Computer Science Trends and Innovations in Computer Engineering against the Backdrop of Russian Armed Aggression

Bannikov Valentyn[1] Zalialetdzinau Kanstantsin[2], Siasiev Andrii[3], Ivanenko Ruslan[4], Saveliev Dmytro[5]

[1]Dataart Solutions, Inc 475 Park Avenue South Floor 15 New York, NY 10016 United States,
[2]Brimit LLC
[3]Oles Honchar Dnipro National University Faculty of Mech & Math Department of Differential Equations Gagarina ave., 72, Dnipro, Ukraine, 49010
[4]Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine, Kyiv, Ukraine, Vasylenko 3, 03113
[5]National University of Civil Defence of Ukraine, Faculty of Operational and Rescue Forces, Department of Engineering and Rescue Machinery 94, Chernyshevska St. Kharkiv Kharkiv Region Ukraine 61023

Summary
Relevance. The research implemented in this article focuses on the problem of freeing the cyber-digital space of Ukraine from the parasitic influences of digital means, the developers and owners of which are the relevant companies of the aggressor state - the Russian Federation. A certain direction of the research is particularly acute against the background of unprovoked large-scale armed aggression, which casts doubt on the speedy resumption of cooperation with representatives of the hostile country's IT cluster. **Objective.** The purpose of the study is to identify vulnerable sectors and determine the vector of development of digital tools that can be safely used on the territory of Ukraine, taking into account the hostile actions of the aggressor state. **Methods.** Determination of the priority vector of development of digital tools and cyber sciences of Ukraine is determined by using methods of statistical research, information research, and analytical definitions, which in the final goal form and target the actual needs of the domestic IT cluster not only in the circumstances of Russian armed aggression but further innovation in achieving civilizational progress and the realization of state interests. **Results.** The results of the study identify sectors of the cyber-digital sphere of Ukraine, which require the urgent intervention of specialized professionals to free certain industry digital tools from the compromised software of the aggressor state, as well as define target goals for further development of the digitalization of Ukraine as a comfortable smart environment, attractive for investment attraction and rapid development Scientific novelty / Scientific novelty.
The novelty of the study is determined by the information-analytical research of the functioning of the cyber-digital space of Ukraine under the Russian aggression, which is manifested not only by armed attacks, but also hybrid attacks, including the use of information and digital threats to state and civil infrastructure with the threats of direct impact on the cyberphysical systems of the state level of differentiation. Practical significance. Based on the results of the study, analytical conclusions and practical recommendations are formed, defining immediate measures to ensure state policy of cyber security and further direction of digital innovation, defining and implementing state goals and priorities. **Conclusions.** Analysis of the current state of functioning of Ukraine's cyber-digital space in the context of large-scale armed aggression of the Russian Federation exposes a number of problems that threaten state security and contradict state interests. Accordingly, a number of recommendations have been developed, aimed both at applying urgent measures to ensure state digital security and determining the vector of further future development of Ukraine's digital industry as a comfortable investment-attractive state with high integration of digital means in a reasonable environment.

Keywords
Digital tool, cybersecurity, attack, vector, development, politics, smart environment.

1. Introduction

Ukraine is a developed digital state, as evidenced, in particular, by the recognition of the success and celebration of the global-state service "Diia" [1] by such profile global awards as Emerging Europe Awards 2022 [2], D&AD Awards 2022 [3], Cannes Lions 2022 [4] Moreover, as defined in the study of digital development of smart media [5], our state is at the top of the smart environment, introducing such global-state services as "Diia. City", "Diia. Business" (a category of "smart grid" according to the classification definition [5]), "E-Resident", "Diia. Digital education" (category "smart living" according to the classification definition [5]), "Helsi", "eHealth" (category "smart healthcare" according to the classification definition [5]), "eDopomoga", "Diia" proper (category "smart government" according to the classification definition [5]) [6]. Hybrid (since February 2014) and military (since February 2022) aggression of the Russian Federation has exposed a number of problems of the Ukrainian cyber space, which require urgent adequate measures:
– significant diffusion of diversified digital tools, the developers of which are organizations of the Russian Federation into the cyber space of Ukraine, which pose a

