ISSN 2664-9969

UDC 005:004
DOI: 10.15587/2312-8372.2020.207066

Mohammad Alhawawsha

DEVELOPMENT OF THE CONCEPT OF ELECTRONIC GOVERNMENT CONSTRUCTION IN THE CONDITIONS OF SYNERGETIC THREATS

Об'єктом дослідження є процес формування концепції побудови електронного уряду в умовах синергізму та гібридності сучасних загроз. Розвиток високих технологій, бурхливе зростання інформаційно-комунікаційних технологій (ІКТ) та обчислювальних ресурсів дозволяють удосконалювати не лише сфери побуту та послуг для суспільства, а й створювати як окремі елементи, так і повномасштабні проекти цифрової держави. Одним з найбільш проблемних місць при формуванні цифрової держави та/або електронного уряду залишається забезпечення безпеки єдиного порталу та/або реєстру. В умовах стрімкого зростання обчислювальних ресурсів кіберзлочинці реалізують комплексування загроз з методами соціальної інженерії, що дозволяє отримати синергетичний ефект і гібридність.

Отримано оцінку можливості квантового комп'ютера, що значно знижує рівень безпеки при використанні традиційної та несиметричної криптографії. Це пов'язано з тим, що запропоновані методи злому симетричних і несиметричних криптосистем реалізуються в постквантовий період з поліноміальною складністю. В роботі запропонована ієрархічна концепція запровадження моделі управління на основі електронного уряду, що дозволяє поглибити принципи демократії, практично позбудеться від корупції при необхідному рівні безпеки. Для його розгортання необхідно забезпечити на кожному рівні захист інформаційно-комунікаційних та мобільних технологій, що забезпечують функціональність електронного уряду. У роботі досліджено основні загрози на критичні кіберфізичні системи, як основу механізмів виконання функцій електронного уряду. З урахуванням побудови повномасштабних квантових комп'ютерів, в роботі формуються основні цілі та завдання концепції побудови електронного уряду. Завдяки цьому забезпечується можливість отримання основних принципів і функціональності на кожному рівні Концепції формування електронного уряду. У порівнянні з аналогічними відомими підходами це забезпечує облік необхідного рівня не тільки комп'ютерної кіберграмотності населення, а й забезпечення повномасштабного покриття кіберпростору держави. Дозволяє забезпечити функціональність електронного уряду в умовах комлексування сучасних загроз

Ключові слова: *електронний уряд, кіберфізичні системи, критичні інформаційно-кібернетичні системи, цифрова держава, інформаційна безпека.*

Received date: 02.02.2020
Accepted date: 13.03.2020
Published date: 30.06.2020

1. Introduction

Revolutionary changes in information and communication systems have shaped cyberspace, which allows not only to expand the range of information and communication services, but also to increase the growth of public (state and municipal services). The dynamic development of the social and political components of public consciousness on the basis of social networks allows us to formulate a new approach to the formation of a public administration paradigm with a «traditional» model for a more democratic and effective model of a digital state [1–3].

The main elements of a digital state are electronic branches of the state, based on the digitalization of all elements of the mechanism of critical information and communication systems that provide the functionality of a particular industry [2]. Fig. 1 presents the structure of the main branches of the electronic state.

The main elements of the mechanism for implementing the electronic components of the digital state are [4–6]:

– information and communication infrastructure – a set of geographically distributed information and information-analytical systems, electronic information resources, means of switching and control of information flows, communication lines, networks and data transmission channels [7, 8]. As well as organizational structures and regulatory acts ensuring their effective functioning;

– information resource – a set of documents in information systems (libraries, archives, data banks, etc.). Or information/knowledge that have value in a specific subject area and can be used by a person in economic activity to achieve a specific goal [9].

The main element of the new model of public administration is e-government, which is understood as a complex of information and mobile technologies and the Internet, created for digital interaction between government bodies

and its various branches, citizens, public organizations, and business. Currently, e-government is perceived as [2]:

– internet technology of the relationship between government and the public;
– an interactive form of cooperation between government and society in the process of solving socially significant problems;
– an instrument of interdepartmental and interdepartmental interaction of public servants;
– a purely technical tool for the provision of public services to the population.

