CHAPTER «NATIONAL SECURITY»

ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS IN STATE GOVERNMENT BODIES

Natalya Blavatska[1]
Olha Berdar[2]

DOI: https://doi.org/10.30525/978-9934-26-499-3-19

Document management becomes truly electronic when scanners disappear in it, and the "PRINT" function is removed from the software

Abstract. The Russian Federation's unprovoked military aggression against Ukraine is rapidly bringing drastic changes to all spheres of our country's life. This is especially true of state authorities. The effectiveness of the management of state bodies in the conditions of martial law depends to a large extent on solving the tasks of operational creation of electronic documents, control over their execution, on the organization of preservation, as well as search and use. Electronic document management allows you to significantly increase work efficiency and reduce time spent on solving problems related to the activities of state bodies.

The system of electronic document circulation is an organizational and technical system that ensures the process of creation, access management and distribution of electronic documents in computer networks, and also provides control over document flows in the organization.

According to the legislation, the system of electronic document circulation must meet the requirements of normative legal acts in the field

[1] Candidate of Technical Sciences, Associate Professor
Educational and Scientific Institute of Information Security and Strategic Communications
of the National Academy of the Security Service of Ukraine, Ukraine
[2] Master's of correspondence form of study,
Educational and Scientific Institute of Information Security and Strategic Communications
of the National Academy of the Security Service of Ukraine, Ukraine

of information protection. In particular, this concerns the provisions of the Law of Ukraine "On the Protection of Information in Information and Communication Systems" and the Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Rules for Ensuring the Protection of Information in Information, Electronic Communication and Information and Communication Systems".

To date, Ukraine has introduced electronic document management in state bodies, all regional state administrations are connected to it, and work is underway to implement electronic document management systems for other state bodies of local authorities.

All work processes in the electronic document management system can be customized, which allows you to take into account the peculiarities of the implementation of any functions. The system provides access to advanced analytics and reporting that allow analyzing business processes and making effective management decisions.

Subjects of electronic document circulation must store electronic documents on electronic data carriers in a form that makes it possible to check their integrity on these carriers. The term of storage of electronic documents on electronic data carriers must not be less than the term established by law for the corresponding documents on paper.

The leading state institution engaged in the storage of electronic documents is the Central State Electronic Archive of Ukraine, created in accordance with the order of the Cabinet of Ministers of Ukraine N 279 of May 12, 2007 to solve the tasks of permanent storage of documents of the National Archival Fund of Ukraine, namely electronic documents, electronic information resources and providing access to the information of these documents.

Although the advantages of using electronic document management systems in government bodies are obvious, the implementation of such systems is not progressing as quickly as desired.

The main problems of the successful implementation and use of electronic document management systems in state bodies are the actual lack of sufficiently effective organizational and legal mechanisms for their implementation, the lack of a general methodology for their use, and the specificity of the work of the state apparatus, which stands in the way of the implementation of standard solutions in this field.

1. Introduction

Relevance of the topic. In the conditions of informatization of society, the daily flow of documents arriving at enterprises, institutions, and organizations is continuously growing every day. As a result, there is a need to introduce the latest systems capable of processing a huge array of data in a short period of time. One of the ways to solve this problem is the introduction of electronic document management systems at enterprises and organizations of Ukraine. It is extremely important to implement electronic document management in state authorities, in particular in local self-government bodies, because it allows to increase the effectiveness of the functioning of all elements of state administration.

Administrative activities of state authorities and local self-government bodies are carried out by issuing organizational and administrative documents. Documentation is used as a method and means of implementing management functions. At the same time, the documents contain information that must be reliably stored for a certain period of time.

Recently, the functions of the board have become significantly more complicated and the volume of tasks assigned to state authorities has increased, the requirements for the quality of documents are changing. At the same time, information technologies are being actively implemented as means of automating processes related to documented information. In addition, new legal objects have appeared in the legislation – an electronic document and an electronic digital signature, new forms of relations based on electronic document flow are developing.

The issue of intensifying the implementation and development of electronic governance in all spheres of social life, one of the important components of which is electronic document flow, has been put on the agenda in Ukraine. This will make it possible to obtain such important qualities of state administration as the efficiency of exchanging electronic documents, the possibility of their remote processing, approval and signing, will ensure the accumulation and general availability of arrays of documents, and will make the creation and use of electronic archives quite natural [14].

The purpose of the study. To analyze the security of electronic document flow of state institutions.

Achieving the specified goal depends on the following **tasks:**

– characteristics of ensuring the security of electronic document circulation of state institutions;

– analysis of ensuring the security of electronic documentation of state institutions and development of methods for their improvement.

The object of the study is to ensure the security of the electronic document flow of state institutions.

The subject of the study is the mechanism for ensuring the security of electronic document circulation of state institutions.

Research methods. Method of theoretical analysis and systematization, methods of observation and abstraction.

The state of scientific research on the topic. The modern importance of ensuring the security of electronic document circulation is of considerable scientific interest. The processes of electronic document circulation were studied by such scientists as A. Grechko [4, p. 2], O. Matvienko [18, p. 5], M. Tsyvin [11, p. 5], O. Loza [16, p. 5], N. Kovalchuk [10, p. 7] and others. Peculiarities, problems and prospects of the introduction of electronic document management of state institutions are described in the scientific works of such scientists as I. Klymenko, K. Lin'ev, I. Horbenko, M. Krukovsky, O. Kukarin and others. Although many scientists were interested in the issue of electronic document circulation, in Ukraine the problems of organizing electronic document circulation of state institutions have not yet been sufficiently studied.

This paper outlines the basic principles of creating and using electronic documents. The principles of organization and functioning of electronic document circulation systems, their general classification, current state and development trends are considered. The basics of the technology of using an electronic digital signature are disclosed. Special attention is paid to the problems of complex protection of information in information and communication systems [15].

2. Electronic document circulation in state authorities and local self-government bodies

The basis of information and analytical support of the organization's work is primarily the processing of documents that are subject to creation, recording and accounting in a certain form.

Documents are used in various fields of knowledge, spheres of human activity and social life. They are the object of research of various scientific disciplines, and therefore the concept of a document is ambiguous and depends on the field in which it is used and for what it is used.

According to Article 1 of the Law of Ukraine "On Information" [26], a document is a physical medium containing information, the main functions of which are its preservation and transmission in time and space.

In other sources, a document is defined as a structured unit of information, intended for human perception and designed and recorded on a material medium in the established order with observance of a certain form of its presentation and the formation of mandatory features:

– functionality – certainty within existing social relations of the expected impact of the document (including the subsequent course of action) on its recipients after receiving and familiarizing themselves with the content;

– authorization – certainty of a natural or legal person who is responsible at a certain time for the existence of the document;

– registration – the certainty of the unique identification of a document in a set of documents.

Article 5 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" [24] defines that an electronic document (ED) is a document in which information is recorded in the form of electronic data, including document details, the composition and arrangement of which is determined by legislation. At the same time, ED can be created, transmitted, stored and transformed by electronic means into a visual form of presentation by displaying the data it contains by electronic means or on paper in a form suitable for perceiving its content by a person. Mandatory details of ED are data, without which it cannot be the basis for its accounting and will not have legal force.

According to Art. 6 of the mentioned Law of Ukraine, *an electronic signature* is a mandatory requisite of an ED, which is used to identify the author or signatory of the ED by other subjects of electronic document circulation and allows to confirm its integrity. The creation of the ED is completed by superimposing an electronic digital signature (EDS). However, it should be noted that only EDS is equal to a handwritten signature (seal) in terms of legal status, and other types of electronic signatures do not have such a status.

In accordance with Article 7 of this Law, an electronic copy of a document with mandatory details, including the EDS of the author, is considered the original ED. At the same time, in the case of sending an ED to several addressees or storing it on several electronic media, each of the electronic copies is considered an original ED. If the author creates an ED and a paper document identical in terms of documentary information and details, each of the documents is an original and has the same legal force. An electronic copy of the ED is certified in accordance with the procedure established by law. A copy of a document on paper for ED is its visual presentation on paper, which is certified in accordance with the procedure established by law.

The status of the ED is determined by its requisites, which take the following values:

– ***version*** – a copy of the ED at the stage of creation, which differs from its other copies in portions of the content;

– ***original*** – copy of ED, which is the first to enter into force, which is indicated in the registration process by the corresponding value of the special requisite;

– ***duplicate*** – a copy of the ED, which has the legal force of the original;

– ***copy*** – a copy of ED that exactly reproduces the content of its original, as well as all its details or part of them;

– ***extract (from ED)*** – a copy of ED that reproduces part of all its structures and part of portions of the content.

Article 8 of this Law defines that the legal force of the ED cannot be denied solely because it has an electronic form, as well as the cases when the ED cannot be used as an original: certificates of the right to inheritance; a document that, in accordance with the law, can be created only in one original copy, except in the case of the existence of a centralized repository of ED originals; in other cases provided by law.

The life cycle of ED consists of four stages: creation, distribution, implementation and use, which are implemented and provided as a set of sequential processes using computers and means of communication. At the same time, the execution of operations for the implementation of processes occurs automatically or is controlled by users of the relevant information and communication systems.

ED creation technologies make it possible not only to use them on an equal footing with paper documents, but also to obtain qualitatively new possibilities for their processing. The most important of them is a significant increase in the efficiency of document flow in the activities of subjects, as well as the possibility of concluding agreements and other transactions using information technologies through publicly available communication channels, that is, remotely.

The term "management documentation support" (bookkeeping) entered scientific and practical circulation approximately from the mid-1970s. technologies.

Clerkship is considered as a field of activity that ensures the creation of official documents and the organization of work with them, namely the organization of the movement of documents from the moment of their creation or receipt to the completion of execution: sending from the organization and directly to the archive.

In a broad sense, document circulation can be defined as the information activity of subjects of information relations, which is implemented by performing certain actions on documents.

A document management system is understood as a set of methods, means and personnel supporting document management within the established document management regulations.

Document flow automation system (electronic document flow system) is an organizational and technical system that ensures the process of creation, access management and distribution of electronic documents in computer networks, as well as control over document flows in the organization.

Of particular importance is the regulation (regulation) of document circulation, which is related to electronic documents.

The document circulation regulation is a set of rules for the information activity of subjects of information relations, defined by legislation, regulatory acts or agreements. The document circulation regulation defines the roles and rights of subjects regarding the creation, possession, use and disposal of documents, the procedure for registration and recording of information on the information carrier.

As a generalized concept, electronic document management (EDM) can be interpreted as information technologies implementing the life cycle of an electronic document. At the same time, the electronic document

management system (EDM) can be defined as an automated information processing system that implements EDM and is connected to other document management systems.

The need to use electronic documents and use the opportunities provided by electronic document circulation for various public needs was on the agenda in Ukraine as early as the second half of the 90s of the last 20th century. This was also motivated by the positive social experience of developed countries in this area. But at that time, not only in Ukrainian society as a whole, but even in the state authorities, there was not yet an available material and technical base and sufficient awareness of the volume and complexity of the tasks that must be solved in order to achieve the specified goal.

The Law of Ukraine "On Electronic Documents and Electronic Document Management" specifies the main concepts and terms in the field of electronic document management:

– ***the author of an electronic document*** is a natural or legal person who created an electronic document;

– ***addressee*** – a natural or legal person to whom an electronic document is addressed;

– ***data*** – information presented in a form suitable for its processing by electronic means;

– ***electronic document*** – a document in which information is recorded in the form of electronic data, including mandatory details of the document;

– ***electronic document circulation*** (circulation of electronic documents) – a set of processes of creation, processing, sending, transmission, receipt, storage, use and destruction of electronic documents, which are performed with the application of an integrity check and, if necessary, with confirmation of the fact of receipt of such documents;

– ***mandatory requisites of an electronic document*** – mandatory data in an electronic document, without which it cannot be the basis for its accounting and will not have legal force;

– ***an intermediary*** is a natural or legal person who, in accordance with the procedure established by law, carries out acceptance, transfer (delivery). Storing, checking the integrity of electronic documents to meet their own needs or providing relevant services on behalf of other subjects of electronic document circulation;

– ***subjects of electronic document circulation*** – the author, signatory, addressee and intermediary, who acquire the rights and obligations provided for by law or contract in the process of electronic document circulation.

The following main *principles and tasks of electronic document circulation* should be singled out:

– one-time registration of a document, which allows it to be uniquely identified in any subsystem;

– the possibility of parallel execution of operations, which makes it possible to reduce the time of movement of documents and increase the efficiency of their execution;

– the continuity of the movement of the document, which allows identifying the person responsible for its execution (task) at each moment of the life cycle of the document (process);

– a single (or agreed upon distribution) database of document information, which makes it impossible to duplicate documents;

– an effectively organized document search system, which ensures the search for documents, having minimal information about them;

– a developed system of reporting for different statuses and attributes of documents, which makes it possible to control their movement through the processes of document circulation and make management decisions based on the data from the reports.

Legal aspects of electronic document circulation in the state administration system

For the introduction of electronic document management (EDM), the authorities have, first of all, the task of creating a regulatory and legal framework that ensures its implementation through the proper organization of relevant processes and compliance with the requirements for document processing, unification of systems of organizational and administrative documentation, development of a single state system of record keeping, a single state system of documentation support for management, etc. It was also supposed to become the basis for regulating relations between subjects in such qualitatively new areas of activity as electronic commerce, electronic trade, electronic reporting, provision of electronic (administrative) services through specialized information systems and public networks, including the Internet.

For this purpose, two basic laws of Ukraine were adopted: "On electronic digital signature" [25] and "On electronic documents and electronic document circulation" [24]. At the same time, it should be noted that the provisions of the first of these laws meet the requirements of Directive 1999/93/EC of the European Parliament and the Council of Europe dated December 13, 1999 "On the system of electronic signatures applied within the Community" [30]. With the adoption of the mentioned laws, subject to compliance with certain requirements, the electronic digital signature was equated in terms of legal status to a handwritten signature (seal), the basic organizational and legal principles of the use of an electronic document and the application of EDM were established.

The Law of Ukraine "On electronic documents and electronic document circulation" [24] regulates relations related to the sending, transmission and receipt of an electronic document. In particular, the sending and transmission of an electronic document is carried out by the author or an intermediary in electronic form using the means of information and communication systems or by sending electronic media on which this document is recorded. At the same time, an electronic document is considered received by the addressee from the moment the author receives a message in electronic form from the addressee about the receipt of this electronic document by the author, unless otherwise provided by legislation or prior agreement between the subjects of electronic document circulation. The integrity of an electronic document is verified by verifying the authenticity of the electronic digital signature affixed to it.

In compliance with the aforementioned laws, the Cabinet of Ministers of Ukraine adopted a number of resolutions that specified the regulation of relations in this area, in particular:

– "On approval of the Procedure for certifying the presence of an electronic document (electronic data) at a certain point in time" [32];

– "On approval of the Procedure for accreditation of the key certification center" [33];

– "On approval of the Regulation on the central certifying body" [34];

– "On the approval of the Procedure for the use of electronic digital signatures by state authorities, local self-government bodies, enterprises, institutions and state-owned organizations" [35];

– "On approval of the Standard procedure for implementing electronic document circulation in executive authorities" [36];

– "On approval of the Procedure for mandatory transfer of documented information" [37].

These resolutions, among others, are aimed at the creation and development of ***Public Key Infrastructure*** in Ukraine to ensure the use of electronic digital signatures, first of all, the creation of its subjects – ***the central certification body*** and ***the control body,*** as well as ***certification centers***. The creation and maintenance of the activities of other subjects of this infrastructure – key certification centers, including accredited key certification centers, is carried out by business representatives.

