INTRODUCTION OF NEW APPROACHES TO INFORMATION SECURITY IN PUBLIC GOVERNANCE

Volodymyr Marchenko[1], Alla Dombrovska[2]

[1]Doctor of Science (Law), professor, H.S. Skovoroda Kharkiv National Pedagogical University, Kharkiv, Ukraine, e-mail: marchenko2210@gmail.com, ORCID: https://orcid.org/0000-0003-1921-3041

[2]Ph.D. (Law), Associate Professor, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine, e-mail: dombrovskalla@gmail.com, ORCID: https://orcid.org/0000-0003-4610-8220

The issue of ensuring the transfer and long-term storage of electronic documents in state archives, museums, libraries, maintaining them in an up-to-date state and providing access to them is identified as one of the main tasks of the Concept of e-government development in Ukraine [1]. However, the draft Green Paper on e-Government in Ukraine [2] draws attention to the regulatory uncertainty of electronic information storage (archiving) processes, storage processes of documents that were received from the customer, and proving legitimacy of these documents over a period of time, which ultimately significantly constrains the implementation of electronic services, and, accordingly, the need to develop procedures for the transfer and long-term storage of electronic resources.

The focus on informatization of society, the rapid spread of information and communication technologies and a significant increase in their number of users, the introduction of e-government, the transition to electronic document management and the use of electronic digital signatures include the accumulation of significant electronic resources and electronic documents. The solution to this problem is closely related to the use of the cutting-edge electronic information and communication technologies, such as blockchain.

Issues of information security, the introduction of digital technologies in the field of public administration have become the object of scientific research of many foreign and domestic scientists, including: M. Atzori [3], D. and A. Tapscott [4], M. Swan [5], M. Walport [6], O. Danilchenko[7], O. Karpenko [8], V.Marchenko [9], D. Timofeev [10], and others.

However, despite the significant achievements in this area, the problems of information security in electronic document management remain unresolved, which determines the relevance of their further study.

The development of the global information society, wide use of information and communication technologies in all spheres of life has raised the problem of the information security. Ukraine aspires to be a full member of the European Union, which makes it necessary to follow European principles, norms and standards in the field of information security as well. It is important to note the regulations that set out

a number of requirements that directly affect the harmonization of legislation of the Member States of the European Union:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [11];
- Directive 98/34/EC Of the European Parliament and of the Council of 22 June 1998 on the laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services [12];
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [13];
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [14];
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.108. [15], etc.

In Ukraine, the main directions of solving the problem of information security at the legislative level are the creation of a fully functional information infrastructure of the state and ensuring the protection of its critical elements; increasing the level of coordination of the activities of state bodies in identifying, assessing and forecasting threats to information security, preventing such threats and ensuring the elimination of their consequences, the implementation of international cooperation on these issues; improving the regulatory framework for information security, including the protection of information resources, combating computer crime, protection of personal data, as well as law enforcement activities in the information sphere; deployment and development of the National Confidential Communication System as a modern secure transport base capable of integrating geographically distributed information systems in which confidential information is processed [16].

In fact, information security can be defined as the ability to neutralize the harmful effects of various types of social information. Security is the absence of a threat or the ability to reliably protect against it. As it was rightly stated by D. Dubov, the protection of information in the system is an activity aimed at preventing unauthorized actions on information in the system [17, p.120]. Such dangerous informational influence should be considered destabilizing and oppressessing the interests of the individual, society, state.

Based on the above, we propose to comprehensively consider the concept of information security in electronic document management as a system consisting of the following interrelated elements:

1) the state of absence of information risks (damage or damage due to inaccuracy, incompleteness, untimeliness of information, unauthorized use of information technology and access to state electronic resources, violation of integrity, confidentiality and availability of electronic information, espionage and cybercrime on the Internet, etc.) or reliable from their influence on the rights and interests of citizens and legal entities, society and the state as a whole;

2) the key direction of public policy and the function of public administration;

3) a mechanism of protection of the information space of e-government and direct information during electronic document management in the executive branch, which includes a set of principles, methods, means of secure provision, receipt, transmission, use and storage of information and its protection;

4) a set of administrative-legal, technical-technological, personnel, financial, methodological and other types of protection of the electronic document management system of executive authorities and directly important and significant information.