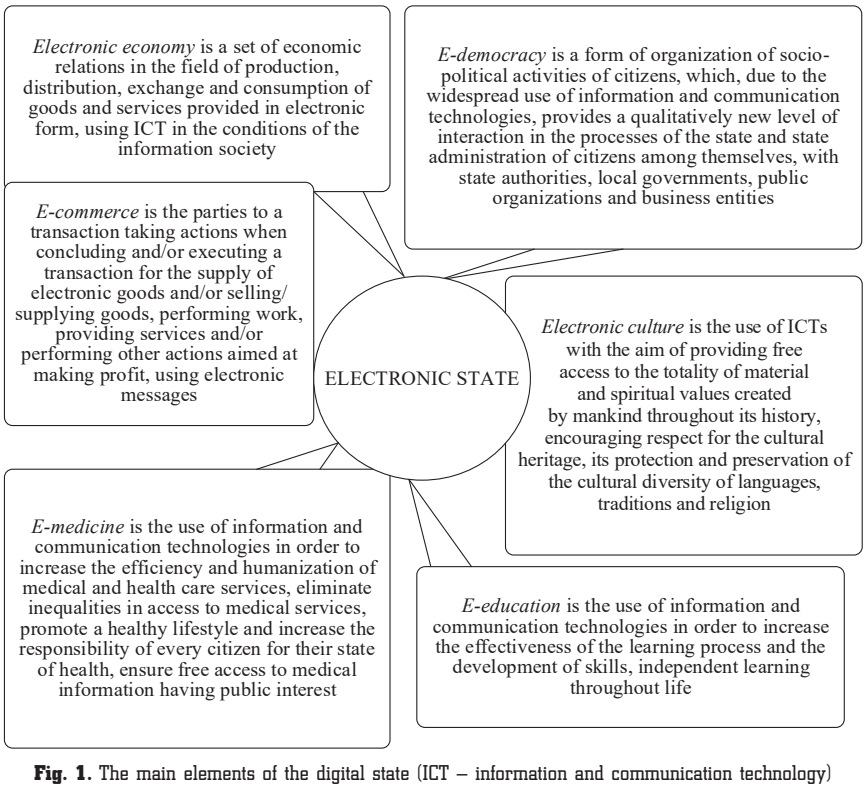

Fig. 1. The main elements of the digital state (ICT – information and communication technology)

At the same time, in almost all areas of the digital state, it is necessary to use:

– cyberphysical (CPS – cyber-physical systems) and/or information and communication systems (ICS – information and communication systems);
– large open knowledge and information base systems (OKIBS – open knowledge and information base systems), which in turn form critical cyber information systems (CCIS – critical cyber information systems) [10, 11].

Therefore, it is urgent to develop a Concept for the formation of electronic government, taking into account the modern vector of cyber threats, the development of computing and information and communication resources.

Thus, *the object of research* is the process of forming the concept of building electronic government in the context of the synergism and hybridity of modern threats. And *the aim of research* is to build the concept of the formation of electronic government in the context of combining modern threats, their manifestation of synergism and hybridity.

2. Methods of research

The main goal of building a digital state is to create favorable conditions for the development of the information society, socio-economic, political and cultural development of a country with a constant and growing market economy. The state is guided by European political and economic values, improving the quality of life of citizens, creating ample opportunities to meet the needs and free development of the individual, ensuring the competitiveness of the state, improving the public administration system using information and telecommunication technologies [11]. At the same time, the basic principles that must be followed to form not only electronic government, but also a digital state are:

– the principle of equal partnership between authorities, citizens and business;
– the principle of cooperation, complicity and involvement of the subjects of the information society for the formation and implementation of the state policy of the information society;
– the principle of decentralization;
– the principle of freedom and equality of access to information;
– the principle of recognition of fundamental human rights and freedoms in the information space, the provision of state guarantees of full and free access to information and knowledge, freedom of expression and self-realization in the global information space for everyone;
– the principle of professionalism, transparency and openness of government;
– the principle of information security;
– the principle of continuing education;
– the principle of common technical standards and mutual compatibility;
– the principle of accountability and accoun tability of government to citizens and society;
– the principle of support for domestic manufacturers of information products and services;
– the principle of a clear delineation of powers and coordinated interaction of authorities;
– the principle of conscientious fulfillment of international obligations undertaken;
– the principle of guaranteed resource support for national programs and projects related to the development of the information society in full.

3. Research results and discussion

To build the concept of a modern digital state, we consider the basic CCIS and their relationship with CPS and/or ICS systems that provide basic functions. In Fig. 2, the relationship of the proposed structure with critical cybernetic information systems (CCIS) is proposed, using the banking sector as an example.

