https://doi.org/10.31891/2307-5732-2025-355-20
УДК 004.056.5

ДЗЮБАН ОЛЕКСІЙ
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
https://orcid.org/0009-0005-9339-310X
e-mail: wfgamer2013@gmail.com

БАГАТОРІВНЕВА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІД ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ СТРУКТУРНОЇ СЕГМЕНТАЦІЇ

Стаття присвячена розгляду та опису моделі захищеної інформаційно-телекомунікаційної мережі організації, яка враховує специфіку сучасних інформаційних загроз. Запропонована модель передбачає чіткий поділ інформаційної мережі на дві основні складові частини: внутрішню мережу, що містить серверні ресурси з конфіденційними даними, та зовнішню мережу, яка містить сервери, призначені для загального доступу. Особливу увагу приділено методам оцінювання стану захищеності мережі від зовнішніх і внутрішніх атак. Модель забезпечує надійний та комплексний захист інформаційної мережі організації, гарантує збереження конфіденційності, цілісності та доступності інформації, а також може бути застосована для побудови систем захисту інформації в державних, комерційних і приватних структурах.

Ключові слова: інформаційна безпека, захист мереж, інформаційно-телекомунікаційна мережа, інформаційні атаки, багаторівнева система захисту.

OLEKSII DZIUBAN
National University «Yuri Kondratyuk Poltava Polytechnic»

MULTI-LEVEL PROTECTION SYSTEM OF INFORMATION AND TELECOMMUNICATION NETWORKS AGAINST INFORMATION SECURITY THREATS BASED ON STRUCTURAL SEGMENTATION

In the modern information space, an information and telecommunication network is a key component of any organization's operations. Such a network enables the transmission, storage, and processing of various types of data, a significant portion of which is confidential or restricted. This may include employees' personal information, financial documentation, strategic plans of the organization, and other data that are vital to the institution's functioning and may become targets for information attacks.

Due to the continuous rise in cyber threats, the issue of information protection in networks becomes one of the most critical tasks ensuring the stable operation of the organization. This article is devoted to the analysis and description of a model of a protected information and telecommunication network for an organization, which takes into account the specific nature of modern information threats.

The proposed model includes a clear segmentation of the information network into two main parts: an internal network containing server resources with confidential data, and an external network that hosts servers intended for public access. Separate protection means and levels are provided for each of these zones, including the use of firewalls, intrusion detection systems, antivirus tools, access control mechanisms, and information protection from unauthorized access. Special attention is paid to methods of assessing the security status of the network against external and internal attacks. The model ensures reliable and comprehensive protection of the organization's information network, guarantees the confidentiality, integrity, and availability of information, and can be applied to building information security systems in government, commercial, and private sectors.

Keywords: information security, network protection, information and telecommunication network, information attacks, multi-level protection system.

Стаття надійшла до редакції / Received 26.05.2025
Прийнята до друку / Accepted 26.06.2025

Постановка проблеми

У сучасних умовах цифрової трансформації діяльність більшості організацій, незалежно від сфери їх функціонування, тісно пов'язана з використанням інформаційно-телекомунікаційних систем. Такі системи забезпечують зберігання, обробку та передавання інформації, значна частина якої має важливе значення для безперервного функціонування підприємств та установ. Зокрема, це можуть бути персональні дані працівників, результати фінансової діяльності, комерційна таємниця, стратегічні плани, аналітичні звіти, технічна документація тощо.

У зв'язку з цим різко зростає актуальність питань, пов'язаних із забезпеченням захисту інформації від несанкціонованого доступу, порушення цілісності та втрати доступності. Кіберзагрози набувають дедалі складніших форм, включаючи як зовнішні атаки (з боку хакерів, кіберзлочинних угрупувань, конкурентів), так і внутрішні (помилки персоналу, зловмисні дії працівників). При цьому об'єктом атак дедалі частіше стають не лише окремі вузли чи програми, а вся інформаційно-телекомунікаційна інфраструктура організації. Наявні підходи до побудови захищених мереж часто не враховують комплексний характер загроз та не забезпечують належної стійкості до комбінованих атак. Проблема ускладняється ще й тим, що багато організацій не мають чітко структурованої моделі захисту, яка враховує сучасні технології сегментації мережі, застосування міжмережевих екранів, систем виявлення вторгнень, інструментів аналітики та моделювання атак.