Approved by the Resolution of the Cabinet of Ministers of Ukraine "Standard procedure for the implementation of electronic document circulation in executive authorities" [36] establishes general rules for documenting administrative activities in the authorities in electronic form and regulates the execution of actions with electronic documents from the moment of their creation or receipt until they are sent or transferred to the appropriate archive. At the same time, all other actions with electronic documents are performed in the government body in accordance with the requirements for actions with paper documents, provided for in the manual of this body. The Standard Procedure applies to all electronic documents created and received by the authority.

At the same time, each state authority, local self-government body, enterprise, institution or organization, regardless of the form of ownership, specifies for its needs the general rules of documentation in electronic form and regulates the execution of actions with electronic documents in accordance with the law.

The authority carries out EDM only under the condition of using reliable means of electronic digital signature (EDS), which must be confirmed by a certificate of compliance or a positive conclusion based on the results of a state examination in the field of cryptographic information protection (CIP), received on these means from the State Special Communications Administration and the presence of enhanced public key certificates (EPKC) of its employees – signatories. At the same time, EDM is carried out by the executive power body through special communication networks or public

communication networks, and the sending of electronic documents through public communication networks is carried out by the decision of the head of this body.

According to the legislation, the electronic document management system (EDMS) of the government body must meet the requirements of regulatory acts in the field of information protection, in particular the provisions of the Law of Ukraine "On the Protection of Information in Information and Communication Systems" [26] and Resolution of the Cabinet of Ministers of Ukraine "On approval of the Rules for ensuring the protection of information in information, communication and information and communication systems" [38].

The creation of archives of electronic documents, their submission to archival institutions of Ukraine and storage in these institutions is carried out in accordance with the procedure established by legislation. In particular, the order of the State Archives Committee of Ukraine approved the "Procedure for storing electronic documents in archival institutions" [51].

A number of legal, organizational and technical issues were settled by other government decisions, regulatory acts and normative documents of the central executive authorities, but today the general problems in this area have not yet been fully resolved.

The resolution of the Cabinet of Ministers of Ukraine "On the approval of the Model Instruction on office management in ministries, other central bodies of executive power, the Council of Ministers of the Autonomous Republic of Crimea, local executive bodies" [29] became the basis for the regulation of clerical issues. The model instruction defines the procedure for conducting general record keeping, and its provisions apply to all official documentation, including those created with the help of personal computers. Computer (automated) technologies for processing document information must meet the requirements of state standards, as well as the specified instructions.

According to the Model Instructions, the head of the institution is responsible for the organization of office management in the institution. Management of records in accordance with the requirements of state standards, this Exemplary Instruction and instructions on record keeping of institutions is entrusted to the management of cases, general departments, offices or secretaries.

At the same time, the main task of the clerical service is to establish a uniform procedure for documenting and working with documents in the institution based on the use of modern computer technology, automated technology for working with documents and reducing the number of documents.

A number of provisions of the Exemplary Instruction to a certain extent already laid the foundation for implementation in EDMS institutions. In particular, they stated that the mechanization and automation of clerical processes is a mandatory condition for the rational organization of clerical work in every institution, a means of increasing productivity and reducing the cost of managerial labor and should be carried out on the basis of an orderly system of documenting managerial activities, unification and reduction of the number of forms of documents used. In addition, these measures are used at all stages of the clerical process of preparing documents, their copying, operational storage and transportation, monitoring of execution, etc, and the means of mechanization and automation of clerical processes must be compatible and provide for the possibility of combining them into a single system.

The Exemplary Instruction also states that the complex of technical means must ensure the collection and transmission of information, its recording on machine media, the input of information into a personal computer, the output of results, its processing in the form of machine or videograms, compatibility with other information systems, and as well as the possibility of combining into a single integrated system. At the same time, during the implementation of new technologies for working with documents, it is necessary to take into account:

– feasibility of implementing technical means;
– the possibility of purchasing technical means in certain terms;
– availability of suitable premises;
– the need to involve specialists in the maintenance of equipment, etc.

The head of the institution is responsible for the effectiveness of the use of mechanized and automated technology for working with documents.

Processing of documents in the institution is carried out according to standard schemes, respectively, for incoming, internal and outgoing documents. In particular, when processing an incoming document, the following stages are distinguished: receipt, preliminary review, registration,

report to management, organization of execution - appointment of executors and setting of tasks, implementation of clerical control over the course and consequences of execution, completion of the case (final registration) and referral to storage.

All actions of an electronic document, if it does not concern the specifics of creation or receipt before sending or transfer to the archive, are performed in institutions in accordance with the requirements for actions with paper documents, provided for by the administrative instructions of these bodies.

Electronic document flow under the conditions of electronic governance

Today, one of the priorities of Ukraine is the development of an information society with its most important component – electronic governance, the implementation of which will contribute to the creation of conditions for effective open and transparent public administration.

The Cabinet of Ministers of Ukraine by its order [47] approved the Concept of the development of e-government in Ukraine. According to the Concept, e-governance is defined as a form of public administration organization that contributes to increasing efficiency, openness and transparency of the activities of state authorities and local self-government bodies using information and communication technologies for the formation of a new type of state focused on meeting the needs of citizens.

The Concept also states that despite the rapid development of information and communication technologies and their widespread use in public administration over the last decade, the following problems remain unsolved:

– lack of uniform standards and regulations for the functioning of the EDO system using EDS, as well as the management of state information resources adapted to international ones;

– limited capabilities of the electronic document circulation system of state authorities and local self-government bodies;

– lack of uniform EDS formats and protocols.

At the same time, taking into account the advantages of technologies used in e-government, the tasks of ensuring its development in Ukraine, in particular, are:

– organization of information interaction of state authorities and local self-government bodies on the basis of EDM using EDS;

– ensuring the transfer and long-term storage of electronic documents in state archives, museums, libraries, maintaining them in an updated state and access to them.

Implementation of the Concept is planned for a certain period and consists of two main stages.

At the first stage, it is assumed:

– development of the necessary normative-legal and normative-technical framework, in particular regarding the provision of administrative services in electronic form, as well as uniform standards, protocols and regulations for the interaction of e-government subjects, their harmonization with international standards;

– creation of a unified nationwide system of electronic document circulation.

At the second stage, it is planned, in particular, to ensure the transfer of electronic documents to state archives, museums, libraries, their long-term storage, maintenance in an updated state and access to them.

Thus, the Concept clearly states that the implementation of the electronic document management system is an important component of the development of electronic governance.

It should be noted that with the development of tasks and technologies of electronic governance, EDM extends to all spheres of state activity and ensures interaction between authorities of all levels and branches, authorities and business structures, authorities and citizens. At the same time, such interactions go beyond the exchange of data (information) in its various forms and applications, which is certainly more complex in the organizational and scientific and technical sense.

The task of creating a unified state-wide system of electronic document circulation is, in the first approximation, realized by introducing a system of electronic interaction of executive authorities [48].

The system is designed to perform the following functions:

– the formation of a single information space for the exchange, processing and storage of organizational and administrative documents in electronic form, which is a prerequisite for the further creation of a central electronic archive of documents;

– reception (transmission) of organizational and administrative electronic documents of the Secretariat of the Cabinet of Ministers and central executive bodies;

– organization of approval of draft normative acts between central bodies of executive power;

– control of the execution of orders of the Secretariat of the Cabinet of Ministers, approval of draft normative documents of the Cabinet of Ministers of Ukraine;

– strengthening control over the execution of organizational and administrative documents;

– increasing the efficiency of management decision-making;

– creation of prerequisites for the transition to internal electronic document circulation in the department using only electronic documents.

The main characteristics of the system:

– Web-oriented architecture. Work with the system is carried out using a standard Web browser. Users can work in the system at any time and in any place, for this only a computer connected to the Internet is needed;

– a single repository of documents. After being placed on the file server, the document is available to addressees and does not need to be moved between them, which enables all users to whom the document is addressed to work on it together;

– integration with SED according to the agreed format (Order of the Ministry of Education and Science, Youth and Sports of Ukraine dated October 20, 2011 N 1207 [55]).

One of the most important tasks that must be solved when exchanging data (documents) between participants in information interaction is the compatibility of data for different systems. This is regulated by the requirements for data formats of electronic document circulation in state authorities, approved by the order of the Ministry of Education and Science, Youth and Sports of Ukraine dated October 20, 2011 N 1207 [55].

This order establishes the requirements for electronic notification, which are applied during the creation of electronic document circulation systems of state authorities and/or when ensuring their interaction, which are mandatory when organizing electronic interaction of all authorities.

The main content of the requirements is as follows.

The software that implements the required format can be a separate autonomous solution or integrated into the internal system of electronic document circulation as its component.

An electronic message is an XML document with the structure and composition of elements and their attributes established by these Requirements. The electronic message is transferred from the sender's electronic document flow system to the recipient's electronic document flow system in the form of a file.

An XML document is a text document created in full compliance with the XML standard. It consists of a prologue, a single XML root element, comments, data type declarations, and symbols.

An electronic message is an XML file into which an electronic document and metadata are attached as required. It as a whole and its constituent parts can be independently certified by electronic digital signatures and (or) encrypted.

The sender of an electronic message is an electronic document management system (EDM), the initiator of information interaction, which forms and sends an electronic message to another EDM.

The recipient of an electronic message is an electronic document circulation system, which during information interaction receives an electronic message and ensures its processing.

The main document may have additional materials – a document or a set of documents, the information of which clarifies, clarifies individual issues, etc.

XML (Extensible Markup Language) is an extensible data markup language. A standard for structured data description, focused, in particular, on the exchange of information between independent participants, proposed by the Word Wide Web Consortium.

The document must have mandatory details – data in the electronic document, without which it cannot be the basis for accounting and will not have legal force.

3. Electronic digital signature

Article 1 of the Law of Ukraine "On Electronic Digital Signature" [25] defines the following terms:

– ***accreditation*** – a procedure for documenting the competence of the key certification center to carry out activities related to the maintenance of enhanced key certification;

– ***key certificate blocking*** – temporary suspension of key certificate validity;

– ***public key*** – a parameter of the cryptographic algorithm for verifying an electronic digital signature, available to the subjects of relations in the field of using an electronic digital signature;

– ***electronic signature*** – data in electronic form, which is added to other electronic data or logically connected with them and intended to identify the signatory of these data;

– ***electronic digital signature*** – a type of electronic signature obtained as a result of the cryptographic transformation of a set of electronic data, which is added to this set or logically combined with it and allows to confirm its integrity and identify the signer. An electronic digital signature is imposed using a private key and verified using a public key;

– ***certification of the validity of the public key*** – the procedure for creating a public key certificate;

– ***means of an electronic digital signature*** – a software tool, software-hardware or hardware device designed for key generation, imposition and/or verification of an electronic digital signature;

– ***personal key compromise*** – any event and/or action that led or may lead to the unauthorized use of a personal key;

– ***reliable means of electronic digital signature*** – a means of electronic digital signature that has a certificate of conformity or a positive expert opinion based on the results of state expertise in the field of cryptographic information protection. Confirmation of compliance and state examination of these means is carried out in accordance with the procedure established by legislation;

– ***private key*** – a parameter of the cryptographic algorithm for forming an electronic digital signature, available only to the signatory;

– ***signatory*** – a person who legally owns a private key and, on his own behalf or on behalf of the person he represents, imposes an electronic digital signature during the creation of an electronic document;

– ***enhanced public key certificate*** (hereinafter – enhanced key certificate) – a key certificate that meets the requirements of this law, issued by an accredited key certification center, certification center, central certification body;

– ***electronic digital signature services*** – provision of electronic digital signature tools, assistance in generating public and private keys, maintenance of key certificates (formation, distribution, cancellation, storage, blocking and renewal), provision of information on valid, canceled and blocked key certificates, services fixing time, consultations and other services defined by this Law;

– ***public key certificate*** (hereinafter – key certificate) – a document issued by the key certification center, which certifies the validity and ownership of the public key to the signatory. Key certificates can be distributed electronically or as a paper document and used to identify the identity of the signer.

Handwritten signature and electronic digital signature

A document in the traditional understanding of this concept implies the presence of an information carrier, which ensures the perception of information only by human senses (sight, hearing, etc.).

The signature affixed by the author of the document on paper (handwritten signature) is a handwritten and sometimes graphically stylized name or other graphic sign that identifies the author (signer) and signifies his agreement with the content of the document. Verification of the authenticity of a handwritten signature is carried out by visually comparing it with the original, which is recorded in the prescribed manner. If necessary, an appropriate examination can be carried out to officially verify the signature.

Unlike a document on paper, an electronic document (ED) can be subject to various changes very easily. Therefore, in order to ensure the possibility of verifying the authenticity of the signature imposed on the ED, it is necessary to apply an appropriate mechanism that makes it possible to unequivocally determine whether any unauthorized changes were made to the content of the ED after it was signed.

Imposing a signature on an ED by graphically reproducing a handwritten signature cannot serve as confirmation that the document is authorized by the signer, since the graphic image can be copied and pasted under any text or other element of the ED, and thus the signer will be attributed illegal authorship of the "document".

For ED, the complete analogue of a handwritten signature under a document on paper today is an electronic digital signature (EDS),

the application of which is implemented with the help of information technologies and is carried out by means of certain cryptographic transformations over ED (a set of electronic data), on the basis of which the content of this ED is reproduced. According to the conditions defined by the legislation, the EDS is equivalent to a handwritten signature and has the same legal force as it.

Electronic digital signature keys

The EDS application technology is based on cryptography methods. From this field, the term "key" was introduced, that is, a set of binary data of a fixed length. In practical cryptography, a pair of interconnected keys is used – a key for encryption and, accordingly, for decryption. The specified data serve as parameters for the corresponding algorithms of cryptographic transformations. In the field of EDS, a similar pair is used – a private key (PK) and a public key (PK), the first of which is used to impose a signature, and the second – to verify it. This pair of keys is created by generating them with the help of EDS tools based on algorithms for obtaining random numbers of large bits. At the same time, a reliable EDS tool is subject to, in particular, a requirement that a pair of keys can be practically generated only once with its help, and their security must be sufficiently guaranteed – in particular, after transferring the keys generated using this tool to an external storage medium. This data in such a device (for example, a personal computer) will be destroyed, that is, it will become unavailable in the future. In addition, the technologies for using a reliable EDS tool must ensure with sufficient assurance that the keys cannot be obtained by derivative methods, and the signature itself is protected from forgery by using available information technologies.

It should be noted that the term "personal key", that is, a key that must be used personally, with access to it blocked by other persons, corresponds to the term "private key" in the English language.

The importance of the value of PK in the application of EDS is emphasized in the relevant provisions of the legislation. In particular, in accordance with Article 7 of the Law of Ukraine "On Electronic Digital Signature" [25], the signer (owner of the PK) is obliged to keep the key confidential, and in accordance with Article 8, the storage of OCs and viewing of them in the key certification center is prohibited.

The legislation does not require the form of storage of the PK, which is used to check the EDS. It can be stored, in particular, on paper – in the form of a record of the corresponding code, as well as on traditional electronic media – diskettes, discs, flash cards, hardware media, etc. Today, there are hardware carriers of key information on the market, which are intended, in particular, for saving and using PK and hardware implementation of cryptographic transformations, and which are manufactured in a form that looks like a flash card with a USB interface. Hardware carriers of key information ensure the security of the process of performing cryptographic transformations, which are carried out using the PK, and prevent access to it from the hardware and software environment of the computer. With the help of a hardware medium, the PK and public key of the signer can be generated and stored in it. At the same time, the signer's PK is stored in the internal memory of the hardware medium, where protection against unauthorized access is provided.