Manuscript received September 5, 2022
Manuscript revised September 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.9.60

potential danger and can be used by the enemy for hybrid attacks on both the information and digital space, and on cyber-physical systems of different levels of differentiation [7 – 9];
– dependence of core industries on the digital means of the aggressor state, which creates economic threats and disruptions in the functioning of certain economic activities [10];
– the inertia of the state digital policy, which in previous years did not have a clear definition of state interests in the digital industry and appropriate incentives for the development of a competitive domestic IT cluster [11].
The study and solution of certain problems affecting not only aspects of state security, but also directly affecting the economic mechanisms of the country is an extremely urgent task, which requires the adoption of urgent adequate measures that meet state interests.
The purpose of the study is to identify priority and future actions for the development of Ukrainian cyberspace, taking into account current security circumstances and modern achievements of the domestic IT cluster.
Study objectives:
– analytical study of the depth of diffusion of software and digital tools of developers from the Russian Federation in the cyber-digital space of Ukraine, taking into account the current security situation;
– identification of critical sectors of the Ukrainian digital infrastructure, subject to the greatest diffusion of digital means of the Russian Federation, requiring the urgent application of appropriate means to remove potentially hostile elements and replace them with alternative developments of Ukrainian developers and developers, whose countries do not infringe on the security and sovereignty of Ukraine;
– based on the analysis of the allocated information array regarding the defeat of cyberspace of Ukraine by digital means of the Russian Federation to develop appropriate recommendations, which should be differentiated by priority: first-priority - for sectors that control critical infrastructure facilities, and promising - defining the current vector of development of the Ukrainian digital environment.

2. Materials and Methods

Basic concepts and research methods of the processes of cyberdigital security paradigm formation in the focus of digital tools and specialized software are formed taking into account the provisions of modern studies of domestic [12 - 14] and foreign [15 - 18] authors based on the approved legal framework in Ukraine, in particular: Law of Ukraine from 21. 06.2018 No. 2469-VIII [19], Law of 05.10.2017 No. 2163-VIII [20], Law of 16.11.2021 No. 1882-IX [21], Law of 12.12. No. 1089-IX [22], Cyber Security Strategy of Ukraine [23], DSTU ISO/IEC 27032:2016 [24], and others.

Armed aggression of the Russian Federation is accompanied by numerous hybrid attacks, among which the information-digital vector of defeat, which can be introduced by the activation of harmful actions of "passive agents" - digital means, which are official software of Russian developers, acquired and involved in various public and private sectors. activities even before the beginning of hostile actions. These software-digital means have a potential danger because in addition to directly harmful actions can collect and transfer to the relevant digital repositories of the Russian Federation confidential data related to both private or economic activities, and data with signs of state secrets and/or state interests. Consequently, it is advisable and logical to direct the study of the cyber-digital space of Ukraine for the diffusion of Russian software and digital tools, which carry the potential threat of the above-mentioned "passive agents".

According to research data [25 - 28], Ukrainian users, despite the already open (since 2014) aggression of the Russian Federation, still actively use in their activities software and digital tools developed by a hostile country, which is also recorded as a potential threat to state security even by foreign researchers [29 - 36]. According to Opendatabot [28], currently, the most used 44 Russian software developments, among which the most common are Bitrix, 1C, AmoCRM, iiko, Jivosite, and others. This dominance of Russian software in the cyber-digital space of Ukraine forms the preconditions for the potential emergence of subsequent threats and critical situations:
– direct harmful influence of "passive agents" of a hostile country on cyber-physical systems of different (including state-wide) levels of differentiation;
– use of features of distributed software known only to developers of the Russian Federation (due to trade secrets), which does not allow without unauthorized interference to determine the degree of security of the code body of software and digital means, and also creates conditions in which these developers can use the vulnerabilities of software products known only to them. with the purpose of destructive influence on the cyber-digital infrastructure of Ukraine;
– use of software and digital products by Russian developers as integrated spies to control and monitor individual infrastructure and information flows and steal individual sensitive data of strategic importance;
– the use by integrated Russian digital assets of servers and cloud storage controlled by a hostile state poses a recurring threat of leaks of sensitive data, both private and public.
Consequently, it becomes logical and expedient to search for alternatives to the aforementioned "passive agents. Opendatabot [28] in cooperation with Netpeak Group [37] with the support of the Ministry of Digitalization [6] developed a list of alternative Russian software-digital tools, which now includes 62 items with found safe analogs of domestic and friendly in Ukraine developers

(#ReplaceRUwithUA) [38]. The list of #ReplaceRUwithUA software highlights the following areas [28, 38]: CRM, accounting systems, asset accounting (EAM/CMMS), end-to-end analytics, POS systems, Email marketing, screenshot/file sharing, antivirus, AI services, educational platforms, corporate social media, online translator, webinar platform, social media monitoring, B2B lead generation, personal finance, website builder, LMS platform, Collaboration, content services, image hosting, SEO, web analytics, chatbots, CRM for beauty, ad blockers, software for hotels, mobile application promotion, task and project management, CRM for e-commerce, CMS for auto sites, the search engine for candidates, CRM for medicine, software for farmers, DLP, etc.