Отже, актуальним завданням є розроблення ефективної моделі захищеної інформаційно-телекомунікаційної мережі організації, яка б базувалася на системному підході до виявлення та нейтралізації загроз, враховувала структурні особливості інформаційних потоків і забезпечувала надійний захист як

внутрішніх, так і публічних сегментів мережі.

Аналіз досліджень та публікацій

Аналіз сучасних наукових досліджень свідчить про посилену увагу до побудови захищених інформаційно-телекомунікаційних мереж в умовах зростання складності кіберзагроз. У працях [1, 2] розглянуто системний підхід до формування архітектури захисту з урахуванням логічного поділу мережі, визначення критичних сегментів, впровадження розмежованого доступу та технічних засобів протидії. Блокчейн-технології як інструмент забезпечення цілісності даних у відкритих підсистемах, зокрема в демілітаризованих зонах, запропоновано у [3]. Використання такого підходу дозволяє досягти прозорості та стійкості до підміни інформації у системах, що потребують особливого рівня довіри. Статті [4, 5] описують механізми адаптивного виявлення атак на основі обробки потокових даних і теорії нечітких множин, що може бути корисним у створенні гнучких моделей захисту з динамічним налаштуванням політик безпеки. Огляд реального стану інформаційної безпеки в Україні подано в [6, 7], де проаналізовано поширені вразливості, рівень інституційної готовності до реагування на кіберінциденти, а також практики забезпечення стійкості ІТ-інфраструктур. Публікації [8, 9] висвітлюють правові та соціальні аспекти кіберзахисту, розкривають проблематику нормативного забезпечення безпеки інформаційного середовища та взаємодії між технічними і юридичними складовими систем захисту. У джерелі [10] описано специфіку організації захисту фінансового сектора як критичного елемента національної інфраструктури.

Формулювання цілей статті

Метою роботи є: розроблення концептуальної моделі захищеної інформаційно-телекомунікаційної мережі організації, яка здатна забезпечити високий рівень інформаційної безпеки в умовах сучасних кіберзагроз. У процесі досягнення цієї мети основна увага приділяється побудові структурованої архітектури мережі з чітким розмежуванням внутрішніх і зовнішніх сегментів, розробці підходів до створення багаторівневої системи захисту, а також використанню сучасних методів виявлення та нейтралізації атак. У межах запропонованої моделі передбачається застосування програмних і програмно-апаратних засобів захисту, інтеграція механізмів фільтрації, контролю доступу, виявлення вторгнень та аналітичного моніторингу. Особливе значення має моделювання поведінки атакуючого за допомогою формальних методів, зокрема мереж Петрі, що дозволяє оцінити ефективність запропонованих заходів захисту в динамічних умовах функціонування мережі. Реалізація поставленої мети сприятиме підвищенню надійності та стійкості інформаційної інфраструктури організації, забезпеченню конфіденційності, цілісності та доступності даних, а також адаптації існуючих теоретичних напрацювань до практичних умов впровадження в різних типах установ.

Виклад основного матеріалу

В основі моделі захищеної інформаційно-телекомунікаційної мережі (ІТКМ) організації лежать можливі загрози, спрямовані на основні компоненти мережі – як програмні, так і програмно-апаратні, – а також методи та засоби їх захисту. На ІТКМ організації можуть впливати як зовнішні, так і внутрішні джерела загроз інформаційній безпеці. Ці джерела можуть використовуватися зловмисниками для реалізації інформаційних атак.

Побудова моделі захищеної інформаційно-телекомунікаційної мережі організації базується на всебічному аналізі можливих загроз, що можуть бути спрямовані як на програмні, так і на програмно-апаратні компоненти мережі. Ці загрози можуть походити як ззовні (внаслідок хакерських атак, мережевого сканування, шкідливого трафіку тощо), так і зсередини (через дії персоналу, помилки конфігурації, зловживання правами доступу). Інформаційні атаки можуть реалізовуватися зловмисниками в різних формах, включаючи перехоплення даних, отримання несанкціонованого доступу, виведення з ладу мережевих вузлів, блокування сервісів, модифікацію або видалення критичної інформації. Для ефективної протидії таким загрозам необхідно розглядати ІТКМ як єдину структуру з чітко визначеними зонами відповідальності, рівнями доступу і захисними механізмами.