In its letter [45], the National Bank of Ukraine recommended that banks of Ukraine consider the issue of reducing risks when using information technologies and software and technical complexes of banks, in particular, by using hardware carriers of key information and the use of these hardware carriers in the cryptographic information protection system of the National Bank.

Security of electronic digital signature

The protection of EDS against reproduction or forgery is based on the application of cryptography methods in the corresponding technologies. Yes, in case of application of the algorithm defined by the State Standard of Ukraine (SSU) 4145:2002 "Information technologies. Cryptographic protection of information. A digital signature based on elliptic curves. Formation and verification" [7], formation and verification of an electronic digital signature with a key length of 264 bits, experts estimate the time required for its possible "breaking" by applying the most modern methods of cryptanalysis using a computer with a processor frequency of 3 GHz to be almost 1,000 years. That is, such a long time is the basis of the guarantee of EDS stability. In addition, an additional obstacle for attackers who can attempt to "crack" the private key is that the term of its use is limited (as a rule, no more than a year) and the signer periodically replaces the

private key and in advance – if there is a suspicion of its compromise, that is, the occurrence of a situation when there is a possibility that it has become available to another person (persons).

Legal status of electronic digital signature

According to Article 1 of the Law of Ukraine "On Electronic Digital Signature" [25] EDS is imposed on a set of electronic data, which is added to this set or logically combined with it. According to Article 6 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" [24], an electronic signature is a mandatory ED requisite used to identify the author and/or signatory of an ED by other subjects of electronic document management. It should be noted that the use of EDS allows you to also confirm the integrity of the ED. At the same time, it should be emphasized that only EDS is equivalent to a handwritten signature (seal) in terms of legal status, and other types of electronic signatures do not have such a status.

In accordance with Article 5 of the Law of Ukraine "On Electronic Digital Signature" [25], state authorities, local self-government bodies, enterprises, institutions and state-owned organizations must use only EDS, and to certify the validity of a public key, use only a reinforced public key certificate. At the same time, it should be noted that in accordance with the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for the use of electronic digital signatures by state authorities, local self-government bodies, enterprises, institutions and organizations of state ownership" [35], the EDS institutions specified in it do not apply:

– for drawing up ED, which cannot be originals in the cases provided for by law;

– for carrying out transactions for an amount exceeding 1 million hryvnias.

Electronic seal

In the event that, according to the law, it is necessary to certify the authenticity of the signature with a seal on the documents and the conformity of the copies of the documents with the originals, a special EDS, called an electronic seal (ES), is used for such purposes. Viewed from a purely technological point of view, EDS and ES are quite similar,

the simultaneous presence of these objects in the legislation on ED is due to different functions that must be provided with their help, and is caused, in particular, by the existence of two different types of subjects, which can be conventionally called " director" and "secretary". Representatives of the first type of subjects sign the document, and representatives of the second type seal the signature.

In accordance with the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for the use of electronic digital signatures by state authorities, local self-government bodies, enterprises, institutions and organizations of state ownership" [35], the institutions specified in its name use an electronic seal only if they have a corresponding seal, which is used for paper documents. At the same time, in the strengthened public key certificate used by the institution for the electronic seal, the special purpose of the EDS and its scope of application are additionally indicated, as well as the text information placed on the corresponding seal (the so-called "wet" seal) is reproduced. The right to put an electronic seal on the ED is granted only to the employee of the institution who puts the corresponding "wet" seal on paper documents.

It is quite obvious that in the absence in the legislation, in addition to the provisions on EDS, there are also provisions on the electronic seal, it is impossible to talk about the full use of ED on a par with paper documents.

The use of EDS and electronic seal, in particular, will make it possible to use ED during elections at various levels. At the same time, it will be possible for the Central Election Commission to more quickly receive the protocols of the election commissions in electronic form, which will contain, along with the EDS, also an electronic seal. According to their legal status, such protocols will have equal force with documents on paper, on which handwritten signatures affixed with a "wet" seal.

Use of electronic digital signature

According to the legislation, EDS is imposed on ED, and more generally – on a set of electronic data and is added to this set or logically combined with it. Such a set can be a file that represents the content of the ED, created, for example, using the Microsoft Word word processor or the Microsoft Excel spreadsheet editor, a text, graphic, audio or video file, etc.

It should be noted that the personal key (PK), public key (PK) and electronic digital signature (electronic seal) are, as a rule, formed, submitted and stored in the information system and on the personal computer in electronic form as files with binary data, similarly to ED.

Superimposition of EDS (ES) on ED (set of electronic data) is carried out with the help of OK, which serves as a parameter for cryptographic transformation of this data. The initial stage of this cryptographic transformation of data, or hashing, which is also called a hash function (convolution function), is to obtain a hash value (hash code) of ED. Sometimes the hash code is also called the digest ("print") of the message. At the same time, the hash code has a fixed length, is unique and uniquely represents the ED (a set of electronic data) that is signed. After that, with the help of the signer's PK, which is also a fixed-length code, the ED hash code is encrypted, and as a result, a fixed-length code is formed, which is actually an EDS superimposed on the ED. It is quite clear that there is no transformation inverse to hashing, with the help of which it is possible to reproduce the ED itself from the ED hash code (a set of electronic data) (Figure 3.1).

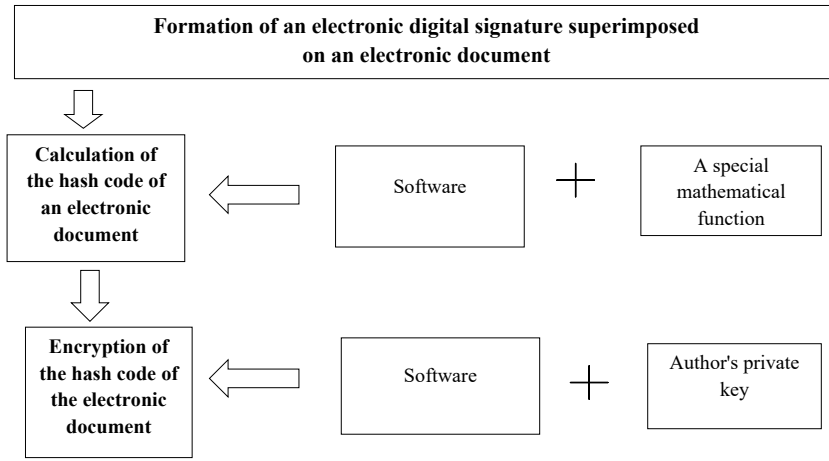

Figure 3.1 Scheme of forming an electronic digital signature

Taking into account the fact that the EDS is a code, that is, a set of electronic data in binary form, it is impossible to "read" the signer's identity data directly from it. For this purpose, a mechanism based on a public key certificate (PKC) exists and is used, which is formed for each specific public key by one of the entities of the public key infrastructure (IPK) – a key certification center (KCC), an accredited key certification center (AKCC), or a certification center.

That is, the two corresponding sets of electronic data (codes) obtained at the same time are different. If we assume that the same code will act as an EDS for different EDs, then taking into account that such a "signature" can be freely copied, or more precisely, another copy of it can be obtained, and its further replication for any number of other "documents" will be possible » without the participation of the author. Thus, it will be possible to impose on the author an ED with which he does not agree, but at the same time he will be obliged to bear responsibility for it. This will mean that in such a situation, the application of EDM with the use of EDS will lose any meaning. Technologies for using a reliable EDS tool must ensure with sufficient assurance that the signer's ID cannot be reproduced from the ED (set of electronic data), its hash code and the EDS superimposed on this ED, or from a combination of such data sets (for different documents). As already mentioned, the length of time required to implement the ability to reproduce a private key by applying the most modern methods of cryptanalysis with the help of a modern computer, it is estimated by specialists to be up to 1000 years old.

Verification of the authenticity of the EDS (ES) superimposed on the ED (electronic data set) is carried out using a public key.

The first step of this procedure is to decrypt the EDS code using the public key code, which results in the original ED hash code, that is, the hash code that was calculated when the EDS was superimposed on the ED. The hash code of the ED being verified is then calculated, since it is not known whether this ED matches the content of the ED being signed.

After that, these two hash codes are compared and based on the positive results of the comparison, a conclusion is made about the authenticity of the EDS and the integrity of the ED (a set of electronic data), that is, that no changes were made to it after the EDS was applied to the ED.

The verification of the authenticity of the electronic signature affixed to the ED is carried out according to the same procedure as the EDS verification (Figure 3.2).

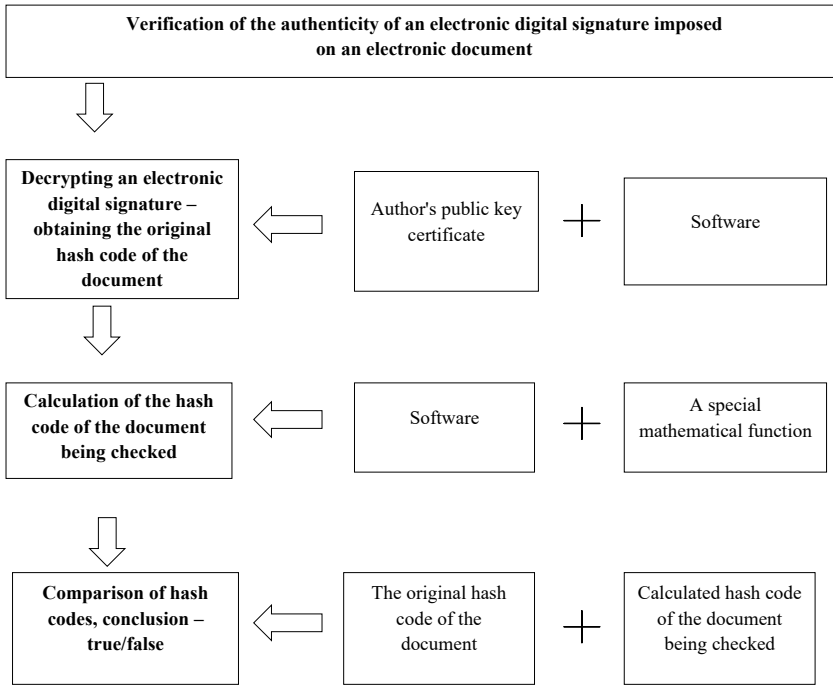

Figure 3.2 Scheme of verification of the authenticity of an electronic digital signature

It should be noted that changes made to ED, more precisely to the corresponding set of electronic data, may be, in particular, a consequence of:

– intentional modification or destruction of data carried out by a certain person;

– exposure to a malicious computer program, i.e. infection by a computer virus;

– a failure, i.e. leaving the regular and switching to the non-regular mode of operation of the information system as a whole, or of a separate computer, or their "freezing";

– effects of technical interference on electrical signals, with the help of which these data were transmitted through telecommunication channels.

In accordance with Article 1 of the Law of Ukraine "On Electronic Digital Signature" [25] EDS allows to check the integrity of electronic data on which it is superimposed and to identify the identity of the signatory. Since the EDS is a code, the public key certificate (PKC) mechanism is used to obtain data about the signer's identity. At the same time, the strengthened public key certificate is a document issued by the Central Certification Authority (Accredited Key Certification Center, Central Certification Authority, Certification Center).

In accordance with Article 1 of the said Law, this document certifies the validity and ownership of the VC to the signatory. At the same time, the public key certificate can be distributed in electronic form or in the form of a document on paper and used to identify the identity of the signatory. The composition of the public key certificate is defined in Article 6 of this Law. It contains, in particular, the main data (details) of the signer – the owner of the private key, as well as the public key that is paired with this private key, which means that these keys were generated together.

If, after checking the authenticity of the EDS superimposed on the ED, with the help of the public key contained in the public key certificate, a positive result is obtained, then the data about the signer of the public key certificate precisely identify this person. In this way, the code (EDS) is compared with the identity of the signatory. At the same time, although the two codes (ESP) superimposed using the same personal key of the signatory on two different EDs will be different, their authenticity is checked using the same public key. With a positive result of the check, the same person will be identified – the signer whose data is indicated in the public key certificate. It should be noted that in accordance with Article 5 of the Law of Ukraine "On Electronic Digital Signature" [25] state authorities, local self-government bodies, enterprises, institutions and state-owned organizations to certify the validity of a public key use only a strengthened public key certificate issued by an accredited key certification center.

In accordance with the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for the use of electronic digital signatures by state authorities, local self-government bodies, enterprises, institutions and organizations of state ownership" [35] the authenticity of the EDS superimposed on ED or other electronic data and the integrity of

this document (electronic data) is checked in compliance with the following requirements:

– EDS must be confirmed using a strengthened public key certificate using reliable EDS tools;

– during the verification, the strengthened public key certificate valid at the time of the EDS application must be used;

– the private key of the signatory must correspond to the public key specified in the reinforced public key certificate;

– at the time of the inspection, a strengthened public key certificate generated by an accredited key certification center and/or a strengthened public key certificate of the corresponding certification center must be valid.

Differences between applying an electronic signature to an electronic document and signing a document on paper

In accordance with Article 6 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" [24], the creation of an electronic signature is completed by imposing an electronic signature. This means, in particular, that all the necessary elements, including its number and the date of signing, must be present in the ED at that moment. Attention should be paid to this circumstance during the implementation and use of ED and EDM with the use of EDS. The practice of traditional document circulation shows that the date and number are usually entered into the document on paper already after it is signed. Entering the date and number to the ED, on which the EDS has already been imposed, will violate the integrity of this ED (data set) and a negative result will be obtained when checking the authenticity of the EDS.

Time stamp

The Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Procedure for Certifying the Availability of an Electronic Document (Electronic Data) at a Specific Moment of Time" [32] defines the conditions and requirements for the certification procedure and creates the legal basis for the key certification center to provide relevant EDS services (more precisely, services in the field of use EDS). The following terms are defined in this Procedure:

– ***time fixing service*** – a procedure for certifying the presence of ED (electronic data) at a certain point in time by adding a time stamp to it or logically combining it with it;

– ***a time stamp*** is a set of electronic data, created using technical means and certified by the EDS of the key certification center, which confirms the presence of ED (electronic data) at a certain point in time.

The approval of the specified Order regulates the functioning of the key certification center – trusted entities in the public key infrastructure, which must provide services for creating time stamps around the clock and have an accurate and reliable time source. In the process of time recording, a time stamp is added or logically combined with electronic data in such a way that it is impossible to make changes to them, as well as save time stamps after the provision of the time recording service. The presence of a time stamp allows you to check the validity of the time of the presence of ED (electronic data). At the same time, it is possible to use a public key certificate, which at the time of checking the EDS superimposed on the ED, has already been canceled or revoked. Otherwise, the validity of the signed ED is limited by the validity period of the public key certificate.

The joint order of the State Committee for Information Science and State Special Communications approved "Technical specifications of the formats for presenting the basic objects of the national electronic digital signature system (time recording protocol)" [52]. The requirements of these Technical Specifications are mandatory for reliable EDS tools, software and technical complexes of an accredited key certification center. The correctness of the implementation of the protocol and the specified formats in EDS tools must be confirmed by a certificate of compliance or a positive expert opinion based on the results of a state examination in the field of cryptographic information protection.

The technical specifications define the procedure for forming a time stamp, in particular the actions performed by the user and the key certification authority.

According to the procedure, the user pre-calculates the hash code (hash value) of the ED (electronic data set). It should be noted that the calculation of this code is an intermediate technological stage in the formation of the EDS, which is superimposed on the ED. After that, the user forms a request for the formation of a time stamp, which contains, including

the calculated hash code, and transmits it to the key certification center. In turn, the key certification center checks the correctness of the request format and processes it, generates a time stamp and a response containing this stamp, or a response with information about the refusal to generate a time stamp.

