digital signature and steganography increases the security of the document, however, these technical means themselves also require protection. After all, an attacker can change both a digital sign and data, a container or digital water sign(DWS) [8, p.160].

The following requirements are imposed on the DWS:

- DWS should be easily (computationally) retrieved by a legitimate user.

- DWS should be stable or unstable to deliberate and accidental influences (depending on the application). If the DWS is used for authentication, then an unacceptable change to the container should lead to the destruction of the DWS (fragile DWS). If the DWS contains an identification code, the name of the teacher, the logo of the company, etc., then it should be preserved with maximum distortion of the container, of course, not leading to significant distortion of the original signal. In addition, the DWS should be robust with respect to affine transformations of the image, that is, its rotations, scaling. In this case, it is necessary to distinguish between the stability of the DWS itself and the ability of the decoder to detect it correctly. Say, when the image is rotated, the DWS will not collapse, and the decoder may be unable to select it. There are applications where the DWS must be stable in relation to one transformation and unstable in relation to others. For example, it may be allowed to copy the image (copier, scanner), but there is a ban on making any changes to it.

- It should be possible to add additional cost center to the stego. The best way out is to add another DWS, after which the first will not be taken into account. However, the presence of several DWSs on a single message can facilitate an attack by an intruder, unless special measures are taken.

An important problem is the determination of the authenticity of the information received, that is, its authentication. Typically, digital signatures are used to authenticate data. However, these tools are not entirely suitable for providing authentication of multimedia information. The fact is that a message equipped with an electronic digital signature must be stored and transmitted absolutely accurately, "bit to bit". The multimedia information may be slightly distorted both during storage (due to compression) and during transmission (the effect of single or packet errors in the communication channel). At the same time, its quality remains acceptable for the user, but the digital signature will not work. The recipient will not be able to distinguish a true, albeit somewhat distorted, message from a false one. In addition, multimedia data can be converted from one format to another. However, traditional means of protecting integrity will also not work. We can say that DWSs are able to protect precisely the content of audio and video

messages, and not its digital representation in the form of a sequence of bits. In addition, an important disadvantage of a digital signature is that it is easy to remove from a message certified by it, and then attach a new signature to it. Deleting the signature will allow the violator to refuse authorship, or to mislead the legal recipient regarding the authorship of the message. The DWS system is designed in such a way as to exclude the possibility of such violations.

A stegosystem can be considered as a communication system. The DWS embedding algorithm consists of three main stages [9]:

1) DWS generation
2) embedding the DWS in the encoder
3) detection of DWS in the detector.

Let **W*, K*, I*, B*** be the set of possible DWSs, keys, containers, and hidden messages, respectively. Then the generation of the DWS can be represented as (1)

$$F = I^* \cdot K^* \cdot B^* \to W^*, W = F(I, K, B), \quad (1)$$

where **W, K, I, B – F** representatives of the corresponding sets. Generally speaking, the function can be arbitrary, but in practice, the requirements for the robustness of the DWS impose certain restrictions on it (2). So, in most cases,

$$F(I, K, B) \approx F(I + \varepsilon, K, B), \quad (2)$$

that is, a slightly modified container does not lead to a change in the composite: DWS (3). Function is usually

$$F = T^{o}G, \quad (3)$$

where

$$G = K^* \cdot B^* \to C^* \text{ and } T = C^* \cdot I^* \to W^* \quad (4)$$

that is, the DWS depends on the properties of the container, as it was mentioned above in this chapter.

The function can be implemented using a cryptographically secure generator PRS (pseudo-random sequences) **G** with **K** as the initial value.

To increase the robustness of the DWS, noise-resistant codes can be used, for example, BFCh(basic frequency characteristics) codes, convolutional codes [5, c. 234]. A number of publications have noted the good results, achieved when embedding DWS in the field of wavelet transformation, using turbo codes. DWS samples take **{-1,1}** usually values from the set, while binary relative phase modulation (BRPhM) can be used to display **{0,1} → {-1.1}.**

The operator ***T*** modifies the code words ***C ****, as a result of which the DWS ***W **** is obtained.

You can not impose irreversibility restrictions on this function, since the corresponding choice already guarantees the irreversibility of ***G***. The function must be chosen so that unfilled container ***I`y,*** filled container ***F*** and slightly modified filled container ***T*** would have generated the same DWS (5):

$$T(C, I_0) = T(C, I_y) = T(C, I'_y), \quad (5)$$

that means, it must be resistant to small changes in the container.

