The Security of Information Systems as a Factor in the Effectiveness of Network Management

UDC: 35:07 DOI: https://doi.org/10.15421/152331

Zaporozhets Tetiana[1]
Dr.Sc., Assoc. Prof., https://orcid.org/0000-0003-1914-9481, zaporozhets.tetiana@kneu.edu.ua
Tsymbalenko Yana[2]
Ph.D., Assoc. Prof., https://orcid.org/0000-0003-0442-7549, eva06102010@gmail.com
[1]Kyiv National Economic University named after Vadym Hetman (Kyiv, Ukraine)
[2]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Kyiv, Ukraine)

Abstract

The purpose of the study is to determine the main aspects and directions of ensuring the security of information systems of state authorities as a factor of effectiveness network management.

The relevance of the research is determined by the importance and necessity of researching the problems in the indicated direction, in particular regarding the protection of networks from unauthorized access, countering data leakage, prevention of cyber attacks, prevention of the spread of viruses, malicious software, etc.

The results. The areas of research of foreign scientists engaged in the scientific search for problems of the functioning of information and analytical networks in the public sector, the role of information in the network economy, management of state information systems, aspects of cyber security and problems of building network infrastructure for public administration entities have been analyzed. Approaches to the modern analysis of standards and policies, which help to determine requirements for the security of networks and information systems, have been studied.

Conclusions. The use of modern technologies, such as cloud computing, artificial intelligence, data analytics significantly improve the functioning of state information networks, emphasize the importance of establishing standards, principles and regulatory rules in the field of information technologies and networks in order to ensure compatibility and security, emphasize the importance of integrating modern technologies, cyber security and effective information management to improve network management and ensure the quality of services to citizens. It was found that scientists apply the concept of "network security management" and justify approaches to improving its architecture, interpreting this process as a set of solutions and strategies designed to implement complex management of information flow in the organization's networks. It was emphasized that information and cyber security are becoming key elements of modern state administration in all spheres of social development, and the use of an automated and integrated architecture of its functioning will ensure the proper quality of network management.

Keywords: network management, information security, cyber security, information systems, public sector, digitalization

Безпека інформаційних систем як чинник ефективності мережевого управління

Запорожець Тетяна[1], **Цимбаленко Яна**[2]
[1]Київський національний економічний університет імені Вадима Гетьмана (Київ, Україна)
[2]Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" (Київ, Україна)

Анотація

Мета дослідження полягає у визначенні основних аспектів і напрямів забезпечення безпеки інформаційних систем органів державної влади як чинника ефективності мережевого управління.

Актуальність дослідження обумовлюється важливістю та необхідністю дослідження проблем за вказаним напрямом, зокрема щодо захисту мереж від несанкціонованого доступу, протидії витоку даних, попередження кібератак, запобігання поширенню вірусів, шкідливого програмного забезпечення тощо.

Результати. Проаналізовано напрями досліджень зарубіжних вчених, які займаються науковим пошуком проблем функціонування інформаційно-аналітичних мереж у державному секторі, ролі інформації в мережевій економіці, управління державними інформаційними системами, аспектів кібербезпеки та проблем розбудови мережевої інфраструктури для суб'єктів державного управління. Досліджено підходи до сучасного аналізу стандартів і політик, які допомагають визначити вимоги до безпеки мереж та інформаційних систем.

Висновки. Використання сучасних технологій, таких як хмарні обчислення, штучний інтелект, аналітика даних значно покращують функціонування державних інформаційних мереж, наголошують на важливості встановлення стандартів, принципів та правил регулювання в галузі інформаційних технологій та мереж з метою забезпечення сумісності та безпеки, підкреслюють важливість інтеграції сучасних технологій, кібербезпеки й ефективного управління інформацією для покращення мережевого управління та забезпечення якості надання послуг громадянам. З'ясовано, що науковці застосовують поняття «управління мережевою безпекою» та обгрунтовують підходи щодо удосконалення її архітектури, тлумачачи цей процес як набір рішень і стратегій, призначених для реалізації комплексного управління інформаційним обігом у мережах організації. Наголошено, що інформаційна та кібербезпека стають ключовими елементами сучасного державного управління в усіх сферах суспільного розвитку, а використання автоматизованої та інтегрованої архітектури її функціонування дозволяє забезпечити належну якість мережевого управління.

