КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056
DOI: https://doi.org/10.17721/ISTS.2024.7.5-10

Serhii DAKOV, PhD (Engin.)
ORCID ID: 0000-0001-9413-3709
e-mail: dacov@ukr.net
Taras Shevchenko National University, Kyiv, Ukraine

Tetiana LAPTIEVA, PhD Student
ORCID ID: 0000-0002-7291-1829
e-mail: tetiana1986@ukr.net
Taras Shevchenko National University, Kyiv, Ukraine

IMPROVEMENT OF COMPUTER SYSTEM PROTECTION ASSESSMENT METHODS AGAINST HARMFUL SOFTWARE CODE

Background. *The issue of ensuring information security (IS) of state information systems today is not only not losing relevance, but with the development of the concept of eGovernment in countries and an increase in the number of e-services, it is becoming increasingly important.*

methods were used against malicious code

Methods. *The work used the method of analyzing the evaluation of the protection of the computer system against malicious software code, with the help of the method of optimization and evaluation of the protection of the computer system, the method of malicious software code was improved.*

Results. *The work improving the method of assessing the information security of computer systems from malicious software includes a recommendatory aspect of building e-government.*

Conclusions. *Cybersecurity threats, such as spam, phishing, spyware, and botnets, pose challenges for governments, especially for such young governments in any developing country. Malicious authors (hackers) create new combined threats to counter the security of the information system. New threats make it possible to bypass system firewalls, workstation configurations and various other intrusion detection systems. Many governments are working on cybersecurity legislation to help protect consumers and themselves. Some legislative efforts are focused on establishing government structures to provide support against systemic attacks. Some government legislation has been designed to prosecute criminals in order to deter criminal activity. The legislation has well developed a basis for the detection, analysis and internal prevention of malicious software.*

To effectively manage cybersecurity threats, governments must be involved from the beginning of the process to the end of the process. Businesses need to know where and to whom to report security risk information, and the government needs to support it. Improving the method of assessing the information security of computer systems from malicious software contains a recommendatory aspect of building an electronic government. The steps of building e-government, in contrast to the existing ones, differ in the completeness of the content of each stage of building e-government.

Keywords: *identification, information security, eGovernment, organization of information security, firewalls.*

Background

The issue of ensuring information security (IS) of state information systems today is not only not losing relevance, but with the development of the concept of eGovernment in countries and an increase in the number of e-services, it is becoming increasingly important.

The issue of ensuring information security (IS) of state information systems today is not only not losing relevance, but with the development of the concept of eGovernment in countries and an increase in the number of e-services, it is becoming increasingly important.

The uncontrolled growth of the influence of information and communication technologies (ICT) on the post-industrial society, the emergence of the danger of a gap between the information elite and consumers has led, in turn, to a significant

complication of the task of extracting data necessary for governments to make weighted, adequate to the conditions of the situation, and also their protection from all sorts of destructive influences – challenges, in fact, undisguised cyber crimes and threats (Prandini, & Ramilli, 2014).

One of the main conditions for the transition of society to the state of a developed information society is to ensure the necessary and sufficient level of IS. The success of creating a sustainable estate system directly depends on how protection against modern Cyber Threats will be implemented. An effective level of IS is the timely identification and assessment of new risks and current cyber threats, regular assessment of the security of eGovernment infrastructure components. The state of IS eGovernment essentially depends on threats that may cause irreparable harm to the entire state system. That is why the study of the main threats and the assessment of IS objects of information activities (OIA) for the construction of effective information systems is relevant.

The purpose of the article. Improving the method of assessing the information security of computer systemsfrom malicious software for formation and development of e -government in the European Union (EU).

Analysis of literary sources. More and more scientists are showing interest in the information society, which quickly began to develop as a concept for a new social order. The basic principles and problems of its development were examined in the works of R. Abdeev, R. Aron, D. Bell, N. Wiener, M. Zgurovsky, M. Castells, S. Kuchinsky, E. Masuda, A. Rakitova, E. Toffler, F. Fukuyama, and other scientists.

In modern conditions, the problem of information security is not a narrow technological category but goes into the area of conceptual substantiation of the management of social processes. And especially today, the problems of information security are of particular importance when the government sets itself the task of developing the information society and integrating it into the global information space.

