UDC 338.24

Yarovoy T.S.
Ph.D. (Public Administration), Associate Professor of Department of Public Administration, Interregional Academy of Personnel Management, Kyiv,Ukraine
tikhon_9563963@ukr.net; ORCID ID: 0000-0002-7266-3829
Kozyrieva O.V.
Dr. Sc. (Economic Sciences), Head of Department of Management and Administration, National University of Pharmacy, Kharkiv, Ukraine
yakakos74@gmail.com; ORCID ID: 0000-0002-2014-4584
Bielska T.V.
Dr. Sc. (Public Administration), Associate Professor, Associate Professor of the Department of Management and Public Administration, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine
tanya_belska@ukr.net; ORCID ID: 0000-0002-2792-4700
Zhuk I.I.
PhD (Economic Sciences), Associate Professor of the Department of Finance, Banking and Insurance, Interregional Academy of Personnel Management, Kyiv, Ukraine
Zhuk_Inna@i.ua; ORCID ID: 0000-0003-4998-1818
Mokhova I.L.
PhD (Public Administration), associate professor of Master's Degree of Public Administration, Center for Postgraduate Education, Donetsk National Technical University, Pokrovsk,Ukraine
julimokhova@gmail.com; ORCID ID: 0000-0002-0093-2620

THE E-GOVERNMENT DEVELOPMENT IN ENSURING THE COUNTRY FINANCIAL AND INFORMATION SECURITY

Abstract. The article substantiates that the country's e-government depends on a coherent government policy and is capable of promoting a high level of financial and information security for the state. The digital economy is based on information and communication and digital technologies and provides for the implementation of a set of tasks that have a positive impact on the economy, business, society and the livelihoods of countries as a whole. The purpose of the article is to identify threats to the e-governance system development of the world-leading countries in order to ensure their information security. Based on the analysis of E-Government Development Index, Global Cybersecurity Index indicators the dynamics of e-government development (Denmark, Australia, Korea, United Kingdom, Sweden, Finland, Singapore, New Zealand, France and Japan) and the dynamics of the global cybersecurity index have been depicted that allowed to identify, on the basis of the analysis, the key public policy trends in the e-government system of these countries to ensure their information security and ways to overcome them. The implementation the results of the research will help to increase technological sustainability, provide better protection of state-owned IT systems, improve the skills and knowledge of citizens, business and government, and strengthen national cooperation on information security.

Keywords: E-governance; informational security; financial security; information technologies; government

JEL O38, D8, L98, P51

Fig.: 2; tabl.: 1; bibl.: 14

Яровой Т.С.
кандидат наук з державного управління, доцент, доцент кафедри публічного адміністрування, Міжрегіональна Академія управління персоналом, Київ, Україна
tikhon_9563963@ukr.net; ORCID ID: 0000-0002-7266-3829

Козирєва О.В.
доктор економічних наук, доцент, завідувач кафедри менеджменту і адміністрування,
Національний фармацевтичний університет, Харків, Україна
yakakos74@gmail.com; ORCID ID: 0000-0002-2014-4584
Бєльська Т.В.
доктор наук з державного управління, доцент,
професор кафедри менеджменту і публічного адміністрування,
Харківський Національний університет міського господарства імені О.М.Бекетова, Харків, Україна
tanya_belska@ukr.net; ORCID ID: 0000-0002-2792-4700
Жук І.І.
кандидат економічних наук, доцент кафедри фінансів,
банківської та страхової справи,
Міжрегіональна Академія управління персоналом, Київ, Україна
Zhuk_Inna@i.ua; ORCID ID: 0000-0003-4998-1818
Мохова Ю.Л.
кандидат наук з державного управління, доцент магістратури державного управління
Центру післядипломної освіти,
Донецький національний технічний університет, Покровськ, Україна
julimokhova@gmail.com; ORCID ID: 0000-0002-0093-2620