Ключові слова: мережеве управління, інформаційна безпека, кібербезпека, інформаційні системи, державний сектор, цифровізація

Стаття надійшла / Article arrived: 07.09.2023 Схвалено до друку / Accepted: 31.10.2023

Вступ.

Щороку кількість пристроїв, підключених до мереж державного сектору росте, відтак забезпечення їх безпеки та відповідне управління стають усе складнішим завданням. Одним із ключових аспектів мережевого управління є постійний моніторинг та керування інформаційними системами. Це включає в себе виявлення та вирішення проблем, збільшення ефективності роботи мереж та забезпечення їх коректного функціонування, що є постійним процесом та вимагає поєднання технологічних, організаційних та людських ресурсів. Мережева діяльність органів державної влади здійснюється у процесі керування та адміністрування інформаційними та комунікаційними взаємозв'язками, які використовуються державними органами для забезпечення ефективного обміну даними, розвитку мережевої інфраструктури, управління інформаційними ресурсами в межах державної системи. У багатьох сферах, таких як медична галузь, транспорт, енергетика, екологія, фінанси критично важливими є надійність, керованість та доступність мереж, оскільки порушення роботи або атаки на такі мережі можуть призвести до серйозних наслідків.

Аналіз попередніх досліджень і публікацій.

Учені з усього світу займаються дослідженням проблем функціонування інформаційно-аналітичних мереж у державному секторі. До прикладу, В. Майєр-Шенбергер (Viktor Mayer-Schönberger), В. Даттон (William Dutton) з Оксфордського університету є відомими дослідниками ролі інформації в мережевій економіці, інформаційних технологій та мереж у державному секторі (Mayer-Schönberger, 2022); (Dutton, 2018). Д. Фаунтейн (Jane Fountain) з Массачусетського Університету є автором публікацій, що стосуються управління державними інформаційними системами (Fountain, 2001). Е. Андерсон (Evan Anderson) з Національного інституту стандартів та технологій (NIST) США вивчає аспекти кібербезпеки та проблеми розбудови мережевої інфраструктури для суб'єктів державного управління (Anderson, 2008).

Мета дослідження полягає у визначенні основних аспектів і напрямів забезпечення безпеки інформаційних систем органів державної влади як чинника ефективності мережевого управління.

Результати дослідження.

Мережеве управління включає в себе низку стратегій, технологій і практик, спрямованих на захист мереж та інформації, що міститься у їх складі. Важливим аспектом забезпечення інформаційної та кібербезпеки є аутентифікація, яка визначає ідентичність користувача, та авторизація, яка надає або відмовляє у доступі до ресурсів на основі цієї ідентичності. При цьому шифрування даних в мережах є критично важливим під час передачі інформації через мережу та захисту її конфіденційності, а моніторинг і аудит діяльності в мережі допомагають виявити потенційні загрози та атаки. Це важливо для вчасного реагування на інциденти та вивчення подій для подальшого покращення безпеки. Окрім того, захист мереж від несанкціонованого доступу, протидія витоку даних, попередження кібератак, запобігання поширенню вірусів та шкідливого програмного забезпечення обумовлюють гостру потребу у забезпеченні інформаційної та кібернетичної безпеки, особливо у випадках надзвичайних ситуацій.

Результати досліджень зазначених вище науковців приводять до висновку, що використання сучасних технологій, таких як хмарні обчислення, штучний інтелект, аналітика даних значно покращують функціонування державних інформаційних мереж, наголошують на важливості встановлення стандартів, принципів та правил регулювання в галузі інформаційних технологій та мереж з метою забезпечення сумісності та безпеки, підкреслюють важливість інтеграції сучасних технологій, кібербезпеки й ефективного управління інформацією для покращення мережевого управління та забезпечення якості надання послуг громадянам.

Суб'єкти державного управління в усьому світі роблять величезні інвестиції в технологічні засоби протидії загрозам у інформаційному просторі. Тим не менш, не всі установи в змозі захистити власні інформаційні активи, оскільки вони покладаються в основному на технічні рішення, які почасти є контекстуально недостатньо сумісними. Шведські дослідники зазначають, що у сучасному цифровому світі безпека даних інформаційних мереж стала головним пріоритетом для організацій задля їх захисту від зловмисних атак. За останні роки кількість кіберзлочинів і витоків даних різко зросла. При цьому значна кількість інцидентів інформаційної безпеки пов'язується з людським фактором.

