DOI: https://doi.org/10.36910/6775-2524-0560-2025-59-30
УДК 004.725.5:004.056
Ухань Єгор Олександрович, аспірант
https://orcid.org/0000-0002-5384-0105
Журавська Ірина Миколаївна, д-р техн. наук, проф.
https://orcid.org/0000-0002-8102-9854
Чорноморський національний університет імені Петра Могили, м. Миколаїв, Україна

ФОРМУВАННЯ КОНТРОЛЬОВАНИХ ЗОН У ЛОКАЛЬНИХ БЕЗДРОТОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Ухань Є. О., Журавська І. М. Формування контрольованих зон у локальних бездротових комп'ютерних мережах. Досліджено формування контрольованих зон (КЗ згідно з НД ТЗІ 3.1-001-07) у локальних бездротових комп'ютерних мережах на базі WiFi-технології. Розглянуто актуальність проблеми, зумовлену захистом від несанкціонованого доступу. Проведено аналіз методів (фізичних, програмних) формування КЗ, виділено особливості цих методів та засоби їх реалізації. Особливу увагу приділено аналізу доцільності використання протоколу WPA3 на заміну більш старих протоколів безпеки типу (WPA, WPA2), а також його переваги у захисті від атак різних видів. У контексті розвитку технології Wi-Fi було розглянуто перспективні можливості майбутнього стандарту WPA4, який, за новітніми дослідженнями IEEE, посилить механізми захисту за рахунок штучного інтелекту. Також протокол WPA4 буде враховувати можливі загрози з боку квантових систем і містити базу різних видів атак для активної протидії. Обґрунтовано використання комбінованого методу формування КЗ, який включає в себе як фізичні (спрямовані антени, джаммери) так і програмні (сегментація мережі за допомогою VLAN, впровадження WIDS моніторингу). Відзначено важливість та доцільність навчання персоналу принципам безпеки, як метод захисту. Результати дослідження підкреслюють необхідність та можливість впровадження розглянутих методів при розгортанні сучасного мережевого середовища.
Ключові слова: контрольована зона, бездротова комп'ютерна мережа, Wi-Fi, локальна обчислювальна мережа, VLAN, WIDS, WPA3, WPA4, джаммер.

Ukhan Ye., Zhuravska I. Forming Controlled Zones in Local Wireless Computer Networks. The formation of controlled security zones (Controlled Access Area according to CNSSI 4009-2015) in local wireless computer networks based on Wi-Fi technology is investigated. The problem's urgency, caused by the need to protect against unauthorized access, is considered. The methods (physical, software) for forming CPs were analyzed, and the characteristics of these methods and the means of their implementation are highlighted. Special attention has been paid to the analysis of the feasibility of using WPA3 to replace outdated security protocols (WPA, WPA2), as well as its advantages in combating various types of attacks. In the context of technology development, the promising capabilities of the future WPA4 standard, according to the latest IEEE research, were examined. It will strengthen protection mechanisms through artificial intelligence. Also, protocol WPA4 considers potential threats from quantum systems and contains a database of attacks of various types for active countermeasures. The use of a combined method of CTA formation, including physical (directional antennas, jammers) and software (network segmentation using VLAN, implementation of WIDS monitoring), is substantiated. The importance and usefulness of training personnel in the principles of security as a method of protection have been emphasized. The research results have emphasized the need and possibility of implementing these methods when deploying a modern network environment.
Keywords: controlled access area, wireless computer network, Wi-Fi, LAN, VLAN, WIDS, WPA3, WPA4, jammer.

Постановка наукової проблеми. В умовах технологічного розвитку бездротових комп'ютерних мережах (БКМ) таких як Wi-Fi, критичним завданням є забезпечення ефективного покриття, захист від несанкціонованого доступу (НСД) до інформації та адаптивність системи. Збільшення клієнтів системи та варіативність пристроїв, а також зміни у правилах та нормах інформаційної безпеки, потребують створення гнучких методів створення контрольованих зон (КЗ, англ. Control Area or CTA) покриття мережі.

На сьогодні існуючі методи до формування КЗ у БКМ не відповідають усім вимогам, а саме: відсутність або складність в інтеграції з системами кібербезпеки, невисокий рівень гнучкості до змін у навантаженні або покритті, певні обмеження до масштабованості.

З цього випливає потреба у нових або вдосконалених методах формування КЗ у БКМ, які б відповідали низки вимог:

- належний рівень кібербезпеки;
- гнучкість до змін у мережі;
- зручність керування та масштабування мережі;
- ефективний розподіл ресурсів мережі.

Аналіз останніх досліджень і публікацій. Розвиток БКМ привернув значну увагу дослідників до вивчення можливих шляхів вирішення проблем: ефективного контролю зон мережі,

адміністрування та стабільності роботи. Формування КЗ виділяють як один з ключових методів забезпечення кібербезпеки та захисту від НСД.

У працях вітчизняних та зарубіжних авторів одним з практичних підходів висвітлюється використання технологій машинного навчання (МН) для визначення контрольованих зон в бездротових мережах.

