UDC 316.774 (477)
JEL Classification: L15, M15
DOI: 10.15587/2312-8372.2019.169592

Prav R.

MONITORING OF THE DEVELOPMENT OF INFORMATION INFRASTRUCTURE IN UKRAINE

Об'єктом дослідження є інформаційна інфраструктура України. Одним з найбільш проблемних місць є відсутність системи оцінки та моніторингу розвитку інформаційної інфраструктури. Виявлено, що основними недоліками існуючих показників моніторингу є відсутність врахування рівня інформаційних загроз. Оцінювання розвитку інформаційної інфраструктури відбувається без врахування ступеня інформаційної безпеки її об'єктів.

В ході дослідження використовувалися методи системного аналізу для оцінки індикаторів розвитку інформаційної інфраструктури в контексті рівня інформаційних загроз. Мета-аналіз наукових праць та нормативно-правових актів використано для систематизації наукових положень щодо проблематики дослідження.

Встановлено, що найчастіше для оцінки інформаційної безпеки використовується система індикаторів, що включає показники рівня розвитку інформаційно-комунікаційних технологій в розрізі основних суб'єктів інформаційної інфраструктури. Це пов'язано з доступністю інформації.

Завдяки розробленій системі оцінки та моніторингу розвитку інформаційної інфраструктури забезпечується можливість отримання знань про рівень інформаційних загроз та безпеки у порівнянні з аналогічними відомими підходами до оцінки, це забезпечує ряд переваг. Зокрема, можливим є визначення критичних об'єктів інфраструктури, що характеризуються найбільшим рівнем впливу інформаційних загроз. Такий підхід довів потребу в забезпеченні захисту інформації приватного сектору інформаційної сфери.

Оцінка стану інформаційної інфраструктури на основі розробленої системи моніторингу дала змогу виявити ряд тенденцій. Розвиток інформаційної інфраструктури підприємств та технологій в інформаційній сфері відбувається швидкими темпами. Це пов'язано зі зростаючим рівнем комп'ютеризації, технологічним переоснащенням, використанням підприємствами соціальних медіа та аналізу «великих даних». Одним з факторів є стрімке поширення хмарних технологій та обчислень. Це водночас дає змогу автоматизувати бізнес-процеси обробки й аналізу інформації. Проте, з іншої сторони, слугує джерелом загроз внутрішній інформації та інформаційній інфраструктурі.

Ключові слова: *інформаційні загрози, інформаційна безпека, система моніторингу, індикатори інформаційних загроз, захист персональних даних.*

1. Introduction

Since the beginning of the military conflict in a hybrid war in Ukraine, the development of the regulatory framework has intensified, which generally contributes to the legislative provision of information security. In 2015–2018 was taken:

– National Security Strategy of Ukraine (2015) [1];
– Cybersecurity Strategy (2016) [2];
– Doctrine of information security of Ukraine (2016) [3];
– The Law of Ukraine «On the Basic Principles of Ensuring the Cyber Security of Ukraine» (2017) [4];
– The Law of Ukraine «On the National Security of Ukraine» (2018) [5].

The Decree of the President of Ukraine «On the National Security Strategy of Ukraine» identifies threats to information security and information resources [1]:

– waging information war against Ukraine and the lack of a coherent communicative policy of the state, an insufficient level of media culture of the society;
– vulnerability of critical infrastructure, state information resources in cyber-attacks;
– physical and moral obsolescence of the system of protection of state secrets and other types of information with limited access;
– critical depreciation of fixed assets of infrastructure facilities in Ukraine and an insufficient level of their physical protection;
– insufficient level of protection of critical infrastructure against terrorist attacks and sabotage;
– ineffective security management of critical infrastructure and life support systems.

The Doctrine defines a number of the most significant and urgent threats to the national interests and national security of Ukraine in the information sphere [3]:

– informational operations;
– demoralization;
– provoking;
– interethnic and interfaith conflicts;
– negative image;
– informational expansion;
– insufficient level of development of information infrastructure and ineffective information policy;
– calls for radical actions of the population;
– other threats.

These threats require continuous monitoring and evaluation.

