Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 6.

DOI: http://doi.org/10.32702/2307-2156.2024.6.4
УДК 351:004.02

K. Tanashchuk,
Doctor of Economic Sciences, Professor, Vice-Rector for Research,
State University of Intelligent Technologies and Telecommunications
ORCID ID: https://orcid.org/0000-0001-7834-1516
O. Tsyra,
PhD, Associate Professor, Acting Head of the Department of Public Administration and Digital Economy, State University of Intelligent Technologies and Telecommunications
ORCID ID: https://orcid.org/0000-0003-3552-2039
R. Ivasenko,
Senior Lecturer of the Department of Public Administration and Digital Economy, State University of Intelligent Technologies and Telecommunications
ORCID ID: https://orcid.org/ 0009-0006-0144-4959
S. Bazyka,
PhD in Public Administration, State University of Intelligent Technologies and Telecommunications
ORCID ID: https://orcid.org/0009-0003-2081-1222

RECOMMENDATIONS FOR MINIMIZING THE IMPACT OF THREATS ON INFORMATION RESOURCES OF PUBLIC ADMINISTRATION BODIES

К. О. Танащук,
д. е. н., професор, проректор з наукової роботи,
Державний університет інтелектуальних технологій і зв'язку
О. В. Цира,
к. філос. н., доцент, в.о. завідувача кафедри публічного управління та цифрової економіки, Державний університет інтелектуальних технологій і зв'язку
Р. М. Івасенко,
старший викладач кафедри публічного управління та цифрової економіки,
Державний університет інтелектуальних технологій і зв'язку
С. К. Базика,
к. держ. упр., Державний університет інтелектуальних технологій і зв'язку

РЕКОМЕНДАЦІЇ ЩОДО МІНІМІЗАЦІЇ ВПЛИВУ ЗАГРОЗ НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІВ ДЕРЖАВНОГО УПРАВЛІННЯ

The article reveals a comprehensive approach to improving the information security of public administration bodies through the integration of control procedures and periodic testing. The study emphasizes the importance of incident accounting in collecting statistical data necessary for effective information security management. The proposed approach includes the creation of a comprehensive system of registration of all security incidents and the implementation of a motivational bonus system for employees who detect security violations. The importance of incident recording is emphasized, noting that it provides the necessary feedback to improve security measures. Without a mechanism to log security incidents, sensitive information remains at significant risk. Regular registration and thorough documentation of security violations allows you to accurately assess the damage caused and identify patterns and trends in security violations, which is important for continuous improvement of the security system.

Regular testing of the current level of information security to identify vulnerabilities is recommended. Involving external organizations can provide an objective assessment of security measures, but internal audits can also be very effective. This testing includes an audit of all risk prevention, incident logging and access control procedures to ensure they are properly implemented and updated. The paper considers the zero-trust security model, which operates on the principle of "never trust, always verify", ensuring constant verification of all access attempts. This approach significantly reduces the risk of unauthorized access and increases the overall level of information protection. The proposed action mechanism also emphasizes the need to evaluate the effectiveness of the information security management system using specific indicators, such as the number of registered security breaches and the assessment of actual damages. Such assessments are vital to making informed decisions about necessary adjustments to security measures.

In addition, the importance of the integration of document management tools for streamlining the information environment of public administration bodies is emphasized. Proper documentation and classification of information resources according to the functional principle are necessary. Over-classification should be avoided to prevent employees from circumventing security measures. This detailed approach is aimed at creating a reliable information security system, ensuring confidentiality, integrity and availability of information in public administration bodies.

Стаття розкриває комплексний підхід з підвищення інформаційної безпеки органів державного управління шляхом інтеграції контрольних

процедур та періодичного тестування. В дослідженні наголошено на важливості обліку інцидентів у збиранні статистичних даних, необхідних для ефективного управління інформаційною безпекою. Запропонований підхід включає створення комплексної системи реєстрації всіх інцидентів безпеки та впровадження мотиваційної бонусної системи для співробітників, які виявляють порушення безпеки. Наголошено на важливості обліку інцидентів, зазначаючи, що він забезпечує необхідний зворотний зв'язок для вдосконалення заходів безпеки. Без механізму реєстрації інцидентів безпеки конфіденційна інформація залишається під значним ризиком. Регулярна реєстрація та ретельна документація порушень безпеки дозволяє точно оцінити завдану шкоду та визначити закономірності і тенденції в порушеннях безпеки, що є важливим для постійного вдосконалення системи безпеки.