У процесі побудови моделі доцільно спиратися на три основоположні поняття: об’єкт захисту, загроза інформаційній безпеці та система захисту об’єкта. Об’єктом захисту виступає інформаційно-телекомунікаційна мережа організації, з усіма її складовими – серверними ресурсами, мережевим обладнанням, каналами зв’язку, прикладним програмним забезпеченням та інформаційними потоками. Загроза визначається як потенційна подія або дія, що здатна порушити конфіденційність, цілісність чи доступність інформації. Система захисту, у свою чергу, включає комплекс організаційних, технічних і програмних засобів, призначених для запобігання або мінімізації наслідків реалізації таких загроз.

Для створення надійної моделі захисту необхідно насамперед визначити, яка саме інформація циркулює в мережі: загальнодоступна чи обмеженого доступу. Далі слід проаналізувати організаційну структуру (відділи, підрозділи, групи користувачів), визначити найбільш критичні зони мережі та сегментувати її з урахуванням логічного та фізичного розмежування. Після цього в кожному сегменті потрібно реалізувати відповідні засоби захисту: міжмережеві екрани, системи виявлення вторгнень, контроль доступу, антивірусний захист тощо. Оцінка захищеності мережі є важливим етапом у формуванні захисної моделі. Найпоширенішою загрозою є витік інформації внаслідок несанкціонованого доступу до внутрішніх ресурсів. Для виявлення таких атак застосовуються як класичні методи (сигнатурний аналіз, контекстне виявлення), так і сучасні підходи на основі штучного інтелекту – зокрема аналіз станів мережі з

використанням формальних моделей), генетичні алгоритми, нейронні мережі та експертні системи. Їх використання дозволяє не лише фіксувати факт атаки, а й прогнозувати її розвиток.

На основі вищезазначеного можна сформулювати алгоритм побудови моделі захищеної ІТКМ (рис. 1)

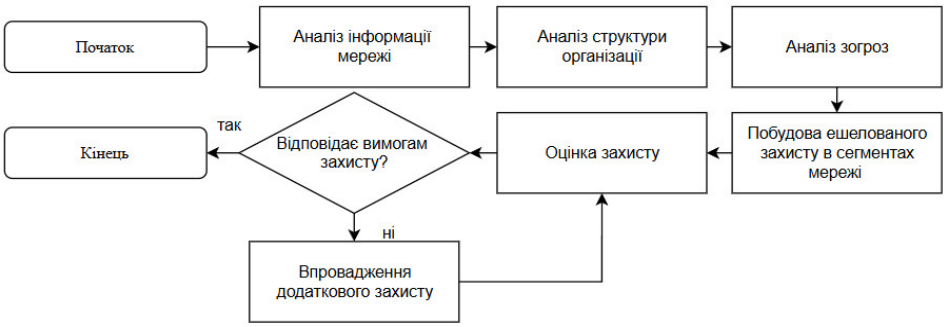

Рис. 1. Блок-схема побудови захищеної моделі ІТКМ

Одним із ефективних інструментів оцінювання захищеності інформаційно-телекомунікаційної мережі (ІТКМ) від інформаційних атак є мережі Петрі. Моделювання за допомогою мереж Петрі ґрунтується на формуванні маркування ІТКМ шляхом послідовного спрацювання переходів інформаційного пакета між хостом користувача, хостом порушника та сервером. На основі алгоритму побудови моделі захищеної ІТКМ на рис. 2 представлено структурну схему мережі.

На цьому рисунку позначено: К – комутатор; М – маршрутизатор; ФВМ – файєрвол; IPS – система виявлення вторгнень. Мережа має дві зони: внутрішню та демілітаризовану (DMZ). ІТКМ організації містить два загальнодоступні сервери, розташовані в демілітаризованій зоні DMZ: зовнішні сервери DNS та WWW. У внутрішній мережі розміщено внутрішні сервери DNS та WWW організації. Трафік локалізується в сегментах *1* та *i*. Зовнішній файєрвол разом із IPS виконує фільтрацію трафіку з зовнішньої мережі для захисту периметра та внутрішньої мережі ІТКМ і функціонує на мережевому та транспортному рівнях. Внутрішній файєрвол спільно з IPS захищає внутрішню мережу від загроз інформаційної безпеки, що походять із зовнішньої мережі та з периметру, і працює на мережевому, транспортному та прикладному рівнях.