The Law of Ukraine «On National Security» [5] provides for the direction of state policy to ensure information security and cyber security of Ukraine. This law

defines the concept of «cyber-threat indicators – indicators (technical data) used to identify and respond to cyber threats», but there is no list of indicators that would make it possible to identify the level of information security of the infrastructure of entities of various forms of ownership. In the Doctrine of Information Security of Ukraine and in the Decree of the President of Ukraine [1], one of the priority directions of the state policy in the information sphere is the creation of an integrated system of information threat assessment and rapid response to them. Another important direction is the «monitoring of cyberspace with the goal of timely detection, prevention of cyber threats and their neutralization». The Ministry of Information Policy of Ukraine notes the need to create an integrated system for assessing and monitoring threats in the information space of Ukraine, which will make it possible to make effective management decisions to state bodies in critical situations [6].

According to the Sustainable Development Strategy of Ukraine – 2020 [7], the strategic indicator of the implementation of the Strategy in the information sphere is the share of broadband Internet penetration. The indicator is calculated according to the World Bank. The figure should be 25 subscribers per 100 people in 2020. In addition, 20 films of Ukrainian production should go into wide release in 2020. In addition, the Strategy provides for the popularization of Ukraine in the world, the promotion of Ukraine's interests in the global information space, the development of media and the information society.

Accordingly, the development of a system for monitoring and evaluating the development of information infrastructure in Ukraine is an urgent task that needs to be addressed due to the need to timely identify information threats and response measures to them.

2. The object of research and its technological audit

The object of research is a system for monitoring the development of information infrastructure in order to ensure the information security of the country and its components. Components of the monitoring system are information threat indicators and information security level indicators. One of the most problematic places is the lack of an integrated system for assessing the development of information infrastructure, which makes it impossible to timely identify information threats and timely respond to them. There is also no approach to assessing the level of development of information infrastructure in Ukraine.

3. The aim and objectives of research

The aim of research is assessing the development of information infrastructure in Ukraine.

The main objectives of research are:

1. Formation of a system of indicators for assessing the level of development of information infrastructure in the context of business entities.

2. Highlighting the main trends in the development of information infrastructure in Ukraine.

3. Formation of directions for improving the state policy of the authorities for the development of information infrastructure.

4. Research of existing solutions of the problem

During 2014–2019 the attention of scientists on the issue of information threats and information security in Ukraine has increased. In a number of works [8, 9], the state of the information infrastructure and the level of information protection in the context of business entities of Ukraine are highlighted and systematized, directions for ensuring information security and ways to counter information threats are proposed.

In work [10] the main information threats of external sources are systematized:

– unauthorized access to information, information infrastructure;
– insufficient level of awareness of the population about the internal political and foreign policy activities of Ukraine;
– spread of misinformation;
– informational impact of structures in various fields;
– violation of the rights of Ukrainian business entities in the field of information security.

The author of [9] justifies the need to monitor threats to national security and identified the monitoring technology as a process of «gathering, storing and analyzing information necessary for effective management».

In Ukraine, there are no developments on the integral indicator of the development of information infrastructure and its main components. The proposed system of indicators will allow a comprehensive assessment of the development of the information infrastructure of the country in the context of the main actors. Information security can be viewed from the point of view of the interaction of subjects and objects. According to this approach, information security is the protection of information, supports the infrastructure from accidental or intentional impact of a natural or artificial nature, and can harm the subjects of information relations. Thus, from the presented definition, it follows that information threats arise in the event of an insufficient level of information protection of subjects of informational relations as a result of various impacts due to an insufficient level of infrastructure development. The information protection level of subjects can be assessed on the basis of monitoring the state of development of information and communication technologies. This will indicate a sufficient or low level of information protection, the degree of impact on objects of information threats. Such an approach will ensure that the need to improve specific areas of government policy to counter them is established [3].

Scientists have proposed a number of methods for monitoring the information space to identify information threats in the information space of Ukraine. Thus, the authors of the studies [11, 12] propose to carry out content monitoring of the information space based on the analysis of information in the media, publications on the Internet, sources of publications and their consequences. [13, 14] note the need to develop models for assessing the impact of information threats on certain areas of social activity in Ukraine for their timely detection and neutralization by means of the state information security system. It is also noted in [15]: «timely monitoring of the nature, characteristics, scale of threats and their forecasting are important for ensuring national security».

ISSN 2226-3780

Among the main directions of solving this problem, identified in the resources of the world scientific periodicals, research can be highlighted [16], but they do not consider the indicators for monitoring information threats. The author of these studies only notes the types of information about cyber threats, that is, the work identified the sources of threats without indicating the level of their danger.

[17] identifies key information threats and problems in the information sphere, but there is an unresolved question of their assessment and criticality.

