**DOI: 10.31319/2519-8106.2(53)2025.341883**
**UDC 004.75:004.49:519.72**

**Pasichnyk Volodymyr**[1], Candidate of Physical and Mathematical Sciences, Associate Professor, Principal developer of Software Engineering and Digital Transformation Company Luxoft
**Пасічник В.А.**, кандидат фізико-математичних наук, доцент, головний розробник компанії з інженерії програмного забезпечення і цифрової трансформації Luxoft
ORCID: 0000-0001-9434-563X
e-mail: vladimir.pasechnik@gmail.com

**Pasichnyk Anatoliy**[2], Doctor of Physical and Mathematical Sciences, Professor, Professor of the Department of Mathematical Modeling and System Analysis,
**Пасічник А.М.**, доктор фізико-математичних наук, професор, професор кафедри математичного моделювання та системного аналізу
ORCID: 0000-0002-8561-1374
e-mail: panukr977@gmail.com

[1] Software Engineering and Digital Transformation Company Luxoft, London, Great Britain
Компанія з інженерії програмного забезпечення і цифрової трансформації Luxoft, Лондон, Велика Британія
[2] Dnipro State Technical University, Kamianske, Ukraine
Дніпровський державний технічний університет, м. Кам'янське, Україна

## METHODS AND ALGORITHMS FOR INCREASING RELIABILITY AND LEVEL SECURITY OF CORPORATE TELECOMMUNICATIONS NETWORKS

## МЕТОДИ ТА АЛГОРИТМИ ПІДВИЩЕННЯ НАДІЙНОСТІ І РІВНЯ БЕЗПЕКИ КОРПОРАТИВНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

*The article proposes original solutions to improve the security of corporate telecommunications networks, which make it possible to reduce potential system vulnerabilities and prevent possible information losses. The proposed model of connection of the Guest Wi-Fi allows you to implement safe architecture through additional user identification with its audit in the middle of the corporate perimeter of the network, while protecting the credentials from external influence and implementing the principle of "ZERO TRUST"* (*"never trust, always verify"*).

*To develop a model of high -security telecommunications corporate telecommunications networks, it is proposed to apply the algorithm of the prompts and encryption of each authentication recording separately by Hint Keys. The proposed architecture with prompts and separate encryption of each entry increases the safety of the network and reduces the effects of a possible break. The results of the study show that the implementation of the proposed models and algorithms for connecting Guest Wi-Fi and functioning of password managers in corporate telecommunications networks will increase the level of safety by isolation of each account and demanding interactive participation of the user to access it.*

***Keywords****: corporate networks, information protection algorithms, authentication, access control.*

*У статті проведено дослідження моделей і алгоритмів систем інформаційної безпеки корпоративних телекомунікаційних мереж. За результатами проведеного аналізу виявлені проблемні питання захисту таких мереж пов'язані із необхідністю удосконалення моделей підключення гостьової системи Wi-Fi та алгоритмів функціонування менеджерів паролів які потребують подальшого розвитку для підвищення рівня безпеки зберігання паролів, автозаповнення та синхронізації між пристроями.*

*Для покращення безпеки корпоративних телекомунікаційних мереж запропоновані оригінальні рішення які дозволяють зменшити потенційні вразливості системи та запобігти можливим інформаційним втратам. Запропонована модель підключення гостьового Wi-Fi дозволяє реалізувати безпечну архітектуру за рахунок додаткової ідентифікації користувача з його аудитом всередині корпоративного периметру мережі, водночас захищаючи облікові дані від зовнішнього впливу та реалізуючи принцип "Zero Trust"* (*"ніколи не довіряй, завжди перевіряй"*).

*Для розробки моделі менеджерів паролів корпоративних телекомунікаційних мереж підвищеного рівня безпеки пропонується застосувати алгоритм підказок та шифрування кожного запису автентифікації окремо за ключами підказок (hint keys). Тобто, менеджери паролів мають еволюціонувати – від централізованого "вулта" до моделі з поетапним доступом та контекстною авторизацією. Запропонована архітектура з підказками та окремим шифруванням кожного запису підвищує безпеку мережі та зменшує наслідки можливого зламу. Результати проведеного дослідження показують, що реалізація запропонованих в статті моделей і алгоритмів підключення до гостьової системи Wi-Fi та функціонування менеджерів паролів корпоративних телекомунікаційних мереж дозволить підвищити рівень безпеки, ізолюючи кожен обліковий запис і вимагаючи інтерактивної участі користувача для доступу до нього.*