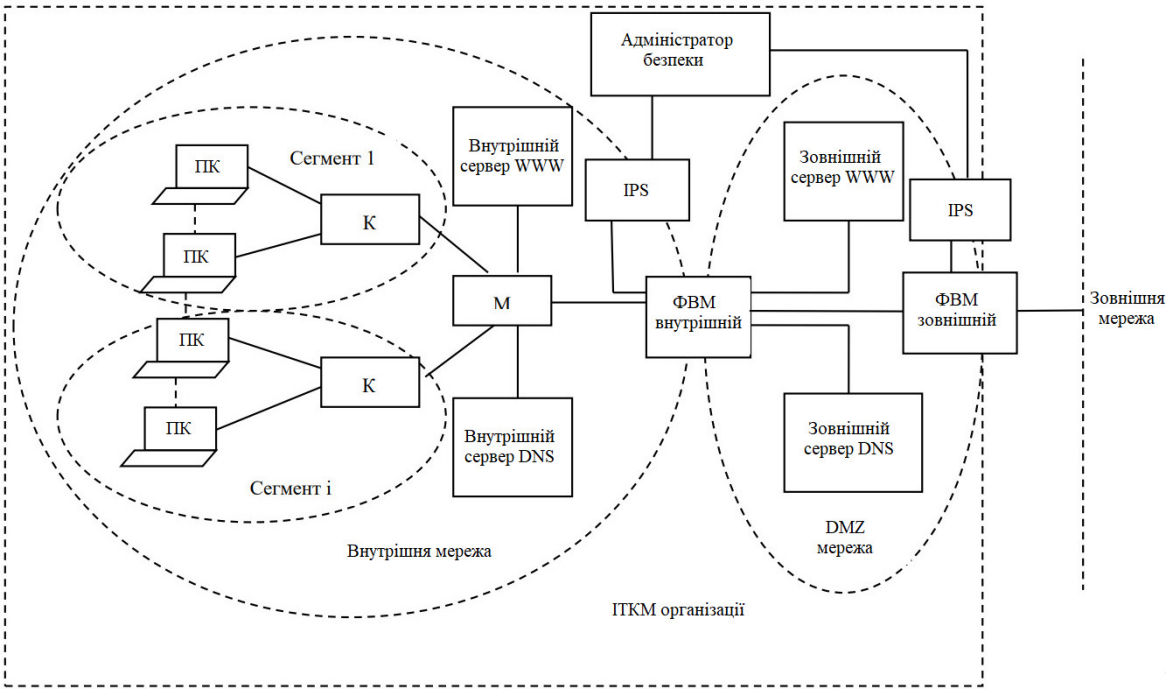

Рис. 2. Схема сегментації інформаційної мережі та меж захисту

Таким чином, мережа має два рубіжі (ешелони) захисту: перший рубіж реалізується за допомогою зовнішнього фаєрвол та IPS другий – на основі внутрішнього фаєрвол та IPS. Крім того, кожен хост у внутрішній та зовнішній мережах має власні засоби захисту, до яких належать антивірусний захист, розмежування прав доступу, аудит, контроль підключень до вузлів, захист від несанкціонованого доступу до каталогів і файлів тощо. У внутрішній мережі розташований сервер, на якому зберігаються дані, що належать до конфіденційної інформації (зокрема, персональні дані працівників організації), а також інформація з обмеженим доступом, наприклад, відомості про напрями розвитку організації, фінансову діяльність тощо. Ця інформація повинна мати властивості конфіденційності, цілісності та доступності. У демілітаризованій зоні розміщується сервер, на якому зберігається інформація про напрями діяльності організації – товари, послуги

тощо. Ця інформація повинна володіти властивостями цілісності та доступності. Доступ до сервера демілітаризованої зони мають мати зовнішні користувачі (користувачі мережі Інтернет). Основні загрози інформаційній безпеці ІТКМ виникають на мережевому рівні та пов'язані з перехопленням трафіку зловмисником, порушенням функціонування компонентів ІТКМ, що призводить до відмови в обслуговуванні. Такі загрози реалізуються з використанням протоколів міжмережевої взаємодії стеку TCP/IP.

На рис. 3 подано граф, що моделює проникнення зловмисника в ІТКМ організації, де S_i – стани мережі внаслідок дій зловмисника. Як зазначалося раніше, однією з основних загроз інформаційній безпеці є витік інформації внаслідок несанкціонованого доступу зловмисника до інформаційних ресурсів організації. У цьому контексті стан інформаційно-телекомунікаційної мережі може описуватись за допомогою трьох основних параметрів: множини об'єктів (сутностей), множини суб'єктів і множини прав доступу суб'єктів до об'єктів. Перехід ІТКМ з одного стану до іншого відбувається внаслідок зміни складу будь-якої з цих множин. Одним із ефективних способів аналізу станів мережі є використання мереж Петрі, які дозволяють враховувати різноманітні параметри атаки. Мережа Петрі являє собою орієнтований граф, що складається зі станів і переходів, з'єднаних між собою дугами.