The globalization of the information space and the development of the information society (eGovernment) leads to the emergence of problems that are rather difficult to cope with within the country. All these problems require further and in-depth study. Unfortunately, a comprehensive study of the problems of eGovernment development, as well as related information security issues, was not enough. Therefore, the study of information security, the problems of formation and development of e-government in the European Union (EU), as well as the study of possible ways to create an information and cybersecurity system in our country are very relevant.

Methods

The work used the method of analyzing the evaluation of the protection of the computer system against malicious software code, with the help of the method of optimization and evaluation of the protection of the computer system, the method of malicious software code was improved.

Results

The European Commission planned to shape the directions of eGovernment in Europe. The EU had no direct influence on the administrations of the Member States, but the EU financed a lot of multinational projects within the Research Framework Programme.

On the European's national level, there exists eGovernment Directives and Master plans at EU, but Ukraine just started development of it in the last decade. On the international level the European Commission (EC) sets the posts; so, under the name "Accelerating eGovernment in Europe for the Benefit of All" the i2010 Government Action Plan was developed. The Progress is different in diverse countries in EU, but the general patter of development is similar. In general, one discerns the following four waves (Marco P., & Marco R., 2021, pp. 285–288):

- Promote access – Web presence;
- Provide (particular) services online;
- Transform the institution so by automating and reengineering of processes;
- Next-Generation-Government (i.e. dropping the "e" as ICT having become self-evident);
- They recognized the following challenges;
- Joining up administrations by establishing interoperability and identity management;
- Increasing usage by better designed services and knowledge enhancement;
- Opening up to Public Governance with systems supporting e-Participation and e-Law.

The track record of sustainable eGovernment initiatives in rural areas is difficult to measure (Benjamin et al., 2015, pp. 391–400). In Richard Heeks's classic paper on eGovernment "Most eGovernment-for-Development Projects Fail" informed that 85% of eGovernment projects in developing countries fail. The World Bank reported in a "Task Managers' ICT Toolkit" that projects with Information and Communication Technology components had an "alarmingly high failure rate", with 50% suffering disputes and 80% requiring contract amendments (Malik, Peter, & Omer (2015), pp. 15–20). Prandini et al. informs, that managers embraced this technology as if it simply were a new, enhanced version of World Wide Web. They neglected the less-obvious aspects of the technology,

and thus bringing on significant security problems. Malicious attackers could quite easily exploit the vulnerabilities in these systems to hijack the process and lead to wrong decisions.

New cyber security threats have been introduced in the last decade or two. Malware developers create more efficient software with the advancement of network security systems. Governmental legislation offers support to companies that operate with sensitive consumer information. Attacks centred on manipulation and fraud of financial markets is one of the top cyber security threats now. Spam, phishing, and spyware were once seen as isolated challenges for organizations, hackers are now creating hybrid threats that can even infiltrate Government systems. Cyber threats such as spam, phishing, spyware and botnets present problems for governments, especially for such young governments as Ukraine or any other developing countries. Hackers create new dangerous mixed threats to circumvent the protection of the organizations information system OIA. The US federal government has taken steps to information protection (IP) the private sector and for government organizations, but efforts must be made as a collective to improve cyber security reporting. Fig. 1 from shows how blended threats may bypass traditional security controls.

On the other hand, as Raiv Sandhu from the University of Texas at San Antonio stated, that the large-scale adoption of internet services across diverse populations is one indicator that the average consumer is reasonably comfortable with the collateral risks. Many nations and militaries, including Ukraine, are preparing offensive and defensive cyber capabilities.

Improving the lives of people by employing the Internet of Things becomes a reality. On the other hand, we must secure the systems against cybercriminals, hackers, and malicious computer applications or systems, who would certainly want to disrupt such systems or try to breach the privacy of people who will be connected to such networks.

Many cybersecurity problems occur on a worldwide scale. Benjamin Edwards, Steven Hofmeyr studded a large high-resolution data set of messages sent from 260 ISPs in 60 countries over the course of a decade.