Based on the result of processing this service, the key certification center sends the user a response containing a time stamp certified by the center's EDS. The generated time stamp, i.e. a set of electronic data created using technical means, includes the hash code of the ED (electronic data set) for which the stamp was created, the time of its creation, and the serial number.

After receiving the response received from the key certification center, the user checks the result of processing his request in the center's response. With a positive result of the processing, the user checks the correspondence of the name of the subject who signed the time stamp, the validity of the certificate of the open key of the center and the authenticity of the EDS superimposed on the stamp received from the center. After that, the user compares the previously calculated ED hash code with the hash code recorded in the timestamp. If the comparison is positive, the time stamp can be added to the ED.

Timestamp verification can be performed by any subject (verifier) using a public key certificate belonging to a key certification center, autonomously, without interaction with this center. For this purpose, the verifier extracts the time stamp from the ED to which it was attached and obtains from it identification information about the key certification authority. On its basis, a public key certificate belonging to the key certification center, which is stored in the center of the certification body (certification center), can be obtained. With the help of a valid (at the time of the mark formation) public key certificate of the key certification center, the verifier verifies the authenticity of the EDS superimposed on the time stamp. After that, by comparing the calculated ED hash code and the hash code stored in the time stamp, it is possible to check the correspondence of the time stamp and the ED to which it was attached.

The time stamp on the ED certifies the exact time for which this document already existed and therefore it will be possible to resolve conflicts related to the use of this document in the future. In particular, it can be used to ensure that the author of the ED does not refuse his EDS.

The presence of a time stamp added to the ED allows you to extend the validity period of the EDS imposed on it. Such a mark (stamp) certifies, for example, that the EDS was applied to the ED before the corresponding public key certificate was revoked (revoked). Thus, the public key contained in the already revoked or revoked certificate can be used to verify the authenticity of the EDS imposed on the ED before the public key certificate is revoked. The chain of time stamps allows you to create archival storage systems of ED, while preserving the authenticity of EDS superimposed on these documents. Otherwise, the authenticity of the signed ED is limited by the validity period of the public key certificate that was valid at the time of the EDS overlay.

It should be emphasized that in order to obtain a time stamp, the user should not send the keys to the certification center, neither the ED itself (electronic data set), nor the EDS superimposed on it. That is, the procedure for forming a time stamp cannot in any way violate the confidentiality of ED (electronic data set) and it can be used, for example, as one of the mechanisms for confirming the authorship of a literary work, an audiovisual work in digital format, a database, a computer program, etc.

Public key certificate

Under the condition of corporate use of EDS, that is, by a certain number of persons, to ensure the verification of the authenticity of the signatures of these persons, it is enough for them to exchange a public key among themselves. The availability and authenticity of public key membership can be achieved through certain rules that must be followed by specified individuals within that corporation.

In order to ensure the possibility of checking the authenticity of EDS by an unspecified number of persons, a mechanism of using a public key certificate has been developed in practice, which is a document issued by the key certification center that certifies the validity and ownership of the public key to the signatory.

According to Article 6 of the Law of Ukraine "On Electronic Digital Signature" [25], the public key certificate contains the following mandatory data:

– name and details of the key certification center (certification authority center, certification center);

– indicating that the public key certificate was issued in Ukraine;
– unique registration number of the public key certificate;
– basic data (details) of the signer – owner of the private key;
– the date and time of the beginning and end of the validity period of the public key certificate;
– public key;
– the name of the cryptographic algorithm used by the owner of the private key;
– information on restrictions on the use of EDS.

At the same time, the strengthened public key certificate, in addition to the mandatory data contained in the public key certificate, must have a corresponding sign (that it is, in fact, a strengthened public key certificate).

Other data can be entered in the strengthened public key certificate at the request of its owner.

Entities of the Public Key Signature Infrastructure

The basis of Public Key Infrastructure consists of entities that are key certification centers, some of which have the status of accredited key certification centers. The main function of the key certificate authority is to enable an unlimited number of users to have access to the public key certificate of the signers through public communication networks, in particular through the Internet. The presence of a public key certificate makes it possible to verify the authenticity of the EDS imposed by the signer and to identify his identity.

The key element of the open key infrastructure is the Central Security Agency, which is determined by the Cabinet of Ministers of Ukraine and maintains the Register of entities – certification centers and accredited key certification centers [54] that provide services defined by the Law of Ukraine "On Electronic Digital Signature" [25] related to Electronic data processing (EDS services). The main function of the certification authority center in the public key infrastructure is to certify the ownership of the public key by the corresponding key certification center, which in turn certifies the ownership of the public key to the signatories. Conventionally speaking, the trust in the certificate authority center extends to the public key certificate belonging to the key certification center, and the trust in the key certification center extends to the public key certificate of the signers,

respectively. Currently, the functions of the certification body center are performed by the Ministry of Justice of Ukraine.

The State Service for Special Communications and Information Protection of Ukraine (State Special Communications) plays an important role in the institutional support of the functioning of the open-key infrastructure. In accordance with Article 12 of the said Law, the functions of the controlling body are performed by a specially authorized central body of the executive power for the organization of special communications and information protection (currently the State Special Communications Administration). In order to ensure the implementation of its functions, the State Special Communications Administration by its order approved the "Regulations on the procedure for state control of compliance with the requirements of legislation in the field of electronic digital signature services" [43], according to which the control body verifies compliance with the requirements of this Law by the center of the certifying body, the center certification body, certification centers and central keys.

In accordance with Article 10 of the said Law, the Cabinet of Ministers of Ukraine, if necessary, determines the certification center of the central executive body to ensure registration, certification of the validity of public keys, and accreditation of a group of key certification centers that provide EDS services to this body and its subordinate enterprises, institutions, and organizations. The certification center in relation to such group of key certification center has the same functions and powers as the center of the certification authority in relation to the key certification center. Other state bodies, if necessary, in agreement with the Cabinet of Ministers of Ukraine, determine their certification centers designated to perform such functions.

According to part seven of Article 5 of the aforementioned Law, the procedure for using EDS in banking activities is determined by the National Bank of Ukraine. In particular, the National Bank of Ukraine adopted the resolution "On the approval of normative legal acts on the functioning of electronic digital signatures in the banking system of Ukraine" [44]. In order to ensure the formation of an open key infrastructure component for the banking system of Ukraine and to create conditions for the further functioning of EDS in banking activities, the Cabinet of Ministers of Ukraine approved the creation of the Certification Center of the National

Bank of Ukraine by a corresponding order [42]. This, in particular, will make it possible to achieve a reduction in the costs of the banking system for EDS services due to the use of a centralized open-key infrastructure, and to accelerate the wider use of EDS in the banking system and contribute to the further development of modern IT in banking.

Key Certification Center

In the presence of a public key infrastructure, any natural or legal person who has expressed a desire to use EDS in their activities can apply to the key certification center (Accredited to the key certification center) or to its authorized representative, who during the registration procedure identifies the applicant and the received from him the data necessary for the formation of a strengthened public key certificate. At the same time, the key certification center creates a signer's public key certificate in the form of a document certified by its signature. A mandatory element of this document is the signer's public key. After the key certification center has generated a public key certificate, it provides it to the signer for whom this public key certificate was generated, and also provides users with free access to this document through public communication channels if the signer agrees.

According to Article 6 of the Law of Ukraine "On Electronic Digital Signature" [25] the key certification center can be a legal entity regardless of the form of ownership or a natural person who is a subject of entrepreneurial activity that provides EDS services and certified its public key in the center of the certification body or certification center in compliance with the requirements of Article 6 of the said Law. The key certification center provides services to individuals and legal entities on a contractual basis.

According to this Law, EDS services are:

– provision of EDS facilities for use;

– assistance in generating a public key and private key;

– maintenance of public key certification (formation, distribution, cancellation, storage, blocking and renewal);

– provision of information on valid, canceled and blocked public key certificates;

– time recording services;

– consultations and other services.

Accredited key certification center

According to Article 9 of the Law of Ukraine "On Electronic Digital Signature" [25], a key certification center accredited in accordance with the established procedure is an accredited key certification center. The accreditation procedure, which is carried out on a voluntary basis, documents the competence of the key certification center to carry out activities related to the maintenance of a strengthened public key certificate. At the same time, the accredited key certification center must fulfill all the obligations and requirements established by law for the key certification center, and is additionally obliged to use reliable EDS tools to provide EDS services.

According to the "Procedure for the use of electronic digital signatures by state authorities, local self-government bodies, enterprises, institutions and organizations of state ownership" [35] the institution, i.e. any entity specified in this Procedure, receives EDS services from an accredited key certification center on a contractual basis, and the use by signatories (employees of the institution) of a personal key, the corresponding public key of which is certified by another accredited key certification center, is prohibited.

Pursuant to the Resolution of the Cabinet of Ministers of Ukraine "On Approving the Procedure for the Accreditation of the Key Certification Center" [33], by order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine (its legal successor is the State Special Communications Administration), the "Rules of enhanced certification" [50] were approved, which determine the organizational, technical and technological requirements for an accredited key certification center during their maintenance of a strengthened public key certificate and ensuring their use. In accordance with the specified Procedure and with the aim of creating the conditions for the technological compatibility of the software and technical complexes of the accredited EDS key certification center and means, the joint order of the State Committee for Information Science and State Special Communications [52] approved the "Technical specifications of the presentation formats of the basic objects of the national electronic digital signature system" containing:

– format of signed data;

– time recording protocol;

– a protocol for determining the status of a strengthened public key certificate.

The requirements of these Technical Specifications are mandatory for reliable EDS tools, software and technical complexes accredited key certification center. The correctness of the implementation of the above formats in EDS tools must be confirmed by a certificate of conformity or a positive expert opinion based on the results of state expertise in the field of cryptographic information protection. The type of EDS format is chosen depending on the requirements for storing signed data.

Distribution of public key certificates

According to the legislation, public key certificates can be distributed in electronic form or in the form of a document on paper and used to identify the identity of the signatory. At the same time, a strengthened public key certificate is a public key certificate that meets the requirements of the Law of Ukraine "On Electronic Digital Signature" [25]. Issued by an accredited key certification center, certification center, certification authority center. In accordance with Article 8 of this Law, the key certification center is obliged to provide 24/7 user access to public key certification and the corresponding electronic lists of public key certificates through publicly available telecommunication channels.

Users, if necessary, obtain the signer's public key certificate from the certificate database of the key certification center, and at the same time, the status of this public key certificate is checked (valid, blocked, revoked). EDS can be checked using the public key contained in the public key certificate only if the certificate is currently valid (Figure 3.3).

Mandatory transfer of documented information of key certification centers

The set of private key certificates stored in an accredited key certification center, relevant registers and other documented information is the main information component of the public key infrastructure. Due to its incompleteness, the circle of subjects applying EDS will be limited and can be reduced only to corporate groups that will independently exchange public keys among themselves. In order to ensure the protection of the rights of entities that use EDS and the stable existence of the public key infrastructure, it is necessary to create legal and organizational conditions under which the specified information will be guaranteed to be saved.

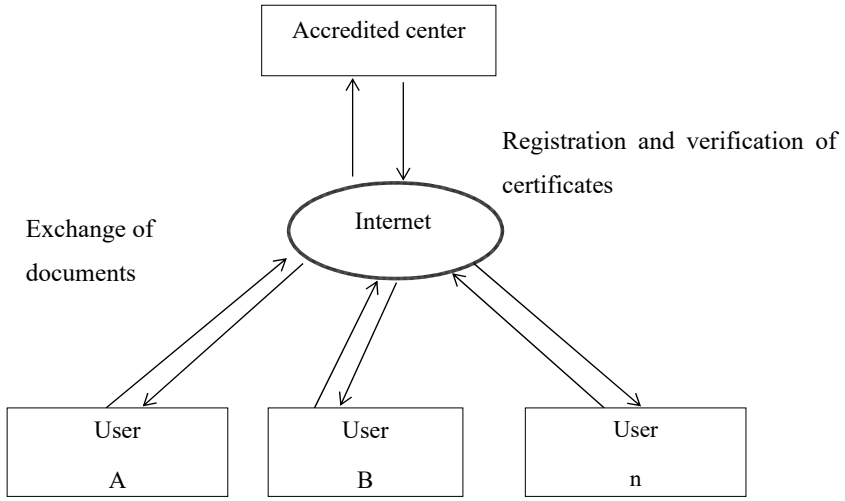

Figure 3.3 Scheme of interaction of users of an electronic digital signature

In accordance with Article 14 of the Law of Ukraine "On Electronic Digital Signature" [25], the key certification center ceases its activities in accordance with the legislation. The key certification center notifies signatories of the decision to terminate its activities three months in advance, unless other terms are specified by law. At the same time, the accredited key certification center additionally informs about the decision to terminate the activity of the center of the certification body or the relevant certification center and within the day specified as the date of termination of its activity, in accordance with the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for the mandatory transfer of documented information" [37] transmits the enhanced public key certificate, the corresponding registers of the enhanced public key certificate and the documented information that is subject to mandatory transfer to the relevant certification center or center of the certification authority.

4. Systems of electronic document circulation

Approved by the Resolution of the Cabinet of Ministers of Ukraine "Standard procedure for implementing electronic document circulation in state authorities" [36] establishes the general rules for documenting administrative activities in the bodies of the executive power in electronic form and regulates the execution of actions with electronic documents (ED) from the moment of their creation or receipt until they are sent or transferred to the archive of the executive power. At the same time, all other ED actions are performed in the executive power body in accordance with the requirements for actions with paper documents provided by the instructions for all EDs created or received by the executive power body.

The executive authority carries out electronic document management (EDM) only under the condition of using reliable EDS means, which must be confirmed by a certificate of compliance or a positive conclusion based on the results of a state examination in the field of cryptographic information protection, received for these means from the State Special Communications Administration, and the presence of a reinforced certificate public key from its employees – signatories. At the same time, EDM is carried out by an executive power body through special communication networks or public communication networks, and ED is sent through public communication networks by the decision of the head of this body.

According to the legislation, the electronic document management system of the executive authority must meet the requirements of the regulatory acts in the field of information protection. In particular, this concerns the provisions of the Law of Ukraine "On the Protection of Information in Information and Communication Systems" [26] and the Resolution of the Cabinet of Ministers of Ukraine "On approval of the Rules for ensuring the protection of information in information, communication and information and communication systems" [38].

According to the Rules, to ensure the protection of information in the information system, a comprehensive information protection system (CIPS) is created, which is designed to protect information from:

– leakage through technical channels, which include channels of side electromagnetic radiation and guidance, acoustic-electric and other channels formed under the influence of physical processes during the functioning

of information processing equipment, other technical equipment and communications;

– unauthorized actions with information, including the use of computer viruses;

– special influence on information processing means, which is carried out by forming physical fields and signals and can lead to violation of its integrity and unauthorized blocking.

The responsibility for ensuring the protection of information in the information system, the timely development of necessary measures and the creation of a comprehensive system of information protection rests with the head (deputy head) of the organization that is the owner (manager) of the information system and the heads of its structural divisions that ensure the creation and operation of IS.

At the same time, the organization and implementation of information protection work in the information system is carried out by the information protection service (IPS), which ensures the definition of information protection requirements in IS, the design, development and modernization of a comprehensive information protection system, as well as the performance of work on its operation and control state of information security.

The formation of the information protection service is carried out in accordance with the decision of the head of the organization that is the owner (manager) of the IS. In the event that the amount of work related to the protection of information in IS is insignificant, the protection of information can be carried out by one person. Information protection at all stages of creation and operation of IS is carried out in accordance with the plan of information protection in IS developed by the information protection service.