Тому державні установи та організації постійно намагаються підтримувати безпеку власних інформаційних активів та інфраструктурних мереж, що, у свою чергу, змушує їх здійснювати величезні інвестиції у технологічні заходи протидії. Однак простого зосередження на технічних аспектах проблем

безпеки недостатньо, оскільки інформаційна та кібернетична безпека є мультидисциплінарною за своєю природою, і не лише людський фактор відіграє в ній головну роль (Khando, Gao, Islam, & Salman, 2021).

Агентство Європейського Союзу з кібербезпеки ENISA є службою, яка опікується досягненням високого рівня кібербезпеки у Європі. Засноване у 2004 році, агентство керується Законом ЄС про кібербезпеку, сприяє формуванню та розвитку кіберполітики ЄС, підвищує надійність цифрових продуктів, послуг та процесів сертифікації, співпрацює з державами-членами ЄС з питань готовності до кібервикликів завтрашнього дня. Через обмін знаннями, потужну роботу із розбудови, підвищення суспільної обізнаності, агентство співпрацює зі своїми ключовими зацікавленими сторонами з метою зміцнення довіри до державних органів, підвищує стійкість мережевої інфраструктури держав-членів ЄС та, зрештою, розвиває європейське суспільство, забезпечуючи цифровий захист громадян. У жовтні 2023 року агентство оприлюднило одинадцяте видання щорічного звіту ENISA Threat Landscape (ETL) про стан ландшафту загроз кібербезпеці на європейському континенті. У документі окреслено головні загрози, що спостерігаються сьогодні, характеристику учасників, основні тенденції розвитку сучасного кібернетичного простору (ENISA Threat Landscape, 2023).

Науковці здійснюють аналіз стандартів і політик, які допомагають визначити вимоги до безпеки мереж та інформаційних систем. Застосовуючи поняття «управління мережевою безпекою», вчені обґрунтовують підходи щодо удосконалення її архітектури та тлумачать цей процес як набір рішень і стратегій, призначених для реалізації комплексного управління інформаційним обігом у мережах організації. Це включає в себе впровадження рішень, які забезпечують централізоване керування мережевою безпекою; використання аудиту та тестування для оцінки інфраструктури мережі та інформаційних систем з точки зору безпеки; розробку процесів, які гарантують, що установа має відповідні ресурси, здатна ефективно ідентифікувати та керувати ризиками безпеки, а також виявляти потенційні загрози безпеці мережі та реагувати на них. Це є критично важлива галузь досліджень, оскільки забезпечення безпеки інформаційних мереж та систем є важливим завданням у сучасному цифровому світі, де загрози кібербезпеці мають тенденцію до зростання (Zhao, & Song, 2020; Bringhenti, Marchetto, Sisto, & Valenza, 2023).

Сьогодні кібербезпека розглядається як невід'ємний цифровий механізм захисту інформаційних мереж національних урядів, підприємств, навчальних закладів, установ та організацій. Сфера застосування кібербезпеки не обмежується лише протидією навмисним атакам, таким як несанкціонований доступ, але також охоплює ненавмисну компрометацію інформаційної інфраструктури, наприклад, спричиненої стихійними лихами, повінню, землетрусом.

Останнє десятиліття стало свідком значного збільшення кількості документів і нормативних актів у всіх сферах державного управління, пов'язаних з необхідністю захисту баз даних та інфраструктурних мереж. Серед основних галузей – охорона здоров'я, освітня сфера, фінанси, соціальний захист, оборона, енергетика, споживчі дані тощо.

До прикладу, кіберзлочини спрямовуються на сектор охорони здоров'я як на одну з найприбутковіших сфер. Незважаючи на те, що фінансові послуги мають найвищий ризик кіберзагроз, фахівці зазначають, що з 2015 року сектор охорони здоров'я є однією з галузей, які найбільше зазнають кібератак. Низка сервісів у медичній сфері базуються на Інтернеті речей (IoT), де кіберпростір взаємопов'язаний із фізичним світом (Paul, Maglaras, Ferrag, & Almomani, 2023).