The main threats to information security in the information sphere are:

1) theft of information that is a secret and protected by law;

2) destruction of information and software that provide data processing or operation of hardware and systems;

3) illegal "interception" of information;

4) modification of information and software;

5) illegal use of information and software;

6) malfunction or failure of computers and networks;

7) concealment (non-notification) of information that affects the interests of a person, citizen, society;

8) collection, accumulation and use of personal data and other actions that violate the basic rights of man and citizen [17, p.122].

In our opinion, the main problem of the electronic document management in executive bodies, by which the legislator understands the set of processes of creation, processing, sending, transmission, receipt, storage, use and destruction of electronic documents, which are performed using integrity checks and, if necessary, with confirmation of receipt such documents, according to Article 9 of the Law of Ukraine "On electronic documents and electronic document management"[18] is to verify the integrity of the electronic document (Article 12 of the Law), which can be done by checking the electronic digital signature, which is also used to identify the author of the electronic document.

However, as rightly stated by I. Kusplyak and A. Serenok, the assessment of the electronic document management system is not an easy task, as in Ukrainian legislation there are many conflicts around the introduction and use of electronic document management in the activities of the authorities [19].

We agree with D. Timofeev who notes that electronic document management systems primarily face the task of ensuring the integrity, accessibility and confidentiality of information, but due to the fact that these systems have become widely used relatively recently, despite all the benefits of their use [10]. Thus, when conducting electronic document management, the question of authenticity immediately arises, because all electronic document management systems have some built-in security features, generally based on the delimitation of access rights depending on the role played by the system user. But this will not be able to prevent the threat of unauthorized use of confidential information by an authorized user, so electronic document management systems should be one of the elements of the information structure, which should be protected not separately but as part of a single information security policy infrastructure.

In this regard O. Garasim, M. Komova and V. Lytvyn argues that the creation of a comprehensive system of information security should be aimed at technological support: protection against leakage of confidential information; protection against viruses and spam; vulnerability analysis; detection and prevention of interventions; firewall; delimitation of access; cryptographic protection; information security monitoring [20].

The Law of Ukraine "On Electronic Documents and Electronic Document Circulation" of May 22, 2003 № 851-IV [18] defined a number of procedures and established requirements for the storage of electronic documents - documents in which information is recorded in the form of electronic data, including mandatory details of the document, and which can be created, transmitted, stored and converted electronically into a visual form.

In particular, Article 13 of the Law establishes the following requirements for the storage of electronic documents and archives of electronic documents:

1) the authoroties of electronic document management must store electronic documents on electronic media in a form that allows to verify their integrity on these media;

2) the term of storage of electronic documents on electronic media must be not less than the term established by law for the relevant documents on paper. If it is impossible to store electronic documents on electronic media during this period, the subjects of electronic document management should take measures to duplicate documents on several electronic media and periodically copy them in accordance with the accounting and copying of documents established by law. If this is not possible, electronic documents should be kept as a copy of the document on paper (in the absence of the original of this document on paper).

When copying an electronic document from an electronic media, it is necessary to check the integrity of the data on this media;

3) the information contained in electronic documents must be available for further use;

4) it must be possible to restore the electronic document in the format in which it was created, sent or received;

5) if available, information must be stored that allows to establish the origin and purpose of the electronic document, as well as the date and time of its sending or receiving;

6) the authoroties of electronic document management may ensure compliance with the requirements for the preservation of electronic documents through the use of the services of an intermediary, including the archival institution, if such institution complies with the requirements of this article. Creation of archives of electronic documents, submission of electronic documents to archival institutions of Ukraine and their storage in these institutions is carried out in the manner prescribed by law [18].

To effectively manage the documentation processes in the database of the institution it is necessary to store information about all documents of the institution with any media. The incoming electronic document is sent to the institution in the form of an XML document, which contains the files of electronic documents that make up the incoming electronic document, the details of the electronic document and its metadata. In this case, the information support service organizes the storage of electronic documents in the mode of access "read-only" to ensure their consistency over time.