***Ключові слова**: корпоративні мережі, алгоритми захисту інформації, автентифікація, контроль доступу.*

**Problem's formulation**

In today's context, information network technologies are one of the main elements of the effective functioning of financial and economic, industrial and social systems and are constantly modernized by introducing new methods and technologies of transmission, processing and storage of information. The widespread use of such technologies ensures the functioning of a single information space, which leads to an increase in cyber threats, which can lead to data leakage, loss of information or even critical stop of activities of organizations and enterprises. Therefore, the development of new approaches based on modern technologies of cryptographic protection, systems of detection and prevention of unauthorized invasions and tools of dynamic monitoring of the state of corporate telecommunications networks (CTM), is extremely important for their adaptation to fast -changing cyberspace conditions. Accordingly, to increase the efficiency of protecting the strategic resources of corporate networks, improving the methods and algorithms for ensuring the reliability and information security of such systems is relevant both scientific and practical.

**Analysis of recent research and publications**

Given the practical importance of increasing the level of information security in computer systems, various aspects of solving this problem are considered in several scientific publications. So, the main methodological approaches to solving the problems of information security of corporate networks in a systematic form are set out in the textbook [1]. Perspective directions have been identified and basic issues of information protection technologies in CTM, monitoring and analysis of the network, use of technologies of internet screens and systems of detection of attacks are considered. The results of the analysis of modern approaches to ensuring the reliability and safety of information in corporate information systems are given in the work [2]. The classification of methods of assessing the risk of security of computer network systems is considered in the article [3]. The analysis of methods of detection and forecasting of threats to corporate computer networks is presented in the publication [4]. The article [5] presents the results of a study of modern methods and means of processing critical information on corporate networks. Data loss prevention technology is proposed as a key combined data protection mechanism, and the features of using botnet use for the abduction of critically important information in corporate networks are considered. A comprehensive security system for the regional corporate network based on the reference 7-level OSI model and the deep protection model is proposed in the work [6]. Analysis of systems of detection of invasions and systems of preventing invasion was carried out in work [7]. The results of a comprehensive study of the problems of safety improvement in the architecture of corporate information systems using the mechanism of deeply echolocated protection were published in the article [8]. [9] proposes to use a new approach to building CTM security systems based on the concept of internal and external circuits of continuous business

processes. The publication [10] is devoted to the analysis and improvement of information protection tools in corporate computer networks by modernizing the technological design of the system. Problems of improving the safety of information network infrastructure of the enterprise in the face of modern challenges and restrictions on available resources are considered in work [11]. The methodological bases of formation of information threats classifier for the design of corporate computer systems are given in the article [12]. The method of protecting information resources in the corporate network using traffic segmentation is presented in the publication [13]. Analysis of modern approaches to improving information safety and ensuring the stability of the system to external and internal threats in corporate networks based on synthesis of typical algorithms and technologies is carried out in the article [14]. Particular attention is paid to cryptographic protection methods that cover data encryption, digital signatures and key management. Authentication and access control technologies that provide user identification and protect the corporate network from unauthorized access are also considered. The classification of information security principles by privacy, integrity and accessibility criteria is given in work [15]. Methodological approaches to the analysis of computer systems and the safety of corporate computer networks are considered in the publication [16]. The method of protecting information resources of corporate computer systems based on the semiotic model of cyberspace is proposed in work [17].

The analysis of the above publications shows that the problems of improving the models of connection to the Guest system Wi-Fi and algorithms for the operation of passwords need further development to increase the level of safety of password storage, auto-fill and synchronization between devices.

**Formulation of the study purpose**

The purpose of this study is to develop new Wi-Fi guest system models in corporate telecommunications networks and algorithms for the operation of password managers of such systems to improve their information security.

**Presenting main materials**

To develop an increased level of information security of the Wi-Fi guest system in corporate telecommunication networks, it is suggested to accomplish the following tasks:

– User identification: Must be able to trace which user connected to the Wi.

– Credential isolation: Guest Wi-Fi credentials must not match or be derived from actual corporate logins.