РОЗВИТОК Е-УРЯДУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇНИ

Анотація. У статті обґрунтовано, що е-врядування країни залежить від узгодженої політики уряду та здатне сприяти високому рівню інформаційної та фінансової безпеки держави. Метою статті є виявлення загроз розвитку системи е-урядування провідних країн світу з метою забезпечення їх інформаційної безпеки. Аналіз Індексу розвитку електронного уряду, Глобального індексу кібербезпеки вказує на динаміку розвитку е-врядування (Данія, Австралія, Корея, Великобританія, Швеція, Фінляндія, Сінгапур, Нова Зеландія, Франція та Японія) та динаміку розвитку глобального індексу кібербезпеки, який дозволив визначити ключові тенденції державної політики в системі електронного урядування цих країн для забезпечення їх фінансово-інформаційної безпеки та шляхи їх подолання. Впровадження результатів дослідження допоможе підвищити технологічну стійкість, забезпечить кращий захист державних ІТ-систем, покращить навички та знання громадян, бізнесу та влади, а також зміцнить національну співпрацю з питань інформаційної безпеки.

Ключові слова: е-врядування; фінансово-інформаційна безпека; інформаційні технології; уряд

Рис.: 2; табл.: 1; бібл.: 14.

Яровой Т.С.
кандидат наук по государственному управлению, доцент, доцент кафедры публичного администрирования,
Межрегиональная Академия управления персоналом, Киев, Украина
Tikhon_9563963@ukr.net; ORCID ID: 0000-0002-7266-3829
Козырева О.В.
доктор экономических наук, доцент, заведующий кафедры менеджмента и администрирования,
Национальный фармацевтический университет, Харьков, Украина
Yakakos74@gmail.com; ORCID ID: 0000-0002-2014-4584
Бельская Т.В.
доктор наук по государственному управлению, доцент, профессор кафедры менеджмента и публичного администрирования,

Харьковский национальный университет городского хозяйства имени А.Н.Бекетова, Харьков,Украина
tanya_belska@ukr.net; ORCID ID: 0000-0002-2792-4700
Жук И.И.
кандидат экономических наук, доцент кафедры финансов, банковского и страхового дела, Межрегиональная академия управления персоналом, Киев, Украина
Zhuk_Inna@i.ua; ORCID ID: 0000-0003-4998-1818
Мохова Ю.Л.
кандидат наук по государственному управлению, доцент магистратуры государственного управления Центра последипломного образования, Донецкий национальный технический университет, Покровск, Украина
julimokhova@gmail.com; ORCID ID: 0000-0002-0093-2620

РАЗВИТИЕ Е-УПРАВЛЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ

Аннотация. В статье обосновано, что е-управление страны зависит от согласованной политики правительства и способно содействовать высокому уровню финансово-информационной безопасности государства. Целью статьи является выявление угроз развития системы е-управления ведущих стран мира с целью обеспечения их информационной безопасности. Анализ Индекса развития электронного правительства, Глобального индекса кибербезопасности указывает на динамику развития е-управления (Дания, Австралия, Корея, Великобритания, Швеция, Финляндия, Сингапур, Новая Зеландия, Франция и Япония) и динамику развития глобального индекса кибербезопасности, который позволил определить ключевые тенденции государственной политики в системе электронного управления этих стран для обеспечения их финансово-информационной безопасности и пути их преодоления.

Ключевые слова: е-управление; финансово-информационная безопасность; информационные технологии; правительство

Рис.: 2; табл.: 1; библ.: 14.

Introduction. E-government is one of the most important components of the information society and an integral part of each country's national information policy. The competitiveness of socio-economic systems is now determined by the e-government development and the introduction and use of the latest information technologies in this field. The e-government development is connected with the general state of political and economic processes in the country, with the implementation of state policy on ensuring its information security, which is of particular relevance in the era of informatization of modern society.

Literature review and the problem statement. The roles of e-government in the country's economic development are devoted to the work of Bertot J.C., Jaeger P.T., McClure C.R [1], Danziger J. N., Kim V. A. [2], Garson D. G [3], Homburg V. [4], Orlova N. [5], Janowski T., Pardo T.A., Davies J. [6], Meijer A. [7]. The authors substantiate the main conceptual categories and methodical approaches for determining the basic components of modern models of economic development and introducing ways of digital economy instruments into the e-government.