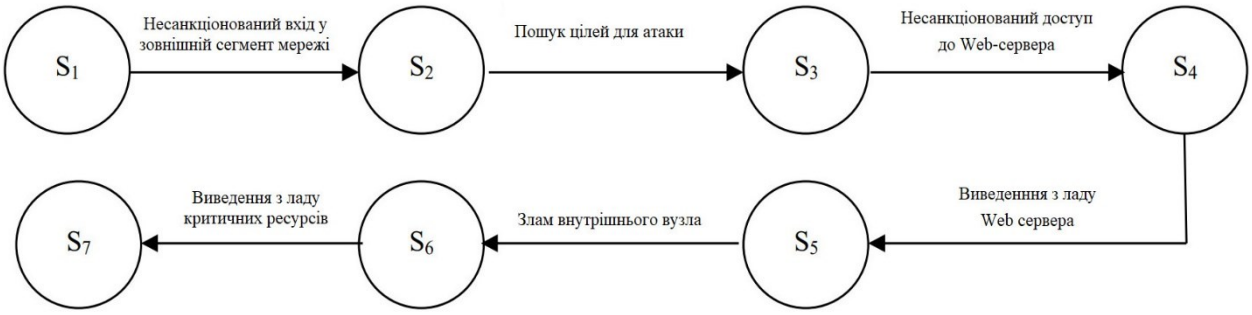

Рис. 3. Модель переходів між станами ІТКМ при інформаційній атаці

Аналізуючи інформаційно-телекомунікаційну мережу на основі мереж Петрі, можна подати мережу організації у вигляді множини станів C:

$$C = \{ S, T, F_{вх}, F_{вих} \}, \quad (1)$$

де $S = \{S_i\}$ – множина станів мережі, $T = \{T_j\}$ – множина переходів мережі, $F_{вх}$ – вхідна функція, що відповідає початковому стану мережі, $F_{вих}$ – вихідна функція, що відповідає кінцевому стану мережі.

З урахуванням характеру інформації, що циркулює в ІТКМ організації, можна зробити висновок, що в внутрішній мережі основними загрозами інформаційній безпеці є втрата конфіденційності, цілісності та доступності, тоді як у демілітаризованій зоні – втрата цілісності та конфіденційності.

Висновки

У статті запропоновано модель побудови захищеної інформаційно-телекомунікаційної мережі організації, яка базується на структурній сегментації та використанні багаторівневої системи захисту. Проведений аналіз сучасних загроз інформаційній безпеці та засобів протидії дозволив визначити ключові напрями формування ефективної архітектури ІТКМ з урахуванням специфіки внутрішніх і зовнішніх інформаційних потоків. Запропонована модель передбачає логічне та фізичне розмежування мережі на окремі зони з відповідним рівнем захисту, впровадження засобів контролю доступу, систем виявлення вторгнень, міжмережевих екранів, антивірусних механізмів та інших технічних рішень.

Також враховано застосування формальних методів, зокрема мереж Петрі, для моделювання та оцінювання рівня захищеності мережі. Особливу увагу приділено виявленню вразливих місць у логіці взаємодії компонентів системи та моделюванню потенційних сценаріїв інформаційних атак. Модель дозволяє виявити критичні ділянки ІТКМ ще на етапі проєктування, що суттєво підвищує ефективність її захисту. Результати дослідження свідчать про доцільність використання комплексного підходу до побудови систем захисту, що забезпечують конфіденційність, цілісність і доступність даних, а також дозволяють ефективно протидіяти сучасним кіберзагрозам. Розроблена модель може бути адаптована для впровадження у різних типах організацій – як у державному, так і в комерційному секторі.

Література

1. Бурячок В. Л., Толюпа С. В., Аносов А. О. Системний аналіз та прийняття рішень в інформаційній безпеці : підручник. Київ : ДУТ, 2021. 345 с.

2. Горбенко І. М., Снігур В. П., Рибалко О. В. Безпека телекомунікаційних систем : монографія. Харків : ХНУРЕ, 2022. 278 с.