У статті [1] продемонстровано підхід для аналізу та прогнозуванню можливих ризиків в БКМ на базі МН. Головним елементом який запропонували автори є вдосконалений баєсів класифікатор, що дало змогу у реальному часі виявляти та класифікувати рівні загрози. За результатами дослідження продемонстрована доцільність використання динамічної аналітики трафіку для формування динамічних КЗ.

У роботі [2] запропонували новий підхід для керування ресурсами в БКМ. Головна риса запропоновано підходу базується на представленні мережі як гетерогенний граф, де кожна точка доступу має свої особливості, за допомогою цього була отримана можливість точного моделювання взаємодій у мережі.

Важливою ланкою у наукових дослідженнях є праці щодо Software-Defined Networking (SDN) та Network Functions Virtualization (NFV). Головною метою зазначених технологій є покращення існуючих методів управління БКМ за допомогою нових математичних моделей. Одну з таких аналітичних моделей розглянуто у праці [3]. В праці підкреслюються можливості концепції значно покращити показники адаптивності та зменшення витрат на підтримання БКМ. Запропоновані методи математичного моделювання ефективності даних систем, що дозволить зменшити час відповіді, збільшити пропускну здатність та провести оптимізацію мережевих ресурсів. На жаль, на даний час ці моделі непридатні для використання у бездротових локальних обчислювальних мережах (ЛОМ) на основі Wi-Fi, але отримали застосування для технологій розгортання та розширення 5G-мереж.

Метод формування КЗ, який надає найкращі показники у захисті, є побудова клітки Фарадея. Але, як видно з праць дослідників з Неґевського університету Бен-Гуріона (Ізраїль) [5], які досліджували можливість НСД на комп'ютерні мережі, захищені клітками Фарадея, були знайдені можливі шляхи витоку інформації. Як видно з їх досліджень, для отримання НСД використовуються магнітні поля, які проходять крізь клітку Фарадея. Їх практичні експерименти довели можливість контролю магнітних полів процесорів приладів в середині клітки Фарадея, а також передавання через низькочастотне магнітне випромінювання інформації на приймач, за межами КЗ. У своїй роботі вони приводять шляхи протидії та принципи моніторингу такої загрози, а саме:

- додаткове магнітне екранування;
- моніторинг випромінення магнітних полів від приладів у клітці Фарадея;
- збір аналітичних даних роботи процесора для виявлення аномальних змін навантаження;
- забезпечення відсутності поблизу КЗ несанкціонованих пристроїв.

Як розвиток технології по використанню кліток Фарадея, науковці з Університету штату Айова (США) провели дослідження із залізовмісними матеріалами *Fe, Fe_2O_3, Fe_3O_4,* карбонільним залізом, *FeO* для оцінки їх потенціалу у відбитті та поглинанні електромагнітних хвиль [6]. Були розглянуті різні методи синтезу та спроби створення композитних матеріалів, які можуть бути синтезовані шляхом поєднання залізовмісних з діелектричними та можливості використання полімерних та вуглецевих наноматеріалів для покращення властивостей кліток Фарадея.

Необхідно зазначити, що аналіз літературних джерел, приведених рішень та методів, свідчить про актуальність проблеми методів побудови КЗ у БКМ. Але доцільно сфокусувати подальші дослідження на знаходження нових або вдосконалені наявних методів та практик задля підвищення захищеності сегментів WiFi-мереж від нових типів атак та НСД.

Формулювання мети дослідження. Метою дослідження є аналіз та розробка методів формування КЗ у БКМ для покращення ефективності роботи мережі, захисту від НСД та зменшення необхідних ресурсів.

Виклад основного матеріалу дослідження. Контрольовані зони у бездротових комп'ютерних мережах – це фізична або віртуальна область, усередині якої забезпечується захист від витоку інформації та від несанкціонованого доступу до персональних даних та пристроїв. Методи побудови таких контрольованих зон можна розділити на фізичні та програмні за принципом їх роботи (табл. 1).

Таблиця 1. Методи формування КЗ

Фізичні	**Програмні**
Регулювання потужності передавача	Мережева аутентифікація
Використання спрямованих антен	VLAN (віртуальні локальні мережі)
Зонування за допомогою джаммерів	WIDS-моніторинг несанкціонованих пристроїв

Регулювання потужності передавача відбувається на рівні прошивки телекомунікаційного пристрою, на базі якого розгортається сегмент мережі; для прикладу розглянемо маршрутизатор від компанії Mikrotik, а саме RB951Ui-2^{nD} [7]. Його максимальна потужність передавача складає 22 dBm, а мінімальна 6 dBm. Регулювання відбувається з прав адміністратора через офіційний застосунок Winbox або через вебінтерфейс, що дозволяє зменшити зону покриття до однієї кімнати. Застосований метод може допомогти розгортанню безпечних локальних мереж у невеликих офісах або у приватних приміщеннях, але не підходить для підприємств.