The main elements of the e-government infrastructure that ensures the interaction of all spheres (areas) of the e-government based on the use (implementation) of CPS and/or ICS are a single portal and register of state and

ISSN 2664-9969

municipal services. A unified system of identification and authentication, a unified system of interagency electronic interaction and workflow allows to provide the necessary principles of a new model of public administration. However, the formation of unified CCIS requires taking into account not only computing resources, but also globalization, hybridity, and the synergy of modern threats, both at the level of cyberspace, and at the level of applications and firmware. However, the further development of computing resources and IT technologies will allow humanity to enter the era of post-quantum cryptography and the use of full-scale quantum computers. This, in turn, will be able to eliminate practically cryptographic protocols and «open» full access to OKIBS resources [12]. Fig. 3 presents the main types of threats to security components: cybersecurity (CS), information security (IS) and information security (SI). This allows to evaluate their synergistic effect when implemented with social engineering methods.

The main tasks that can be solved on a quantum computer include the following:

1) the quantum Shor's factorization algorithm;

2) Grover's quantum algorithm for finding an element in an unsorted base;

3) Shor's quantum algorithm for solving the discrete logarithm in a finite field;

4) quantum algorithm for solving a discrete logarithm in a group of points of Shore's elliptic curve (EC);

5) quantum cryptanalysis algorithms for transformations into a ring factor;

6) quantum algorithm of cryptanalysis of Xiong and Wang and its improvement and the like.

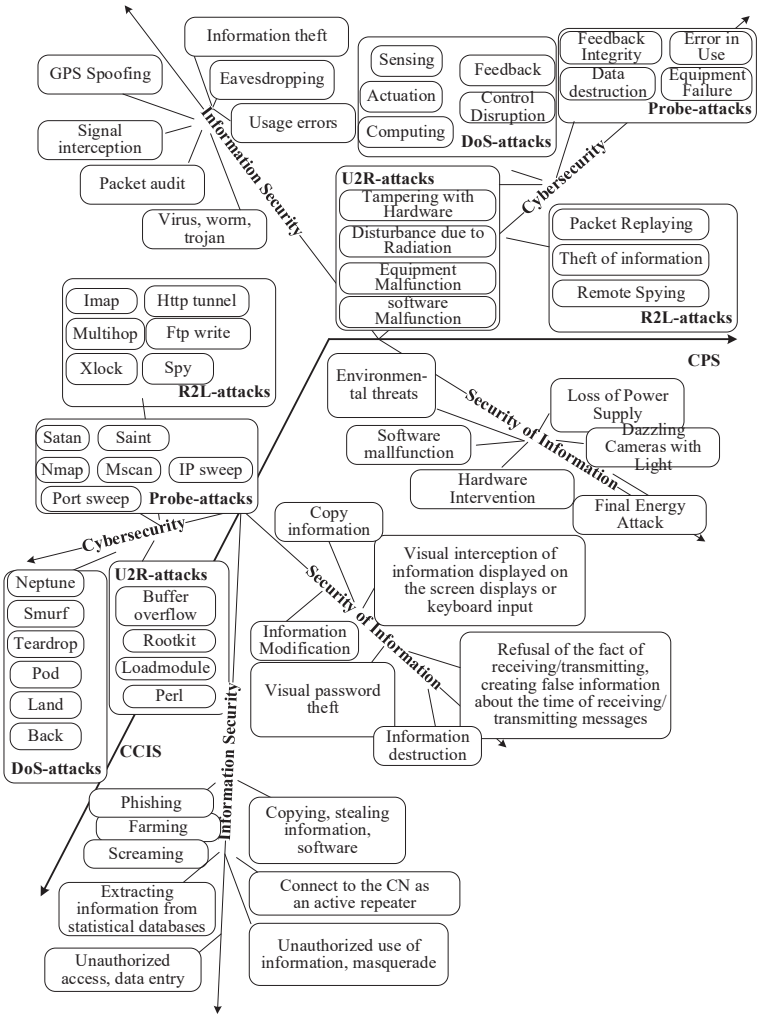

Fig. 3. The structural diagram of the synergetic model of synthesis threats on CCIS and CFS: CPS – cyber-physical systems; CN – computer networks [10]