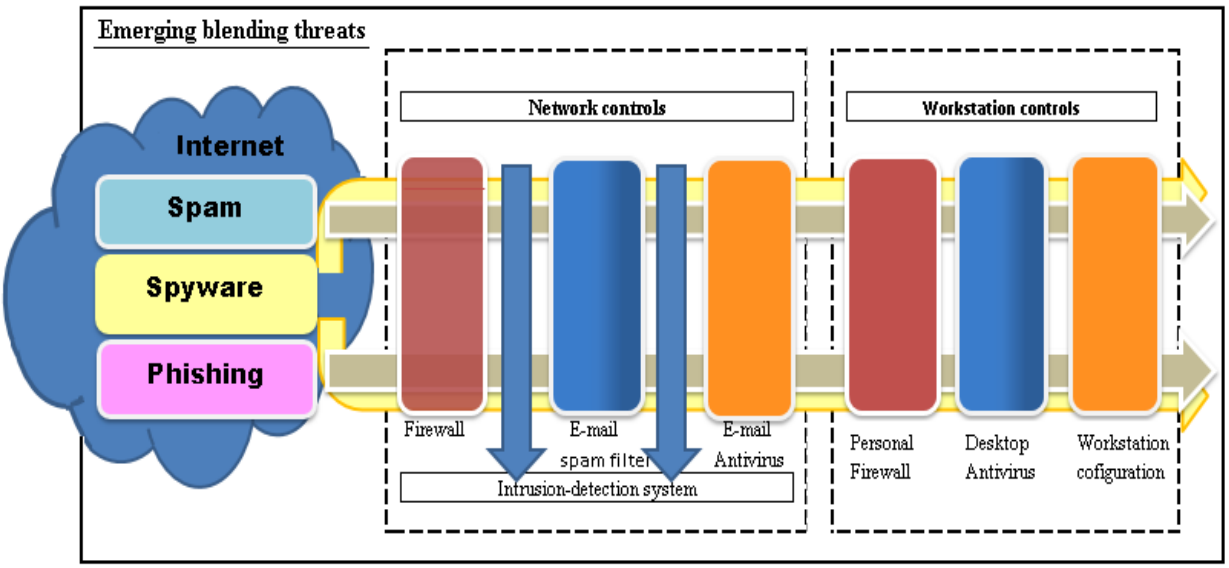

Fig. 1. Blended Threaths Bypassing Traditional Security Controls

They found, that many cybersecurity problems occur at a global scale, involving nations, corporations, or individuals whose actions have impact around the world. Another security problem is related to insecure sharing data. "Sharing data is gaining importance in recent years due to proliferation of social media and a growing tendency of governments to gain citizens' trust through being transparent". They stress that privacy enhancement techniques must be used to prevent unsavoury disclosure of personal data

Existing and in-development solutions. In V. Z. Tabakov, Malik Shahzad Awan and Peter Burnap investigate stealthy and dynamic techniques and attack vectors used by cyber criminals. They have made network infrastructure more vulnerable to security breaches the organization. Cyberattacks involving advanced evasion techniques often bypass security controls, and even if detected at a later time could still remain in the system for a long time without any monitorable trace. Such types of cyber-attacks are costing billions of dollars to the OIA and

ISSN 2707-1758

for management organizations across the globe. It has been predicted that a 50% increase in security budgets will be observed to rapidly detect and respond to targeted attacks.

It's a well know approach to use firewalls between business and process control networks and many believe that this is an ideal solution for plant floor Cyber Security. But research shows that few firewalls are properly configured and that many control system security incidents bypass the firewall. Many organizations have implemented several levels of firewall defences even between different divisions in the same organization. It allows the prevention of a breach in the system if the whole organization firewall was bypassed.

To improve information security and data protection of eGovernment and Governmental information resources and system of systems on the governmental level, the authors propose to analyze security threats before malicious attacks, during attacks and after attacks:

1) Before attacks:

- All equipment and all software, applications and systems must be certified, as is described in (Laptev 2020), especially this is related to all open source systems and proprietary products;
- All critical software must be patched and updated regularly or as fast as possible after any vulnerability or security threat was discovered. Many organizations have their own test labs to test obtained software applications and systems for security risks;
- As we mentioned above, we suggest using several levels of firewall defences even between different divisions in the same organization. It will allow the prevention of a breach in the system more deeply and isolate problem inside of the organization;
- Security information and event management (SIEM) implementation.