Studies of the e-government development in the context of information security, issues of public administration of national and information security are considered in the researches of G. Sytnik [8], V. Bogdanovich [9], A. Semenchenko, V. Dreshpak [10]. The authors have developed a methodology and practical recommendations for improving the information security effectiveness as a component of state national security.

However, a considerable number of issues related to the introduction of the electronic services management practice and, in general, the formation of a qualitative protected digital national innovation space within the global system, remain undiscovered and their solutions are of great importance for the economic development of countries.

The purpose of the article is to identify threats to the e-government development in order to ensure information security of the country.

The results of the research. Electronic governance is an integral part of a modern democratic society and effective government action through the use of information technology. E-government is seen as a form of public administration that helps to increase the efficiency of the public authority's activity by using information and telecommunication technologies to form a new type of a state oriented to meet the citizens' needs. Electronic government ensures openness and transparency of the state apparatus, prevents corruption.

The development of e-government is directly related to the economic situation in the country. Evidence for this is the analysis of macroeconomic indicators of social and economic development (gross domestic product — GDP) and the indicator characterizing the processes of improving the e-governance system (E-Government Development Index — EGDI). An analysis of the relationship between economic development and the improvement of e-governance suggests the emergence of a synergistic effect in the information and economic spheres. The presence of a synergistic effect leads to an increase in the positive impact of the state administration system on the country.

The EGDI Index, developed by the United Nations Department for Economic and Social Affairs, combines the three most important aspects of e-government: the scope and quality of online services (OSI Index), the status of telecommunications infrastructure development (Telecommunication Infrastructure Index — TSI) and the human Capital (Human Capital Index — HCI) and is calculated as the arithmetic mean of these three components [11].

The countries that are the world leaders in the e-governance development are listed in *Table*. Countries like Denmark, Estonia, Norway, and Finland have made significant progress over the past few years in developing national digital identity programs. Estonia is characterized by the best practice of implementing an advanced e-government, backed up by reliable electronic services for all citizens: voting, banking, tax filing, as well as access to medical documents and recipes. Denmark, Australia and the Republic of Korea are leading the world in providing public services and information through the Internet. Other countries from the top ten are Great Britain, Sweden, Finland, Singapore, New Zealand, France and Japan.

Table

The world leaders in the e-governance development

Country	Region	OSI	HCI	TII	EGDI	2016 Rank	2018 Rank
Denmark	Europe	1.0000	0.9472	0.7978	0.9150	9	1
Australia	Oceania	0.9722	1.0000	0.7436	0.9053	2	2
Republic of Korea	Asia	0.9792	0.8743	0.8496	0.9010	3	3
United Kingdom	Europe	0.9792	0.9200	0.8004	0.8999	1	4
Sweden	Europe	0.9444	0.9366	0.7835	0.8882	6	5
Finland	Europe	0,9653	0.9509	0.7284	0.8815	5	6
Singapore	Asia	0.9861	0.8557	0.8019	0.8812	4	7
New Zeland	Oceania	0.9514	0.9450	0.7455	0.8806	8	8
France	Europe	0.9792	0.8598	0.7979	0.8790	10	9
Japan	Asia	0.9514	0.8428	0.8406	0.8783	11	10

Source: United Nations [11].

The main reasons that lead to the problems of safe operation of e-government systems can be attributed to: the complexity and heterogeneity of software and hardware used in e-government systems; a large number of control nodes in e-government systems; external access to the e-government system; functioning of maintenance and information security groups.

At present, both for the national and global economy, the issues of ensuring the efficiency of digital technologies and strengthening their positive impact on economic growth and socio-economic development of countries are relevant. When building modern e-government systems, it is necessary to take into account the experience of different countries around the world in implementing the basic principles, approaches and methods of providing information security.

Modern e-government systems are susceptible to information security threats. The cost of combating such crimes has doubled from 3 trillion USD in 2015 to 6 trillion USD in 2018 [12].

In the current context of development, 58% of states have a national information security strategy (in 2017 — 50%), 91% of states (177 countries) have laws related to network protection compared to last year's figure of 79%. *Fig. 1* provides information on the number of world countries that implement information security measures in public administration and those that do not identify information security as a key indicator of the government programs effectiveness.