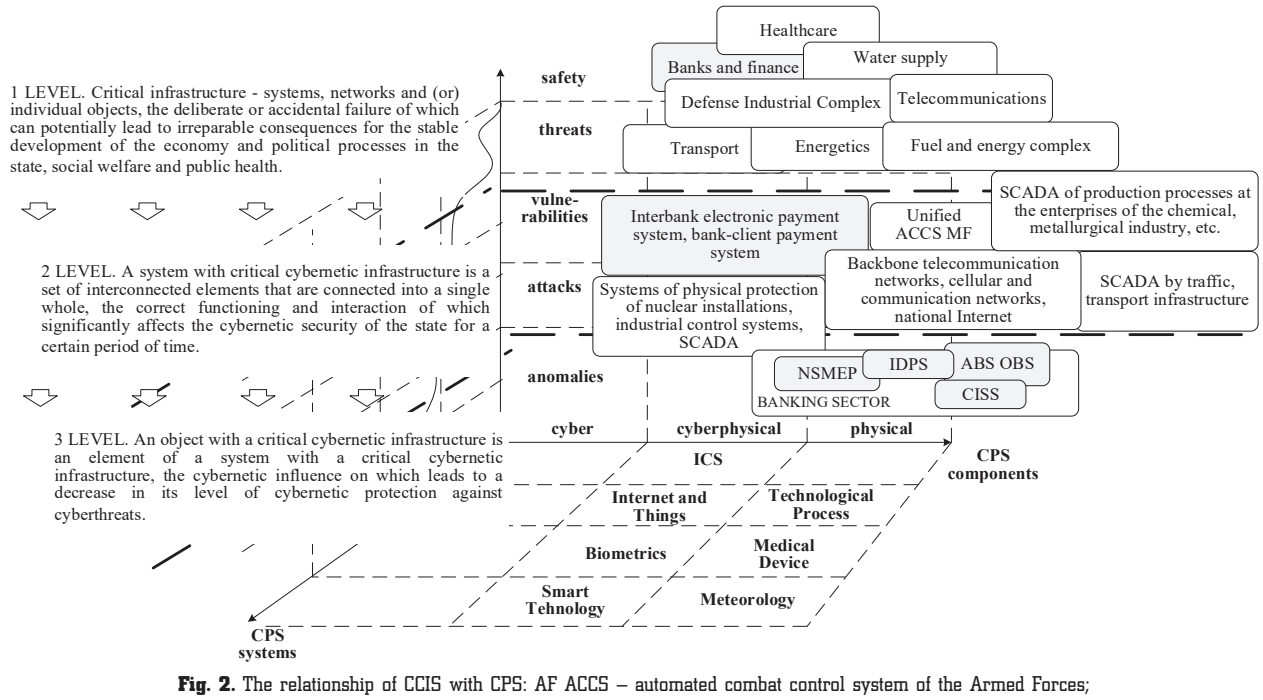

Fig. 2. The relationship of CCIS with CPS: AF ACCS – automated combat control system of the Armed Forces; SCADA – dispatch control and data collection system; APCS – automated process control systems; NSEMP – national system of electronic mass payments; MOS – management organization system; ABS BSO – automated banking systems of banking sector organizations; IISS – integrated information security systems; ICS – information and communication systems [10]

Table 1 shows the results of a comparative analysis of the factorization complexity for classical and quantum algorithms, in Table 2 – the complexity of implementing the Shor's method of discrete logarithm to a group of EC points.

Presented in the Tables 1, 2 results of comparisons indicate a significant reduction in energy costs for the implementation of hacking cryptographic algorithms of asymmetric cryptography. In the conditions of post-quantum cryptography, specialists from the National Institute of Standards and Technology (NIST, USA) propose considering special-type attacks (SIDE-CHANEL ATTACKS). The implementation of these attacks is aimed at finding vulnerabilities in the practical implementation of the cryptosystem, primarily cryptographic protection means.

The following classification of special attacks is proposed according to the following criteria:

– control over the computing process;
– way to access the system or tools;
– method of direct attack and the like.

The basis of protection against attacks of a special kind can be put features:

– fixed number of hash function calls, data randomization;
– independence of keys from values and the like.

The main requirements of NIST for safety in the conditions of the post-quantum period are:

1) safety requirements:
– replacement of the electronic signature (ES) standard FIPS 186;
– replacement of key distribution standards SP 800-56A, SP 800-56B;
– use of the new standard in the protocols: TLS, SSH, IPSec;
– security model for encryption and distribution scheme of «semantically secure encryption». Security Model – IND-CCA2;
2) safety conditions:
– attacker access to less than 264 pairs of ciphertext – keys;
3) sustainability requirements:
– 128 bits of classical security/64 bits of quantum security (AES-128 stability margin);
– 128 bits of classical security/80 bits of quantum security (safety margin SHA-256/SHA3-256, SHA-384/SHA3-384);
– 256 bits of classical security/128 bits of quantum security (AES-256 stability margin).

