# Interoperability of Criteria for Evaluating Disinformation Detection Services in the Conditions of Public Administration Digitalization

UDC: 351:004 DOI: https://doi.org/10.15421/152401

**Osmak Anton**[1]
**Ph.D., Assoc. Prof., http://orcid.org/0000-0002-1960-8353, osmak.anton@kneu.edu.ua**
**Karpenko Yuliia**[1]
**Ph.D., Assoc. Prof., http://orcid.org/0000-0001-9169-7576, karpenko.yuliia@kneu.edu.ua**
**Kachmarskyi Yevhenii**[2]
**Ph.D., https://orcid.org/0009-0001-8369-8090, evgenij113@gmail.com**
*[1]Kyiv National Economic University named after Vadym Hetman (Kyiv, Ukraine)*
*[2]V. M. Koretsky Institute of state and law of National Academy of Sciences of Ukraine (Kyiv, Ukraine)*

**Abstract**
At present a serious problem for all Ukrainian authorities is the lack of the necessary conditions to evaluate the provision of governance services to citizens. The article identifies the main problems and shortcomings of existing quality assessment criteria for government services across different public administration systems. A factual analysis of global rankings assessing the level of economic digitization has been conducted.

The purpose of the article is to carry out factual analysis of evaluation criteria for disinformation detection services in digital form in order to develop a comprehensive system of their interoperability. The main criteria for evaluating disinformation detection services in the context of public administration digitalization have been determined. An interpretation of the term "assessment compatibility of disinformation detection services" as a unified system of basic quality criteria and their implementation has been proposed, allowing for appropriate evaluation regardless of the operational delivery technology. A comprehensive interoperable structure of comparative assessment criteria for various disinformation detection services has been developed based on determinant components considering the specifics of their provision. It has been established that the process of digital implementation of disinformation detection services directly depends on data collection, registration, accumulation, storage, adaptation, modification, updating, utilization, dissemination, depersonalization, transformation, and destruction. The basic determinants of evaluating disinformation detection services have been improved by classifying them according to the following components: reliability, responsiveness (timeliness), competence, accessibility, politeness, communicativeness, trust, security, understanding/knowledge.

**Keywords:** information, disinformation, information interoperability, disinformation detection services, digital services, standards of service activity, public administration digitalization, digital transformation

# Інтероперабельність критеріїв оцінювання сервісів виявлення дезінформації в умовах цифровізації публічного управління

**Осьмак Антон**[1], **Карпенко Юлія**[1], **Качмарський Євгеній**[2]
*[1]Київський національний економічний університет імені Вадима Гетьмана (м. Київ, Україна)*
*[2]Інститут держави і права імені В. М. Корецького НАН України (м. Київ, Україна)*

**Анотація**
Наразі серйозною проблемою для всіх органів влади України є відсутність необхідних умов для оцінки надання громадянам послуг з управління. В статті виявлено основні проблеми та недоліки існуючих оціночних критеріїв якості сервісів органів влади у розрізі різних систем функціонування публічного управління. Проведено фактологічний аналіз світових рейтингів оцінювання рівня цифровізації економіки.

Метою статті є визначення критеріїв оцінювання сервісів виявлення дезінформації в цифровій формі з метою розробки комплексної системи їх взаємодії. Визначено основні критерії оцінювання сервісів виявлення дезінформації в умовах цифровізації публічного управління. Запропоновано трактувати термін «оціночна сумісність сервісів виявлення дезінформації» як єдину систему базових критеріїв якості з їх реалізації, що дозволяє здійснити відповідне оцінювання незалежно від технології операційного надання. Розроблено комплексну інтероперабельну структуру порівняльних оціночних критеріїв для різних сервісів виявлення дезінформації на основі складників детермінант із урахуванням специфіки їх надання. Встановлено, що процес цифрової реалізації сервісів виявлення дезінформації безпосередньо залежіть від збирання, реєстрація, накопичення, зберігання, адаптування, зміни, поновлення, використання й поширення, знеособлення, трансформації та знищення даних. Удосконалено базові детермінанти оцінювання сервісів виявлення дезінформації шляхом їх класифікації за такими складниками: надійність, реактивність (оперативність), компетентність, доступність, ввічливість, комунікативність, довіра, безпека, розуміння/знання.