Рекомендується проведення регулярного тестування поточного рівня інформаційної безпеки для виявлення вразливостей. Залучення зовнішніх організацій може забезпечити об'єктивну оцінку заходів безпеки, але внутрішні аудити також можуть бути дуже ефективними. Тестування включає аудит усіх процедур з попередження ризиків, реєстрації інцидентів і контролю доступу, щоб гарантувати їх правильне впровадження та оновлення. В роботі розглянуто модель безпеки zero-trust, яка діє на принципі "ніколи не довіряй, завжди перевіряй", забезпечуючи постійну перевірку всіх спроб доступу. Такий підхід значно знижує ризик несанкціонованого доступу та підвищує загальний рівень захисту інформації. Пропонований механізм дій також підкреслює необхідність оцінки ефективності системи управління інформаційною безпекою за допомогою конкретних показників, таких як кількість зареєстрованих порушень безпеки та оцінка фактичних збитків. Такі оцінки є життєво важливими для прийняття обґрунтованих рішень щодо необхідних коригувань заходів безпеки.

Крім того, наголошується на вагомості інтеграції інструментів управління документами для впорядкування інформаційного середовища органів державного управління. Належне документування та класифікація інформаційних ресурсів за функціональним принципом є необхідними. Слід уникати надмірної класифікації, щоб запобігти обхідним шляхам співробітників для уникнення заходів безпеки. Цей детальний підхід спрямований на створення надійної системи інформаційної безпеки, забезпечуючи конфіденційність, цілісність та доступність інформації в органах державного управління.

Keywords: *information security, Governmental bodies/administration, risk management, security audit, effectiveness of security measures, document management tools, confidentiality.*

Ключові слова: *інформаційна безпека, органи державного управління, керування ризиками, аудит безпеки, ефективність заходів безпеки, інструменти управління документами, конфіденційність*.

Statement of the problem in a general form and its connection with important scientific or practical tasks. The rapid pace of computerization and the development of the information society inevitably lead to the creation of a unified global information space. This space will accumulate all means of collecting, accumulating, processing, storing, and exchanging information between individuals, organizations, and states. At the core of these shifts lie the national information management infrastructures of developed countries such as the USA, China, Europe, and Japan. Consequently, there are solid grounds for the significant growth of political, economic, and military superiority of developed nations due to their leading role in informatization.

Technological capabilities are increasingly being applied in crucial areas of societal activity, such as telecommunications, energy, transportation, financial and banking systems, water supply, national security, and the sustainable operation of government ministries. The Internet, along with global and local computing networks, is now becoming an integral part of the infrastructure. All this impacts the volume and speed of information exchanges, as well as the security of utilizing such resources. These issues present a wide range of challenges that need to be addressed.

Analysis of recent research and publications. Information security is revealed as one of the most important concepts in science and various spheres of human activity in the scientific works of both domestic and foreign specialists: V.I. Shulga, N.R. Nyzhnyk, Y.M. Zharkov, V.T. Bilous, R. Kalyuzhny, N. Wiener, K. Shannon, L. Brillouin, and others. The relevance of methodological research is due to the importance of ensuring a high level of security of the information space, which contributes to its formation and development in the interests of the individual, society and the state. This requires appropriate legal norms and security institutions that guarantee the constant availability of data for making strategic decisions and

protecting the country's information resources.

The purpose of the article. The purpose of the study is to develop a comprehensive approach to improving the information security of public administration bodies, which includes the establishment of comprehensive control procedures to ensure permanent protection of information resources. The research is aimed at determining effective risk management methods, improving security measures and ensuring confidentiality, integrity and availability of information in public administration systems.