As a preliminary criterion, NIST offers an approach in which quantum attacks are limited by a set of fixed operating time, or «depth» of the circuit. This parameter is called MAXDEPTH.

Possible values for the MAXDEPTH range:

– 2^{40} logic gates, that is, the approximate number of gates that will be executed sequentially per year;
– 2^{64} logical gates that modern classical computing architectures can perform sequentially in ten years;
– no more than 2^{96} logic gates, that is, the approximate number of gates that atomic-scale qubits with the speed of time of propagation of light can perform for millennia.

Thus, the analysis shows that the desire of mankind to form a new model of public administration on the basis of a digital state may face serious problems for which it is not yet ready. The construction of the concept of e-government should be implemented in the context of taking into account the growth of computing resources and ICT, ensuring not only the implementation of the basic services of the digital state in each area of its activity, but also the capabilities of cybercriminals and cyber terrorists.

The analysis of the principles and functionality of building a digital state and, in particular, electronic government allows to formulate a concept for its construction. Under conditions of influence and or potential impact both from the side of cybercriminals (cyberterrorists), and from the side of industrialized globalization corporations and communities. The concept is presented in Fig. 4.

The proposed concept of e-government construction has a hierarchical structure and provides resistance to modern hybrid threats in the formation and deployment of e-government infrastructure. This approach allows timely consideration of the integration and synergy of modern threats in the post-quantum period and the rapid growth of computing resources.

Table 1

Comparative analysis of factorization complexity for classical and quantum algorithms

Module size N, bits	The number of necessary qubits $2n$	The complexity of the quantum algorithm $4n^3$	The complexity of the classical algorithm
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Table 2

The complexity of implementing the Shor's method of discrete logarithm to a group of EC points

Algorithm for calculating a discrete logarithmic equation			
The size of the order of the base point, bit	The number of necessary qubits $f(n)=7n+4\log_2 n+10$	The complexity of the quantum algorithm $360n^3$	The complexity of the classical algorithm
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