Програми IoT для охорони здоров'я містять дані пацієнтів із численних джерел у формі електронних медичних карт (EHR), які можуть передаватися через Інтернет або зберігатися в хмарі. Окрім того, стрімко зростає взаємна інтеграція різних інформаційних систем та мереж у сфері охорони здоров'я, таких як системи електронної медичної документації, медичні пристрої, лабораторні інформаційні системи, що збільшує кримінальну зацікавленість для атак і вимагає посиленого кіберзахисту. Інформаційним та кіберзагрозам піддається і сфера освіти. Навчальні заклади зазвичай мають велику кількість інформації, включаючи академічні дані, бюджети, договори та іншу конфіденційну інформацію. Ці загрози можуть мати серйозні наслідки для навчальних установ, студентів, викладачів та адміністраторів.

IT-рішення для фінансової індустрії – це складна мережа з безліччю завдань та функцій. На додаток до «стандартних» мережевих вимог, таких як висока доступність і планування пропускної здатності, фінансова сфера також містить низку галузевих проблемам, пов'язаних з функціонуваням систем та мереж. Мережі фінансових послуг включають широкий спектр окремих мереж, розташованих у кількох місцях,

як-от філії, банкомати, корпоративні центри обробки даних і домашні офіси для віддалених працівників. Окрім того, високочастотна торгівельна діяльність, де кожен аспект повсякденних операцій та наносекунди можуть мати значення, є характерним прикладом того, наскільки важливою є ефективність мережі у фінансовому секторі. Від високої продуктивності мережі залежить рівень довіри і міжнародних партнерів, і пересічнх громадян, тому гучні зломи чи інші проблеми можуть завдати серйозної шкоди довгостроковій репутації. Це означає, що безпека мережі є головним пріоритетом для кожного суб'єкта державного управління фінансового сектора.

Сфера соціального захисту стикається з численними проблемами функціонування інформаційних систем, які можуть впливати на ефективність та надійність надання соціальних послуг та захисту потреб громадян. Основні проблеми включають: конфіденційність та захист особистих даних громадян; нестабільність мережевих систем та можливість збоїв; обмеженість доступу до послуг через бюрократичні бар'єри; несумісність та розрізненість інформаційних систем; застарілі технології та програмне забезпечення; можливість зловживання та шахрайства в системах.

Прогрес у цифровізації енергетичного сектору забезпечує суттєві економічні переваги, зокрема завдяки оптимізації та підвищенню ефективності процесу споживання енергії. Тим не менш, сьогодні, під час воєнного стану в Україні, такий прогрес у цьому секторі також посилює загрозу кібератак, які спрямовані на мережі енергетичної інфраструктури.

Протягом останніх років США та ЄС неухильно прагнуть дотримуватись низки правил і політик для захисту енергетичного сектору від потенційних кібератак. Науковці вирізняють декілька відмінностей у підходах ЄС і США. США віддали перевагу схемі «поглибленої безпеки» з детальними та суворими правилами в деяких секторах, в той час як ЄС прийняв вичерпну та гнучку систему з широким охопленням спектру питань щодо впровадження стандартів для держав-членів. З огляду на докладні та точні правила кібербезпеки та їх застосування, схема США є надзвичайно прогресивною, відтак на сьогодні відбувається процес гармонізації нормативних актів між США та ЄС для запровадження спільних стандартів інформаційної та кібербезпеки. Зазначене підкреслює необхідність спільного підходу до боротьби з кіберзагрозами відповідно до Європейського Порядку Денного з безпеки 2015-2020 (European Agenda on Security 2015-2020, 2017).

За останні два десятиліття мережі у оборонній сфері динамічно трансформувались. Сучасний ринок кібербезпеки включає різноманітні рішення, починаючи від прикладних аспектів, хмарних середовищ, бездротової безпеки, які можуть виконувати різні завдання та забезпечити надійний захист у багаторівневому мережевому управлінні. Ці рішення включають в себе управління безпекою інформації, рішення для аналізу мережевого потоку, інтеграцію базової уніфікованої системи керування загрозами тощо. Зростаючий ризик кібератак на критично важливу інфраструктуру залишається вирішальним рушієм еволюції технологічних рішень кібербезпеки. За оцінками експетрів, розподіл коштів на різні військові програми, включно з розподілом ресурсів на дослідження та розробку рішень інформаційної та кібербезпеки для наземних бойових систем зв'язку, оцінюється як найбільші майбутні тенденції для оборонної промисловості.