– Limited reuse: If stolen, the credentials must not be usable outside the guest Wi-Fi context.

– Session accountability: Should be able to log MAC, IP, session time, and user association.

– Support for unmanaged devices: Users may connect from laptops, phones, etc. without prior provisioning.

Corporate telecommunications networks with increased safety requirements for separation of segments, protection of end devices and accounting of accounting data are standard practice. However, access algorithms for guest Wi-Fi have several disadvantages. Providing by third-party or uncontrolled devices the ability to connect to Wi-Fi using real corporate credentials poses a serious threat. If the device is infected with viral or malicious software, these credentials can be stolen, used in phishing campaigns or to build attacks on a chain.

Usually, a typical algorithm of connection to the corporate information network through Wi-Fi is implemented as follows:

– An employee or external partner connects to guest Wi-Fi using their corporate email and password.

– The network is logically segmented, with strict firewall rules to prevent lateral movement.

– However, the device is unmanaged and potentially compromised (e.g., by malware or spyware).

When using such an algorithm for the attackers, it is possible to access current corporate credentials. In doing so, even if there are certain restrictions on their use, they can be used for:

– Infer corporate naming conventions and identity schemes.

– Mount phishing attacks against internal staff.

– Attempt credential stuffing on other systems.

This situation leads to a violation of two particularly important key principles for the security of the corporate information network:

– Credential minimization: Only expose the minimum necessary secrets.
– Contextual limitation: A credential used for Wi-Fi should not be valid anywhere else.

To solve this problem and increase the level of information security for the implementation of Wi-Fi guest access in the corporate telecommunications network, it is proposed to use such an algorithm.

***Step 1**: Pre-authentication via Internal Portal***.**

To log in to the portal from your personal device is made:

– Authenticates the user via Single Sign-On (SSO).
– Issues a temporary access token (JWT) or short-lived X.509 certificate.
– Optionally provides a QR code or string-based token for manual entry.

***Step 2**: Wi-Fi Connection with Token***.**

The Wi-Fi infrastructure (e.g., RADIUS + EAP-TLS) is configured to:

– Accept tokens or client certificates.
– Validate them via internal backend.
– Grant access only if token is valid and unexpired.

The access token contains:

– A unique session ID.
– An expiration time (eg several hours).
– A non-identifiable alias (e.g., user123-guest-abcde).

***Step 3**: Internal Correlation and Logging***.**

The backend logs the mapping between:

– User identity (from SSO).
– MAC/IP address of the device.
– Device fingerprint (if available).
– Time of issuance and session expiration.

This information is stored securely and used solely for auditing and threat forensics.

*The given algorithm provides such benefits:*

– No reuse of passwords or credentials outside Wi-Fi.
– If the device is compromised, the token is short-lived and limited in scope.
– Users are identifiable internally but anonymous externally.
– No need to issue real usernames or passwords to guests or unmanaged devices.
– Strong alignment with Zero Trust principles ("Never trust, always check").

The proposed model of connection of guest Wi-Fi allows you to implement safe architecture, which provides the ability to identify the user and its audit in the middle of the corporate perimeter of the network, while protecting credentials from external influence and use and can be successfully used in such technologies: SSO Providers: Okta, Azure AD, Keycloak; Token Issuance: OAuth2/JWT, short-lived API tokens; Wi-Fi Integration: RADIUS, EAP-TLS, WPA2-Enterprise; Session Logging: SIEM systems, ELK stack, custom dashboards.

To develop a model of high -security telecommunications corporate telecommunications networks, it is proposed to apply the algorithm of the prompts and encryption of each authentication recording separately by Hint Keys.

Traditional password managers are used by centralized storage facilities (vault) and autofilling functions, which leads to excessive data exposure after unlocking the storage. In particular, the model of global unlocking is currently widespread, despite the use of encryption, after entering the main password creates a single point in a complete compromise that provides:

– Availability of user to all credentials in RAM.
– Availability of viewing of individual records without additional confirmation.

This approach leads to a disruption of the least necessary access (Least Privilege) for the safety of the corporate information network and has significant risks, since access to all stored credentials is opened when entering the main password. In this case, if the attacker gets access to the repositor.