Subjects of the electronic document circulation system must store ED on electronic media in a form that allows checking their integrity on these media, and their storage period must not be less than the period established by law for the corresponding documents on paper.

In case of impossibility of storing ED during such a period, EDM subjects must take measures to duplicate documents on several electronic media and carry out their periodic copying in accordance with the procedure for recording and copying documents established by law. If it is impossible to fulfill the specified requirements, ED must be kept in the form of a copy

of the document on paper (in the absence of the original of this document on paper).

Creation of ED archives, submission of ED to archival institutions of Ukraine and their storage in these institutions is carried out in accordance with the procedure defined by legislation.

It should be noted that today in Ukraine electronic document management systems and ED archival storage systems are perceived as different systems, although from a functional point of view they are extremely close. Probably, the trend of the further development of these systems will be their integration.

Pursuant to the Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Standard Procedure for Electronic Document Management in Executive Power Bodies" [36], the State Archives Committee of Ukraine approved the "Procedure for storing electronic documents in archival institutions" [51]. This Order establishes general rules:

– operational storage of ED, created in accordance with the legislation on EDS, ED and EDM by state authorities, local self-government bodies, enterprises, institutions, organizations regardless of the forms of ownership (institutions);

– preparation and transfer of ED for long-term storage to the archival division of the institution;

– long-term storage of ED in the archival division of the institution.

At the same time, the requirements for ensuring the protection of ED are formed for each automated system separately in accordance with the requirements of regulatory and legal acts in the field of information protection.

Preparation of ED for transfer to the archival division of the institution in the form of electronic files includes:

– verification of all electronic signatures;

– examination of the value of ED;

– execution of electronic cases;

– compilation of descriptions of electronic cases;

– preparation of a set of accompanying documentation.

The procedure and deadlines for transferring ED for permanent storage to a state or other archival institution, as well as the formats for submitting data in an electronic file and a set of accompanying documentation are

determined by a specially authorized central body of the executive power in the field of archival affairs and record keeping.

Normative provision of electronic document management systems

Pursuant to the Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Standard Procedure for Electronic Document Management in Executive Authorities" [36] "Technical conditions for the electronic document circulation system of the executive authority" were approved by order of the State Department for Communication and Informatization of the Ministry of Transport and Communications (Technical conditions of Ukraine 30.0-33240054-001:2005) [53]. These Technical Terms apply to the electronic document management system, designed to ensure the exchange of ED and messages in compliance with the requirements of the specified Standard Procedure.

Compliance with the Technical Terms provides the opportunity to:

– unification of information exchange formats between executive authorities;

– integration of the electronic document management system into the unified national system of electronic document management of executive authorities.

The general procedure for creating and adopting an electronic document management system must meet the requirements of the State Standard of Ukraine 34.601-90 "Automated systems. Stages of creation" [8].

The adoption of the electronic document management system is carried out by the state (interagency) commission, which must include representatives of the system developer, the executive authority and authorized bodies responsible for the implementation of EDM in the executive authorities of Ukraine, and is approved by the act of acceptance and delivery of scientific and technical products.

One of the stages of implementing an electronic document management system is the purchase or creation of appropriate software (software). In order to settle issues of supply, creation or technical support of software products (software) that are purchased or created to the order of state bodies, including during the implementation of tasks (projects) of the National Informatization Program, in particular, on the creation of an electronic document management system, the Cabinet of Ministers of Ukraine adopted

the Resolution "On approval of general requirements for software products that are purchased or created on the order of state bodies" [39].

It should also be noted that the issue of creating a system of electronic document circulation is relevant for many countries, including members of the European Union. In particular, within the IDA program of the European Commission, Cornwell Management Consultants plc (formerly Cornwell Affiliates plc) developed the MoReq (Model Requirements) Specification "Typical Requirements for Automated Electronic Document Management Systems" [57]. This specification has a universal character and does not contain any national specifics. It does not determine how the processes of registration, agreement and execution of documents should be carried out in a specific organization, but what functional requirements an automated system should meet in order to support any regulations for working with documents.

The specification describes typical requirements for management of ED (Management of Electronic Record) or requirements for EDM and focuses mainly on functional requirements for management of EDM using automated electronic document management systems (AEDM).

When developing the specification, it was assumed that the users of the automated electronic document management system include not only administrators, clerks and archivists, but also employees of general administrative and functional structural units who use the automated electronic document management system in their daily activities to create ED access to them.

The specification also notes that ED management is a complex task that requires a wide range of functionality and a high level of implementation. It is obvious that an automated electronic document management system that meets these requirements requires specialized software. Such software may be a specialized package, multiple integrated packages, custom development, or a combination of the above; in all cases, the decision must be supplemented by organizational measures and management policies (methods). The nature of the automated electronic document management system will be decided from institution to institution. This specification does not make assumptions about the nature of a specific automated electronic document management system. Users of this specification must determine for themselves how the functional requirements should be implemented to meet their needs.

One of the examples of the sectoral implementation of EDM can be called a complex related to the transportation of goods by railway transport. By order of the Cabinet of Ministers of Ukraine [46], the Action Plan was approved, which provides, in particular:

– approval of the format of the electronic transport document;

– making changes to a number of regulatory documents;

– development and implementation of EDM technologies in automated systems for managing cargo transportation by railway transport;

– creation of a specialized hardware and software complex;

– ensuring the use of electronic transport documents during the transportation of goods by rail within Ukraine.

The Ministry of Infrastructure of Ukraine issued a corresponding order [42] to implement the Action Plan, which, in particular, made changes to a number of rules and instructions.

The second example is the creation of a multifunctional complex system "Electronic Customs". The concept of its creation was approved by the relevant decree of the Cabinet of Ministers of Ukraine [41].

Among the ways of implementation of the Concept are defined, in particular:

– introduction of EDS for officials, customs authorities;

– creation of a system of electronic document circulation and electronic declaration.

One of the priority directions for the creation of the technological infrastructure of electronic government in Ukraine is the unification of information systems that exist in state authorities and local self-government bodies, as well as systems that will be developed in the future, into a single information and analytical complex that should function in a single information and communication environment. An important component of this complex should be the integrated system of electronic document management (ISED).

The purpose of creating an integrated electronic document management system:

– ensuring the movement of ED (decrees, resolutions, laws, orders, notices, reports, analytical reports, etc.);

– shortening the period of preparation and decision-making by automating the processes of collective creation and use of ED in state authorities.

The main tasks that are solved with the help of an integrated electronic document management system:

– мautomation of ED processing, search and selection of necessary information, mailing of processed EDs for further processing;

– exchange of ED between nodes of the integrated system of electronic document circulation, unification of technological procedures of passage, transfer and processing of ED, collection, registration, accumulation, processing and analysis of information received by each of the nodes, ensuring constant communication and exchange of information between nodes;

– automation of management of work synchronization processes;

– automation of ED execution control;

– automation of ED registration processes using classifiers and directories, provision of mechanisms for annotated description of ED and collection of resolutions, delivery of reports on the execution of assignments;

– automation of data collection on the results of execution of technological processes, formation of arbitrary analytical reports;

– mailing, storage and use of incoming, outgoing and internal ED according to a single numbering since the beginning of the year;

– sending, receiving and processing e-mail;

– operational search for information about incoming, outgoing and internal EDs;

– end-to-end control of information exchange;

– maintaining a system of classifiers and directories;

– constant updating and administration of the main database;

– ensuring reliable storage of all versions of ED and other information objects;

– organization of copy-restoration and information protection services;

– formalization of information processing technological processes, determination of typical route technological schemes for their implementation;

– definition and assignment of levels of access to information, authorizations and rights of users;

– improvement of methods of supporting decision-making on EDM issues.

The integrated system of electronic document management consists of complexes:

– "Preparation of documents by computer means";

– "Registration and entry of electronic documents into the operational electronic archive";

– "Maintenance of electronic archive, support of paper archive and organization of access to its information";

– "Control of executive activity";

– "Design of document movement routes";

– "Data exchange";

– "Support for the formation of analytical and statistical reporting and operational analysis";

– "Maintenance of normative and reference information";

– "Administration";

– "Unified client site" [13].

At the level of central executive bodies and local self-government bodies, depending on the state of informatization and the structure of the body, the means (information systems) of EDM are used, which can mainly be divided into the following (Figure 4.1).

The main properties of corporate systems of electronic management of ED are:

– the possibility of managing the life cycle of ED – from the author's development to the final revision, approval, distribution and archiving;

– provision of distributed editing of ED, which enables employees working in different geographically separated units to jointly use ED on local servers, while maintaining the integrity of ED on the scale of the entire body (unit) with a distributed structure;

– a full set of ED management tools – registration, receipt (subscription), version control, full-text search in the scope of the entire managed information content of systems, control logs, the ability to work with templates, providing notifications about ED changes, etc.;

– possibility of editing/approving ED;

– multi-level control of ED versions with the organization of their creation and preservation of drafts;

– data protection using certified industrial-level encryption tools, full-scale user identification tools;

– support for various types of ED presentation files, including text, graphic images, spreadsheets, audio and video data, Web documents, etc.

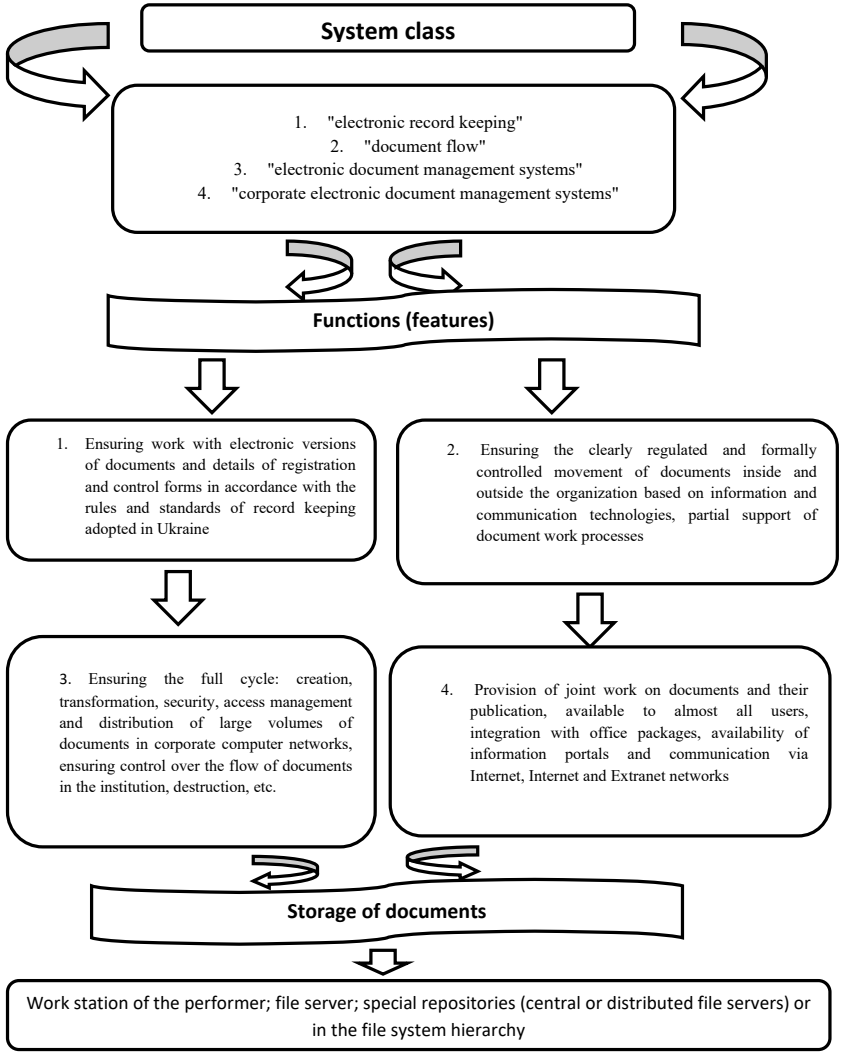

Figure 4.1 Classification of electronic document management systems

ED management is generally understood as the organization of ED movement between departments of the institution, individual users or their groups. At the same time, the movement of ED does not mean their physical movement, but the actual transfer of rights to their use (access), which is accompanied by appropriate notification of this to specific users, as well as control over the execution of ED.

Expected results from the implementation of an integrated electronic document management system:

– more effective management of electronic document flow due to automatic control of execution, transparency of the institution's activities at all levels;

– support for effective accumulation, management and access to information and knowledge;

– ensuring personnel flexibility due to greater formalization of the activities of each employee and the possibility of preserving the entire history of his activities;

– elimination of duplication and multiple conversion of information;

– clear authorization of access to information with limited access, due to which the personal responsibility of employees for actions performed strictly within the framework of the granted powers increases;

– recording of the activity of the institution as a whole (internal official investigations, analysis of the activity of units, identification of "hot spots" in the activity, etc.);

– optimization of management processes, automation of their execution and control;

– elimination or maximum possible reduction of circulation of paper documents;

– saving resources due to the reduction of costs for managing ED flows in the organization;

– eliminating the need or significantly simplifying and reducing the cost of saving paper documents due to the availability of an operational electronic archive.

The integrated electronic document management subsystem should ensure the improvement of the ED processing process and the performance of functions:

– support of the ED object model, including building relationships between objects;

– control and management of the processes of creating ED, providing the user with the opportunity to perform all necessary operations for ED, including their dynamic composition, as well as providing search, saving, viewing and printing of ED;

– providing transparent access through the ED archive to archives of other data or working databases with the possibility of performing operations on this data;

– access to electronic document circulation located in the electronic storage, routing of the entire set of actions on ED from applications;

– development of specialized applications for integration with other IS, in particular with the postal system.

5. Protection of information in electronic governance

Information security plays an important role in ensuring the interests of any state. The creation of a developed and protected information environment is a condition for the development of society and the state. Recently, there have been qualitative changes in management processes in the world, due to the intensive implementation of modern information technologies. At the same time, the danger of unauthorized interference in the operation of information systems increases, and the severity of the consequences of such interference has greatly increased. As a result, in many countries, more and more attention is paid to the problems of information protection and finding ways to solve them.

The basic characteristic of information security should be considered the probability of an increased risk of the realization of a threat or danger for the activities of executive authorities as a whole and for each of its structural elements in particular. The criterion for the effectiveness of ensuring information security is a high level of security with a minimum of relevant costs. The combination of internal and external informational threats creates prerequisites for disrupting the safe functioning of the system of executive authorities.

The directions of ensuring information security in the internal system functioning of executive authorities are characterized by their very competence, which is related to the performance of the functions and tasks assigned to them by the state. The characteristics that make it possible to describe this system include the following:

– availability – the possibility to receive the necessary information service within an acceptable time by any subject of the executive power;

– integrity – relevance and consistency of information, its protection against destruction and unauthorized change;

– confidentiality – protection against unauthorized access.

The essence and content of information security are manifested in a special way at each of the levels of the system of authorities, in particular at:

– strategic (nationwide);

– tactical (authorities, institutions, etc.);

– operational (structural subdivisions of state authorities, local executive authorities, the leading place among which is occupied by local state administrations).

Thus, we can talk about the manifestations of information security in the very process of its provision. In this regard, the following levels should be distinguished:

– legislative and regulatory – laws, regulatory acts, etc.;

– administrative – actions of a general nature, used by executive authorities;

– procedural – specific procedures for ensuring information security;

– software and technical – specific technical measures to ensure information security.

The problem of effective provision of information security in the state involves solving such large-scale problems as:

– development of theoretical foundations for ensuring information security;

– creation of a system of bodies and structures responsible for information security;

– solution and automation of information protection management problems;

– creation of a normative and legal framework that regulates the solution of all tasks of ensuring information security;

– adjustment of the production of means of software and technical protection of information;

– organization of training of relevant specialists, etc.