It should be noted that electronic documents from the time of creation (receipt) and before transfer for permanent storage to the state archival institution, the archival department of the city council or destruction are stored in the archival system of the institution. In order to ensure the safety of electronic documents, the office of the institution determines the access rights of employees to draft electronic documents, the right to create details of electronic documents that arise during the passage and storage of electronic documents, and information about electronic documents during these processes. In particular, the right to create a document is granted only to heads of departments and persons responsible for the organization of office work, to create new details and information about electronic documents after their transfer to the archive - only employees of the archives, temporary access to electronic documents - employees of other departments institutions with the permission of the head of the structural unit, which is responsible for the operational storage of these electronic documents, temporary access rights to electronic documents - third-party institutions (persons) with the permission of the head of the institution. At the same time, the access rights of employees of other structural subdivisions of the institution and third-

party institutions are limited only by the possibility to get acquainted with the content of documents [21].

It is also important to note that for electronic documents of permanent and long-term (more than 10 years) storage, paper copies of such electronic documents are created immediately after their completion. In addition, the legislation provides for the examination of the value of electronic documents on the same principles, criteria and in the manner prescribed by law as the examination of the value of documents with paper media. Elimination of the revealed shortcomings by results of check of electronic documents is carried out by the persons responsible for the organization of office work in structural division of establishment.

Investigating the issue of storage of electronic documents in the executive authorities, it should be noted that electronic documents of institutions transferred by state archives; electronic information resources; electronic documents and information resources of personal origin, transferred by state archives and owners of such documents; official publications in electronic form, which do not come in the prescribed manner to the Book Chamber of Ukraine and libraries - depositories; accounting documents and archival directories are part of the documents of the Central State Electronic Archive of Ukraine. Thus, it is the Central State Electronic Archive that performs the tasks and functions of the state for the management of archival affairs and record keeping, ensures the accounting, preservation of electronic documents of the National Archival Fund and electronic information resources and the use of their information.

As we can see, Ukraine as a whole has all the prerequisites for ensuring an effective process of long-term storage of electronic resources, which is very important for the development of e-government in the executive branch.

However, it is worth agreeing with I. Klymenko regarding the fact that creating a reliable single repository for documents and knowledge, it is necessary to provide a procedure for easy access, inquiries to it for both civil servants and clients of public institutions from anywhere and at any time [22, p.61]. In addition, as the number of electronic documents is growing rapidly every year, there is a problem of preservation of these documents, in particular those created in public authorities, institutions and organizations. The urgency of this problem is due to the need to solve the problem of permanent, long-term (more than 10 years) storage of electronic documents that accumulate so rapidly with the constant improvement of information technology and systems in state enterprises and institutions, as well as simplifying access to them [23, p. .225].

It is interesting to note that the archive storage system must include such subsystems as tape or disk libraries; specialized infrastructure of server access to storage devices; stored data management software; service quality management

system and centralized backup and recovery system. Today, the most common software products that serve archival storage of electronic documents and are the most functional are Qstar HSM from Qstar Technologies (USA) and "Saperion" from the German company Saperion AG (Berlin / Zurich) [23, p.225-238]. The main advantage of these software products is that they are designed with the requirements of archival storage of documents, the disadvantage is the high cost.

Electronic archives are organized depending on the tasks of the archive for data storage and economic opportunities of a particular institution. Most often, data is stored on hard disks, using common software products, storing copies on tapes, optical disks, disks made by UDO technology (Central State Electronic Archive of Ukraine, archival departments of UkrINTEI, National Library of Ukraine named after VI Vernadsky, Kyiv and Crimea laser observatory, Hydrometeorological Center and others).

The innovative breakthrough and progress of society over the last decade in the field of BigData, innovative technologies and public administration are associated with the use of blockchain technologies.

The profile technical committee of the International Organization for Standardization (ISO) TC307 "Blockchain and distributed ledger technologies" considers the following definitions :

Distributed ledger is a register that is stored in a distributed, decentralized manner on a number of network nodes, rather than centrally located in one specific location.