It is necessary to implement the following information security measures at the OIA:

- Industrial control systems (ICS) and Supervisory control and data acquisition (SCADA) networks for supervisory purposes as well as control capabilities for process management;
- Virtual Private Network solutions (VPN); Network Access Control (IAM/NAC);
- Application Control.

2) During attacks:

- Intrusion Prevention System (IPS), which is a technique combining the techniques of the firewall with that of the IDS properly. IDS – is a defence system, which detects hostile activities in a network: to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection;
- Full packet capture (FPC);
- Antivirus software;
- Email/Web security solutions.

3) After attacks:

- Intrusion Detection Systems (IDS);
- Forensic Capture System (Forensics);
- Security information and event management (SIEM).

As an example of a security web services framework we present a Multi-Level Secure Framework (MLSF) for web services from at Fig. 2.

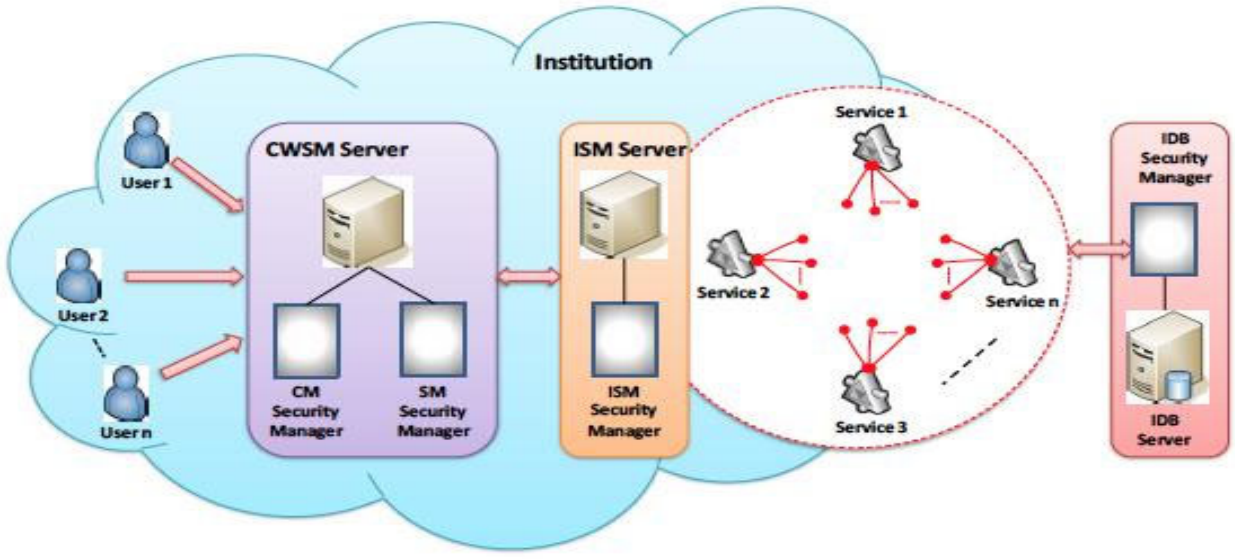

Fig. 2. Architecture for Multi-Level Secure Composite Web Services

The demonstrated framework provides essential infrastructure for various operations such as acquiring user information, connectivity, authentication and communication to facilitate secure web services for multiple users. CM is the Client Manager, CWSM is the Composite Web Services Manager, ISM – Institution Service Manager, SM – Service Manager, IDB – Institution DB. More information about shown framework can be obtained from .

In turn, considering information security in government organizations and in other OIA, information security should consist of the following parts: audit of point analysis, protection of access to the infrastructure, monitoring at all levels of the network. It is also necessary to conduct an analysis of system vulnerabilities, possible scenarios for the realization of threats, probability of realization of the threats and their origin.

The probability of implementing each *i*-th threat in relation to the j-th asset is determined using equation (1):

$$d_{rj} = 1 - p_{ri} \times \prod_{i=1}^{m}(1 - p_{rji}), \quad (1)$$

where *n* – the number of threats; *m* – the number of assets; p_{ri} – possibility of carrying out the *i*-th threat; d_{rj} – the possibility of implementing at least one threat of the *j*-th asset.