Among the main principles of state policy in the field of ensuring information security, the following can be noted:

– the state forms an information security program that combines the efforts of state organizations and commercial structures in creating a unified information security system;

– the state exercises control over the creation and use of means of information protection through mandatory certification and licensing of activities in the field of information protection;

– restricting access to information is an exception to the general principle of openness of information and is carried out only on the basis of legislation;

– responsibility for storage, classification and declassification of information is personified;

– access to information, as well as access restrictions, are carried out taking into account the legally stipulated property rights to this information;

– the state forms a legal framework that regulates the rights, duties and responsibilities of all objects operating in the information sphere;

– legal entities and individuals who collect, accumulate and process personal data and confidential information are responsible for storage and use;

– the state pursues a protectionist policy, which supports the activities of domestic manufacturers of means of informatization and information protection, and implements measures to protect the domestic market from the penetration of low-quality means of informatization and information products;

– the state strives to abandon foreign information technologies for informatization of state authorities and management as competitive domestic information technologies and means of informatization are created [3].

Comprehensive information protection
as a component of information provision of executive authorities

According to the Law of Ukraine "On Information Protection in Information and Communication Systems" [26], the basic terminology of information protection systems uses the following concepts:

– blocking information in the system – actions that prevent access to information in the system;

– leakage of information – the result of actions, as a result of which information in the system becomes known or available to individuals and/or legal entities who do not have the right to access it;

– access to information in the system – obtaining the opportunity for the user to process information in the system;

– protection of information in the system – activity aimed at preventing unauthorized actions regarding information in the system;

– destruction of information in the system – actions, as a result of which information in the system disappears;

– information (automated) system – an organizational and technical system in which information processing technology is implemented using technical and software tools;

– information and communication system – a set of information and communication systems, which in the process of information processing act as a single entity;

– comprehensive system of information protection – an interconnected set of organizational and engineering and technical measures, means and methods of information protection;

– user of information in the system (hereinafter – the user) – a natural or legal person who, in accordance with the procedure established by law, received the right to access information in the system;

– cryptographic information protection – a type of information protection implemented by transforming information using special (key) data for the purpose of hiding/restoring the content of information, confirming its authenticity, integrity, authorship, etc;

– unauthorized actions regarding information in the system – actions carried out in violation of the procedure for accessing this information, established in accordance with the legislation;

– processing information in the system – performing one or more operations, in particular: collection, input, recording, conversion, reading, storage, destruction, registration, acceptance, receipt, transmission, which are carried out in the system with the help of technical and software means;

– violation of the integrity of information in the system – unauthorized actions regarding information in the system, as a result of which its content changes;

– the procedure for accessing information in the system – the conditions for the user to be able to process information in the system and the rules for processing this information;

– technical information protection – a type of information protection aimed at ensuring, with the help of engineering and technical measures and/or software and technical means, the impossibility of leakage, destruction and blocking of information, violation of the integrity and regime of access to information [26].

The objects of protection in the system are the information processed in it and the software that is designed to process this information.

The subjects of relations related to the protection of information in the information systems of government bodies are:

– owners of information;

– system owners;

– users;

– authorized body in the field of information protection in systems.

In order to ensure the protection of information with limited access, the requirement for the protection of which is established by law, the following procedures must be performed in information, communication and information and communication systems (hereinafter – the system):

– authentication – the procedure of establishing the identity of the user of the information in the system (hereinafter – the user) of the identifier presented by him;

– identification – the procedure of recognizing a user in the system, usually with the help of a predetermined name (identifier) or other a priori information about him, which is perceived by the system.

During the processing of confidential and secret information, its protection against unauthorized and uncontrolled reading, modification, destruction, copying, distribution must be ensured.

Access to confidential information is granted only to identified and authenticated users. Attempts to access such information by unidentified persons or users with an ID that has not been confirmed during authentication must be blocked.

The transfer of confidential and secret information from one system to another is carried out in encrypted form or through protected communication channels in accordance with the requirements of the legislation on technical and cryptographic information protection.

The procedure for connecting systems in which confidential and secret information is processed to global data transmission networks is determined

by legislation [22]. To ensure the protection of information in the system, a comprehensive system of information protection (hereinafter – the protection system) is created, which is designed to protect information from:

– leakage through technical channels, which include channels of side electromagnetic radiation and guidance, acoustic-electric and other channels formed under the influence of physical processes during the functioning of information processing facilities, other technical facilities and communications;

– unauthorized actions with information, including the use of computer viruses;

– special influence on means of information processing, which is carried out through the formation of physical fields and signals, and can lead to a violation of its integrity and unauthorized blocking.

Protection of information from unauthorized actions, including computer viruses, is ensured in all systems. Protection of information from special influence on means of information processing is provided in the system, if the decision on the need for such protection is made by the owner (administrator) of the information [26].

The complexity of the approach to information protection is a solution within the framework of a single concept of two or more multifaceted tasks. A modern information protection system should include structural, functional and temporal complexity. Structural complexity implies ensuring the required level of protection in all elements of the information processing system.

Functional complexity means that protection methods should be directed to all performed functions of the information processing system. Temporal complexity assumes the continuity of measures to protect information both in the process of its immediate processing and at all stages of the life cycle of an information processing object [26].

The composition of the complex protection system is determined on the basis of the study of all information processes and flows of the telecommunications system and, as a result, the development of such a threat model to ensure the minimization of losses. Based on the threat model, the concept and policy of information security of state authorities should be developed and implemented, and a comprehensive information protection system should be created, which should provide the following functions:

– confidentiality of information – property of information when unauthorized persons who do not have access to information cannot disclose the content of this information;

– integrity of information – the property of information, which is that it cannot be changed intentionally or accidentally by a user or process. And also the property that none of its components can be removed, modified or added in violation of the security policy;

– accessibility – a property of the system resource (information), which consists in the fact that an authorized user can access the resource only with the specified content and quality;

– observability is a property of an information technology resource that allows you to register all user actions, access by name, according to identifiers and authorities, as well as react to these actions in order to minimize possible losses in the system, which is also carried out through the use of cryptographic information protection (CIP) [56].

The comprehensive means of information protection includes measures and means that implement methods, methods, mechanisms of information protection against:

– leaks through technical channels, which include channels of side electromagnetic radiation, acoustic-electric and other channels;

– unauthorized actions and unauthorized access to information, which can be carried out by connecting to equipment and communication lines, masquerading as a registered user, overcoming security measures for the purpose of using information or imposing false information, using collateral devices or programs, using computer viruses, etc;

– special influence on information, which can be carried out by forming fields and signals with the aim of violating the integrity of information or destroying the protection system.

For each specific information system, the composition, structure and requirements for a comprehensive means of information protection are determined by the properties of the processed information, the class of the automated system (AS) and the conditions of its operation.

One of the requirements for ensuring information protection must be implemented using protected technology, which contains software and technical means of protection and organizational measures that ensure the fulfillment of general information protection requirements. General requirements include:

– availability of a list of confidential information that is subject to automated processing;

– if necessary, it can be classified within a category according to its intended purpose, the degree of access restriction of a separate category of users, and other classification features;

– the presence of a responsible unit, which is empowered to organize and implement information protection technology, control over the state of information security (protection service in AS, PSI);

– creation of a complex information protection system, which is a set of organizational and engineering and technical measures, software and hardware aimed at ensuring information protection during the operation of the AS;

– development of an information protection plan in the AS;

– availability of a certificate of compliance of the complex information protection system in the AC with normative documents on information protection;

– the possibility of defining several hierarchical levels of user authority and several classification levels of information by means of a complex information protection system;

– mandatory registration of all users and their actions in relation to confidential information;

– the possibility of granting authorized and controlled access to confidential information processed in the AS to users only under the condition of official necessity;

– prohibition of unauthorized and uncontrolled modification of confidential information in the AS;

– carrying out with the help of SHI the accounting of the initial data received during the solution of the functional task, in the form of printed documents containing confidential information, in accordance with the governing documents;

– prohibition of unauthorized copying, reproduction, distribution of confidential information in electronic form;

– ensuring with the help of the information protection service control over authorized copying, reproduction, distribution of confidential information, in electronic form;

the possibility of unique identification and authentication of each registered user;

– provision of a comprehensive system of information protection, the possibility of timely access of registered users of the automated system to confidential information.

The above requirements are basic and are used in the protection of information from unauthorized access (USA) in all types of automated systems [19].

Therefore, taking into account the above, access to information in the subjective sense is a state-guaranteed opportunity for individuals, legal entities and state bodies to freely obtain the information they need to exercise their rights, freedoms and legitimate interests, perform tasks and functions that are not violates the rights, freedoms and legitimate interests of other citizens, rights and interests of legal entities [2].

Having assessed the need to protect information from unauthorized access, it is possible to judge the complexity of a complex information protection system, assess the likelihood of emerging threats to the information system, as well as form a model of the offender, after which you should proceed with the formation of protective measures. Based on the requirements for the protection of information against unauthorized access [34], it is possible to state the main principles of protective measures against unauthorized access in an automated system.

The first principle is the validity of access. This principle consists in the mandatory fulfillment of two main conditions: the user must have a sufficient "form of admission" to receive information of the required level of confidentiality, and this information is necessary for him to perform his production functions. In the field of automated information processing, users can act as active programs and processes, as well as information carriers of varying degrees of complexity. Then the access system assumes the definition for all users of the appropriate software and hardware environment or information and software resources that will be available to them for specific operations [23].

The second principle is sufficient depth of access control. Information protection means should include access control mechanisms to all types of information and software resources of the automated system, which should be divided between users in accordance with the principle of reasonableness of access.

The third principle is the separation of information flows. To prevent a violation of information security, which, for example, can occur when secret information is recorded on non-secret media and in non-secret files, its transfer to programs and processes not intended for processing secret information, as well as when secret information is transmitted over unsecured channels and communication lines communication, it is necessary to carry out the appropriate separation of information flows.

The fourth principle is the purity of reused resources. This principle consists in cleaning resources containing confidential information when they are deleted or released by the user before redistribution of these resources to other users.

The fifth principle is personal responsibility. Each user must bear personal responsibility for his activity in the system, including any operations with confidential information and possible violations of its protection, as well as for accidental or intentional actions, which may lead to unauthorized access to confidential information, its distortion or destruction, or exclusion of the possibility of access to such information by legitimate users.

The sixth principle is the integrity of means of protection. This principle implies that the means of information protection in the AC must accurately perform their functions in accordance with the listed principles and be isolated from users, and for their support must include a special protected interface for control means, signaling about attempts to violate information protection and actions on processes in the system [21].

When considering issues of information security in an automated system, they always talk about the presence of some "desired" states of the system. These desired states (which are usually represented in terms of a model of the automated system itself) describe the "security" of the system.

So, there are three components associated with a system security breach:

– "threat" – a source of violation of the "security" property external to the system;

– "object of attack" – a part of the system that is affected by the threat;

– "channel of action" is the medium of transmission of malicious action.

The integral characteristic that unites all these components is the security policy – a qualitative (or qualitative-quantitative) expression of security

properties in terms that represent the system. The description of the security policy should include or take into account the properties of the threat, the attack object and the action channel.

According to the definition [6; 18], information security policy means a set of laws, rules, restrictions, recommendations, etc., which regulate the procedure for processing information and are aimed at protecting information from certain threats. The term "security policy" can be applied to an organization, an automated system, an operating system (OS), a service implemented by a system (a set of functions) to provide protection against certain threats, etc.

The information security policy in the automated system is part of the general security policy of the executive authority and may inherit, in particular, the provisions of the state policy in the field of information protection. For each automated system, the information security policy may be individual and may depend on the implemented information processing technology, operating system features, physical environment and many other factors. Moreover, the same automated system can implement several different information processing technologies. Then the information security policy in such an automated system will be complex and its parts corresponding to different technologies may differ significantly.

The security policy should define the resources of the automated system that need protection, in particular, establish the categories of information processed in it. The main threats to the operating system, personnel, information of various categories and requirements for protection against these threats should be formulated. As components of the general information security policy, there should be policies to ensure the confidentiality, integrity and availability of processed information. The responsibility of personnel for the implementation of the provisions of the security policy should be personalized [20].

The methods of ensuring information security are:

– obstacles – physical obstacles to an attacker's access to protected information;

– access control – protection of information by regulating the use of all computer information system resources;

– masking – protecting information by cryptographically closing it;

– regulation – protection of information, which creates such conditions of automated processing, storage and transmission of protected information, under which the possibility of unauthorized access to it would be minimized;

– coercion – protection for which system users and personnel are forced to comply with the rules of processing, transfer and use of protected information, under the threat of material, administrative or criminal liability;

– inducement – protection that encourages the user and system personnel not to violate the established order due to compliance with moral and ethical norms that have developed.

Characteristics of threats to the information security of the system of executive authorities

Threats to information security, on the one hand, are an organizational component of the functioning of the system of executive authorities, and on the other, an indicator of the effectiveness of its functioning. After all, the realization of threats and their development into danger indicate the inefficiency of the functioning of this system, and vice versa. Today, it is necessary to consider any threats in the information sphere taking into account the context in which they arise and manifest themselves. Information wars are the most dangerous at this stage of the development of Ukrainian society [9].

Today, it is information wars that pose one of the greatest dangers to the normal functioning of the system of executive authorities. This determines our detailed consideration of issues related to the definition of the concept and establishment of essential features of information warfare.

Information warfare arises from new approaches to the use of information, determining its role and place. Two definitions of information war can be distinguished: humanitarian and technical.

It is believed that, in the humanitarian sense, information warfare represents active methods of transformation of the information space, which are reflected in the system of imposing world models, which are designed to ensure the desired types of behavior, attacks on the structures of information generation - reasoning processes. At the same time, the technical interpretation of this concept is that hardware, software, etc. are destroyed with the help of special programs. As for the other understanding of the concept of information warfare, i.e. the technical one, it is a prerequisite

here that the conduct of information warfare is the result of concerted activity to use information as a weapon of warfare in any sphere of life. At the same time, the information war includes the following actions:

– influence on the infrastructure of life support systems – telecommunications, transport networks, power plants, etc.;

– hacking – hacking and use of personal data, identification numbers, information with limited access, etc.

The goals of information warfare are somewhat different from war in the usual sense: not the physical destruction of the enemy and the liquidation of his armed forces, but the large-scale disruption of financial, transport and communication networks and systems, the destruction of economic infrastructure and the subjugation of the population of the attacked country to the will of the country-winner [8; 22].

In the West, information war is defined as a "non-physical attack on information, information processes and information infrastructure", and the goal of information war is to influence the system of knowledge and ideas of an external adversary. Knowledge here means objective information. General for everyone, and under ideas – information of a subjective nature. The main tool of information warfare is information weapons.

To "information weapons" we will include, first of all, means of an information and technical nature that destroy, distort or steal information, despite the protection system, limiting access to this information by legitimate users. Secondly, it is undoubtedly information systems through disinformation, formation of false logical information concepts, interpretations, etc., thereby influencing public opinion and the functioning of executive authorities.

Thus, information weapons are devices and means designed to inflict maximum damage on the opposing party during the information struggle (through dangerous informational influences).

Based on the content of the research, the objects of influence of information weapons can be: information-analytical and information-technical systems, which include channels and means of communication of executive authorities, information resources, state mass media, as well as the psychological state of a specific employee of the body.