**Ключові слова:** інформація, дезінформація, інформаційна сумісність, послуги виявлення дезінформації, цифрові послуги, стандарти сервісної діяльності, цифровізація публічного управління, цифрова трансформація

Стаття надійшла / Article arrived: 04.02.2024 Схвалено до друку / Accepted: 31.03.2024

**Introduction**.

Information interoperability is the ability of two or more systems to interact in the information space and synchronize information flows. Information interoperability is an element of semantic interoperability, which is defined as the ability of systems to understand the meaning of the data being exchanged. This includes factors such as data dictionaries, ontologies, and logic rules. Through a semantic approach and leveraging artificial intelligence algorithms, interoperable approaches can be employed to combat deepfakes by consolidating data on known deepfakes and manipulated media samples and creating early warning systems. These systems involve the collective sharing of information about potential sources of deepfakes and taking preventive measures to prevent their widespread dissemination.

The urgency of the problem. At present a serious problem for all Ukrainian authorities is the lack of the necessary conditions to evaluate the provision of governance services to citizens. The reason is that most officials do not understand the essence of service activities of public authorities, do not perceive citizens as recipients of services, but operate according to an administrative-bureaucratic system that is not focused on the citizen and his needs and expectations. In addition, modern digital transformations require a change in the paradigm of public authority service activity. The main components that cause this problem are:

- identification of the entities within the authorities and their territorial units, which is mainly caused by their administrative location and subordination, which creates additional difficulties in finding a specific governance service provider;
- complexity of the procedure of providing services due to the lack of appropriate regulatory norms of the procedure for their provision, the need to refer citizens to several executive bodies to resolve issues, the availability of various data that are not related and, as a consequence, the need to collect customer confirmatory information;
- the length of time for the provision of services through the necessary organizational activities (preparation of meetings, commissions, executive committees, sessions, etc.);
- lack of proper information on governance services, lack of comprehensive list of services;
- lack of facilities for reception of citizens;
- lack of respect of the authorities for the visitors since some public officials still do not feel a proper moral obligation to the taxpayers.

At the same time, approaches to digital services from the point of view of the classical criteria of their evaluation do not allow to do it at the proper level due to the difference in the procedures of the service activity. That is why it is necessary to identify, formulate on the basis of existing and generalize common criteria for the evaluation of such services, and separate specific criteria in the field of digital services. In order to distinguish common and specific criteria, first of all it is necessary to examine the criteria for the provision of classic governance services and to identify the components that correspond to the specifics of the service process of public authorities in the light of the latest digital transformations.

**The purpose of the article** is to carry out factual analysis of evaluation criteria for disinformation detection services in digital form in order to develop a comprehensive system of their interoperability.

**Analysis of research and publications**.

In the scientific literature the issues of quality criteria for the provision of governance services by executive authorities have been investigated in the works of such well-known Ukrainian and foreign scholars as V. Bakumenko (2010), O. Karpenko (2016), S. Kvitka (2023), O. Kiliyevych and V. Tertychka (2009), A. Chemeris (2004), T. Horan, T. Abhichandani, T. and R. Rayalu (2006), C. Halaris (2007). Paying tribute to the results of scientific research, it should be noted that the problem of developing interoperable evaluation criteria for the provision of disinformation detection services in the conditions of public administration digitalization remains unresolved.

**Main material**.

The question of the evaluation of governance services is quite abstract, since it is a subjective assessment of the expected result. For example, quality can be considered as the degree of satisfaction and expectations of consumers (in this sense, the term is fixed in the international standards ISO 9000), as the degree of compliance with the requirements and standards, in terms of conformity of the services provided, their value, etc. (Soloviova, 2014). Considering that in Ukrainian the legislation quality of service is defined as a set of consumer properties of the service (continuity, accessibility, etc.), which determine its ability to meet the needs of the consumer and are characterized by established indicators (Pro zatverdzhennia Pravil nadannia ta otrymannia telekomunikatsiinykh posluh, 2012), we can define *the quality of the governance service* as a set of its characteristics, which determine the ability to meet the established or expected needs of the customer. Under such a condition, the notion of quality of the digital governance service should be singled out as a set of characteristics that meet certain digital criteria.