And on the impact of new technologies on the level of information security and threats to information infrastructure facilities is indicated in [18]. However, in this work the degree of information security in the conditions of digitalization is not fully disclosed. The authors of the work [19] show that cloud computing and technologies pose a threat to information security and create a number of risks. The authors of this work also consider risk assessment schemes based on a reverse approach, minimizes such risks at minimal cost, but the question remains of assessing the risks of other technologies: «big» data analysis technology, social media, websites.

An alternative solution to the problem, described in [20], provides for the creation of an information model for monitoring threats to national security. The author offers methods of discrete mathematics and statistical analysis of threat assessment. However, the results obtained do not contain requirements for systems for monitoring and assessing information security threats.

Methods of the impact of various information and communication technologies on the safety of economic agents are shown in [21]. However, in this work there are no parameters for the degree of such influence on the information security of the subjects of the information infrastructure. The authors of the work [22] emphasize the importance of using an integrated strategic approach for developing a methodology for identifying potential hybrid threats. Although this statement can be considered in the context of information threats.

Thus, the results of literary analysis suggest that scientists propose a number of approaches, methodologies and methods for assessing and identifying threats, as well as detail information threats and the impact of new technologies on information security. And they offer risk assessment schemes and threat assessment information models. From which it is possible to conclude that the development of a system for assessing and monitoring the state of the information infrastructure in Ukraine is a promising task.

5. Methods of research

Statistical analysis of information infrastructure development indicators and the level of information threats are used in research. Based on the methods of analysis and synthesis of scientists' works, the main trends in the development of the information infrastructure in Ukraine, the directions of improving the state policy of countering information threats in Ukraine are summarized. And also the need to develop a system of indicators for monitoring the quality of public policy is highlighted.

6. Research results

The Ministry of Information Policy of Ukraine is supposed to organize and ensure monitoring of threats to national interests and national security in the information sphere in the established manner [1]. In addition, the division of the State Cyber Defense Center of the State Special Communication Service CERT-UA [23] is charged with monitoring and identifying, accumulating and analyzing data on cyber threats.

Assessment of the state of protection of state information resources in state bodies, local governments, military units, enterprises, institutions and organizations, regardless of ownership, is carried out in accordance with the annual plan, which is approved by order of the State Service for Special Communication Administration.

To monitor (evaluate) the development of information infrastructure in Ukraine, a system of indicators for assessing the level of information security in the context of business entities was formed. The main indicators in Ukraine include:

1) N_s – the number of communication subscribers, in particular the Internet, including the number of Internet subscribers by region, characterizing the number of points of potential information security (IS) threats on a territorial basis;

2) P_{bb} – provision of the population with broadband Internet access. The indicator reflects the presence and ability to use and prevent problems in the field of information and communication technologies (ICT) and generally reflects the level of potential threats in the information sphere. The growth of the index indicates an increase in the level of threats to the population's misinformation in Ukraine;

3) N_e – the number of enterprises that used computers, units; the proportion of enterprises that used computers, in % of the total number of enterprises that participated in the survey. The indicator reflects the ability to use reliable means of protection and control in the field of computer security as one of the components of information security;

4) N_a – the number of enterprises that had access to the Internet, units, and the share of enterprises that had access to the Internet, in % of the number of enterprises that used computers. Indicators characterize the level of potential threats to IS of enterprises, institutions and organizations;

5) N_{sp} – the number of enterprises that had specialists in the field of information and communication technologies: characterizes the ability of enterprises to protect information and information infrastructure through self-financing;

6) N_{web} – the number of enterprises that had a website that operated on the Internet, reflecting the level of the company's modern development, the capabilities of enterprises in different business lines, units (Fig. 1). The development of e-commerce contributes to the development of Ukrainian enterprises, but at the same time points to the defeat of potential information threats;

7) U_{sn} – use of social media in enterprises, which characterizes the degree of integration of enterprises in the media space and the capabilities of enterprises in different activities, units (Fig. 2). A fairly significant proportion of enterprises use social media, which simultaneously have the opportunity to have a negative impact on the internal environment and the information infrastructure of companies;

8) N_{cc} – the use of cloud computing services as a whole characterizes the financial capabilities of enterprises and their technological level of development, affects the state of private information infrastructure in Ukraine (Fig. 3). Cloud services, technology and computing greatly simplify the work of enter-

prises and streamline business processes. The technological level of development of Ukrainian enterprises is growing, ensuring the development of the information infrastructure in Ukraine of the private sector, and therefore indicates the possibility of financing information security measures;

9) N_{bd} – statistics of the analysis of «big data» by enterprises, characterizing the state of information security of business entities, in particular, individuals and legal entities (Fig. 4). The use of data by enterprises for the purposes of developing activities at the same time may violate the information security of other entities, and therefore state authorities should improve the personal data protection policy. This should include the use of data in the required amounts and not harm citizens.