Presentation of the main research. International organizations and institutes specializing in complex information security issues have developed concepts of auditing and information risk management, formalized as international and national standards: ISO 15408, ISO 270xx, COBIT, PCI DSS, SAC, COSO, and others. Notably, the ISO 27000 series continues to evolve, setting out standards for ISMS requirements, risk management systems, metrics, and control mechanism effectiveness, along with implementation guidelines.

Ukraine has adopted a series of international standards for information security management, DSTU ISO/IEC 27000:2015. This standard defines information security as "the preservation of confidentiality, integrity, and availability of information, with potential inclusion of other properties such as authenticity and non-repudiation" [1].

Risk assessment is recognized as the most effective method for setting priorities in information protection. To establish a risk management system in IT security, the CRAMM (UK Government Risk Analysis and Management Method) is frequently used. Developed and standardized in Great Britain, CRAMM is globally utilized and is noted for its ability to economically justify an organization's information security management costs. Familiarity with these standards is a crucial first step in reducing threats to public administration information resources [2].

The second step in minimizing threats involves defining the structure of information resources and determining the confidentiality levels of stored information. Information must be structured to identify protection objects effectively. Typically, information resources are classified based on function. This approach entails appointing information resource owners and determining confidentiality

levels. Over-classification should be avoided, as overly restrictive access can lead employees to find ways around existing prohibitions. The confidentiality level can be indicated by an expert assessment of potential losses from information leakage [3].

To organize the information environment within public administration, it is advisable to implement document management tools. Department heads can be tasked with assessing the criticality of information. The guiding principle should be that information remains publicly accessible unless there is a compelling reason for confidentiality. Over-classification can hinder the efficiency of public administration bodies [4].

The third step is to establish a system for regulating access to information resources. The process for granting access should be clearly defined and governed by regulations, ensuring it is efficient since the effectiveness of the public administration depends on it. However, oversimplifying this process can lead to unauthorized access to confidential information. It's essential to strike a balance between protecting information and allowing free exchange within and outside the public administration. Excessive restrictions can lead to alternative, unprotected methods of information exchange, nullifying protection efforts.

The next step involves creating a plan to enhance the security of information resources in public administration. This plan should detail the timing and scope of necessary actions to prevent or minimize damage in the event of risk realization. It should specify who will perform these actions, where and when they will take place, what resources are needed, and what threats will be mitigated. Each identified priority risk should have corresponding mitigation measures, ideally addressing multiple risks simultaneously. Responsibilities, deadlines, budgets, and control points should be clearly defined [5].

The planning process should result in a detailed schedule of activities aimed at eliminating or minimizing damage from realized risks. However, it is crucial not only to create this plan but also to implement it on time. Delays can render previous efforts ineffective. The goal of the information security management process is to execute planned measures to minimize risks, monitor the quality of results, and adhere to timelines. Introducing control procedures into existing processes can be part of this plan, enhancing preventive measures and overall information security [6].

Furthermore, it is essential to establish a system for recording security incidents involving information resources of public administration bodies. Incident logging provides valuable statistical data for feedback, necessary for managing information security. Without a registration mechanism, confidential information remains at risk, even if incidents are occurring unnoticed. Regularly documenting security violations helps assess the damage caused and identify patterns. To motivate employees, a bonus system for identifying security breaches can be implemented. Initially, a simple spreadsheet can be used to record incidents, with all staff contributing to this log. Having such statistics over time allows for better risk assessment and evaluation of the effectiveness of security measures.

An essential step in risk minimization is organizing regular testing of the public administration's information security levels. Regular security testing is crucial, and while external organizations can be hired to identify vulnerabilities, this task can often be more effectively handled internally. Information security testing involves auditing all procedures related to risk prevention, incident logging, and access control [7].

Such testing verifies the effectiveness of current preventive measures and highlights areas for improvement. Control procedures can range from simple to complex. For instance, any document issued by a public administration body should be created with the involvement of at least two people, or access to materials should require confirmation from two individuals from different departments [5].