Unlike the classical evaluation system, the provision of governance services in digital form is primarily determined by specific features,

such as quality of perception, controllability, comprehensibility, logic and simplicity of the interface, compatibility, interoperability, multi-platform, reliability functions of personalization, etc. On the other hand, the overall criteria for evaluating the quality of a digital service, given its specific nature, are not conclusive.

The concept of interoperability assessment should be introduced in order to combine criteria for evaluating services in different ways of providing. So, *the evaluation interoperability of the disinformation detection services* is the only set of basic criteria for evaluating the quality-of-service provision, which allows the consumer to evaluate it regardless of the technology used to provide it.

The basic criteria that combine both classic and digital services can be defined as the degree of customer expectations, the degree of compliance with the proposed requirements and standards, the total set of technical, technological, and operational characteristics by which the service meets the needs of the consumer.

In any case, all quality criteria, both classical and digital, should be reflected in a single standard of governance service – a document that contains comprehensive information on the reasons for the service activity, a list of documents required to obtain the service, the procedure and amount of payment for its provision, term of governance service provision, privileges for its receipt, type of administrative act adopted as a result of provision of the relevant governance service, grounds for refusal to provide governance vein service, as well as the organization of the administrative body for the provision of such services (Cherevchenko, 2019).

In order to determine the criteria for assessing the quality of disinformation detection services, the audience of the recipients of such services should first be identified. Determining the audience is possible through rating indices to assess the level of digitization of the economy. The most famous rankings are based on the following indices (Pizhuk, 2019): ICT Development Index (IDI); Digital Economy and Society Index (DESI); Digital Evolution Index (DEI); IMD World Digital Competitiveness Index (WDCI); Networked Readiness Index (NRI); Digital Acceleration Index BCG (e-Intensity).

The ICT Development Index (IDI) has been implemented by the International Telecommunication Union (ITU) since 2009 and calculates 14 indicators across three groups of processes: access to ICT, ICT usage and ICT skills.

At the same time the Digital Economy and Society Index (DESI) is based on six major groups of indicators (European Commission, 2019):

- connection level – the state of the connection measures the deployment of broadband infrastructure and its quality (access to fast and ultra-fast broadband services – a prerequisite for competitiveness);
- human capital / digital skills – the measurement of human capital measures the skills needed to take advantage of the opportunities offered by digital technology;
- use of Internet services by citizens – the parameter of use of Internet services explains various online actions, such as consumption of online content, video calls, as well as purchases on the Internet and banking services;
- enterprise digital integration – the measurement of digital integration measures the digitization of business and e-commerce;
- digital public services – the measurement of digital public services determines the digitization of public services;
- ICT R&D – R&D and ICT represent an analysis of trends in the ICT sector.

Based on these indexes we can distinguish two main factors that influence the formation of criteria for evaluating disinformation detection services:

- technical factor – the technological level of the digital infrastructure and the technical level of the service recipient;
- social factor – the level of digital competence of the serviced recipient.

These aptitude factors influence the assessment of the quality of digital governance service delivery and determine the technical capability to provide / obtain a disinformation detection services and the level of digital skills.

The factor of technical ability to obtain digital governance service is determined by the level of Internet penetration among the population. At the same time, a social factor determines the level of digital skills and competences and reflects the degree of consumer readiness to receive digital services.

The composition of the common criteria reflects the main problems faced by consumers in the process of obtaining them, and therefore is mandatory for all governance services. In addition to the general criteria, specific criteria that reflect the specific features of the process of providing a certain type of governance service should be used. The specific criteria for each type of governance services are determined individually with regard to specific features and there are several problems in the delivery process.

The criteria for evaluating disinformation detection services also include the quality of digital information perception, the logic and simplicity of the interface, the reliability features of personalization, multi-platform etc.

The most important characteristics of service evaluation, which ensures its ability to meet certain needs, are reliability; politeness; confidentiality; accessibility; communicativeness; attentive attitude.

The recipient, when evaluating the quality of the service, compares some of the actual values of the quality parameters with the expected values, and if these expectations match, the quality of the services is considered satisfactory. V. Zaitaml, A. Paramurman and L. Berry (1988) identified ten criteria by which consumers judge services and ranked them as the complexity of the assessment increased. The following determinants are defined: reliability, reactivity (responsiveness), competence, accessibility, politeness, communicativeness, trust, safety, understanding / knowledge, sensitivity and basic components that correspond to each of the determinants.