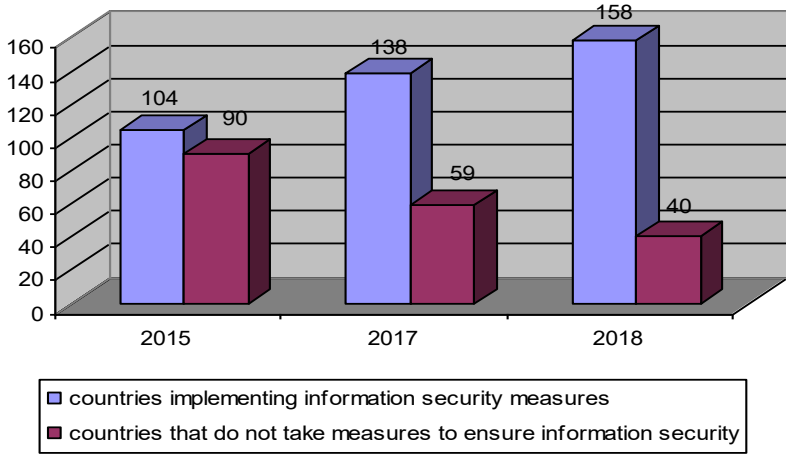

Fig. 1. **Countries implementing information security measures**

Source: International Telecommunication Union [12].

In 2015, government programs in 104 countries included information security in public policy performance. In 2017, the number of countries implementing information security measures in public administration increased by 32.7% (138 states), and in 2018 there were already 158 countries working in this direction (an increase of 14.5% compared to 2017 year). The number of countries that do not implement information security measures in public policy gradually decreased during 2015—2018: from 90 of the countries in 2015 the number decreased to 40 in 2018 (a downturn of 55.6%).

The analysis of the data showed that during 2015—2018 the value of information security for the governments increased, which is confirmed by the enhancement and improvement of the information security measures undertaken by countries' authorities. States are developing more sophisticated e-governance, increasing the availability of online services and integrated service delivery systems, which can intensify the threat in the information field.

Europe and the CIS regions contain the largest number of countries with national information security strategies; African region has the smallest one (14 out of 44 countries).

The information society encounters such threats to information security as denial of electronic services, breach of data integrity and data confidentiality. Global information security issues embrace a special place in international information policy and are reflected in the reports of international organizations (UN, OSCE, EU and others) [10].

The availability of information security assessment indicators in the country is a criterion that the country has a recognized set of measures to ensure balanced and unbiased information on the effectiveness of information security development. 47% of countries (91 countries) have indicators to measure the information security development at the national level. To determine the level of information security the following indices are used:

National Cyber Security Index (NCSI), a global index developed by e-Governance Academy that measures countries' readiness to prevent the fundamental threats extension in the field of information security, cyber-incident management, crime and large-scale cybercrisis [13]; Global Cybersecurity Index (GCI) is an index that combines 25 indicators for monitoring and comparing the level of information security obligations of countries in the main areas: legal, technical, organizational, capacity building, cooperation. The purpose of the GCI is to help countries identify areas of improvement in information security and to motivate them to take measures for improving

their rankings, thereby helping to increase the overall level of information security around the world [12].

Information security is a central point for implementing effective digital governance by organizations and countries. Information security is necessary to protect government infrastructure, awareness of public confidence, which envisages the close link between information security indexes and e-government. *Fig. 2* presents the results of e-government leaders (Denmark, Australia, Korea, United Kingdom, Sweden, Finland, Singapore, New Zealand, France, and Japan) and the global level of information security.