Following the implementation of these measures, it is necessary to assess the effectiveness of the information security management system. Evaluation can be based on the following indicators:

- the number of recorded information security incidents;
- assessment of actual damages resulting from security breaches;
- average time taken for information protection procedures;
- percentage of implementation of the approved information protection plan;
- comparison of expert estimates of damage from information security risks against the costs of implementing security measures.

From a technical standpoint, minimizing the impact of threats on public administration's information resources begins with protecting workstations, as they

are the starting point for any computer network. This includes:

- operating system protection tools;
- antivirus software;
- additional user authentication devices;
- tools to prevent unauthorized access to workstations;
- application-level encryption tools.

These measures form the first layer of the information security subsystem in automated systems [8].

In the second stage, individual workstations are connected to local networks, dedicated servers are installed, and internet access is organized through the local network. At this stage, second-level information protection tools are employed, including:

- security measures for network operating systems;
- tools for resource access control;
- domain protection mechanisms for the local network;
- user authentication servers;
- firewall proxy servers.
- tools for detecting attacks and vulnerabilities in local network protection.

When local networks are connected to a common intranet using public networks (including the Internet) as a communication medium, information exchange security is ensured through VPN technology, forming the third level of information security.

Given that many modern threats arise and spread due to low awareness among personnel, the zero-trust model has gained wide acceptance in global practice. This model operates on the principle of "never trust, always verify," ensuring a higher level of security.

This strategic approach to protection is based on the mandatory verification of each entity within the network architecture of public administration information resources. Trust is no longer a binary attribute nor granted indefinitely. It is unrealistic to assume that internal objects are inherently trustworthy and can be managed directly to reduce risk, or that a single check is sufficient. The zero-trust security model mandates the validation of every access attempt [2].

Traditional security approaches assume that all objects within public administration information resources can be trusted. This assumption is outdated due to factors such as mobility, bring-your-own-device (BYOD) policies, the Internet of Things (IoT), the shift to cloud solutions, increased collaboration, and a focus on sustainable management processes. Under the zero-trust model, all resources are treated as third-party entities and are continuously validated before access is granted. Moreover, access rights are provided only to the extent necessary.

The zero-trust model enhances control over users, devices, containers, networks, and applications by verifying the reliability of the source for every resource access request. By segmenting resources and granting access with the minimum necessary rights, this model reduces the attack surface within the public administration environment. It strikes an optimal balance between security and usability. Security professionals can make it more challenging for attackers to achieve their objectives, such as credential harvesting, gaining network access, or lateral movement. Meanwhile, users can work stably, securely, and efficiently regardless of their location, the endpoints they use, or the type of applications (local or cloud) they interact with.

Future research should focus on the following areas to enhance the effectiveness of information security in public administration:

- Advanced Threat Detection and Response: investigating the integration of artificial intelligence and machine learning algorithms to improve real-time threat detection and automated response mechanisms. These technologies can help identify and mitigate threats faster and more accurately than traditional methods.
- User Behaviour Analytics (UBA): developing models that analyse user behaviour to detect anomalies that could indicate potential security breaches. This approach can be particularly useful in identifying insider threats and preventing unauthorized access.
- Blockchain Technology: exploring the potential of blockchain technology in enhancing the security of information systems. Blockchain's decentralized and immutable nature can provide an additional layer of security for sensitive data.
- Enhanced Training Programs: conducting studies to assess the

effectiveness of current training programs and developing more comprehensive training modules that focus on the latest security threats and best practices. Emphasizing the role of human factors in information security can significantly reduce the risk of breaches caused by human error.

- Policy and Regulatory Frameworks: analysing the impact of evolving policy and regulatory frameworks on information security practices. Understanding the implications of new regulations can help in adapting and updating security measures to ensure compliance and protect against emerging threats.

- Cross-Organizational Collaboration: investigating the benefits and challenges of cross-organizational collaboration in information security. Sharing knowledge, resources, and best practices between different public administration bodies can lead to more robust and unified security strategies [4].