With the introduction of digital governance services, the characteristics of their provision require new approaches, taking into account the specifics and technical principles of providing such services. Thus, some of the basic characteristics are unacceptable for the evaluation of digital services and the technological features of their provision require advanced formulation and identification of specific conditions and evaluation criteria for such services. For the comprehensive evaluation of governance services, it should be taken into account the specifics of digital service delivery in such determinants as: reliability, responsiveness, competence, accessibility, security and confidentiality and the determinants of courtesy, communication, and sensitivity – to introduce the attributes of digital services.

*Reliability* is defined as the ability of the provider to accurately provide a regulated service. Quality assurance should begin with the development of a quality service program. The basis for assessing reliability is the competence of the service personnel and the compliance of the technical support with the conditions laid down in the regulations for each service.

The following components and quantitative indicators of the reliability of disinformation detection services can be distinguished (Vasilevskyi, & Podzharenko, 2010):

- failure-free – characterizes the ability to perform the given functions in the given conditions;
- stability – the ability to perform specified functions in the conditions of interference (errors, failures, failures);
- correctness – characterizes adaptability to finding and eliminating errors and making changes in the process of operation;
- security and durability. – properties to avoid moral aging in the case of prolonged use. Security is characterized by the likelihood of distortion in the case of third-party interference, and durability is sometimes a failure due to moral aging.

*Efficiency (response speed)* – the ability to help the customer obtain the service without delay. Because digital administrative service involves the provision of remote services, being responsive is the ability to deal with an emergency or specific requirements of the service recipient. In such cases, the ability of the service provider to find an effective solution is assessed. For digital governance services, this is a criterion for evaluating the effectiveness of support. Reactors of digital public services can also be attributed to the form, timeliness, and effectiveness of support channels: by hotline number; chatting on the provider's website / service page; with the help of messengers.

*Competence* – a set of professional knowledge; ability to perform certain professional functions; an integrative characteristic of a specialist who demonstrates readiness and determines his ability to successfully pursue professional activity as an important component of the professionalism subsystem (Mudryk, 2012). In the case of the provision of digital governance services, the level of digital competence is the ability of staff to resolve procedural and technical issues that arise in the process of providing such a service.

*Accessibility*, as a basic concept, is a criterion that assesses the level of public service available to all populations and the ease of liaising with service personnel. As a criterion in the field of digital governance services, the concept of accessibility has several basic properties. They are accessibility, as a fact and accessibility, as assistive technology.

So, for digital governance services, accessibility is a feature that a user and / or process that has the appropriate authority can use this resource according to the rules set by the security policy without waiting for a longer (acceptable) time interval. The essence of the property is that the required information resource is in the form required by the user, in the place required by the user, and at the time when he needs it.

In the case of providing a digital governance service, the criterion is based on web accessibility, which is based on four components: perception, manageability, understandability, and compatibility (Dyzain-systema derzhavnykh saitiv Ukrainy, 2018: W3C, 2008):

- perception – the user interface and content must be presented in a form that can be perceived by users through the accessible organs of perception;
- manageability – users have access to the content in any way they like, such as using a keyboard or voice commands;

- understandability – users can understand the content of the resource or how the service works (readability, predictability, help with entering information);

- content compatibility with applications used by the service user, including legacy browsers and assistive technologies.

Accessibility is also considered an opportunity for low-mobility groups and people with special needs to access certain services, products, devices, etc. (Henry, Abou-Zahra, & Brewer, 2014).

*Civility* and respect for the citizen as an assessment criterion includes equal treatment of all service users, availability of proper household amenities in the premises of the administrative body, etc. (Tymoshchuk, 2012). Staff, including in the mode of providing digital online services, should politely communicate with visitors, quickly and at a high professional level find solutions to the issues that are addressed to it (Єдині вимоги (стандарт) до якості обслуговування відвідувачів центрів надання управлінських послуг). Courtesy, as an element of digital culture, should be the standard of administration.