 ISSN 2664-9969

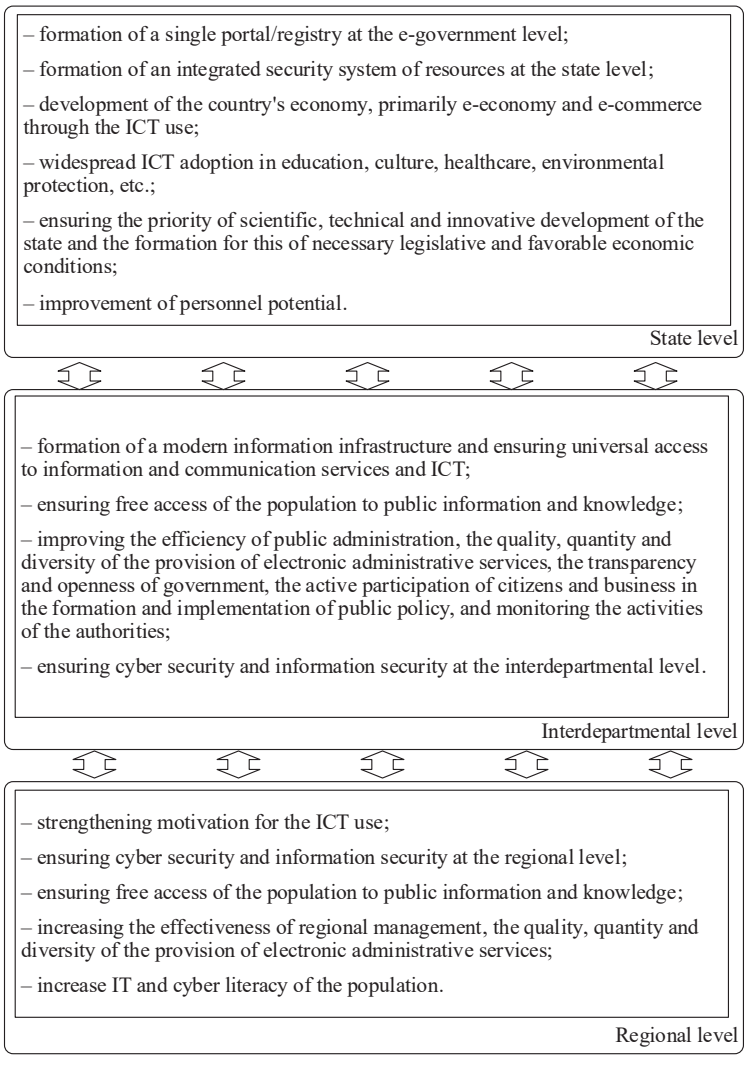

Fig. 4. The concept of building e-government

4. Conclusions

The analysis of the principles and functionality of the digital state during the work shows that its construction requires a transition from the existing «traditional» model of government to a new governance model that ensures further growth of democracy and management efficiency. The main mechanisms for ensuring the development of both electronic government and the digital state are modern ICTs based on cyberspace and mobile communications technologies. However, their use is associated with an increase in cyber threats to all elements of the e-government infrastructure and (the scope of the digital state). This determines the need to take into account the criticality of such mechanisms and related systems (cyberphysical and information and communication systems).

The analysis of threats in the context of the rapid growth of computing resources, both of cyber technologies and G technologies, showed their orientation vector for combining with social engineering methods to obtain new characteristics, such as synergy and hybridity. Humanity's entry into the era of post-quantum cryptography (the emergence of a full-blown quantum computer) puts forward more stringent security requirements in both ICS and CPS, which form the core of CCIS. In conditions of possible security chaos (breaking by symmetric and asymmetric cryptosystems by quantum algorithms), a synergetic threat model is put in first place in the analysis of the current security state, which allows for the integration of threats by security components: IS, CS, SI.

References

1. Goncharenko, G. K. (2016). Future deveuopment of mechanisms of euectronic democracy in Russia. *Ot sinergii znanii k sinergii biznesa,* 464–468. Available at: https://elibrary.ru/item.asp?id=28331769
2. Golovenchik, G. G. (2019) Building a modern digital state. *Nauka i innovacii, 11 (201),* 50–58. Available at: https://elibrary.ru/item.asp?id=41852762
3. Pont, S. (2013). *Digital State: How the Internet is Changing Everything.* Kogan Page, 256. Available at: https://www.bynder.com/en/digital-transformation/
4. Yakunina, G. E. (2020). Research of digital communications models within organizations and at the state level in the countries-leaders in the use of digital communication technologies. *E-Management, 2 (4),* 41–50. doi: http://doi.org/10.26425/2658-3445-2019-4-41-50
5. Kassen, M. (2019). Building digital state: Understanding two decades of evolution in Kazakh e-government project. *Online Information Review, 43 (2),* 301–323. doi: http://doi.org/10.1108/oir-03-2018-0100
6. *Building a 21st Century Platform to Better Serve the American People*. Available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html
7. Bertrand, A. (2019). *The digital revolution is generating new opportunities for governments to transform how they work and deliver better outcomes for citizens.* Available at: https://www.ey.com/en_gl/government-public-sector/how-to-build-the-digital-state
8. Savina, A. (2016). *How Estonia became the most modern digital state in the world.* Available at: https://medium.com/@annasavina/how-estonia-became-the-most-modern-digital-state-in-the-world-f777d853aaa6
9. *Pro skhvalennia Stratehii rozvytku informatsiinoho suspilstva v Ukraini* (2013). Rozporiadzhennia Kabinetu Ministriv Ukrainy No. 386-r. 15.05.2013. Available at: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text
10. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for a classifier of threats to cyberphysical systems design. *Eastern-European Journal of Enterprise Technologies, 3 (9 (105)),* 6–19. doi: http://doi.org/10.15587/1729-4061.2020.205702
11. Charles Raul, A. (2012). *Privacy and the Digital State: Balancing Public Information and Personal Privacy.* Springer Science & Business Media, 148. Available at: https://books.google.com.ua/books?id=x9jVBQAAQBAJ&dq=Building+a+modern+digital+state&hl=ru&source=gbs_navlinks_s
12. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography.* doi: http://doi.org/10.6028/nist.ir.8105

Mohammad Alhawawsha, *Postgraduate Student, Department of Information Systems, Taras Shevchnko National University of Kyiv, Ukraine, e-mail: mhawawsha@gmail.com, ORCID: http://orcid.org/0000-0001-5587-3501*