To solve the specified problem and increase the level of information security for the implementation of corporate telecommunication networking managers functions, it is proposed to use the algorithm for each password encrypted separately, using a hint of a short phrase defined by the user (for example: works4home, @admin23, Safe-nigh):

– Isolated Encryption: Each password is encrypted separately using a symmetric key derived from the user's hint.

– On-Demand Decryption: Credentials are decrypted only at the time of access, after successful hint entry.

– No Global Unlock: There is no universal decryption step that exposes all credentials simultaneously.

– Contextual Use: Users can associate different hint keys with different accounts, based on risk level or usage context (e.g. work, family, banking**).**

– In accordance with the proposed algorithm, the saving model of each authentication has the following format:

```
{
 "id": "entry_12345",
 "encryptedPassword": "base64-encoded string",
 "salt": "randomSaltValue",
 "metadata": {
  "username": "...",
  "hintLength": 8,
  "creationTime": "..."
 }
}
```

For decryption it is necessary to provide:

– The correct hint key entered by the user.

– The vault’s global master key (used only to protect metadata and structure).

– Sequence of operations of selling the decryption algorithm:

– The user selects or triggers a login for a specific entry.

– The UI prompts for the corresponding hint key.

– The system derives a decryption key via a KDF (e.g. PBKDF2 or Argon2) using the hint and stored salt.

– The password is decrypted just-in-time and cleared from memory after use.

Applying the proposed algorithm for the implementation of corporate telecommunication networks of high security networks will allow you to get the following benefits:

– Security Isolation: One stolen password does not expose others.

– No vault-wide compromise: Attackers cannot bulk-extract data, even with partial access.

– User-in-the-loop: Active participation is required, making phishing and malware-based exfiltration harder.

– Customizable Risk Profiles: Users can protect sensitive accounts (banking, admin, crypto) with stronger or more obscure hints.

It should also be noted that the application of the proposed approach has the following features:

– User friction: Slightly increased interaction time may reduce convenience.

– Hint recovery complexity: If users forget a hint, the password may be irretrievable unless recovery options are in place.

– Autofill incompatibility: Integration with browser autofill will require secure hint entry UX or trusted hardware.

## Conclusions

Proposed solutions to improve corporate telecommunication networks, taking into account modern challenges, reduce the potential vulnerability of the system and prevent possible information losses. Passwords must evolve from the centralized "vault" to a model with gradual access and contextual authorization. The proposed architecture with prompts and separate encryption of each recording significantly increases the safety and reduces the effects of a possible break. The results of the conducted research show that the implementation of the Wi-Fi Guest and Corporate Telecommunication Wet Managers' Guest System Managers and algorithms will increase the safety level, isolate each account and demand interactive participation of the user to access it.

Further studies may include integration of biometrics for the introduction of tips, UX-model auto-filling with confirmation, maintaining the recovery of tips.

## References


[1] Zhylin A.V., Shapoval O. M., Uspens′kyy O. A. (2021). Tekhnolohiyi zakhystu informatsiyi v in-formatsiyno-telekomunikatsiynykh systemakh: navch. posib. ISZZI KPI im. Ihorya Si-kors′koho. – Kyyiv: Vyd-vo “Politekhnika”. 213.

[2] Bolduyev. M.V., Bolduyeva O. V., Lyshchenko O. H. (2024). Suchasni pidkhody do zab-ezpechennya nadiynosti ta bezpeky informatsiyi v korporatyvnykh telekomunikatsiynykh sys-temakh. *Ahrosvit*, 13, 40-47. doi: 10.32702/2306-6792.2024.13.40.

[3] Tsurkan V., Shapoval O. (2022). Analiz metodiv otsinyuvannya ryzyku bezpeky komp'yuternykh merezh. *Information Technology and Security*, 10(2). 204–215.

[4] Hrebennyk, A. H., Trunova, O. V., Kazymyr, V. V., Mishchenko, M. V. (2020). Vyyavlennya ta prohnozuvannya rivnya zahroz dlya korporatyvnoyi komp’yuternoyi merezhi. *Tekhnichni nauky ta tekhnolohiyi*, 2(20), 175–185. doi: 10.25140/2411-5363-2020-2(20)-175-185.

[5] Hural′nyk O. B., Savenko O. S. (2025). Obroblennya krytychnoyi informatsiyi v korporatyv-nykh merezhakh na osnovi kombinovanoho pidkhodu DLP systemy z systemoy vyyavlennya botnetiv. *Tsentral'noukrayins'kyy naukovyy visnyk. Tekhnichni nauky*. 11(42), II, 63-69. doi: 10.32515/2664-262X.2025.11(42).2.63-69.