Blockchain - a type of distributed registry technology in which confirmed and verified groups of transactions are stored in blocks connected to each other in the rack against unauthorized interference and allows only the addition of a chain starting with the primary block (genesis block), and in which each block contains a hash of the previous block of the chain [24].

The essence of the blockchain concept is the idea of distributed, decentralized storage of registry entries on a number of network nodes, rather than centrally in one place. Typically, transactions registered in a distributed registry involve several parties, and each party has its own copy of the records of the transactions in which it participates.

One of the main tasks of Distributed Ledger Technology (DLT) is to provide secure, resilient online transactions between parties. Using DLT technology requires a process that ensures the same instances of the transaction record on all nodes where such a record is stored, as well as the consistency of the contents of the record by the parties involved in the transaction. The set of entries in the distributed register must be verified and audited.

According to experts from the International Organization for Standardization (ISO), blockchain technology and distributed systems are becoming an important new direction in the development of information technology, they can be used in many areas to solve a wide range of problems. Based on these technologies, it is possible to create new solutions that will have great potential, especially in cases where transactions between individuals or organizations require reliable and immutable documents, without the involvement of a trusted third party.

Blockchain technology allows to optimally solve the above problems, minimize costs on the part of participants in electronic interaction, opens new opportunities in the creation and management of electronic registers and their promotion in a network economy. Blockchain technology can be implemented to solve information management problems.

In particular, O. Danilchenko believes that blockchain technology can be adapted to carry out any transactions, one way or another related to the registration, accounting or transfer of various assets (financial, tangible and intangible); at the same time, neither the type, nor the number of participants, nor their geographical location matter, which may change the very model of public administration in the future [7].

Areas in which the use of blockchain in the public sphere is possible are:

1. Electronic document management.
2. Public opinion poll.
3. Audit of public procurement.
4. Protection of intellectual property on the basis of smart contracts.
5. Redistribution and exchange of excess energy between network users.
6. Maintaining registers of bank guarantees.
7. Tracking drug supply chains.
8. Maintaining patient registers in the medical field.

A separate case of the use of blockchain technology is the system of public administration. Blockchain technology allows you to maintain decentralized state registers, including registers of ownership of land, real estate, etc., it can be used as a file storage of huge amounts of information, allowing you to effectively manage any assets or information through high transparency.

In April 2017, the State Agency for E-Government of Ukraine and BitFury signed a memorandum of cooperation in the field of blockchain technologies [25]. The project involves the transfer of all government data stored electronically to the blockchain platform. It is planned to transfer state registers, social services, security, health care and energy bodies of Ukraine to the new system. As a result, it will allow the Government of Ukraine to control all changes in state assets, including the results of privatization tenders. According to K. Yarmolenko, Advisor to the Head of the

State Agency for Electronic Government of Ukraine, the Ministry of Justice of Ukraine in 2017 is ready to introduce blockchain technology in the system of sales of confiscated property "SETAM" and in basic registers, as technology prevents fraud in state registers as inside when bribing an administrator or registrar, and externally when cyberattacks take place [26].

The development of blockchain technology gives impetus to new implementations of e-government, especially in the field of information security from falsification. Data on citizens, real estate, certificates, permits, property rights, etc. after entering in the state blockchain registers is almost impossible to change. Data from state registers can be used as full-fledged documents that have legal force and are available to all stakeholders.

However, along with the advantages of blockchain technology, certain disadvantages should be taken into account.

Existing blockchain solutions are optimized to manage "tokens", which are different types of assets, and are not suitable for storing documents, because the documents themselves do not fit into the blockchain (otherwise due to the rapid increase in volume it would be extremely difficult to maintain copies of the register on numerous computers). The blockchain in this case stores only hashes of documents or documented information, i.e. the blockchain solution acts as a trusted timestamp system that operates without the use of traditional public key infrastructure (PKI).

According to the current legislation, in some cases changes should be made to the register: this may be necessary, for example, by a court decision that declared certain agreements invalid. However, the world community of experts is much more concerned about the legislation on personal data protection and privacy, especially in its European version, which provides for the "right to be forgotten" and considers the right to personal data protection as a fundamental, inalienable human right. he cannot refuse.