*Communicativeness* – the ability to provide a service that eliminates misunderstandings between the provider and the service recepient because the required information will be provided to him in a timely manner and without further request from the client. Ability to receive information from the recipient of the digital service, process it and transmit the information to the recipient in a language accessible to him, using a convenient communication channel for the client, willingness to avoid professional jargon in case of complaint, notification of changes related to the nature of work.

*Security*. In the context of digital transformations, a critical indicator of evaluation is the degree of cybersecurity and the level of cryptographic protection of personal data used in the process of providing a governance service. Personal data are defined by the legislation of Ukraine as information or a set of information about an individual who is identified or can be specifically identified, for processing of it specific requirements and legal relations (Pro zakhyst personalnykh danykh, 2010). In particular, it is prohibited (except for a certain list of exceptions) processing personal data of racial or ethnic origin, political, religious or ideological beliefs, membership of political parties and trade unions, early criminal conviction, as well as health, sexual, biometric or genetic data.

Information systems, including governance services, are analyzed in three major sectors: hardware, software, and communications, for identification and application of industry information security standards as protection and prevention mechanisms at three levels (physical, personal and organizational). Essentially, procedures or rules are in place to inform administrators, users, and operators of the use of security mechanisms to ensure information security within organizations (Hladun, & Khala, 2017).

*Privacy* – the ability of staff to inspire confidence and to safeguard personal information. Privacy is a non-publicity feature it includes trusting, secrecy, privacy. Privacy in a digital system is a property of information so that this information cannot be obtained by an unauthorized user or by the process of the information system. The information is kept confidential if the rules for its familiarization are followed. From the point of view of service activity of public authorities, the criterion of confidentiality has three main sub-criteria (Bohush, Kryvutsa, & Kudin, 2004).:

- governance confidentiality – ensures the confidentiality of information in accordance with the principles of access control;

- trustworthy confidentiality – provides confidentiality of information in accordance with the principles of access control of confidentiality;

- confidentiality of information – the information cannot be obtained by an unauthorized user and (or) process (the information retains confidentiality if the established rules of familiarization with it).

Because the process of providing a digital governance service is any action or set of actions with personal data, such as collection, registration, accumulation, storage, adaptation, modification, renewal, use and distribution (distribution, implementation, transfer), impersonation, destruction, the criterion for assessing the confidentiality of such data is one of the keys.

Integrity is the internal interoperability of all parts of information resources during their processing, storage, and transmission, as one whole in the information system. It is the state of the data, or information system, when the data and programs are used in an established manner that ensures stable work of the system; automatic recovery in case of potential system error detection; automatic use of alternative components instead of failures. For a digital system, concepts such as data integrity, information integrity, database integrity, information system integrity can be considered. System integrity is a feature of the system that none of its components can be removed, modified, or added in violation of a security policy. The integrity of the information can be compromised by both the attacker and the objective environment. It is believed that information security should be complex (Honcharova et al, 2013).

*Availability* – a property of an information resource is that a user and (or) process, that has the

appropriate authority can use the resource according to the rules set by the security policy without waiting for a longer (acceptable) time interval. The essence of the property lies in the fact that the required information resource is in the form necessary to the user, in the place required by the user, and at the time when he needs it (Troian, 2012).

*Tangibility*. Services are characterized by insensitivity, that is, they cannot be evaluated by the use of sensory organs and thus obtain their specific characteristics (Prymak, & Kostiuchenko, 2008). This means that services cannot be demonstrated, seen, tried, transported, stored, packaged or examined until the time of receipt. The result of the digital governance service for providing the criterion of sensitivity should be displayed in the condition of confidentiality of information, or in a format accessible to the recipient.

Having analyzed the determinants and their components, we can deduce the structure of the digital components of the criteria for complex evaluation of the provision of digital governance services, taking into account the specifics of their provision that are given in Table 1.