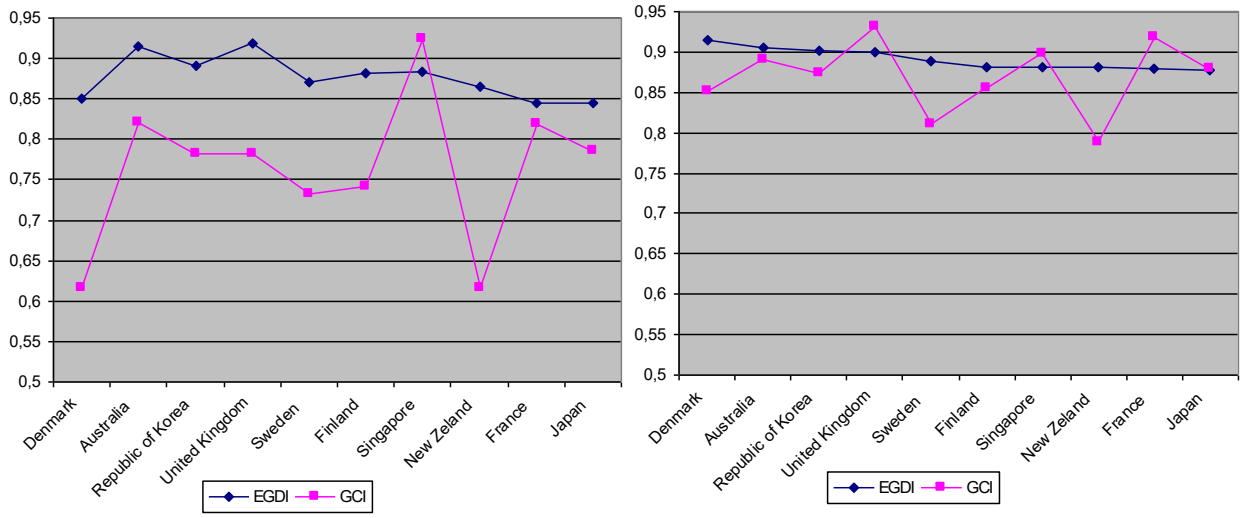

Fig. 2. **Dynamics of EGDI and GCI Indices, 2017—2018 years**

Analysis of *Fig. 2* allowed concluding that despite the significant achievements of countries in the field of e-government, information security indexes remain low. In 2017, it is possible to highlight the prudent and effective public policy of Singapore (EGDI = 0.8828, GCI = 0.925), when the government took into account possible information threats when formulating its e-government development strategy. In 2018, Leadership in e-government (Denmark, Australia, Korea, United Kingdom, Finland, Singapore, France, Japan) succeeded in developing coherent information security strategies, significantly improving the global level of information security in these countries (Denmark: EGDI = 0.915, GCI = 0.852; Australia: EGDI = 0.9053, GCI = 0.89; Korea: EGDI = 0.901, GCI = 0.883; United Kingdom: EGDI = 0.8999, GCI = 0.931; Finland: EGDI = 0.8815, GCI = 0.856; Singapore: EGDI = 0.8812, GCI = 0.888; France: EGDI = 0.879, GCI = 0.918; Japan: EGDI = 0.8883, GCI = 0.88). Sweden, Singapore and France occupy the top ranking positions in terms of significance of values in information security.

In 2018, these countries implemented measures to develop information security strategies. In Denmark, a special unit for the information protection has been set up for each of the major sectors of society (telecommunications, healthcare, energy, finance, maritime transport, transport). Each sector develops a specific strategy, taking into account the specific threats and vulnerabilities relevant to the sector. The Danish government and the Digital Security Council have started security audits based on ISO 27001, which generates digital security and ways to improve it.

Since 2016, the Australian Government has launched an information security strategy in the country, allocating 230 million USD. Republic of Korea recognizes that information security is a national security issue and has one of the fastest and most mobile IT infrastructures in the world. The UK is working with a local Netcraft company on information security initiatives. This includes anti-phishing and malware based in the UK, as well as government-targeted phishing. The partnership helped prevent 34,550 potential attacks on government agencies over the last six months of 2018, or 200 incidents per day [12].

The National Bureau of Investigation in Finland (NBI) has joined forces with the National Cybersecurity Center (NCSC) to investigate a number of major cyber-attacks against public service

websites. The NBI and NCSC plan to work more closely with public and private organizations to enhance their skills and ability to better protect Finland's critical IT infrastructure against cyberattacks.

Singapore has launched digital technology center for small and medium business (specialized center to provide targeted information security consultancy), implemented National Information Security Research Program to promote such research collaboration (provided state support to 2020 in the amount of 190 million USD) [14].