Conclusions and prospects of further investigations in this direction. The research underscores the critical importance of a comprehensive and structured approach to information security within public administration bodies. The adoption of international standards such as ISO 27000 and methodologies like CRAMM provides a robust framework for risk management and the preservation of information confidentiality, integrity, and availability. The emphasis on regular testing, incident logging, and the zero-trust security model offers a multi-layered defence strategy that significantly mitigates the risks associated with unauthorized access and data breaches. The findings highlight that while establishing stringent security measures is vital, it is equally important to balance these measures with operational efficiency. Overly restrictive policies can lead to counterproductive behaviours where employees may seek ways to bypass security protocols, thereby compromising the entire security infrastructure. Therefore, the study advocates for a balanced approach that ensures security without hampering the workflow and productivity of public administration bodies.

By addressing these areas, future research can provide deeper insights and more effective solutions for protecting the information resources of public administration bodies, ensuring that they remain resilient in the face of evolving cyber threats.

Література

1. Василюк В. Об’єкти захисту інформації. Методи та засоби захисту інформації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2006. № 2 (13). С. 88-102.
2. Методика управління ризиками інформаційної безпеки корпорації Microsoft. Вебсайт компанії Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/risk-management/microsoft-purview-insider-risk-management (дата доступу: 05.05.2024).
3. Гловацький В.В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів. *Зв’язок*. 2016. № 5. С.13-16.
4. Wilson, E. (2000) Network Monitoring and Analysis. Fault finding methods: a practical guide. Prentice Hall. 359 c.
5. Казакова Н.Ф., Скопа О.О. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем. *Системи обробки інформації*. 2009. № 7 (79). С. 48-54.
6. Казакова Н.Ф. Розробка та дослідження ефективних алгоритмів визначення надійності пристроїв управління резервним обладнанням інформаційних мереж: дис. канд. техн. наук: 05.12.02 / Український НДІ зв’язку. Київ, 2005. 215 с.
7. Присяжнюк М.М., Бєлошевич Я.С. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету ім. Тараса Шевченка*. 2013. № 1 (39). С. 37-40.
8. Головань С.М., Давиденко А.М., Щербак Л.М. Про термінологію в області безпеки інформації. *Моделювання та інформаційні технології*. 2010. № 57. С. 37-41.
9. Пузиренко О.Г., Івко В.О., Лаврут О.О. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. *Системна обробка інформації*. 2015. № 3 (128). С.76-77.

References

1. Vasylyuk, V. (2006), “Objects of information protection. Methods and means of information protection”, *Legal, regulatory and metrological support of the information protection system in Ukraine*, vol. 2 (13). pp. 88–102.
2. Website of Microsoft corporation (2024), “Information security risk management methodology of the Microsoft corporation”, Available at: https://www.microsoft.com/uk-ua/security/business/risk-management/microsoft-purview-insider-risk-management (Accessed 5 June 2024).

3. Glowatsky, V.V. (2016), “Methods of assessing the state of security and threats of information resources”, *Zv'yazok*, vol. 5, pp. 13-16.

4. Wilson, E. (2000) Network Monitoring and Analysis. Fault finding methods: a practical guide. Prentice Hall. 359 c.

5. Kazakova, N.F. and Skopa, O.O. (2009), “Analysis of the development of modern directions of information security of automated systems”, *Information processing systems*, vol. 7(79), pp. 48-54.

6. Kazakova, N.F. (2005), “Development and research of effective algorithms for determining the reliability of devices for managing backup equipment of information networks”, diss. Ph.D. Technical Sciences: 05.12.02, Ukraine, 215 p.

7. Prysiazhnyuk, M.M. and Beloshevich, Y.S. (2013), “Information security of Ukraine in modern conditions”, *Bulletin of the Kyiv National University named after Taras Shevchenko*, vol. 1 (39), pp. 37-40.

8. Golovan, S.M., Davydenko, A.M. and Shcherbak, L.M. (2010), “About terminology in the field of information security”, *Modelling and information technologies*. vol. 57, pp. 37-41.

9. Puzyrenko, O.G., Ivko, V.O. and Lavrut, O.O. (2015), “Application of information security risk assessment models in information and telecommunication systems”, *System information processing*, vol. (128), pp. 76-77.

Стаття надійшла до редакції 10.06.2024 р.