The system of indicators for assessing and monitoring the state of effectiveness of the implementation of state policy by the authorities in countering information threats is defined, which allows analyzing the main trends in the level of information security in the context of the main subjects of the information space of Ukraine (Table 1).

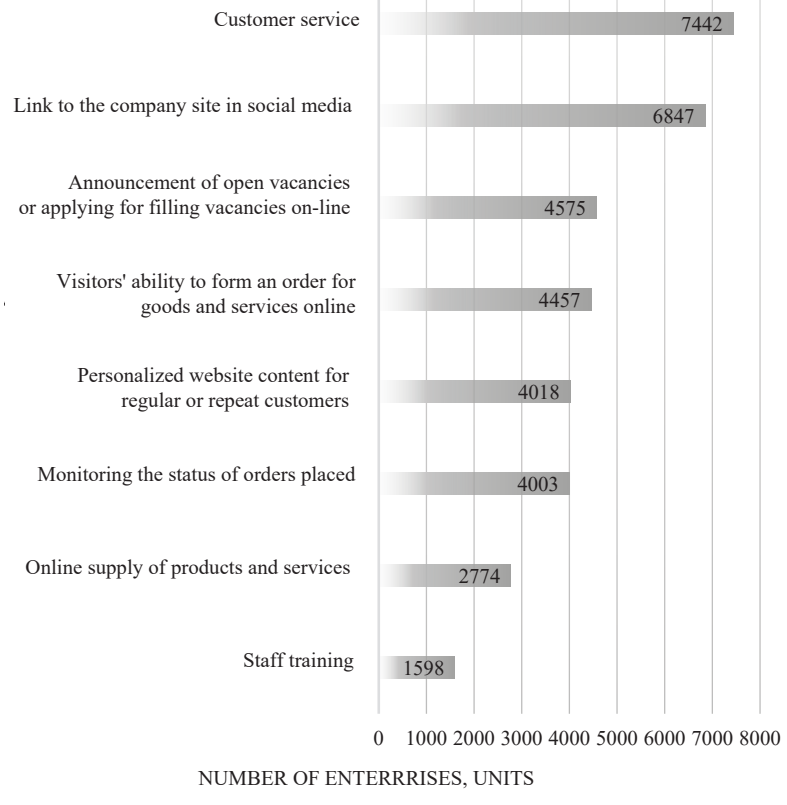

Fig. 1. The number of Ukrainian enterprises that had a website that functioned on the Internet in terms of site capabilities in 2017 [24]

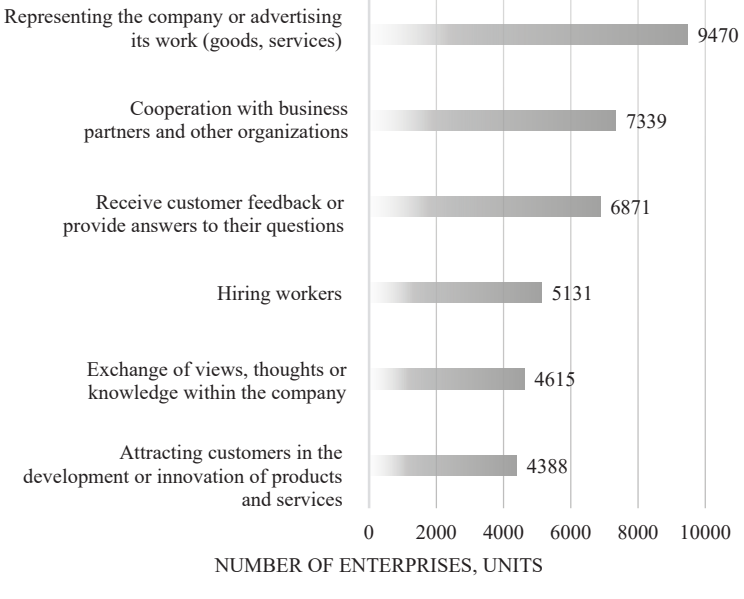

Fig. 2. The use of social media in enterprises of Ukraine for the purpose of use in 2017, units [24]