In France, there is an approved national cybersecurity strategy that focuses on the following goals: ensuring a decisive response to cybercrime, informing the public, transforming digital security into a competitive advantage for the French government. In 2018, the Japanese government amended the Basic Cybersecurity Act 2014, which allows the country to set up a specialized council to promote cyber security activities.

As these Member States are leaders in their regions, they can help to create and develop various forms of cooperation with neighboring countries to improve regional information security cooperation.

The countries that occupy lowest positions in the ranking of e-government and information security are Sweden (EGDI = 0.8882, GCI = 0.81) and New Zealand (EGDI = 0.8806, GCI = 0.789). The main reasons are: the vast majority of companies are in the process of digitizing production, including system integration, cloud-based state security, lack of cybersecurity and data security strategies. The most common cyber-attack in Sweden and New Zealand was business process disruption, including malware, viruses and phishing and information security threats.

Conclusions. In order to improve the efficiency of public administration, ensure the development of e-government and information security, reliable tools have to be applied to protect information from unauthorized access in order to ensure confidentiality; provide the integrity of information by protecting it from unauthorized modification or destruction.

The main threats to the e-government development among the studied countries are: Denmark — the threat of cyber espionage against private companies and public authorities, the increase of various types of cyber attacks; cyber-activation of hackers as a result of political events and incidents; Australia — widespread exploitation of vulnerable systems through malware, organized cybercrime; Korea has an unsecured infrastructure vulnerable to cyberattacks, an inefficient information security strategy; UK — e-crime, the risk of industrial cyber espionage, cyber terrorism; Sweden — cyberattack, cloud security, viruses and phishing; Finland — cyberattacks, low levels of public awareness of cybercrime; Singapore — external cyber-attacks, web-site hosting, phishing and imperfect software, Internet fraud, e-commerce scams; New Zealand — cyber espionage and theft of intellectual property, cyber terrorism, damage to critical infrastructure systems, fraud on the Internet, counterfeit investments, insecurity of personal data, cyber-vandalism; Japan — viruses, cyberattacks against government agencies, a shortage of IT professionals, software inconsistency.

Analysis of the key components of e-governance and information security for EU countries has led to the conclusion that the information security indexes of the studied countries are low compared to the significant achievements of the countries in the field of e-governance. Among countries that have sound and effective public policies that take into account e-governance strategies in line with existing information threats, Singapore, the United Kingdom and France can be identified.

The e-government enhancement has a significant impact on information security crimes. In the current conditions of online Internet services development, authorities of developed countries of Denmark, Australia, Korea, United Kingdom, Sweden, Finland, Singapore, New Zealand, France, Japan are developing effective government measures to counter existing threats and ensure information security of the country. The experience of these countries can be used to implement public policies for the e-governance and information security development in other countries where the number of threats is significant.

Література

1. Bertot J. C. Citizen-Centered E-Government Services: Benefits, Costs, and Research Needs / J. C. Bertot, P. T. Jaeger, C. R. McClure // The Proceedings of the 9th Annual International Digital Government Research Conference. — Montreal, Canada, 2008. — P. 137—142.
2. Danziger J. N. The impacts of information technology on public administration: an analysis of empirical research from the «golden age» of transformation / J. N. Danziger, V. A. Kim // International Journal of Public Administration. — 2002. — № 25 (5). — P. 591—627.
3. Public Information Technology and E-Governance / D. G. Garson. — Sudbury : Jones and Bartlett Publishers, Burlington, USA, 2006.
4. Homburg V. Understanding E-Government: Information Systems in Public Administration / V. Homburg. — Routledge, New York, USA, 2008.
5. Orlova N. Methodology of the Electronic Government Evaluation of the European Union Countries based on Taksonometric Method / N. Orlova, I. Mokhova, O. Diegtiar, O. Khomutenko // 33rd IBIMA International Business Information Management Conference Granada, Spain. — 2019. — April 10—11. — P. 505—512.
6. Janowski T. A. Government Information Networks — Mapping Electronic Governance cases through Public Administration concepts / T. A. Janowski, J. Pardo, Davies // Government Information Quarterly. — 2012. — № 29 (1). — P. 1—10.
7. Meijer A. E-governance innovation: Barriers and strategies / A. Meijer // Government Information Quarterly. — 2015. — № 32 (2). — P. 198—206.
8. Ситнік Г. П. Державне управління національною безпекою України : монографія / Г. П. Ситнік. — Київ : НАДУ, 2004. — 408 с.
9. Богданович В. Ю. Інформаційна безпека України та шляхи її забезпечення : навч. посібник / В. Ю. Богданович. — Київ : Вид-во НАДУ, 2005. — 100 с.
10. Семенченко А. І. Електронне урядування та електронна демократія : навч. посібник / А. І. Семенченко, В. М. Дрешпак. — Київ : ФОП Москаленко О. М., 2017. — 72 с.
11. E-government survey 2018 [Electronic resource] / United Nations. — Avaible at : https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf.
12. Global Cybersecurity Index 2018 [Electronic resource] / International Telecommunication Union. — Avaible at : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
13. Україна в глобальному рейтингу кібербезпеки [Електронний ресурс]. — 2019. — Режим доступу : https://matrix-info.com/2019/10/09/ukrayina-v-globalnomu-rejtyngu-kiberbezpeky.
14. Cybersecurity best practices in Singapore [Electronic resource]. — Avaible at : https://www.lexology.com/library/detail.aspx?g=5f3a1553-5010-42a8-a0dd-0f6e5355e7ac.