Information systems rarely exist for more than 10 years. Using a blockchain to store permanent storage information (such as land cadastres) is risky because it is unclear what will happen if the blockchain solution is decommissioned.

A quantum computing revolution is expected in the coming years. Quantum computing is essentially a parallel computing system capable of much faster search for options when solving cryptographic problems. Their emergence may require the replacement of all existing cryptographic algorithms, which will most directly affect the security of existing blockchain solutions and trust in them.

The legal security of a blockchain system can be ensured if its development, implementation, operation and decommissioning are carried out in such a way that

over time, despite changes in legal, technological or social conditions, the following requirements are met:

- documents stored (or managed by) a blockchain system must retain their business or legal value for as long as necessary;
- interaction with courts and regulators (especially in situations where courts will request documents or information or require them to be deleted, modified or blocked) should not have catastrophic consequences for the system (say, by violating the principle of record-keeping);
- it should be possible (technical and legal) to submit certain documents to the court or the regulator (it should be determined who and how will certify them);
- the authenticity, integrity, usability and confidentiality of both the system itself and the documents stored in it should be ensured so that it can be demonstrated to the regulator and the court;
- comply with existing legal and regulatory requirements for storage and protection of personal data;
- it should be clear who is responsible for the proper functioning of the system and who compensates for the losses;
- operators (or the stakeholder community) should monitor legislative and regulatory changes and take appropriate action;
- make efforts to solve the problem of ensuring long-term storage of information in the blockchain.

A key innovation in the use of DLT-systems is a new model of trust, which, unlike traditional systems, does not rely on the authority of the organizer and trust of its participants, nor on the rules of specific jurisdiction and generally does not require the use of trusted third parties. including certification centers and timestamp services. The DLT system itself seeks to become a universal intermediary that organizes direct interaction between the parties to transactions.

A number of states are already using blockchain solutions as an additional tool independent of the state and some specific commercial organizations to ensure the credibility of electronic data and documents.

The important point is that in a blockchain system built on the type of bitcoins, there is neither an official owner and jurisdiction, nor an operator to which claims and claims could be made (which, depending on the circumstances and tasks, can be as good , and bad).

Such uncertainty can be useful where, for example, it is necessary to circumvent barriers to cross-border cooperation related to the sovereignty of states and to limit the ability of individual states to interfere in the management of the system, seize information and impose sanctions. A blockchain solution can be intentionally created as a neutral trusted intermediary "without citizenship". Due to the lack of an official

owner and operator, it is difficult for law enforcement agencies in a particular country to access confidential information belonging to DLT participants.

The fundamental distribution and / or decentralized blockchain solutions make them catastrophic as well as resistant to the influence of certain states.

It follows from the general considerations that solutions based on blockchain and distributed registry technologies can be quite effective as a tool to support initially decentralized and non-centrally controlled activities and processes. Conversely, traditional solutions should be expected to continue to be more effective where activities are centralized or centrally controlled.

Summarizing the above, we conclude that the main problems of information security in electronic document management in the executive branch are the following:

1) imperfection of legal support (lack of information security strategy in electronic document management, lack of unity in policy to address this issue, the powers of which are vested in a number of executive bodies, conflicts in existing regulations on the use of electronic digital signatures, etc.);

2) inefficiency of technical, technological, organizational, personnel, financial, methodological support of the electronic document management system;

3) inefficiency of functioning of the uniform information infrastructure in executive bodies, lack of the adjusted interdepartmental interaction, coordination and control, etc .;

4) the lack of adequate mechanism of protection of information in electronic document management provided by the executive authorities;

5) high level of information risks associated with the vulnerability of the information society from harmful or poor quality information, widespread cases of fraud and industrial espionage in electronic networks and the Internet, cybercrime, unauthorized and illegal influence of outsiders on the process of electronic document management destruction of information, software that ensure data processing or operation of hardware and systems, etc.

Solving these issues will increase the efficiency of electronic document management, which is the basis of modern e-government, the quality of procedures for providing and receiving electronic services by citizens and businesses, openness and transparency of the executive branch in Ukraine.