ISSN 2226-3780

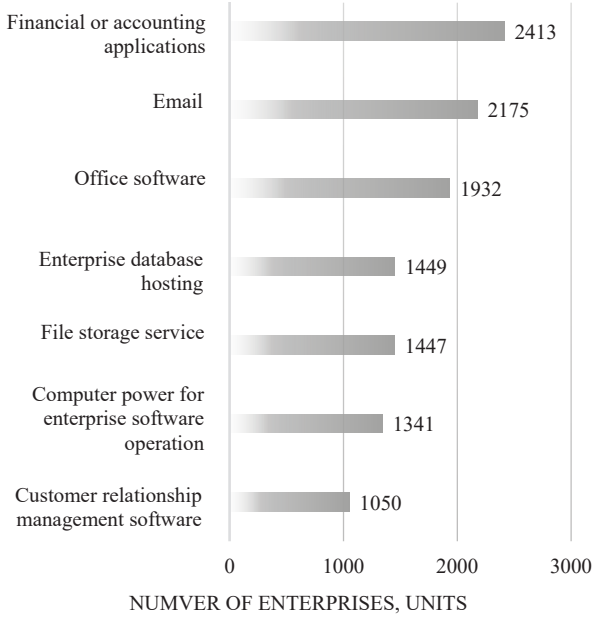

Fig. 3. The number of enterprises buying cloud computing services during the year in terms of services in Ukraine in 2017, units [24]

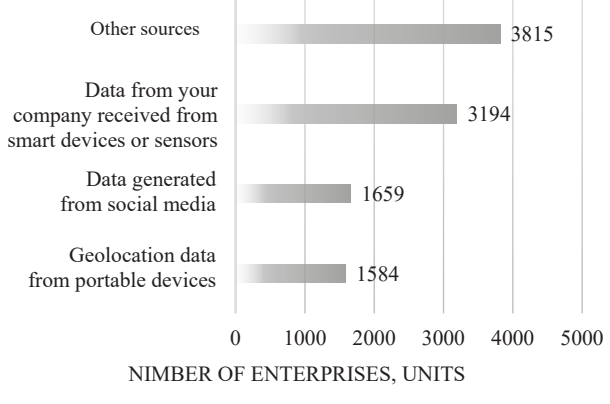

Fig. 4. The number of enterprises that conducted the analysis of «big data» according to sources for analysis in Ukraine in 2017, units [24]

The data in the Table 1 indicate a weak level of development of information and communication technologies in Ukraine. Only more than half of the population of Ukraine has access to the Internet. Enterprises are characterized by a high level of information and communication technologies, they actively use the Internet for various purposes. This indicates the development of private information infrastructure, which requires effective protection against information threats from the state. Ukrainian enterprises are actively using websites and social media to promote their products on the Internet, and this indicates potential risks of threats in the information space.

Table 1

The system of indicators for monitoring the development of information infrastructure in Ukraine in 2017

No.	Indicator	Unit	2017
1	N_s	thousand people	23632.3
2	P_{bb}	thousand people	22625.8
3	N_e	–	–
3.1	Number of enterprises using computers	units	40327
3.2	Share of enterprises using computers	in % of the total number of enterprises	95.4
4	N_a	–	–
4.1	Number of enterprises that have access to the Internet	units	39582
4.2	Share of enterprises that have access to the Internet	in % of the total number of enterprises	98.2
5	N_{sp}	units	10660
6	N_{web}	units	16240
7	U_{sn}	units	23849
8	N_{cc} Number of enterprises buying cloud computing services during the year	units	4135
9	N_{bd}	units	–
9.1	Number of enterprises that conducted the «big data» analysis	units	10252
9.2	Number of enterprises in which the «big data» analysis was carried out	units	8526

Note: developed based on data from [24–26]

Fig. 5 reflects the dynamics of fixed broadband Internet access in Ukraine in 2005–2017.

There is a positive growth trend in fixed broadband Internet access in Ukraine in 2005–2017. However, the share of Internet penetration according to the Internet Association of Ukraine was 65 % as of August 2017 (in cities with a population of over 100,000 people – 75 %, in villages – 54 % [27]). The number of Internet subscribers as of October 1, 2018 is 26014.9 people [24].