1) The process of embedding the DWS into the original image $\mathbf{I_0\ (i,\ j)}$ can be described as a superposition of two signals:

$$\varepsilon : I^* \cdot W^* \cdot L^* \to I^*_y, \quad (6)$$

$$I_W(i, j) = I_0(i, j), \quad (7)$$

$$\oplus L(i, j)W(i, j)p(i, j), \quad (8)$$

where **L(i,j)** is the DWS embedding mask that takes into account the characteristics of the visual human systems, serves to reduce the visibility of DWS; **p (i, j)** is the design function depending on the key; the sign $\oplus$ denotes the superposition operator, which includes, besides addition, truncation and quantization. The design function carries out the "distribution" of the DWS in the region Images. Its use can be considered as the implementation of the diversity of information on parallel channels. In addition, this function has a certain spatial structure and correlation properties that are used to counter geometric attacks.

CONCLUSIONS. As a result of the available methods analysis of classification and systematization of steganographic methods, the optimal system of classification of these methods was created.

It should be taken into account that the creation of a stego-system requires a certain relationship between the resistance of the built-in message to external influences (including stegoanalysis) and the size of the built-in message.

For most modern methods used to hide messages in digital containers, there is an exponential dependence of system reliability on the amount of embedded data. This dependence shows that when increasing the amount of embedded data the reliability of the system (with the same size of the container) reduces. Thus used in the stego system, the container imposes restrictions on the size of the embedded data.

Thus, today the development of steganographic methods of information protection move into top gear, a theoretical basis is created, and more absolute hiding message methods to various effects on the steganocontainer.

To increase the security of files, it is proposed to sign the entire container (electronic document or copyright object) with implemented DWS and electronic digital signature obtained using the private key of the document's author. The signature must be kept at a certification authority (CA).

Each legal user can use the public key (they are all stored in the CA in the public domain) to verify the authenticity and immutability of the file. The digital watermark ensures that even if the attacker signs the file on his behalf, the results of the verification of his electronic signature and the DWS will not match and it will be possible to establish a violation. DWS acts as an additional level of protection, which is sometimes diffi-

cult to even detect, and even more so to circumvent. This level of protection allows you to prove authorship during the examination.

During the experimental verification of the usage of several technical protection measures at the same time (DWS, EDS and timestamps), a significant result was obtained that suggests an increase in the level of security of an electronic document in the system provided that such protection is organized and used.

REFERENCES

1. Urazgaliyev, V. Sh. (2016). Ekonomichyeskaya bezopasnost`. Uchyebnik i praktikum [Economic security]. *Yurajt*. Moskow. (in Russian)

2. Tsyvilnyi kodeks Ukrainy [Civil Code of Ukraine] - URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (accessed 1 October 2020)

3. Bodnar, I. (2005). Mizhnarodna informatsiia: navchalnyi posibnyk [International information: textbook]. *Lviv Commercial Academy*. Lviv. (in Ukrainian)

4. Eriashvili, N. D. (2014). Ekonomichieskaia biezopasnost: Uchiebnoie posobiie [Economic analysis of the enterprise: Textbook]. *Unity-Dana*. Moskow. (in Russian)

5. Skamay, L. G. (2014). Ekonomichieskii analiz dieiatielnosti priedpriiatiia: Uchiebnoie posobiie [Economic analysis of the enterprise: Textbook]. *NITs INFRA-M*. Moscow (in Russian)

6. Shennon, K. (1963). Raboty po teorii informatsii i kibernetiki [Works on information theory and cybernetics]. *Inostrannaya literatura*. Moscow. (in Russian)

7. Schneier, B. (1995). Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. *John Wiley and Sons*. New York, 662 p. (in English)

8. Poniatye stehanohrafycheskoi stoi kosty [The concept of steganographic bone stasis]. URL: http://mf.grsu.by/UchProc/livak/b_protect/zst.htm (accessed 20 March 2020)

9. Hrybunyn, V. H., Okov, Y. N., Turyntsev, Y. V. (2009). Tsyfrovaya stehanohrafyya [Digital steganography]. *SOLON-Press*, Moscow, 272 p. (in Russian)

10. Kolenko, V. V., Narozhnyy, A. V., Nosov, P. S. (2009). Sistemy zashchity elektronnoy informatsii na osnove steganograficheskikh algoritmov [Electronic information security systems based on steganographic algorithms]. Proceedings of the *Sovremennye problemy i puti ikh resheniya v nauke, transporte, proizvodstve i obrazovanii '2009*, Odessa: Chernomor'e, pp. 145-156 (in Russian)

11. Tarasov, D. O. (2010). Klasyfikaciya ta analiz bezkoshtovnyh programnyh zasobiv steganografiyi [Classification and analysis of free steganography software]. Informacijni systemy ta merezhi. *Visnyk NU «Lvivska politexnika»*. No. 673. (in Ukrainian)

12. Stasyuk, O. I. (2011). Suchasni steganografichni metod` zahystu informaciyi [Modern steganographic methods of information protection]. Zahyst informaciyi. Vol. 13. No. 1 (50). (in Ukrainian)

Стаття надійшла 11.01.2021.