Статтю рекомендовано до друку 27.05.2020 © Яровой Т. С., Козирєва О. В., Бєльська Т. В., Жук І. І., Мохова Ю. Л.

References

1. Bertot, J. C., Jaeger, P. T., & McClure, C. R. (2008). Citizen-Centered E-Government Services: Benefits, Costs, and Research Needs. The Proceedings of the 9th Annual International Digital Government Research Conference. Montreal, Canada, 137—142.
2. Danziger, J. N., & Kim, V. A. (2002). The impacts of information technology on public administration: an analysis of empirical research from the «golden age» of transformation. *International Journal of Public Administration, 5* (5), 591—627.
3. Garson, D. G. (2006). Public Information Technology and E-Governance. Sudbury: Jones and Bartlett Publishers, Burlington, USA.
4. Homburg, V. (2008). Understanding E-Government: Information Systems in Public Administration, Routledge, New York, USA.
5. Orlova, N., Mokhova, I., Diegtiar, O., & Khomutenko, O. (2019, April 10—11). Methodology of the Electronic Government Evaluation of the European Union Countries based on Taksonometric Method. 33rd IBIMA International Business Information Management Conference Granada, Spain. (pp. 505—512).
6. Janowski, T. A., & Pardo, Davies, J. (2012). Government Information Networks — Mapping Electronic Governance cases through Public Administration concepts. *Government Information Quarterly, 29* (1), 1—10.
7. Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, *32* (2), 198—206.
8. Sytnik, H. P. (2004). *Derzhavne upravlinnia natsionalnoiu bezpekoiu Ukrainy [State management of national security of Ukraine]*. Kiev: NADU [in Ukrainian].
9. Bohdanovych, V. Yu. (2005). *Informatsiina bezpeka Ukrainy ta shliakhy yii zabezpechennia [Information security of Ukraine and ways to ensure it]*. Kiev: NADU [in Ukrainian].
10. Semenchenko, A. I., & Dreshpak, V. M. (2017). *Elektronne uriaduvannia ta elektronna demokratiia [E-government and e-democracy]*. Kiev: FOP Moskalenko O. M. [in Ukrainian].
11. United Nations (2018). E-government survey 2018. Retrieved from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf.
12. International Telecommunication Union. (2018). Global Cybersecurity Index 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
13. *Ukraina v hlobalnomu reitynhu kiberbezpeky [Ukraine in global rating of cyber security]*. (2019). Retrieved from https://matrix-info.com/2019/10/09/ukrayina-v-globalnomu-rejtyngu-kiberbezpeky [in Ukrainian].
14. Cybersecurity best practices in Singapore. (n. d.). Retrieved from https://www.lexology.com/library/detail.aspx?g=5f3a1553-5010-42a8-a0dd-0f6e5355e7ac.

The article is recommended for printing 27.05.2020