[6] Dudykevych V. B., Mykytyn H. V., Murak T. YE. (2025). Kompleksna systema bezpeky rehio-nal′noyi korporatyvnoyi merezhi na osnovi etalonnoyi modeli OSI ta modeli “hlybokoho zakhystu”. *Computer systems and networks*, 7(1), 119–130. doi: 10.23939/csn2025.01.119.

[7] Moroz R. V. (2020). Systemy vyyavlennya vtorhnen′ (IDS) ta systemy zapobihannya vtorhnennyam (IPS). *Tekhnolohiyi zakhystu informatsiyi*, 20(3), 115–128.

[8] Onyagu C. L., Okonkwo O. R., Akawuku G., John J. (2024). Enhancing Security in Internet of Things (IoT) Architecture through Defense-in-Depth Mechanism: A Comprehensive Study. *Newport international journal of engineering and physical sciences*, 4(1), 17–22. doi: 10.59298/NIJEP/2024/411722.1.1100.

[9] Pohasii S., Milevskyi, S., Tomashevsky B., Voropay N. (2022). Development of the double-contour protection concept in socio-cyberphysical systems. *Advanced Information Systems*, 6 (2), 57–66. doi: 10.20998/2522-9052.2022.2.10.

[10] Savyts′ka L., Korobeynikova T., Kostyuk O., Kolesnyk I., Dudnyk O. (2024). Zasoby zakhystu Internet of things v korporatyvniy komp’yuterniy merezhi. *Informatsiyni tekhnolohiyi ta komp’yuterna inzheneriya*, 59(1), 83–93. doi: 10.31649/1999-9941-2024-59-1-83-93.

[11] Syrotyns′kyy R. M., Tyshyk I. YA. (2024). Pokrashchennya bezpeky merezhevoyi infra-struktury pidpryyemstva v umovakh suchasnykh vyklykiv ta obmezhenykh resursiv. *Computer systems and networks*, 6, (1), 155–164. doi: 10.23939/csn2024.01.155.

[12] Shmatko, O., Balakireva, S., Vlasov V., ets, (2020). Development of methodological founda-tions for a classifier of threats to cyberphysical systems design. *Eastern-European Journal of Enterprise Technologies*, 3/9 (105), pp. 6–19.

[13] Tolkachov M., Dzheniuk N., Yevseiev S., ets. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic. *Eastern-European Journal of Enterprise Technologies*. 5 (9 (131). Pp. 63–78. doi: 10.15587/1729-4061.2024.313158.

[14] Shkitov, A., Kropyvnyts′kyy, D. (2024). Syntez typovykh alhorytmiv zakhystu informatsiyi v korporatyvnykh merezhakh. *Upravlinnya rozvytkom skladnykh system*, (60), 129–135. doi: 10.32347/2412-9933.2024.60.129-135.
[15] Chernenko, I. H. (2023). Pryntsypy informatsiynoyi bezpeky: Konfidentsiynist′, tsilisnist′, dostupnist′. *Naukovyy visnyk Uzhhorods'koho universytetu. Seriya: Informatsiyni tekhnolohiyi*, 2(1), 89–102.
[16] Zhang G.-L. (2024). Analysing Computer System Security and Computer Network Security. *Engineering Technology Trends*. 2 (4), 11–15. doi: 10.37155/2972-483X-0204-3.
[17] Zakharzhevskyy, A. G., Tolkachov, M. Yu., Dzhenyuk, N. V., ets. (2024). The method of protecting information resources is based on the semiotic model of cyberspace. *Modern Information Security*, 57 (1), 57–68. doi: 10.31673/2409-7292.2024.010007.