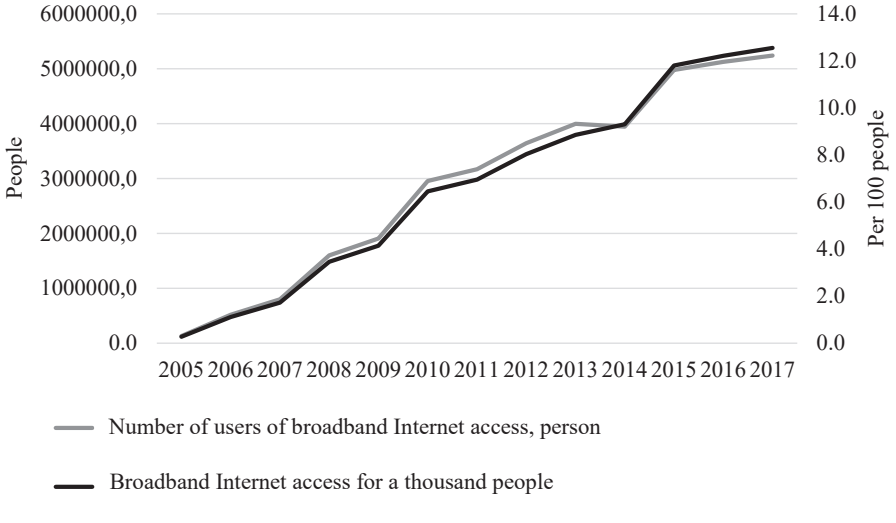

Fig. 5. Dynamics of fixed broadband Internet access in Ukraine in 2005–2017 (per 100 people) [26]

The author of [10] notes that in Ukraine the development of the Internet is hampered due to negative factors, namely: outdated telecommunication networks, a low level of computerization, and low incomes of the population. Therefore, citizens may be subject to misinformation and propaganda from other information sources. If we consider the statistics of the number of Internet subscribers by regions in Ukraine (Table 2), then the largest number in more developed areas is Kyiv (13 %), Odessa (11 %), Donetsk (8 %), Dnipropetrovsk (7 %), Lviv (6 %), Kharkiv (6 %), Kyiv (4 %).

Table 2

Number of subscribers on the Internet for regions in Ukraine in the January 1 of 2019

Regions	Total	Of them				
		Home	In rural areas		With broadband access	
			Total	Including home	Total	Including home
Ukraine	26066.8	23354.2	652.9	629.5	25312.7	22861.1
Vinnytsia	968.2	862.1	31.0	29.6	929.4	836.9
Volyn	576.3	513.2	11.5	10.9	558.7	501.8
Dnipropetrovsk	1796.5	1608.1	16.2	15.7	1746.2	1575.9
Donetsk	1800.4	1608.6	16.6	16.3	1788.4	1600.6
Zhytomyr	689.7	616.2	28.4	28.0	669.1	603.0
Zakarpattia	583.7	520.2	21.6	20.9	575.6	514.9
Zaporizhzhia	865.1	771.4	23.2	22.2	855.5	765.2
Ivano-Frankivsk	659.8	589.4	33.8	32.8	651.7	584.2
Kyiv	1215.3	1088.9	19.2	18.9	1146.4	1044.3
Kirovohrad	465.7	415.3	6.5	6.0	459.1	411.0
Luhansk	913.4	814.3	3.8	3.5	907.5	810.5
Lviv	1664.8	1475.6	82.0	78.9	1588.4	1425.6
Mykolaiv	800.7	723.1	8.6	8.2	768.4	702.3
Odesa	2688.6	2438.6	56.5	54.9	2610.0	2388.3
Poltava	749.8	667.3	40.2	38.6	735.1	656.4
Rivne	593.3	529.0	25.5	24.5	579.1	519.7
Sumy	548.4	489.0	9.7	9.2	539.4	483.1
Ternopil	511.7	454.8	38.0	35.1	505.8	451.0
Kharkiv	1582.4	1402.2	21.7	21.2	1522.9	1363.7
Kherson	534.5	476.4	21.7	20.4	524.6	469.1
Khmelnytskyi	653.1	581.3	13.9	13.3	641.4	573.7
Cherkasy	692.1	614.4	15.8	15.0	667.9	598.8
Chernivtsi	421.0	377.4	17.9	17.4	416.2	373.7
Chernihiv	673.7	599.9	13.7	13.2	642.8	579.9
City of Kyiv	3418.6	3117.5	75.9	74.8	3283.1	3027.5

Note: developed based on data from [26]

According to the National Commission for Government Regulation in the Field of Communication and Information, these regions have the highest density of telecommunications service providers [28, 29] (in 2017). Therefore, the subjects of these regions may be exposed to information threats to a greater extent. This requires the establishment of priorities for regional information security and the financing of activities primarily in these regions.