The advantages of electronic archives for storing electronic resources of executive authorities are as follows:

1) higher level of information security (protection against unauthorized access, etc.);

2) reliability of preservation (less risk of damage, loss and destruction of documents, etc., the possibility of almost "eternal preservation");

3) operative search of documents;

4) the possibility of simultaneous use by many users of the same resource, document;

5) the possibility of remote access to the electronic archive and others.

The success of the introduction of blockchain technologies in e-government depends on solving the following tasks: implementation of a legally verified and controlled mechanism for entering information / data into state registers (blockchain technology guarantees only the consistency of data, not their accuracy and reliability); management of access rights to data registers and contracts in terms of roles and smart contracts; introduction of a multidimensional user identification system based on biometric data; implementation of global data synchronization (guarantee that the execution of any operation at any time and in any node will give the same result); development of a mechanism for validating user interfaces; end-to-end use of Data Center resources. Barriers to the use of blockchain technologies can be: legal restrictions, novelty of technology; lack of knowledge and skills of staff working with technology; lack of sufficient state support and high cost.

Since blockchain technology is a document management technology, its further development would benefit from the application of theoretical and practical knowledge accumulated by archival science.

Currently, the technology is not ready to guarantee long-term storage of legally relevant information and documents at intervals of about 10 years or more, so its use for archival storage is associated with serious risks. It can be used in the presence of a thorough legal and regulatory framework and the formation of judicial practice in the management of documents in the short and medium term.

References:

1. Rozporiadzhennia Kabinetu Ministriv Ukrainy «Pro skhvalennia Kontseptsii rozvytku elektronnoho uriaduvannia v Ukraini» vid 13.12.2010 r. № 2250-r. [Order of the Cabinet of Ministers of Ukraine "On approval of the Concept of e-government development in Ukraine" dated 13.12.2010 № 2250] [E-resource]. – Access mode: http://zakon2.rada.gov.ua/laws/show/2250-2010-%D1%80/ed20110926

2. The Green Paper on the Electronic Governance in Ukraine. [E-resource]. – Access mode: http://etransformation.org.ua/2014/11/24/355/

3. Atzori, M. (2017). Blockchain Technology and Decentralized Governance: is the State Still Necessary? Journal of Governance and Regulation, 6(1), 45-62. https://virtusinterpress.org/IMG/pdf/10.22495_jgr_v6_i1_p5.pdf

4. D. & A. Tapscott. Blockchain revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. URL : http://dontapscott.com/books/blockchain-revolution

5. Swan Melanie. Blockchain: Blueprint for a New Economy / Melanie Swan - Sebastopol CA : O'Reilly Media, 2015. – 152 p.

6. Walport M. Distribution Ledger Technology: Beyond the Blockchain.URL : https://drive.google.com/file/d/0B9yzAtU8an7tdHlUZEQ0bnlWY0k/view

7. Danylchenko O. Blokchein: yuryst yz mashyny // [Blockchain: lawyer from the car] // ЮРИСТ&ЗАКОН. 2017. № 21. June. URL : http://uz.ligazakon.ua/magazine_article/EA010438