In contrast to the above-mentioned management-organizer software products, engineering digital tools of Russian development could not achieve significant diffusion into the Ukrainian engineering cyberspace, on the contrary, the specialized Ukrainian software has received almost no alternative use in the territory of Russia: the vivid representatives of this phenomenon are PC Lira-SAD, developer of LIRALAND [39] and SCAD Office, developer of SCAD Structure [40], accredited in Russia to perform structural design and simulation In the territory of Ukraine, the software product Compass-3D by the developer ASCON is widely spread, however, even this software has not occupied a dominant position, as it is not technically [50] able to provide speed and functionality of the industry leader AutoCAD by the developer Autodesk [41], on the contrary, the software heritage of the USA tends to displace from the profile sector of the Russian software market [42].

3. Results

According to Opendatabot [43], the Ukrainian IT sector is the only sector of economic activity that was able to achieve an increase in profits in 2022 in a full-scale war compared to the same period last year - Fig. 1.

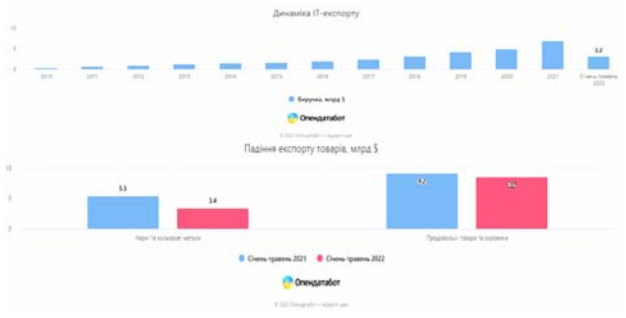

Fig. 1. Dynamics of export indicators of Ukraine's IT sector under martial law in comparison with other leading sectors of economic activity [43]

The significant potential of Ukraine's IT cluster is noted by Outsourcing Journal [44] (first place in IT outsourcing in Central and Eastern Europe by results of 2017), Good Country Index [45] (first place in the world by contribution to science and technology development), IT Ukraine Association [46] (average growth of export potential of IT services in Ukraine is 27% per year) and other ratings - Fig. 2.

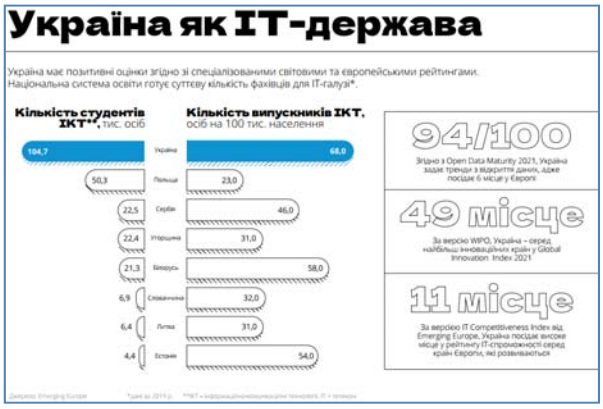

Fig. 2. Ratings of Ukraine as an IT country [46]

According to the data [46 - 48], the modern profile of the IT sector in Ukraine is marked by a significant service (including cloud services), less engaged in the development of their own software products - Fig. 3.

The development of the IT sector cannot be without the attention of the state, because in the actual and forecasted dynamics of economic activity forms indicators that are significantly higher than the basic budget-forming industries - Fig. 4.

It is the significant impact of the economic performance of the IT sector in Ukraine that prompts the state to pursue regulatory and stimulative policies through appropriate legislative initiatives, as example - Law of Ukraine No. 2075-IX of 17/02/2022 [49].