**Table 1.**

**Determinants of disinformation detection services quality assessment, basic and additional digital components**

| Determinants | Basic components | Additional digital components |
|---|---|---|
| Reliability | Failure to provide services; Provision of services in due time; The fulfillment of their pledges; Accurate record keeping | Failure; Stability; Correctness; Protection and durability |
| Efficiency | The desire or willingness of the staff to provide the service to the recipient; Quick answer calls; Timely provision of customer service; Immediate submission of relevant documents | Support service efficiency; Communication channel performance |
| Competence | Knowledge and skills of staff contacting clients; Knowledge and skills of technical staff; The ability of an organization to conduct the necessary research | The level of digital competence |
| Accessibility | No obstacles to contact; Easy to receive services; Short waiting time to receive services; Convenient location of the place where the service can be provided | Perception; Controllability; Intelligibility; Compatibility; Availability and effectiveness of assistive technology |
| Politeness | Polite, respectful attitude towards the client; Friendliness of the contact staff; Respectful attitude to the client's property; Neat appearance of the contact staff | Digital culture. |
| Communicative | Providing clients with the necessary information in a clear language; Ability to listen and understand customers' wishes; Ability to choose the appropriate style of conversation with a specific client; Explanation of the essence of the service; Bringing information on the cost of the service, if any; The client is convinced that the service provider is ready to solve his problem | Analyze and process information and bring it into a recipient-friendly form |
| Security | Absence of threats, risks or doubts; Physical security; Financial reliability; Privacy | Confidentiality is administrative; Trustworthy confidential; Confidentiality of information; Integrity; Information accessibility; Cryptographic protection of personal data |
| Understanding /knowledge | Pursuit of customer awareness; Knowledge of customers' specific requirements; Possibility of an identified approach to clients; Knowledge of constant professional needs | |
| Tangibility | Material possibilities; Appearance of service personnel; Availability of tools and equipment needed to provide services; Availability of material confirmation of the service provided | Display the result of the service |

Thus, the system for evaluating the quality and accessibility of disinformation detection services a broad range of metrics and evaluation criteria based on the principles of customer-orientation and service-orientation. A deep, objective assessment of the quality and accessibility of governance services should undoubtedly be complex and take into account all of the above criteria.

**Conclusions**.

The research has revealed the main problems and shortcomings of the existing evaluation criteria of the quality of disinformation detection services in the context of different systems of their provision. The specific features of digital disinformation detection services are defined, namely: quality of perception, controllability, comprehensibility, logic and simplicity of the interface, compatibility, interoperability, multiplatform, functions of reliability of personalization. In order to combine the criteria of evaluation of services in different variants of their provision, the concept of evaluation interoperability of governance service was introduced. The factual analysis of world rating indices of estimation of the level of digitalization of the economy is carried out and two main factors that influence the formation of criteria for the evaluation of disinformation detection services (technical and social) are identified.

The following determinants have been defined and expanded for the conditions of implementation of disinformation detection services, taking into account the features and technical basics: reliability, reactivity (responsiveness), competence, accessibility, politeness, communicativeness, trust, security, understanding / knowledge, sensitivity and basic components that correspond to each determinant. On the basis of the determinants analysis, the structure of the digital components of the criteria for complex evaluation of the provision of disinformation detection services has been deduced, taking into account the specifics of their provision.

## REFERENCES


Bakumenko, V. D. (2010). Derzhavno-upravlinskyi protses. *Entsyklopedychnyi slovnyk z derzhavnoho upravlinnia*. Kyiv.

Bohush, V. M., Kryvutsa, V. H., & Kudin, A. M. (2004). *Informatsiina bezpeka: Terminolohichnyi navchalnyi dovidnyk*. Kyiv.

Chemeris, A. O., Lesechko, M. D., & Lipentsev, A. V. (2004). *Administratyvni posluhy mistsevykh orhaniv derzhavnoyi vykonavchoyi vlady*. (Monohrafiia). Lviv: LRIDU NADU.

Cherevchenko, L. P. (2019). *Kontseptsiia polipshennia yakosti nadannia upravlinskykh posluh*. Retrieved from https://khm.gov.ua/uk/file/78769/download?token= 3A0WD--Y

*Dyzain-systema derzhavnykh saitiv Ukrainy*. (2018). Retrieved from https://design.gov.ua/ua

European Commission. (2019). Shaping Europe's digital future. *The Digital Economy and Society Index (DESI)*. Retrieved from https://ec.europa.eu/digital-single-market/en/desi

Halaris, C., Magoutas, B., & Papadomichelaki, X., & Mentzas, G. (2007). Classification and synthesis of quality approaches in e-government services. *Internet Research* 17(4), 378-401.