8. Karpenko O. Vykorystannya blokchejn-sistem organamy publichnoi vlady: ukrains'kij ta zarubizhnij dosvid [Use of blockchain systems by public authorities: Ukrainian and foreign experience]/ O. Karpenko, A. Osmak // Actual problems of public administration. - 2018. - Issue. 1.- C. 57-62. - [E-resource]. – Access mode: http://nbuv.gov.ua/UJRN/apdyo_2018_1_11
9. Marchenko V. V. Problemy informacionnoj bezopasnosti v ehlektronnom dokumentooborote [Information security problems in electronic document management]: V. Marchenko // Право и закон. – 2014. – № 2. – P. 49-53.
10. Timofeev D. S. Problemi zabezpechennya bezpeky v sistemakh elektronnogo dokumentoobigu [Security issues in electronic document management systems] / D. Timofeev, O. Tretyak. – [E-resource]. – Access mode: http://www.rusnauka.com/10_NPE_2010/Informatica/62531.doc.htm
11. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal L 281. 23/11/1995. - P. 0031-0050.
12. Directive 98/34/EC Of the European Parliament and of the Council of 22 June 1998 on the laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services // Official Journal L 204. 21.7.1998. – P.37
13. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. [E-resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093
14. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). [E-resource]. – Access mode: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0021
15. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.108. [E-resource]. – Access mode: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
16. Pro Osnovni zasadi rozvitku informacijnogo suspil'stva v Ukraïni na 2007-2015 rr. [On the Basic Principles of Information Society Development in Ukraine for 2007-2015] : Zakon Ukraïni vid 09.01.2007 r. № 537-V // Vidomosti Verkhovnoï Radi Ukraïni (VVR). – 2007. - № 12. – St.102.
17. Dubov D.V., Dubova S.V. Osnovy elektronnoho uriaduvannia [Fundamentals of e-government]: Navchalnyi posibnyk. – K.: Tsentr navchalnoi literatury, 2006. – 176 s.
18. Pro elektronni dokumenty ta elektronnyi dokumentoobih [On electronic documents and electronic document management]: Zakon Ukrainy vid 22.05.2003 r. № 851-IV // Vidomosti Verkhovnoi Rady Ukrainy. – 2003. - №36. – St.275.
19. 100 mist – krok vpered. Monitorynh vprovadzhennia instrumentiv elektronnoho uriaduvannia, yak osnovy nadannia administratyvnykh posluh v elektronnomu vyhliadi [100 cities - a step forward. Monitoring the implementation of e-government tools as a basis for providing administrative services in electronic form] / Za. zah. red. I.S. Kuspliak, A.O. Serenok. – Vinnytsia: HO «Podilska ahentsiia rehionalnoho rozvytku», 2014. – 86 s.
20. Harasym O.R. Orhanizatsiia zakhyshchenoho elektronnoho dokumentoobihu v merezhakh elektronnoho uriaduvannia [Organization of secure electronic document management in e-government networks] / Harasym O.R., Komova M.V., Lytvyn V.V. [E-resource]. – Access mode: http://vuzlib.com.ua/articles/book/10571-Organ%D1%96za%D1%81%D1%96ja_zakhishhenogo_/1.html
21. Nakaz Ministerstva yustytsii Ukrainy «Pro zatverdzhennia Poriadku roboty z elektronnymy dokumentamy u dilovodstvi ta yikh pidhotovky do peredavannia na arkhivne zberihannia» [On the statement of the Order of work with electronic documents in office work and their preparation for transfer on archival storage] vid 11.11.2014 r. №1886/5. [E-resource]. – Access mode: http://zakon4.rada.gov.ua/laws/show/z1421-14
22. Klymenko I.V. Tekhnolohii elektronnoho uriaduvannia [E-government technologies]: Navchalnyi posibnyk / I.V. Klymenko, K.O. Lynov. – Kyiv: Vyd-vo DUS, 2006. – 225 s.

23. Solonina N. Obgruntuvannia vyboru prohramnoho zabezpechennia dlia arkhiviv elektronnykh dokumentiv derzhavnykh pidpryiemstv ta ustanov [Justification of the choice of software for archives of electronic documents of state enterprises and institutions] / N. Solonina // Naukovi pratsi Natsionalnoi biblioteky Ukrainy im. V. I. Vernadskoho. – 2010. – Vyp. 28. – S. 225-238.
24. [E-resource]. – Access mode: https://www.iso.org/committee/6266604.html
25. Ukraina pidpysala uhodu z naibilshym blokchein-proektom BitFury. [Ukraine has signed an agreement with the largest blockchain project BitFury] - [E-resource]. – Access mode:
https://hromadske.ua/posts/ukraina-pidpysala-uhodu-z-naibilshym-blokchein-proektom-bitfury
26. Ministerstvo Yusticii Ukrainy na poroge vnedreniya tekhnologii blokchejn [The Ministry of Justice of Ukraine is on the verge of introducing blockchain technology] - [E-resource]. – Access mode: http://www.embassyofbitcoin.com.