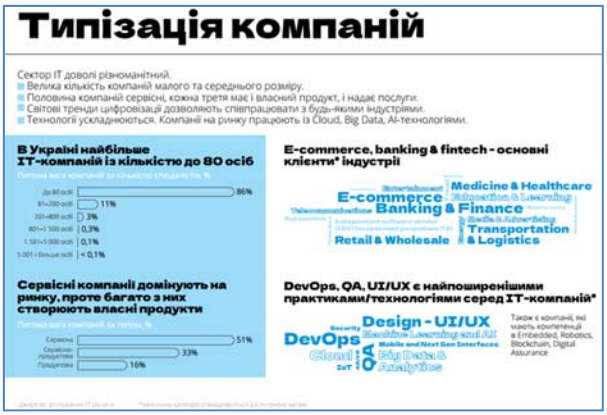

Fig. 3. Profiling of the IT sector in Ukraine [46]

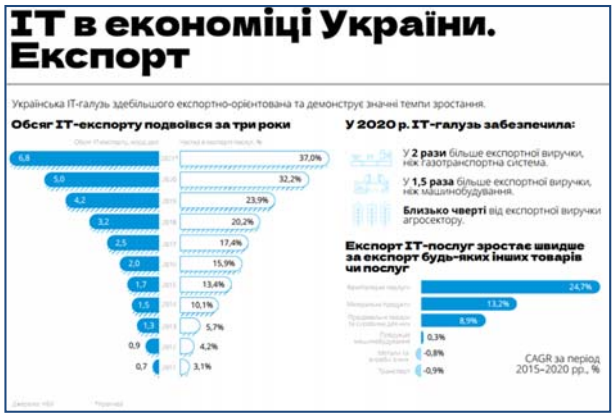

Fig. 4. Economic achievements of the IT sector in Ukraine in comparison with the basic budget-forming industries [46]

The vector of digital engineering in Ukraine to such developed as service, however, according to [46] a number of promising companies engaged in the development of software and digital tools for design and engineering activities, including Digicode, Infopulse, SoftServe, TECHIIA Holding, Valtech, LIRALAND, SCAD Structure, etc. are noted. Digital developments of these companies are successfully used in various industries in Ukraine and other states. Consequently, in the field of computer engineering of the Ukrainian IT cluster prevail the use of cloud services and the continued development of highly specialized digital modeling tools, such as PC Lira-SAD [39] and SCAD Office [40].

4. Discussion

According to the results of the study and determine the potential vector of development of software-digital tools should be nurtured the following theses:
– software products developed by representatives of the Russian Federation still have significant diffusion into the Ukrainian cyberspace, pose a potential threat to Ukraine's cyberdigital infrastructure: from the theft of strategic confidential data to direct harmful effects on cyberphysical systems of different levels of differentiation;
– in view of the potential threats identified, the first target in increasing Ukraine's cyber security is to replace Russian software mainly in the management and organizational areas;
– vector of digital engineering is sufficiently developed in Ukraine and does not need to be forced and stimulated as opposed to software tools of management and organization;
– Ukrainian IT cluster has significant potential for the development and formation of Ukraine as a digital state with a high equal development of a smart environment;
– promising vectors for the development of IT services in Ukraine the development of cloud and other core services with the development of appropriate software;
– computer engineering in Ukraine is at a fairly high level and requires further natural evolution.
Thus, entire studies have been achieved, namely the priority target goals of taking urgent measures to ensure cyber security of Ukrainian cyber infrastructure have been identified, as well as promising vectors of development of software and digital tools and services, including for the vector of computer engineering.

5. Conclusions

The study of the current functioning of Ukraine's cyberdigital space in the context of large-scale armed aggression by the Russian Federation revealed key aspects:
– Ukraine is still dependent on Russian software;
- Ukraine is a developed digital state with great potential in the IT sphere.

Consequently, the direct correlation of the identified aspects allows us to formulate the main opinion of the study
- Ukraine has enough technical capabilities and profile specialists that can secure its cyber infrastructure and downtime from the potentially dangerous influence of Russia.

According to the results of a detailed analysis of the vector of computer engineering, it was found that specialized Ukrainian software products are even non-alternative to the hostile state, which once again emphasizes the high technical development of our state and points to the need for state support for the further natural evolution of digital engineering tools.

According to the objectives of the study as recommendations for the development of the Ukrainian cyberdigital space, the following should be noted:
– taking urgent measures to isolate and eliminate Russian software and services;
- taking forward-looking measures to develop, stimulate and attract innovation in the IT sector of Ukraine;
- developing state support programs and promoting the development of computer engineering.