Henry, S. L., Abou-Zahra, S. & Brewer, J. (2014). The Role of Accessibility in a Universal Web. *Proceeding W4A '14 Proceedings of the 11th Web for All Conference,* (Article No. 17). ISBN 978-1-4503-2651-3.

Hladun, A., & Khala, K. (2017). Taksonomiia standartiv informatsiinoi bezpeky. *Nauka, tekhnolohii, innovatsii*, 2, 53-64. Retrieved from http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM =2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1& Image_file_name=PDF/STI_2017_2_9.pdf

Honcharova, L. L., Voznenko, A. D., Stasiuk, O. I., & Koval, Yu. O. (2013). *Osnovy zakhystu informatsii v telekomunikatsiinykh ta kompiuternykh merezhakh*. Kyiv.

Horan, T., Abhichandani, T., & Rayalu, R. (2006). Assessing user satisfaction of e-government services: development and testing of quality-in-use satisfaction with advanced traveler information systems (ATIS). *Proceedings of the 39th Hawaii International Conference on System Sciences*. Hawaii.

Karpenko, O. V. (2016). *Mekhanizmy formuvannia ta realizatsii servisno-oriientovanoyi derzhavnoyi polityky v Ukraini*. (Dys.... d-ra nauk z derzh. upr.: spets. 25.00.02 "Mekhanizmy derzhavnoho upravlinnia"). Nats. akad. derzh. upr. pry Prezydentovi Ukrainy.

Kiliievych, O., & Tertychka, V. (2009). *Derzhavna polityka: analiz ta mekhanizmy yii vprovadzhennia: metodychni rekom*. Kyiv: NADU.

Kvitka, S., & Korsun, V. (2023). Mechanisms of Network Management of Interaction between Public Authorities and Civil Society. *Public Administration Aspects*, 11(2), 81-87. https://doi.org/10.15421/152322

Mudryk, A. B. (2012). Profesiina kompetentnist derzhavnykh sluzhbovtsiv : teoretyko-empirychnyi analiz fenomenu. In *Aktualni problemy derzhavnoho upravlinnia na suchasnomu etapi derzhavotvorennia: Materialy VI nauk.- prak. konf*. (22 listopada 2012 r., m. Lutsk). Lutsk: SPD Hadiak Zhanna Volodymyrivna, drukarnia «Volynpolihraf».

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). A Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality. *Journal of Retailing*, 64, 12-40.

Pizhuk, O. I. (2019). Suchasni metodolohichni pidkhody do otsiniuvannia rivnia tsyfrovoi transformatsii ekonomiky. *Biznes Inform*, 7, 39-47. https://doi.org/10.32983/2222-4459-2019-7-39-47

Pro zakhyst personalnykh danykh. (2010). *Zakon Ukrainy*. Vidomosti Verkhovnoi Rady Ukrainy, 34, st. 481. Retrieved from https://zakon.rada.gov.ua/laws/show/ 2297-17

Pro zatverdzhennia Pravil nadannia ta otrymannia telekomunikatsiinykh posluh. № 295. (2012, April 11). *Postanova KMU*. Retrieved from https://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF#Text

Prymak, T. O., & Kostiuchenko, A. M. (2008). Marketynhovi aspekty prosuvannia posluh. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika"*, 633, 585-589. Retrieved from https://vlp.com.ua/files/84.pdf

Soloviova, O. M. (2014). Shchodo problemnykh pytan yakosti upravlinskykh posluh. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu: Seriia: Pravo*, 24(3), 122-125.

Troian, S. (Ed.). (2012). *Zakhyst informatsiinykh resursiv: navchalno-metodychnyi posibnyk do kursu "Zakhyst informatsiinykh resursiv"*. Retrieved from https://library.udpu.edu.ua/library_files/6365_01.pdf

Tymoshchuk, V. (2012). *Administratyvni posluhy: Posibnyk*. Kyiv: TOV «Sofiia-A».

Vasilevskyi, M., & Podzharenko, V. (2010). *Normuvannia pokaznykiv nadiinosti tekhnichnykh zasobiv: navchalnyi posibnyk*. Vinnytsia: VNTU.

W3C. (2008). *Web Content Accessibility Guidelines (WCAG) 2.0*. Retrieved from https://www.w3.org/Translations/WCAG20-ru/#perceivable