3. Василишин С., Опірський І. Розробка безпеки систем електронного урядування на основі блокчейну // *Ukrainian Information Security Research Journal*. 2022. Т. 24, № 2. С. 58–70. DOI: 10.18372/2410-7840.24.16931.

4. Zybin S., Sobchuk A., Rovda V. Real-time false information detection prediction accuracy model // *Ukrainian Information Security Research Journal*. 2023. Vol. 25, No. 2. P. 58–63. DOI: 10.18372/2410-7840.25.17673.

5. Korystin O. E., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. O. Comparative risk assessment of cyber threats based on average and fuzzy sets theory // *International Journal of Computer Network and Information Security*. 2024. Vol. 16, No. 1. P. 24–34. DOI: 10.5815/ijcnis.2024.01.02.

6. Hryshchenko S., Savchenko V., Kumeiko A., Patsuriia N., Rieznikova V. Current state of information security in Ukraine // *DANUBE: Law and Economics Review*. 2025. Vol. 16, No. 1. P. 16–29. DOI: 10.2478/danb-2025-0002.

7. Yehorycheva S., Hlushko A., Khudolii Y. Issue of Ukrainian financial sector information security // *Development Management*. 2023. Vol. 22, No. 4. P. 45–52. DOI: 10.57111/devt/4.2023.45.

8. Trofymenko O., Prokop Y., Loginova N., Zadereyko O. Cybersecurity of Ukraine: Analysis of the current situation // *Ukrainian Information Security Research Journal*. 2019. Vol. 21, No. 3. P. 150–157. DOI: 10.18372/2410-7840.21.13951.

9. Sopilko I. Information security and cybersecurity: Comparative and legal aspect // *Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law"*. 2021. No. 2(59). P. 110–115. DOI: 10.18372/2307-9061.59.15603.

10. Sopilko I., Rapatska L. Social-legal foundations of information security of the state, society and individual in Ukraine // *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28, No. 1. P. 44–54. DOI: 10.56215/naia-herald/1.2023.44.

References

1. Buriachok V. L., Toliupa S. V., Anosov A. O. Systemnyi analiz ta pryiniattia rishen v informatsiinii bezpetsi : pidruchnyk. Kyiv : DUT, 2021. 345 s.

2. Horbenko I. M., Snihur V. P., Rybalko O. V. Bezpeka telekomunikatsiinykh system : monohrafiia. Kharkiv : KhNURE, 2022. 278 s.

3. Vasylyshyn S., Opirskyi I. Rozrobka bezpeky system elektronnoho uriaduvannia na osnovi blokcheinu // Ukrainian Information Security Research Journal. 2022. T. 24, № 2. S. 58–70. DOI: 10.18372/2410-7840.24.16931.

4. Zybin S., Sobchuk A., Rovda V. Real-time false information detection prediction accuracy model // Ukrainian Information Security Research Journal. 2023. Vol. 25, No. 2. P. 58–63. DOI: 10.18372/2410-7840.25.17673.

5. Korystin O. E., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. O. Comparative risk assessment of cyber threats based on average and fuzzy sets theory // International Journal of Computer Network and Information Security. 2024. Vol. 16, No. 1. P. 24–34. DOI: 10.5815/ijcnis.2024.01.02.

6. Hryshchenko S., Savchenko V., Kumeiko A., Patsuriia N., Rieznikova V. Current state of information security in Ukraine // DANUBE: Law and Economics Review. 2025. Vol. 16, No. 1. P. 16–29. DOI: 10.2478/danb-2025-0002.

7. Yehorycheva S., Hlushko A., Khudolii Y. Issue of Ukrainian financial sector information security // Development Management. 2023. Vol. 22, No. 4. P. 45–52. DOI: 10.57111/devt/4.2023.45.

8. Trofymenko O., Prokop Y., Loginova N., Zadereyko O. Cybersecurity of Ukraine: Analysis of the current situation // Ukrainian Information Security Research Journal. 2019. Vol. 21, No. 3. P. 150–157. DOI: 10.18372/2410-7840.21.13951.

9. Sopilko I. Information security and cybersecurity: Comparative and legal aspect // Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law". 2021. No. 2(59). P. 110–115. DOI: 10.18372/2307-9061.59.15603.

10. Sopilko I., Rapatska L. Social-legal foundations of information security of the state, society and individual in Ukraine // Scientific Journal of the National Academy of Internal Affairs. 2023. Vol. 28, No. 1. P. 44–54. DOI: 10.56215/naia-herald/1.2023.44.