Implementation scenarios for security objects can be presented by bayesian networks of trust

$$BN_{O3} = \langle A, Tab_{O3} \rangle, \quad (2)$$

where $A = \{a_i\}_{i=1}^{N_A}$ the plurality of offending actors; *NA* – number of all offender actions; Tab_{03} – the set of probability tables for each of the actions ai with "parent" actions parents (ai) .

If we consider dangerous programs as tools of unauthorized exposure, to assess the effectiveness of the organization's IP tools, the task is to synthesize a complex indicator based on the systematization of the relevant particular indicators and solve it as the task of building an optimal assessment.

It is also necessary to pay attention to the analysis of threats to IS resources in management systems and consider the means of integrated IP as an element of an integrated security system. Since one of the main causes of confidential information (CI) leakage is the human factor, it is advisable for an OIA to proceed from the suggestions of the author. And for the effective solution of questions on IP it is proposed to create a mathematical model of the CI and take appropriate countermeasures.

The following tasks can be solved in this direction:

a) a study of the motives pushing people to violate contracts and offenses;

b) the development of mechanisms for managing sensitive information carriers;

c) development of methods for informational impact on users of automated systems.

When building a model of a problem situation, let us denote by i the number of the operator-secret carrier:

$$i = \overline{1, N}. \quad (3)$$

The next step is to determine the full amount of confidential information Q:

$$Q = \sum_{i=1}^{K} q_i \ , \quad (4)$$

where q_i – is the volume of the *CI* block used by the *i*-th operator.

Then, $k(q_i)C(q_i)$ – is the "sale price" of the q_i block for a competitor, where $k(q_i)$ – is the utility coefficient of the q_i block for a competitor, $k(q_i) > 0$. And $C(q_i)$ – is the cost of qi block, consisting of the cost of its development, implementation and operation at Fig. 3.

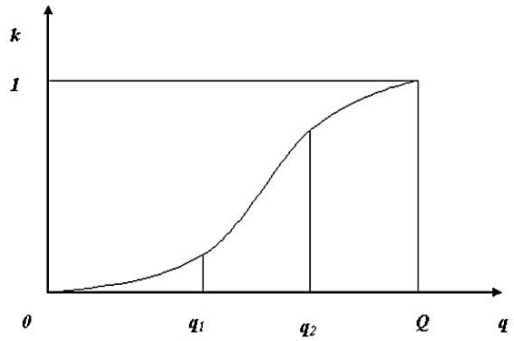

Fig. 3. Typical dependence of the utility coefficient of information k (qi) on its volume qi

A typical dependence of the utility coefficient of information $k(qi)$ on its volume q_i is shown in Fig. 3

To exclude the sale of confidential information, we presume that it is enough to fulfill the condition:

$$pl_i(nD(q_i) + lB(q_i)) + p2_i R(q_i) \triangleright$$
$$\triangleright k(q_i)C(q_i) - S(q_i) - p3_i U(q_i).$$

Where *pli* – the probability of exposing the seller; *N* – the number of months, the seller would work in the organization without offense; $D(q_i)$ – monthly salary; *l* – the number of awards; $B(q_i)$ – the size of premiums; *p*2*i* – probability of damage in case of exposure; $R(q_i)$ – the amount of moral and material damage, expressed in money.

If the manager of the *j*-th unit acts as the seller of confidential information, then i and qi should be replaced, respectively, by *j* and *mj*. If the seller is the administrator, then q should be replaced by *Q*.

Discussion and conclusions

Cybersecurity threats, such as spam, phishing, spyware, and botnets, pose challenges for governments, especially for such young governments in any

ISSN 2707-1758

developing country. Malicious authors (hackers) create new combined threats to counter the security of the information system. New threats make it possible to bypass system firewalls, workstation configurations and various other intrusion detection systems. Many governments are working on cybersecurity legislation to help protect consumers and themselves. Some legislative efforts are focused on establishing government structures to provide support against systemic attacks. Some government legislation has been designed to prosecute criminals in order to deter criminal activity. The legislation has well developed a basis for the detection, analysis and internal prevention of malicious software.