Technical protection of information

In the general complex of measures to ensure the national security of the state, an important place is occupied by measures related to the direct protection of information from threats, the implementation of which can cause political, economic, financial and other losses to a person, society, and the state [1]. Among information threats, due to their dangerous consequences, a special place is occupied by:

1. Acquisition of information by technical intelligence in the field of defense, economy, science and technology, foreign relations, state security and law enforcement

Despite the positive changes in the international situation around Ukraine, the activities of technical intelligence agencies of foreign countries to gather information continue. Intelligence is continuously conducted against Ukraine by multi-functional space, air, ground, sea systems and technical intelligence complexes. The world's leading countries continue to modernize their intelligence services, improve technical intelligence, and increase its capabilities.

2. Unauthorized access to information that is processed and circulated in information and communication systems, as well as special influence on information for the purpose of its distortion, destruction, destruction, disruption of the normal functioning of information processing systems

Given the insufficient nomenclature of domestically developed information processing tools and software, foreign-made products are widely used in information and communication systems, which mostly do not have objective evaluations of protection mechanisms, and also create prerequisites for the introduction of information technologies into all spheres of the life of a person, society and the state caused by the wide deployment of information and communication systems, a sharp increase in the amount of information that is processed and stored in these systems, a significant increase in the number of users who have direct access to information resources, etc.

At the same time, in the absence of competitive domestic models, preference is given to foreign-made information technologies and technical means of information processing, which mostly do not provide information protection, and also create prerequisites for the uncontrolled use of special software and hardware tools ("storage devices").

In the world, there is a tendency to spread the scale of computer crime, the spread of computer viruses, first of all, with the use of the Internet, the danger of the consequences of illegal actions, technical and technological errors and failures in the use of information and communication systems is increasing significantly, which is especially relevant in the conditions of a wide entry of domestic information and communication systems into global ones.

Individual states implement the "concept of information warfare", which consists in the implementation of measures for special influence on information infrastructure with the aim of damaging (destroying) information resources and destroying the management system in the fields of defense, economy, security, finance, etc.

3. Leakage of information with limited access through technical channels due to the occurrence of side electromagnetic radiation and guidance of acoustic and optical-electronic intelligence in the immediate vicinity of the object of information activity

In the process of carrying out information activities for the storage, processing and transmission of information, including information with limited access, technical means of various purposes are widely used (computer equipment, office equipment, communication means, automated systems, etc). At the objects of information activity, official issues are discussed in various directions of the institution's activities, during which information with limited access can be voiced.

However, certain physical processes occurring in technical means and during the discussion of information and other factors create objective prerequisites for the appearance of technical channels of information leakage, which necessitates the implementation of measures to create complexes (systems) of technical information protection aimed at preventing leakage of information through these channels.

The active development of international cooperation with foreign countries in the political, military, economic and other spheres leads to the wide opening of foreign diplomatic institutions and representative offices, foreign commercial institutions located in the immediate vicinity of state bodies and institutions creates prerequisites for the acquisition by technical means of intelligence of information with limited access, which circulates on the objects of information activity, which is especially relevant due

to the wide use of unprotected imported technical means of information processing.

All these factors significantly increase the vulnerability of information and, as a result, determine the need to take appropriate measures on the part of the state. At the same time, the importance of the negative consequences of information threats, primarily with limited access, for national security determine the national importance of measures to prevent such threats, and also determine the need to transition from a fragmented departmental approach to the formation and implementation of measures to ensure technical information protection to a systematic and comprehensive approach, attracting the necessary personnel potential, accumulating the necessary In order to counter the mentioned threats, a system of technical information protection has been created, is functioning and is developing in the state, which is a set of organizational structures combined with the goals and objectives of information protection, regulatory, legal and material and technical base.

In accordance with the Concept of Technical Information Protection in Ukraine, technical information protection is defined as an integral part of ensuring the national security of Ukraine.

The goal of state policy in the field of technical information protection is to create legal, organizational, and economic foundations for the functioning of the technical information protection system.

State policy in the field of technical protection of information is determined by the priority of national interests, aims to prevent the realization of threats to information and is carried out in the directions of regulatory and legal and organizational support, scientific and technical and industrial activities. The importance for the security of the state of the field of technical protection of information, its scientific capacity requires the concentration of efforts of the scientific and technical and production potential of ministries, other central bodies of executive power, and the Academy of Sciences [5].

In accordance with this, the main principles and conceptual foundations of the organization of technical information protection in Ukraine have been determined. These include:

– maintaining the balance of the interests of the individual, society and the state, their mutual responsibility;

– the unity of approaches to ensuring technical protection of information, which are determined by threats to information security and the mode of access to it;

– complexity, completeness and continuity of technical information protection measures;

– harmonization of normative legal acts and regulatory documents on technical information protection with relevant international treaties of Ukraine and international standards;

– mandatory protection by engineering and technical measures of information that is a state and other secret provided by law, confidential information that is the property of the state, open information that is important for the state, regardless of where the specified information circulates, as well as open information that is important for the individual and society, if this information circulates in state authorities, other state bodies and local self-government bodies, in auxiliary bodies and services of the President of Ukraine, the National Academy of Sciences, the Armed Forces, other military formations, internal affairs bodies, in state enterprises, in state institutions and organizations;

– compliance by subjects of information relations at their own discretion with regard to the technical protection of information that is their property and open information important for the individual and society, if the latter circulates outside the boundaries of state organizations;

– assigning responsibility for the formation and implementation of state policy in the field of technical information protection to a specially authorized central body of the executive power;

– the hierarchical structure of the organizational structure of the technical information protection system, the subjects of which belong to the sphere of management or are subordinate to the relevant state organization, and the management of the activities of these subjects within the limits of the powers granted by regulatory and legal acts;

– methodical management of the activities of the organizational structures of the technical information protection system by the specially authorized central body of the executive power in the field of technical information protection;

– financial security of the technical information protection system at the expense of the state budget, local budgets and other sources.

The organizational structure of the technical information protection system has a hierarchical tree-like structure with vertical subordination and accountability from the bottom up and the independence of subjects of the same level of the hierarchy.

The functions of the authorized state body in the field of technical information protection are performed by the State Special Communications Service.

At the departmental level, measures to ensure technical information protection are carried out directly by the subjects of the technical information protection system – ministries and other state authorities and enterprises and institutions subordinate to them, and the responsibility for the organization and state of information protection rests with their managers. They should create or define units for assessing the state of threats to information, developing and implementing plans for measures to protect it, coordinating the activities of other subjects in the field of subordination, making calculations and justifying the funds required for this.

Today, the legal basis for the functioning of all elements of the organizational structure of the technical information protection system, the tasks and functions of the subjects of technical information protection, their rights and obligations, the order of their interaction and the implementation of their activities, are fully determined by the regulatory legal acts, as well as the procedure for the functioning of such basic elements as the system of product licensing and evaluation, training and retraining of personnel.

One of the important areas of activity in the field of technical intelligence is the organization of countermeasures against technical intelligence. The organization of countermeasures, timely development and implementation of the necessary measures is entrusted to the head of the state authority, the local self-government body, the management body of the Armed Forces of Ukraine and other military formations formed in accordance with the legislation of Ukraine (hereinafter – the body), enterprises, institutions, organizations (hereinafter – the organization). The implementation of countermeasures is entrusted to a full-time or freelance technical information protection unit or an appointed person created or determined by order of the head of the body (organization).

Countering technical intelligence (CTI) is an integral part of the systems of protection of state secrets and protection of information with limited access,

which is the property of the state (organization of protection of information with limited access) and is carried out by implementing measures to prevent violations of the confidentiality of the organization of protection of information with limited access means of technical intelligence. The set of implemented organizational and engineering-technical measures, software and technical means, which are used to ensure countermeasures, are an integral part of the complex of technical information protection, aimed at hiding the protection of information with limited access and misinforming technical intelligence.

It should be noted that the modern system of combating technical intelligence was built on the foundation laid even under the Soviet Union. At the time of Ukraine's independence, the state had a system of countering foreign technical intelligence (SCFTI), the organizational structure of which was based on full-time units of the SCFTI of bodies and organizations.

With Ukraine's declaration of independence, the system of combating foreign technical intelligence was transformed into a system of technical information protection, and in most state bodies and organizations whose activities are related to the protection of restricted access information, technical information protection units were created on the basis of units of the system of countermeasures against foreign technical intelligence, which were entrusted with the solution of countermeasures and whose activities must be coordinated with the activities of regime-secret agencies. At the same time, the process of developing domestic regulatory documents on the technical protection of information and the creation of means of information protection and protected technical means began. The accumulated experience in countermeasures was not lost – the normative documents of the system of countermeasures against foreign technical intelligence were carefully revised and some of them were given effect (mainly it concerns norms and methods).

Thus, today the organizational structure of countering technical intelligence (SCTI) is an integral part of the infrastructure of technical protection of information (TPI), and its activities are coordinated with it.

Licensing of activities in the field of technical information protection

One of the essential levers of activity regulation in the field of technical information protection is the licensing procedure of business entities.

The mechanism of licensing activities in the field of technical information protection has been implemented in Ukraine since 1995.

The purpose of the licensing procedure is the formation of a controlled market for services with technical protection of information in Ukraine, the fulfillment of the requirements of regulatory documents on information protection, the distribution of systems and means of technical protection of information that comply with the legislation of Ukraine, as well as the exclusion of:

– prerequisites for the possibility of using the means of technical protection of information in illegal and criminal actions, as a result of their uncontrolled circulation in the country;

– the possibility of compromising information with limited access due to the provision of unqualified services and the use of low-quality technical means of information protection, which can lead to real threats to the safety of the individual, society and the state;

– distribution of means of technical protection of information that do not meet the requirements of regulatory documents or means of low quality, in particular means of foreign production, which can lead to the destruction of the domestic industry of development and production of reliable, competitive means of technical protection of information.

Thus, in addition to the directly regulatory and control functions, licensing activity is also aimed at the development of the material and technical base of the technical information protection system.

A total of 7 types of work are subject to licensing in the field of technical information protection, namely:

– development, implementation, effectiveness research, maintenance at the objects of information activity of complexes (systems) of technical protection of information, the consequences of which are acoustic fields, provision of advisory services;

– development, implementation, effectiveness research, maintenance at the objects of information activity of complexes (systems) of technical protection of information, carriers of which are electromagnetic fields and electric signals, provision of advisory services;

– development, production, implementation, effectiveness research, support of means and complexes of technical protection of information in information systems, information technologies with protection of information from unauthorized access, provision of consulting services;

– detection and blocking of the leakage of language and species information through embedded devices at the objects of information activity, provision of advisory services;

– production of means of ensuring technical protection of information, the carriers of which are acoustic fields;

– production of means of ensuring technical protection of information, the carriers of which are chemical substances, provision of advisory services;

– development, implementation, effectiveness research, maintenance at the objects of information activity of complexes (systems) of technical protection of information, the carriers of which are chemical substances, provision of advisory services.

Certification of means of technical protection of information

The object of certification in the field of technical protection of information is separate means of technical protection of information, which can be produced both serially and single samples, including means of imported production may be subject to certification. The procedure is intended to provide the consumer with means of imported production. The procedure is intended to provide the consumer with technical means of information protection with guarantees of conformity of these means with the regulatory document. Such a guarantee can be provided after carrying out certain organizational and technical measures. The result of the certification works is a special document of the established model – a certificate of conformity.

The creation of a system of certification of means of technical protection of information in Ukraine was started back in the mid-90s, and the difficulty was that previously neither in the Soviet Union nor in Ukraine was certification of means of technical protection of information, moreover, at that time there was a lack of the necessary to achieve this goal of the regulatory and legal and material and technical base.

The procedure and requirements for the certification of technical means of information are determined by the Procedure for conducting work on the certification of means of ensuring the technical protection of general purpose information, which is mandatory for both the bodies accredited in the system for the certification of technical means of information and

testing laboratories, as well as for enterprises, institutions and organizations, including foreign ones, which manufacture and (or) supply means of technical protection of information to state and non-state institutions, where information subject to protection in accordance with the law circulates.

State expertise in the field of technical information protection

The introduction of the procedure for expert assessment of complex information protection systems in information and communication systems (ICS), technical and software and hardware means of information protection is due to the logical complexity of modern software and hardware complexes, as well as the significant impact on information security of specific conditions of operation of information and communication systems, in other words, such objects do not repeat each other and each of them has its own unique personality. In cases of assessment of software and hardware of foreign production, as a rule, there is no technical documentation necessary for their certification, it is practically impossible to assess production conditions, organization of interaction of certification bodies with foreign manufacturers of protective equipment.

The legal basis of this procedure is the Law of Ukraine "On Scientific and Scientific-Technical Expertise". The methodological basis is the examination of technical solutions and organizational measures. which are based both on the generalization of the conclusions of individual experts and on the results of instrumental measurements and tests of a complex of software, hardware and technical means of information protection [28].

The procedure for conducting a state examination in the field of technical information protection, the main functions and rights of subjects of the examination are determined by the Regulations on State Examination in the Field of Technical Information Protection.

In accordance with the legislation, it defines the subjects of the examination (the Customer, the Organizer of the examination, the expert), the main functions of the State Service of Special Communication and Information Protection of the Security Service of Ukraine and the subjects of the examination, the procedure for their interaction, the procedure for the preparation of the documentary result of the examination and Issuance of an expert opinion (for individual means of information protection) and

a certificate of conformity for complex information protection systems in information and communication systems.

The presence of a positive decision regarding the tool is the basis for its inclusion in the List of technical information protection tools of general purpose, which are allowed to be used for the purpose of technical protection of information, and the presence of a certificate of conformity is the basis for obtaining a permit for processing in information and communication systems information subject to protection.

The state examination system has been operating since the beginning of 2000 and during this time has become one of the most important factors in the implementation of state policy in the field, and its results are the development of the material and technical base of the technical information protection system and the filling of the market with effective competitive software and hardware means of information protection.

To date, 44 organizations have been registered and authorized to conduct expert tests, and about 265 highly qualified specialists in the field of technical information protection have been entered into the Register of Experts.

In total, an examination was carried out and 98 expert opinions were issued on individual means of information protection and 467 certificates of conformity on a comprehensive system of information protection in information and communication systems.

6. Conclusions

The introduction of electronic document management in state authorities, in particular in local self-government bodies, is extremely important, because it allows to increase the effectiveness of the functioning of all elements of state administration.

The issue of intensifying the implementation and development of electronic governance in all spheres of social life, one of the important components of which is electronic document flow, has been put on the agenda in Ukraine. In addition, new legal objects have appeared in the legislation – an electronic document and an electronic digital signature, new forms of relations based on electronic document circulation are developing [14].

According to Article 1 of the Law of Ukraine "On Information" [27], a document is a physical medium containing information, the main functions of which are its preservation and transmission in time and space.

The need to use electronic documents and use the opportunities provided by electronic document circulation for various public needs was on the agenda in Ukraine as early as the second half of the 90s of the last 20th century. This was also motivated by the positive social experience of developed countries in this area. But at that time, not only in Ukrainian society as a whole, but even in the state authorities, there was not yet an available material and technical base and sufficient awareness of the volume and complexity of the tasks that must be solved in order to achieve the specified goal.

For the introduction of electronic document circulation, the authorities faced, first of all, the task of creating a regulatory and legal framework that ensures its implementation through the proper organization of relevant processes and compliance with the requirements for document preparation, unification of organizational and administrative documentation systems, development of a single state system of record keeping, a single state system of documentation support for management, etc.

For this purpose, two basic laws of Ukraine were adopted: "On electronic digital signature" [25] and "On electronic documents and electronic document management" [24]. At the same time, it should be noted that the provisions of the first of these laws meet the requirements of Directive 1999/93/EC of the European Parliament and the Council of Europe dated December 13, 1999 "On the system of electronic signatures applied within the Community" [30].