Висновки.

Таким чином, стандарти безпеки інформаційних систем як чинник ефективності мережевого управління є потребою часу та невід'ємною складовою будь-якої галузі, яка безпосередньо чи опосередковано стосується інформаційних мереж та віддаленого доступу. Стандарти безпеки допомагають ідентифікувати потенційні загрози та встановлювати проактивні заходи для захисту мереж та інформації від кібератак, дають можливість збудувати стійку та надійну інфраструктуру, що сприяє безперебійному функціонуванню мережі; дозволяють ідентифікувати, оцінювати та керувати ризиками, пов'язаними з інформаційними системами, тим самим покращуючи ефективність управління. Органи влади стають все більш залежними від новітніх технологій для ефективного забезпечення різних аспектів своєї діяльності. Це вимагає посилення інформаційної та кібербезпеки. Значний приріст кількості нормативних документів в усіх сферах державного управління, які пов'язані із захистом інформаційних баз даних та інфраструктурних мереж, обумовлюються наступними факторами: зростанням кіберзагроз, що ускладнює функціонування інформаційних ресурсів та мережевих інфраструктур у різних сферах; необхідністю забезпечення технологічної відповідності стандартам безпеки; зростанням обсягів даних, включаючи конфіденційну та особисту інформацію, що вимагає збільшеної уваги до її захисту; потребою змін в законодавстві

та формуванням нових регуляторних положень з проблем інформаційної та кібкербезпеки.

У зв'язку з цим, уряди та органи влади активно реагують на зазначені виклики шляхом розробки та впровадження стратегій кіберзахисту, нормативно-правового регулювання та створення міжнародних партнерств для обміну інформацією та спільної боротьби з кіберзагрозами. Інформаційна безпека, кібербезпека стають ключовими елементами сучасного державного управління в усіх сферах суспільного розвитку. Через певні загрози громадській безпеці та значні фінансові збитки національні уряди розглядають універсальні методи безпеки, визначені в різноманітних нормативних актах і галузевих стандартах. Незалежно від обсягів і складності інформаційних мереж і систем, прийнятої стратегії управління ризиками, важливим завданням є використання автоматизованої та інтегрованої архітектури, що дозволить оперативно функціонувати у великих масштабах, забезпечуючи належну якість мережевого управління.

REFERENCES

A European Agenda On Security. (2017). Retrieved from https://home-affairs.ec.europa.eu/system/files/2020-09/20170907_a_european_agenda_on_security_-_state_of_play_en.pdf

Anderson, E. (2008). Enterprise information security strategies. *Computers & Security*. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0167404808000060

Bringhenti, D., Marchetto, G., Sisto, R., & Valenza, F. (2023). Automation for Network Security Configuration: State of the Art and Research Trends. *ACM Computing Surveys*, 56(3). Retrieved from https://dl.acm.org/doi/pdf/10.1145/3616401

Dutton, W. (2018). *Fostering a cybersecurity mindset*. Retrieved from https://www.hiig.de/en/fostering-cybersecurity-mindset/

ENISA Threat Landscape. (2023). Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Fountain, J. (2001). *Building the virtual state: Information technology and institutional change*. Retrieved from https://www.academia.edu/646758/Building_the_virtual_state_Information_technology_and_institutional_change

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: a systematic literature review. *Computers & Security*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404821000912

Mayer-Schönberger, V. (2022). *Access Rules: Freeing Data from Big Tech for a Better Future*. Retrieved from https://www.oii.ox.ac.uk/research/publications/access-rules-freeing-data-from-big-tech-for-a-better-future/

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: a study on privacy and security concerns. *ICT Express*, 9(4). Retrieved from https://www.sciencedirect.com/science/article/pii/S2405959523000243

Zhao, G., & Song, J. (2020). Network security model based on active defense and passive defense hybrid strategy. *Journal of Intelligent & Fuzzy*. Retrieved from https://www.researchgate.net/publication/345205330_Network_security_model_based_on_active_defense_and_passive_defense_hybrid_strategy