7. SWOT analysis of research results

Strengths. The strengths of the research to assess the development of information infrastructure:

– key threats to information security are identified;
– state of information security of the subjects of the information infrastructure is assessed;
– priority information infrastructure facilities are identified that require funding and increase information security; provides identification of key threats to the information infrastructure;
– level of technological deterioration of information infrastructure facilities is revealed;
– level of computerization of the private sector of information security us revealed;
– level of technological equipment and enterprise development is revealed;
– integration degree of enterprises in the media space is determined.

Weaknesses. Weaknesses of the research conducted to assess the development of information infrastructure:

– there is no analysis of information for assessing indicators that allow to evaluate information threats to objects that exist in the media space;
– lack of indicators for the development of information infrastructure in the regional context;
– there are no data for the last time periods.

Opportunities. Opportunities for further research of the information infrastructure development monitoring system:

– development of an integral indicator for assessing the development of information infrastructure based on indicators of the monitoring system;
– development of a forecasting model for the development of information infrastructure;
– development of a model for automating the process of calculating indicators for monitoring the development of information infrastructure;
– reduction of costs for countering information threats in the context of timely monitoring of critical threats based on the developed system of indicators;
– possibility of timely response to existing information threats to information infrastructure facilities.

Threats. Threats to the monitoring system of the development of information infrastructure:

– rapid pace of development of ICT leads to the transformation of threats to information infrastructure facilities, and this requires the inclusion of new indicators in the monitoring system;
– inclusion of new indicators requires time-consuming to evaluate them, finding sources for collecting information for assessing indicators;
– substantial amounts of funding to assess the performance of the monitoring system for the development of information infrastructure in the information space;
– essential costs of conducting research and collecting information on existing information threats to information infrastructure facilities.

8. Conclusions

1. A system of indicators for assessing the level of development of information infrastructure in the context of business entities is formed. This system includes indicators for monitoring the level of information security

ISSN 2226-3780

and the level of information threats in the context of the main business entities.

2. The main trends in the development of information infrastructure in Ukraine are highlighted. The estimated values of the monitoring system indicators make it possible to argue about the need to finance the information infrastructure of the private sector. This will increase the level of public access to the Internet and ensure the protection of personal information, eliminate the impact of propaganda and disinformation of the population. The development of the information infrastructure of enterprises and technologies in the information sphere is proceeding at a rapid pace. This is due to the following factors: the growing level of computerization, technological re-equipment, the use by enterprises of social media and the analysis of «big data», cloud technologies and computing. New technologies simultaneously allow to automate business processes of processing and analyzing information and serve as a source of threats to internal information and information infrastructure.

3. The main directions of improving the state policy of the authorities for the development of information infrastructure are formed, which include:

– protection of personal data of the private and public sectors;

– stimulating the development of private sector information infrastructure facilities;

– development of public-private partnership in order to develop information infrastructure.