To effectively manage cybersecurity threats, governments must be involved from the beginning of the process to the end of the process. Businesses need to know where and to whom to report security risk information, and the government needs to support it. Improving the method of assessing the information security of computer systems from malicious software contains a recommendatory aspect of building an electronic government. The steps of building e-government, in contrast to the existing ones, differ in the completeness of the content of each stage of building e-government.

Authors' contribution: Serhii Dakov – analysis of sources, preparation of a literature review or theoretical foundations of research; Tetiana Laptieva – conceptualization; methodology, collection of empirical data and their validation; empirical research.

REFERENCES

Marco, P., & Marco, R. (2021). Security considerations about the adoption of web 2.0 technologies in sensitive eGovernment processes. *In Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance,* ICEGOV'11 (pp. 285–288), New York, USA, ACM.

Benjamin, E., Hofmeyr, S., Forrest, S., & Michel, van Eeten (2015). Analyzing and modeling longitudinal security data, Promise and pitfalls. *In Proceedings of the 31st Annual Computer Security Applications Conference*, ACSAC 2015 (pp. 391–400), New York, USA, ACM.

Malik, S., Peter, B., & Omer, F. Rana (2015). Estimating risk boundaries for persistent and stealthy cyber-attacks. *In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, SafeConfig*'15 (pp. 15–20), New York, USA, ACM.

Отримано редакцією журналу / Received: 17.03.24
Прорецензовано / Revised: 27.03.24
Схвалено до друку / Accepted: 13.05.24

Сергій ДАКОВ, канд. техн. наук
ORCID ID: 0000-0001-9413-3709
e-mail: dacov@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

Тетяна ЛАПТЄВА, асп.
ORCID ID: 0000-0002-7291-1829
e-mail: tetiana1986@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

УДОСКОНАЛЕННЯ МЕТОДІВ ОЦІНЮВАННЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ СИСТЕМИ ВІД ШКІДЛИВОГО ПРОГРАМНОГО КОДУ

В с т у п . *Питання забезпечення інформаційної безпеки державних інформаційних систем нині не лише не втрачає актуальності, але з розвитком концепції електронного урядування в країнах та збільшенням кількості електронних послуг, стає все важливішим для протидії шкідливому програмному коду.*

М е т о д и . *Використано метод аналізу оцінювання захисту комп'ютерної системи від шкідливого програмного коду; за допомогою методу оптимізації оцінювання захисту комп'ютерної системи вдосконалено метод захисту від шкідливого програмного коду.*

Р е з у л ь т а т и . *Удосконаленням методики оцінювання інформаційної захищеності комп'ютерних систем від шкідливого програмного забезпечення є рекомендаційний аспект побудови електронного урядування.*

В и с н о в к и . *Загрози кібербезпеці, такі як: спам, фішинг, шпигунське програмне забезпечення та ботнети, створюють проблеми для урядів, особливо для молодих урядів, у будь-якій країні, що розвивається. Зловмисники (хакери) створюють нові комбіновані загрози для протидії безпеці інформаційної системи. Нові загрози дозволяють обійти системні брандмауери, конфігурації робочих станцій і різні інші системи виявлення вторгнень. Багато урядів працюють над законодавством про кібербезпеку, щоб допомогти захистити споживачів і себе. Окремі законодавчі зусилля зосереджено на створенні державних структур для забезпечення підтримки проти системних атак. З метою стримування злочинної діяльності розроблено певні державні законодавства для переслідування зловмисників. Законодавством також добре розроблено основу для виявлення, аналізу та внутрішньої профілактики шкідливого програмного забезпечення.*

Для ефективного управління загрозами кібербезпеці уряди мають брати участь у цьому процесі від початку до його завершення. Підприємства повинні знати, куди та кому повідомляти інформацію про ризики у безпеці, а держава має це підтримувати. Удосконалення методики оцінювання інформаційної захищеності комп'ютерних систем від шкідливого програмного забезпечення містить рекомендаційний аспект побудови електронного уряду. Етапи побудови електронного урядування, на відміну від існуючих, відрізняються повнотою змісту кожного етапу побудови електронного урядування.

К л ю ч о в і с л о в а : *ідентифікація, інформаційна безпека, електронний уряд, організація інформаційної безпеки, брандмауери.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.