Approved by the Resolution of the Cabinet of Ministers of Ukraine "Standard procedure for the implementation of electronic document circulation in executive authorities" [36] establishes general rules for documenting administrative activities in the authorities in electronic form and regulates the execution of actions with electronic documents from the moment of their creation or receipt until they are sent or transferred to the appropriate archive.

The executive authority carries out electronic document management (EDM) only under the condition of using reliable means of electronic digital signature (EDS), which must be confirmed by a certificate of compliance or a positive conclusion based on the results of state expertise in the field of cryptographic information protection, received for these means from the Administration of State Special Communications and presence of a

strengthened public key certificate (PSPKC) of its employees – signatories. At the same time, EDM is carried out by a government body through special communication networks or public communication networks, and the sending of electronic documents through public communication networks is carried out by the decision of the head of this body.

According to the legislation of the electronic document circulation system (EDCS) of the executive authority, it must meet the requirements of regulatory acts in the field of information protection, in particular the provisions of the Law of Ukraine "On the Protection of Information in Information and Communication Systems" [26] and Resolution of the Cabinet of Ministers of Ukraine "On approval of the Rules for ensuring the protection of information in information, communication and information and communication systems" [38].

According to the Rules, to ensure the protection of information in the information system, an information protection system (IPS) is created, which is intended for information protection.

It should also be noted that the issue of creating an electronic document management system (EDM) is relevant for many countries, including members of the European Union. In particular, within the IDA program of the European Commission, Cornwell Management Consultants plc (formerly Cornwell Affiliates plc) developed the MoReq (Model Requirements) Specification "Typical Requirements for Automated Electronic Document Management Systems" [57].

Information security plays an important role in ensuring the interests of any state. Recently, there have been qualitative changes in management processes in the world, due to the intensive implementation of modern information technologies. At the same time, the danger of unauthorized interference in the operation of information systems increases, and the severity of the consequences of such interference has greatly increased.

The need to ensure information security is determined by many factors: the need to ensure the national security of Ukraine as a whole; the existence of threats to the information sphere of the country, which can cause significant damage to the general national interests; the possibility of influencing people's consciousness and behavior with the help of information. The main strategic task of Ukraine's information security is the creation of a powerful national information space, as the main aspect

of the state's presence in the world information space. In addition, this task includes the creation of a system for countering information threats and the protection of the state's own information space, information infrastructure, and information resources.

In general, the tasks of ensuring information security of the state are considered to be: identification, assessment and prediction of the behavior of sources of threats to information security, which is carried out through operational monitoring of the information situation; development, coordination and introduction of a unified state policy in the field of information security; creation and operation of information security systems; development, coordination and implementation of a unified state policy in the field of information relations, in particular in the direction of forming the image of the state [49].

Despite a number of problems of the information security of the state, it is possible to assert that the provision of information security relies on the information organization of the state. This organization must guarantee the information security of the state and its subjects, including during a full-scale invasion of the Russian Federation into the territory of our state. Unfortunately, there are many negative factors in Ukraine that prevent or make it difficult to create such an information organization, not the least of which is the inconsistency of state authorities in ensuring information security. Therefore, the scientific understanding of the complex of problems related to the development and implementation of state policy in the information sphere is of particular importance today, since their solution will contribute to the development of the information society in Ukraine and, thus, to ensuring the national and information security of our state.

References:

1. White book of State Special Communications. Technical protection of information. Available at: https://www.dstszi.gov.ua/control/uk/publish/article?art_id=49942&cat_id=49941 (application date: April 22, 2024).

2. Boyko A. I. The philosophy of modernization of education in the system of market transformations : worldview and philosophical analysis : abstract of a dissertation for obtaining the scientific degree of Doctor of Philosophical Sciences, 2010. 31 p.

3. Havrylenko O.V. Technical channels of information leakage. Procedure for creating complexes of technical protection of information : training manual. Kyiv : KPI, 2016. 104 p.

4. Grechko A.V. Basics of electronic document flow: a study guide. Kyiv : KNEU, 2006. 156 p.

5. Hulak H.M. Information protection methodology. Aspects of cyber security : a study guide. Kyiv : National Academy of the Security Service of Ukraine, 2020. 256 p.

6. Durnyak B.V., Sabat V.I. Semantic protection of information in document management systems. Information technologies : monograph. Lviv : Ukrainian Academy of Printing, 2010. 160 p.

7. State Standard of Ukraine 4145:2002. Information technologies. Cryptographic protection of information. A digital signature based on elliptic curves. Formation and verification. [Effective from 2003-07-01]. The publication is official. Kyiv, 2003. 36 p. (Information and documentation).

8. State Standard of Ukraine 34.601-90 Information technology. Complex of standards for automated systems. Automated systems. Stages of creation. [Effective from 1992-01-01]. The publication is official. Kyiv, 1990. 5 p. (Information and documentation).

9. Zima I.I., Nikolaev I.M. Information war and information security (review of the opinions of foreign political scientists and military specialists). Science and defense. Kyiv, 1998. N 1. P. 56-58.

10. Kovalchuk N. V. Trends and prospects for the development of documentation support for library management : dissertation. Available at: http://www.nbuv.gov.ua/sites/default/files/disser/dis_31.pdf (application date: June 7, 2024).

11. Electronic document management in state administration : a study guide / Klymenko I.V., Lin'ov K.O., Horbenko I.D., Onoprienko V.V. Kyiv : National Academy of Public Administration, 2009. 232 p.

12. Klymenko I.V., Lynov K.O. The system of electronic document circulation in the state administration : educational and methodological manual. Kyiv : National Academy of State Administration, 2006. 32 p.

13. Krukovsky M.Yu. Electronic document management solution : Kyiv : "Azimut-Ukraine", 2006. 112 p.

14. Kuzmenko B.V. Organizational-legal and software-technical means of ensuring information security : training manual. Kyiv : National Academy of Management, 2008. 164 p.

15. Kukarin O.B. Electronic document management and information protection : a study guide. Kyiv : National Academy of Public Administration, 2015. 85 p.

16. Loza O. V. Bookkeeping and documentation of managerial activities : a study guide. Kyiv : UAAU, 1997. 67 p.

17. Marchuk O.V. Protection of information. Encyclopedia of public administration : study guide. Kyiv : National Academy of Public Administration, 2011. 170-172 p.

18. Matvienko O.V. Basics of organization of electronic document flow : a study guide. Kharkiv : Center for Educational Literature, 2008. 111 p.

19. Normative document on technical information protection 1.1-002-99 General provisions on protection of information in computer systems against unauthorized access : order of the State Service for Special Communications and

Information Protection of the Security Service of Ukraine dated December 28, 1999 (Amendment N 1). order of the State Special Communications of Ukraine dated December 28, 2012 N 806), 1999. 26 p.

20. Normative document on technical information protection 1.1-003-99 Terminology in the field of information protection in computer systems against unauthorized access : order of the State Service of Special Communications and Information Protection of the Security Service of Ukraine dated April 28, 1999. N 22, 1999. 26 p.

21. Nesterenko O.V. The principles of ensuring the necessary level of security information of state authorities. Available at: https://www.nbuv.gov.ua/portal/soc_gum/nac_bez/2009_4/pdf/nesterenko.pdf.

22. Pocheptsov H.G. Semantic and information wars. Information society. Kyiv, 2013. Issue 18. P. 21–27.

23. On state secrets : Law of Ukraine dated January 21, 1994 N 3855-XI. *Information of the Verkhovna Rada of Ukraine*. 2008, N 27-28, Art. 252.

24. On electronic documents and electronic document circulation : Law of Ukraine dated May 22, 2003 N 851-IV. *Voice of Ukraine*. 2003. N 119.

25. On electronic digital signature : Law of Ukraine dated May 22, 2003 N 852-IV. *Voice of Ukraine*. 2003. N 119.

26. On the protection of information in information and communication systems : Law of Ukraine dated May 07, 1994 N 80/94-VR. *Voice of Ukraine*. 2005. N 116.

27. On information : Law of Ukraine dated October, 02, 1992 N 2657-XI. *Information of the Verkhovna Rada of Ukraine.* 1992. N 48, Art. 650.

28. On scientific and scientific and technical expertise : Law of Ukraine dated February 10, 1995 N 52/95-VR. *Information of the Verkhovna Rada of Ukraine*. 1995. N 9 of Art. 56.

29. On the approval of the Exemplary instructions for record keeping in ministries, other central bodies of executive power, the Council of Ministers of the Autonomous Republic of Crimea, local bodies of executive power : Resolution of the Cabinet of Ministers of Ukraine dated October 17, 1997 N 1153. *Official Gazette of Ukraine*. 1997. N 43, Art. 50.

30. On the system of electronic signatures used within the Community : Directive 1999/93/EC of the European Parliament and the Council of 12/13/1999 (DIRECTIVE 1999/93EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures). *Official Journal* L013, 19/01/2000, 0012 – 0020.

31. On the approval of the Procedure for the use of computer programs in the bodies of executive power : Resolution of the Cabinet of Ministers of Ukraine dated September 10, 2003 N 1433. *Official Gazette of Ukraine*. 2003. N 37, Art. 1989.

32. On the approval of the Procedure for certifying the existence of an electronic document (electronic data) at a certain point in time : Resolution of the Cabinet of Ministers of Ukraine dated May 26, 2004 N 680. *Official Gazette of Ukraine.* 2004. N 21 of Art. 1428.

33. On approval of the Procedure for accreditation of the key certification center : Resolution of the Cabinet of Ministers of Ukraine dated July 13, 2004 N 903. *Government courier*. 2004. September 15. (N 173).

34. On the approval of the Regulation on the central certifying body : Resolution of the Cabinet of Ministers of Ukraine dated October 28, 2004 N 1451. *Government Courier*. 2004. (N 214).

35. On approval of the Procedure for the use of electronic digital signatures by state authorities, local self-government bodies, enterprises, institutions and state-owned organizations : Resolution of the Cabinet of Ministers of Ukraine dated October 28, 2004 N 1452. *Government courier*. 2004. (N 214).

36. On the approval of the Standard procedure for the implementation of electronic document circulation in the bodies of executive power : Resolution of the Cabinet of Ministers of Ukraine dated October 28, 2004 N 1453. *Official Gazette of Ukraine.* 2004. N 44, Art. 2895.

37. On approval of the Procedure for mandatory transfer of documented information : Resolution of the Cabinet of Ministers of Ukraine dated October 28, 2004 N 1454. *Official Gazette of Ukraine*. 2004. N 44, Art. 2896.

38. On the approval of the Rules for ensuring the protection of information in information, communication and information-communication systems : Resolution of the Cabinet of Ministers of Ukraine dated March 29, 2006 N 373. *Government Courier*. 2006. (N 73-74).

39. On the approval of general requirements for software products that are purchased or created on the order of state bodies : Resolution of the Cabinet of Ministers of Ukraine dated August 12, 2009 N 869. Available at: https://ips.ligazakon.net/document/KP090869 (application date: April 25, 2024).

40. On the approval of regulatory acts on the functioning of electronic digital signatures in the banking system of Ukraine : Resolution of the National Bank of Ukraine dated June 17, 2010 N 284. Available at: https://ips.ligazakon.net/document/view/re18329?an=16 (application date: April 25, 2024).

41. On the approval of the Concept of creating a multifunctional complex system "Electronic Customs" : Order of the Cabinet of Ministers of Ukraine dated September 17, 2008 N 1236. *Official Gazette of Ukraine*. 2009. N 93.

42. On approval of the creation of the Certification Center of the National Bank of Ukraine : Decree of the Cabinet of Ministers of Ukraine dated June 05, 2009 N 483. Available at: https://zakon.rada.gov.ua/laws/show/483-2009-%D1%80#Text (application date: April 28, 2024).

43. On the approval of the Regulation on the procedure for state control over compliance with the requirements of legislation in the field of electronic digital signature services : order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated July 24, 2007 N 143. Available at: https://zakon.rada.gov.ua/laws/show/z0914-07#Text (application date: April 25, 2024).

44. On making changes to some normative legal acts : order of the Ministry of Infrastructure of Ukraine dated August 06, 2011 N 138 (registered in the Ministry

of Justice of Ukraine dated June 24, 2011 under N 763/19501). *Official Gazette of Ukraine.* 2000. N 18 of Art. 733.

45. On the use of hardware carriers of key information of cryptographic information protection systems : Letter of the National Bank of Ukraine dated December 10, 2010 N 24-112/2550-22346. Available at: https://zakon.rada.gov.ua/laws/show/v2550500-10#Text (application date: April 22, 2024).

46. On the approval of the plan of measures for the introduction of electronic document flow related to the transportation of goods by railway transport : order of the Cabinet of Ministers of Ukraine dated December 16, 2009 N 1557. Available at: https://zakon.rada.gov.ua/laws/show/z0478-11#Text (application date: April 25, 2024).

47. On the approval of the Concept of the development of e-government in Ukraine : Decree of the Cabinet of Ministers of Ukraine dated December 13, 2010 N 2250. Available at: https://zakon.rada.gov.ua/laws/show/2250-2010-%D1%80#-Text (application date: April 25, 2024).

48. The issue of implementation of the system of electronic interaction of executive authorities : Decree of the Cabinet of Ministers of Ukraine dated December 28, 2011 N 1363-d. Available at: https://zakon.rada.gov.ua/laws/show/2250-2010-%D1%80#Text (application date: April 25, 2024).

49. On the decision of the National Security and Defense Council "On Information Security Strategy" : Decree of the President of Ukraine dated October 15, 2021 N 685/2021. *Official online representation of the President of Ukraine*. 2021. Available at: https://www.president.gov.ua/documents/6852021-41069 (application date: April 25, 2024).

50. On the approval of the Rules of enhanced certification : order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine: dated January 13, 2005 N 3. *Official Gazette of Ukraine*. 2005. N 5.

51. On approval of the Procedure for storing electronic documents in archival institutions : Order of the State Archives Committee of Ukraine dated April 25, 2005 N 49. *Official Gazette of Ukraine*. 2005. N 23 of Art. 1324.

52. On the approval of the Technical Specifications of the presentation formats of the basic objects of the national electronic digital signature system : order of the State Committee of Ukraine on Science, Innovation and Informatization and the Administration of the State Service of Special Communications and Information Protection of Ukraine dated August 13, 2010 N 8/229. *Official Gazette of Ukraine*. 2011. N 42, Art. 1735.

53. On the approval of the Technical Conditions for the electronic document management system of the executive authority : order of the State Department for Communications and Informatization of the Ministry of Transport and Communications of Ukraine dated July 06, 2005 N 70. Available at: https://ips.ligazakon.net/document/FIN14540 (Technical conditions of Ukraine 30.0-33240054-001:2005).

54. Register of entities – certification centers and accredited key certification centers. Available at: https://www.gov.ua/index.php?page=reestr (application date: April 22, 2024).

55. On requirements for data formats of electronic document circulation in state authorities. Email format : order of the Ministry of Education and Science, Youth and Sports of Ukraine dated October 20, 2011 N 1207. Available at: https://zakon.rada.gov.ua/laws/show/z1306-11#Text (application date: April 25, 2024).

56. Technical specifications of cryptographic message formats. Protected data : Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated May 14, 2010 N 112. Available at: https://zakononline.com.ua/documents/show/106441___106441 (application date: April 25, 2024).

57. Standard requirements for automated electronic document management systems: MoReq specification. Available at: https://visnyk.kh.ua/web/uploads/pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D0%A2%D0%BE%D0%BC%2029(2)_2022-15-34.pdf (application date: April 22, 2024).