**Список використаної літератури**

1. Жилін А. В., Шаповал О. М., Успенський О. А Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во “Політехніка”, 2021. 213 с.
2. Болдуєв М. В., Болдуєва О. В., Лищенко О. Г. Сучасні підходи до забезпечення надійності та безпеки інформації в корпоративних телекомунікаційних системах. *Агросвіт*, 2024, №13. С.40-47. doi: 10.32702/2306-6792.2024.13.40.
3. Цуркан В., Шаповал О. Аналіз методів оцінювання ризику безпеки комп'ютерних мереж. *Information Technology and Security*. 2022. Vol. 10(2). С. 204–215.
4. Гребенник, А. Г., Трунова, О. В., Казимир, В. В., & Міщенко, М. В. Виявлення та прогнозування рівня загроз для корпоративної комп’ютерної мережі. *Технічні науки та технології*, 2020. В. 2(20), С.175–185. doi: 10.25140/2411-5363-2020-2(20)-175-185.
5. Гуральник О. Б., Савенко О. С. Оброблення критичної інформації в корпоративних мережах на основі комбінованого підходу DLP системи з системою виявлення ботнетів. *Центрально-український науковий вісник. Технічні науки.* 2025. В.11(42), ч.ІІ. С.63-69. doi: 10.32515/2664-262X.2025.11(42).2.63-69.
6. В. Б. Дудикевич, Г. В. Микитин, Т. Є. Мурак. Комплексна система безпеки регіональної корпоративної мережі на основі еталонної моделі OSI та моделі “глибокого захисту”. *Computer systems and networks.* 2025. В.7(1). С.119–130. doi: 10.23939/csn2025.01.119.
7. Мороз, Р. В. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). *Технології захисту інформації*, 2020. В.20(3), С.115–128.
8. Onyagu C. L., Okonkwo O. R., Akawuku G., John J. Enhancing Security in Internet of Things (IoT) Architecture through Defense-in-Depth Mechanism: A Comprehensive Study. Newport international journal of engineering and physical sciences. 2024. Vol.4(1). P.17–22. doi: 10.59298/NIJEP /2024/411722.1.1100.
9. Pohasii, S., Milevskyi, S., Tomashevsky, B., Voropay, N. Development of the double-contour protection concept in socio-cyberphysical systems. *Advanced Information Systems*, 2022. В. 6(2), С.57–66. doi: 10.20998/2522-9052.2022.2.10.
10. Савицька, Л., Коробейнікова , Т., Костюк, О., Колесник, І., Дудник, О. Засоби захисту Internet of things в корпоративній комп’ютерній мережі. *Інформаційні технології та комп’ютерна інженерія*, 2024. В.59(1). С.83–93. doi: 10.31649/1999-9941-2024-59-1-83-93.
11. Сиротинський Р. М., Тишик І. Я. Покращення безпеки мережевої інфраструктури підприємства в умовах сучасних викликів та обмежених ресурсів. *Computer systems and networks*, 2024, В.6(1). С. 155–164. doi: 10.23939/csn2024.01.155.
12. Shmatko, O., Balakireva, S., Vlasov, A., ets. Development of methodological foundations for a classifier of threats to cyberphysical systems design. *Eastern-European Journal of Enterprise Technologies*, 2020. В.3/9(105), С. 6–19.
13. Tolkachov M., Dzheniuk N., Yevseiev S. ets. Development of a method for protecting information resources in a corporate network by segmenting traffic. *Eastern-European Journal of Enterprise Technologies*. 2024. В.5/9 (131). С. 63–78. doi: 10.15587/1729-4061.2024.313158.

14. Шкітов, А., Кропивницький, Д. Синтез типових алгоритмів захисту інформації в корпоративних мережах. *Управління розвитком складних систем*, 2024. № 60. С. 129–135. doi: 10.32347/2412-9933.2024.60.129-135.
15. Черненко, І. Г. Принципи інформаційної безпеки: Конфіденційність, цілісність, доступність. *Науковий вісник Ужгородського університету. Серія: Інформаційні технології*, 2023. В.2(1). С. 89–102.
16. Zhang G.-L. Analysing Computer System Security and Computer Network Security. Engineering Technology Trends. 2024. Vol. 2(4). P. 11–15. doi: 10.37155/2972-483X-0204-3.
17. Zakharzhevskyy, A. G., Tolkachov, M. Yu., Dzhenyuk, N. V., ets. The method of protecting information resources is based on the semiotic model of cyberspace. *Modern Information Security*, 2024. Vol.57(1), 57–68. doi: 10.31673/2409-7292.2024.010007.

*Надійшла до редколегії 15.09.2025*
*Прийнята після рецензування 26.09.2025*
*Опублікована 23.10.2025*