References

1. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy No. 287/2015. 06.05.2015 / VR Ukrainy // Baza danykh «Zakonodavstvo Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/287/2015#n14
2. Stratehiia kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy No. 96/2016. 27.01.2016 / VR Ukrainy // Baza danykh «Zakonodavstvo Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11
3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy No. 47/2017. 29.12.2016 / VR Ukrainy // Baza danykh «Zakonodavstvo Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/47/2017
4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy No. 2163-VIII. 08.07.2018 / VR Ukrainy // Baza danykh «Zakonodavstvo Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/2163-19/conv
5. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy No. 2469-VIII. 21.06.2018 / VR Ukrainy // Baza danykh «Zakonodavstvo Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/2469-19?lang=en
6. Zolotukhin D. Monitorynh zahroz u informatsiinomu prostori dopomozhe efektyvnishe spravliatysia z krytychnymy sytuatsiiamy. 2018. URL: https://mip.gov.ua/news/2431.html
7. Pro Stratehiiu staloho rozvytku «Ukraina – 2020»: Ukaz Prezydenta Ukrainy No. 5/2015. 12.01.2015 / VR Ukrainy // Baza danykh «Zakonodavstvo Ukrainy». URL: https://zakon.rada.gov.ua/laws/show/5/2015
8. Dougan O. D. Legal bases of formation and development of information security // Information security man, society and the state. 2015. Issue 3 (19). P. 6–17.
9. Kobko Ye. V. Monitoring of Threats to the State National Security: Foreign Experience and Ukrainian Realities of Public-Legal Provision // Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav. 2018. Issue 1 (106). P. 122–134.
10. Kovalova K. V., Pershko O. L. Proektnyi menedzhment: sotsialne proektuvannia innovatsii v orhanizatsiiakh // Financial mechanisms of innovative economic development of Ukraine in conditions of European integration. Kyiv, 2018. P. 275–277.
11. Molodetska-Hrynchuk K. V. Analysis of influence threats of an information security of the state in a social internet-service to the spheres of public activities // Upravlinnia rozvytkom skladnykh system. 2017. Issue 30. P. 121–127.
12. Fedorenko R. M. Kontent-monitorynh informatsiinoho prostoru yak chynnyk zabezpechennia informatsiinoi bezpeky derzhavy u voiennii sferi // Suchasnyi zakhyst informatsii. 2015. Issue 2. P. 21–25.
13. Pakhnin M. L. Pryntsypy, zavdannia ta instrumenty derzhavnoi informatsiinoi polityky Ukrainy v suchasnykh umovakh // Teoriia ta praktyka derzhavnoho upravlinnia. 2014. Issue 3. P. 87–95.
14. Tkachuk T. Yu. Mekhanizmy protydii informatsiinym zahrozam zovnishnikh dzherel // Visnyk NTUU «KPI». 2017. Issue 1/2 (33/34). P. 242–246.
15. Tkachuk T. Suchasni zahrozy informatsiinii bezpetsi derzhavy: teoretyko-pravovyi analiz // Informatsiine pravo. 2017. Issue 10. P. 182–186.
16. Rizov V. Information Sharing for Cyber Threats // Information & Security: An International Journal. 2018. Vol. 39, Issue 1. P. 43–50. doi: http://doi.org/10.11610/isij.3904
17. Parker D. B. A Comprehensive List of Threats To Information // Information Systems Security. 1993. Vol. 2, Issue 2. P. 10–14. doi: http://doi.org/10.1080/19393559308551348
18. Fried L. Information security and new technology Potential Threats and Solutions // Information Systems Management. 1994. Vol. 11, Issue 3. P. 57–63. doi: http://doi.org/10.1080/07399019408964654
19. Kar J., Mishra M. R. Mitigating Threats and Security Metrics in Cloud Computing // Journal of Information Processing Systems. 2016. Vol. 12, Issue 2. P. 226–233. doi: http://doi.org/10.3745/jips.03.0049
20. Suchkov A. P. The information structure of threats to national security // Systems and Means of Informatics. 2017. Vol. 27, Issue 2. P. 113–124. doi: http://doi.org/10.14357/08696527170210
21. Dainow B. Threats to Autonomy from Emerging ICTs // Australasian Journal of Information Systems. 2017. Vol. 21. P. 1–16. doi: http://doi.org/10.3127/ajis.v21i0.1438
22. Monov L., Karev M. How to Counter Hybrid Threats? // Information & Security: An International Journal. 2018. Vol. 39, Issue 2. P. 113–126. doi: http://doi.org/10.11610/isij.3909
23. Pidrozdil Derzhavnoho tsentru kiberzakhystu Derzhspetszviazku CERT-UA. URL: https://cert.gov.ua/
24. Vykorystannia informatsiino-komunikatsiinykh tekhnolohii na pidpryiemstvakh za 2017 rik. URL: http://www.ukrstat.gov.ua
25. Kilkist abonentiv zviazku na 1 zhovtnia 2018 roku. URL: http://www.ukrstat.gov.ua
26. Stan i rozvytok zviazku za 2017 rik. URL: http://www.ukrstat.gov.ua
27. Ofitsiinyi sait Internet Asotsiatsii Ukrainy. URL: https://inau.ua/pro-asociaciyu
28. Provedeno opratsiuvannia zvitiv operatoriv pro yakist telekomunikatsiinykh posluh za 2017 rik. URL: http://spz.nkrzi.gov.ua/golovna/yakist-poslug/dani-pro-yakist/
29. Obsiah realizovanykh posluh u sferi telekomunikatsii ta poshtovoho zviazku za 9 misiatsiv 2018 roku. URL: http://www.ukrstat.gov.ua

Prav Roman, *Postgraduate Student, Department of Management and Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine, e-mail: romaprav@gmail.com, ORCID: http://orcid.org/0000-0001-8064-2836*