References

[1] Diia [Electronic resource] / Government services online. – URL : diia.gov.ua, 2022.
[2] Emerging Europe Awards 2022 [Web resource] / Emerging Europe. – URL : emerging-europe.com, 2022.
[3] D&AD Awards 2022 [Web resource] / D&AD. – URL : dandad.org, 2022.
[4] Cannes Lions 2022 [Web resource] / Cannes Lions International Festival of Creativity. – URL : canneslions.com, 2022.
[5] Li, W. Mapping Two Decades of Smart Home Research: A Systematic Scientometric Analysis [Web resource] / W. Li [et

al.]. // Technological Forecasting and Social Change. – 2022. – Vol. 179. – pp. 1-25. // URL : doi.org/10.1016/j.techfore.2022.121676, 2022.
[6] Projects [Electronic resource] / Ministry and the Committee of Digital Transformation of Ukraine. – URL : thedigital.gov.ua, 2022.
[7] Sparkes, M. Why hasn't Russia waged an all-out cyberwar against Ukraine? [Web resource] / M. Sparkes // New Scientist. – 2022. – Vol. 253. – Iss. 3378. – pp. 9 – 10. // URL : doi.org/10.1016/S0262-4079(22)00459-6, 2022.
[8] Samarasekera, U. Cyber risks to Ukrainian and other health systems [Web resource] / U. Samarasekera // The Lancet Digital Health. – 2022. – Vol. 4. – Iss. 5. – pp. 297 – 298. URL : doi.org/10.1016/S2589-7500(22)00064-4, 2022.
[9] Stokel-Walker, C. The digital battleground [Web resource] / C. Stokel-Walker. // New Scientist. – 2022. – Vol. 253. – Iss. 3376. – pp. 10 – 11. // URL : doi.org/10.1016/S0262-4079(22)00358-X, 2022.
[10] Cyber Security Situation Center [Electronic resource] / Ukrainian Security Service. – URL : ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky, 2022.
[11] Ukraine 30. Security of the country [Electronic resource] / All-Ukrainian forum. – URL: ukraine30.com/national_security/#schedule, 2022.
[12] Veselova, L. Yu. Administrative-legal bases of cybersecurity in the conditions of hybrid war [Text]: Thesis for the degree of Doctor of Law on specialty 12.00.07 - administrative law and process; financial law; information law; 08 - Law / Veselova, L. Yu. - Odessa State University of Internal Affairs. - Odessa, 2021. – 500 p.
[13] Bobalo, Yu. Ya. Information Security [Text]: Textbook / Bobalo, Yu. Ya. [et al]. - Lviv: Lviv Polytechnic Publishing House, 2019. – 580 p.
[14] Protsenko, O. B. Cybersecurity in the system of national security of Ukraine: priority directions of development [Text]: Collection of materials of the scientific round table. Mariupol, April 26, 2018 / O. B. Protsenko, K.V. Merkulova. - Mariupol: Mariupol State University, 2018. – 145 p.
[15] Alexandrou, A. Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices [Text] : Monograph / A. Alexandrou. – CRC Press, 2022. – 455 p.
[16] Mangesh, G. M. Cyber Security and Digital Forensics: Challenges and Future Trends [Text] : Monograph / G. M. Mangesh, P. Sabyasachi. – Wiley-Scrivener, 2022. – 432 p.
[17] Khanna, K. Cyber Security and Digital Forensics [Text] : Monograph / K. Khanna, V. V. Estrela, J. J. P. C. Rodrigues. – Springer, 2022. – 623 p.
[18] Lehto, M. Cyber Security: Critical Infrastructure Protection [Text] : Monograph / M. Lehto, P. Neittaanmäki. – Springer, 2022. – 486 p.
[19] About national security of Ukraine [Electronic resource] : Law of Ukraine from 21.06.2018 № 2469-VIII About national security of Ukraine (With the latest amendments introduced by the Law of Ukraine from 16.07.2021 № 1702-IX) / Verkhovna Rada of Ukraine. - Official website of the Verkhovna Rada of Ukraine : URL : zakon.rada.gov.ua, 2022.
[20] On the basic principles of cybersecurity of Ukraine [Electronic resource] : Law of Ukraine of 05.10.2017 № 2163-VIII On the basic principles of cybersecurity of Ukraine (As amended by the Law of 18.11.2021 № 1907-IX) / Verkhovna Rada . - Official website of the Verkhovna Rada of Ukraine: URL : zakon.rada.gov.ua, 2022.
[21] About critical infrastructure [Electronic resource]: Law of Ukraine of 16.11.2021 № 1882-IX About critical infrastructure / Verkhovna Rada of Ukraine. - Official website of the Verkhovna Rada of Ukraine: URL : zakon.rada.gov.ua, 2022.
[22] On electronic communications [Electronic resource]: The Law of Ukraine from 16.12.2020 № 1089-IX On electronic communications / Verkhovna Rada of Ukraine. - Official website of the Verkhovna Rada of Ukraine : URL : zakon.rada.gov.ua, 2022.
[23] Cyber Security Strategy of Ukraine [Electronic resource]: Decree of 01.02.2022 № 37/2022 On the Decision of the National Security and Defense Council of Ukraine of 30.12.2021 On the Plan of implementation of the Cyber Security Strategy of Ukraine / President of Ukraine. - Official site of the President of Ukraine: URL : president.gov.ua, 2022.
[24] DSTU ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Information technology. Methods of protection. Guidelines for cybersecurity [Text] : DSTU (State Standard of Ukraine) / Technical Committee on Standardization "Information Technology" (TC 20). - Kiev: State Enterprise "UkrNINTS", 2018. – 44 p.
[25] Davydiuk, A. V. Using Special Software to Analyze Information Aggression of the Russian Federation against Ukraine [Electronic Resource] / A. V. Davydiuk, V. M. Petryk // Information Technology and Security. – 2017. – Vol. 5, Iss. 1 (8). – pp. 21 – 28. // URL : doi.org/10.20535/2411-1031.2017.5.1.120552, 2022.
[26] Mozghovyi, S. Russian software: to be or not to be? [Electronic resource] / S. Mozghovyi, V. Shatokhin, I. Klymenko // Accounting Internet Portal. – 2022. // URL : ibuhgalter.net/ru/articles/886, 2022.
[27] Babak, A. V. Ukraine still uses 44 Russian programs. Opendatabot listed IT-products that can replace them [Electronic resource] / A. Babak // Programmers Community. – 2022. – URL : dou.ua/lenta/news/ukraine-still-uses-44-russian-programs, 2022.
[28] List of software of Russian origin [Electronic resource] / Opendatabot. – URL : opendatabot.ua/analytics/russian-software, 2022.
[29] Qureshi, A. Russia–Ukraine war and systemic risk: Who is taking the heat? [Web resource] / A. Qureshi [et al.]. // Finance Research Letters. – 2022. – Vol. 48. // URL : doi.org/10.1016/j.frl.2022.103036, 2022.
[30] Serpanos, D. The Cyberwarfare in Ukraine [Web resource] / D. Serpanos, T. Komninos // Computer. – 2022. – Vol. 55. – Iss. 7. – pp. 88 – 91. // URL : doi.org/10.1109/MC.2022.3170644, 2022.
[31] Jakub, P. Russia's war on Ukraine: Timeline of cyber-attacks [Web resource] / P. Jakub // EPRS: European Parliamentary Research Service. – 2022. // URL : policycommons.net/artifacts/2476881/russias-war-on-ukraine/3498934, 2022.
[32] Mohee, A. Cyber war: The hidden side of the Russian-Ukrainian crisis [Web resource] / A. Mohee // SocArXiv. – 2022. // URL : doi.org/10.31235/osf.io/2agd3, 2022.

[33] O'Connor, P. Ukraine: The Cyber Battlefield [Web resource] / P. O'Connor // ITNOW. – 2022. – Vol. 64. – Iss. 2. – pp. 42 – 43. // URL : doi.org/10.1093/itnow/bwac053, 2022.
[34] Eichenseh, K. E. Ukraine, Cyberattacks, and the Lessons for International Law [Web resource] / K. E. Eichenseh // AJIL Unbound. – 2022. – Vol. 116. – pp. 145 – 149. // URL : doi.org/10.1017/aju.2022.20, 2022.
[35] Thornton-Trump, I. Russia: the cyber global protagonist [Web resource] / I. Thornton-Trump // The EDP Audit, Control, and Security Newsletter. – 2022. – Vol. 65. – Iss. 3. – pp. 19 – 26. // URL : doi.org/10.1080/07366981.2022.2041226, 2022.
[36] Svyrydenko, D. Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine [Web resource] / D. Svyrydenko, W. Możgin // Future Human Image. – 2022. – Iss. 17. – pp. 39 – 46. // URL : ceeol.com/search/article-detail?id=1046451, 2022.
[37] Netpeak Group [Web resource] : URL : netpeak.group, 2022.
[38] List of Russian SaaS and Ukrainian alternatives [Web resource] : URL : replace-ru-with-ua.com, 2022.
[39] LIRALAND [Web resource] : URL : liraland.ua, 2022.
[40] SCAD Structure [Web resource] : URL : scadsoft.com, 2022.
[41] Autodesk [Web resource] : URL : autodesk.com, 2022.
[42] Gindis, E. J. The future of AutoCAD [Web resource] : Up and Running with AutoCAD® 2022 / E. J. Gindis, R. C. Kaebisch. – Academic Press, 2022. // URL : doi.org/10.1016/C2020-0-03148-8, 2022. // pp. 825 – 828 // URL : doi.org/10.1016/B978-0-323-89923-9.15013-9, 2022.
[43] IT services - the only business sector to grow in 2022 [Electronic resource] / Opendatabot. ¬– 2022. // URL : opendatabot.ua/analytics/itexport-increased-2022, 2022.
[44] Ukraine 4.0 – Afternoon Meeting at the Embassy of Ukraine in Germany July 4th [Web resource] / Outsourcing Journal. – 2017. // URL : outsourcing-journal.org/ukraine-4-0-afternoon-meeting-at-the-embassy-of-ukraine-in-germany-july-4th, 2022.
[45] Good Country Index [Web resource] / Good Country : URL : index.goodcountry.org, 2022.
[46] Ukraine IT Report 2021 [Web resource] / IT Ukraine Association. – 2021. // URL : reports.itukraine.org.ua/?fbclid=IwAR1wBmRIieJuKiuy36DY3gsv3QxJUi2dQNU7UHpZsmcmwF9vvxv0qsJY4Ps, 2022.
[47] Ovcharenko, D. Trends and prospects of IT-outsourcing development in Ukraine and the world [Electronic resource] / Ovcharenko, D. // Alcor. – 2022. // URL : alcor-bpo.com/uk/your-own-rd-office-news/tendencies-of-it-outsourcing-growth-in-ukraine-and-the-world, 2022.
[48] Oliinyk, A. Cloud future of SaaS contracts in Ukraine [Electronic resource] / Oliinyk, A.// GOLAW. – 2021. // URL : golaw.ua/ua/insights/publication/hmarne-majbutnye-saas-dogovoriv-v-ukrayini, 2022.
[49] About cloud services [Electronic resource] : the Law of Ukraine from 17.02.2022 № 2075-IX About cloud services (enters into force on 16.09.2022) / the Verkhovna Rada of Ukraine. - Official website of the Verkhovna Rada of Ukraine: URL : zakon.rada.gov.ua, 2022.
[50] Zalialetdzinau, K. "Automation of Organizations Using Cloud Technologies: Security Issues". COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION, no. 47 (July 1, 2022): 21-25. Accessed August 2, 2022. http://cit-journal.com.ua/index.php/cit/article/view/344.

Bannikov Valentyn
master's degree, Project Manager Dataart Solutions, Inc 475 Park Avenue South Floor 15 New York, NY 10016 United States, bannikov.valentyn@gmail.com
ORCID ID: 0000-0001-8865-3767

Zalialetdzinau Kanstantsin
software engineer Brimit LLC
kostya.zolya@gmail.com, ORCID ID: 0000-0003-1938-0122

Siasiev Andrii
PhD, Associate Professor Oles Honchar Dnipro National University
Faculty of Mech & Math Department of Differential Equations
Gagarina ave., 72, Dnipro, Ukraine, 49010, syasev@i.ua
https://orcid.org/0000-0002-0654-7360

Ivanenko Ruslan
Senior Researcher Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine, Kyiv, Ukraine, 03113, Vasylenko 3, indior@ukr.net ORCID ID: 0000-0002-1447-6275

Saveliev Dmytro
Candidate of Technical Sciences, Senior Lecturer National University of Civil Defence of Ukraine, Faculty of Operational and Rescue Forces, Department of Engineering and Rescue Machinery 94, Chernyshevska St. Kharkiv Kharkiv Region Ukraine 61023, savelev@nuczu.gov.ua, 0000-0002-4310-0437