Мережева аутентифікація давно є стандартом у кожній точці доступу та маршрутизаторі. Існують чотири версії протоколу безпеки для захисту бездротових мереж Wi-Fi Protected Access (WPA): WPA, WPA2, WPA3, WPA4 (табл. 2). На сьогодні більшість пристрої працюють на WPA2, який не надає надійного захисту та має багато недоліків з боку безпеки. Головною загрозою з 2017 р. для цього протоколу є атаки з перевстановленням ключа (англ. Key Reinstallation Attack, KRACK). Під час такої атаки пристрій підключається до Wi-Fi через захищений WPA2. Перевірка відбувається через процес 4-way handshake (процес обміну чотирма повідомленнями між точкою доступу – Автентифікатором – і клієнтським пристроєм – Заявником – для створення деяких ключів шифрування, які можна використовувати для шифрування фактичних даних, надісланих через бездротове середовище) [8]. Під час цього обміну зловмисник має можливість перехопити й повторно пройти частину процесу, що може привести до перехоплення даних: логін, паролі та ін. [9; 10].

Таблиця 2. Порівняння стандартів захисту технології Wi-Fi

Характеристика	**WPA**	**WPA2**	**WPA3**	**WPA4**
Рік випуску	2003	2004	2018	2026–2028
Ключ шифрування, біт	64	128	192 / 256	256
Протокол аутентифікації	TKIP+RC4	802.1X / EAP	SAE	NIST, Zero Trust
Захист від розподілених атак на відмову в обслуговуванні (DDoS)	Відсутній	Відсутній	Є	Є (за рахунок ШІ для аналізу та активної протидії)
Захист від атак перехоплення (Man-in-the-Middle)	Відсутній	Відсутній	Захист за допомогою аутентифікації на основі обміну пакетами	Динамічна зміна рівнів шифрування в залежності від типу атаки
Підтримка застосування на пристроях, випущених до 2018 р.	Відсутня	Відсутня	Можливість роботи в режимі «WPA3-перехід» для підтримки пристроїв, випущених до 2018 р.	Не визначено; технологія ще у розробці

Для захисту від KRACK-атак у 2018 р. було створено протокол безпеки WPA3, який використовує новий тип шифрування SAE (Simultaneous Authentication of Equals). В зазначеному методі одночасної рівноправної автентифікації кожна сесія індивідуально шифрується для захисту від перехоплення даних. Головною складністю для введення у роботу WPA3 є відсутність даного протоколу на пристроях, які розроблені до 2018 р. [11; 12].

У 2019 р. була сформована робоча група IEEE 802.11be, яка досліджує та аналізує новітні технології Wi-Fi 7 та WPA4 [12]. Відміною WPA4 від попередніх версій протоколу стануть новітні

рішення у механізмах аутентифікації та безпеки. Головним інструментом є впровадження більш просунутих технологій шифрування, які будуть базуватися на квантових обчисленнях. Для протидії DDoS-атакам досліджується можливість використання штучного інтелекту (ШІ) [13; 14], який буде аналізувати атаку та чинити активну протидію. Також у WPA4 планується спростити процес підключення й при цьому підвищити рівень безпеки. Головним інструментом, як вважають дослідники, стане покращений принцип криптографії з відкритим ключем. Дослідники вважають, що WPA4 зможе вирішити проблеми, пов'язані з атаками погодження часу, пам'яті та даних (англ. Time Memory Trade-Off, TMTO).

Одною з технологій, що мають перспективу для захисту окремих сегментів в бездротовій ЛОМ, є створення логічно відокремлених віртуальних локальних мереж (англ. Virtual Local Area Network, VLAN). В такому разі фізичну мережу розділяють на декілька віртуальних, в яких сформовано окремі політики доступу до інформації для різних типів працівників та відвідувачів:

а) VLAN 10 – гостьові користувачі;
б) VLAN 20 – співробітники з низьким доступом;
в) VLAN 30 – співробітники з привілейованим доступом;
г) VLAN 40 – керівництво;
д) VLAN 50 – сервери.

Розмежування даного типу захищає дані від зловмисників як зовні, так і в середині, оскільки зловмисник, отримавши доступ до одного сегменту мережі, не отримає повної інформації про всю мережу та дані.

Завдяки одночасного використання WIDS-моніторингу бездротової мережі, під час якого проводиться аналіз радіоефіру у пошуках підозрілих приладів або НСД, проводиться фільтрацію MAC-адрес по «білому списку» (список MAC-адрес приладів, які дозволені у мережі) та перевіряється їх активність. Головна задача даних систем – сповістити адміністраторів про порушення КЗ або автоматично вжити заходів протидії (блокувати відфільтровані MAC-адреси). Такі системи в залежності від налаштувань здатні виявити [15–17]:

- фальшиві точки доступу (англ. Rogue AP);
- копії точок доступу по типу «злого двійника» (англ. Evil Twin AP);
- пристрої сканування мережі;
- пристрої, які спрямовані на атаки типу DDoS й та ін.

У разі потреби покрити WiFi-сигналом певну вузьку КЗ, без потреби у покритті на 360 градусів, доцільно використання спрямованих антен, які передають сигнал у конкретному напрямку. Застосування певного типу антен обумовлено кутом огляду, який забезпечується у кожному форм-факторі (табл. 3).

Таблиця 3. Порівняння кутів огляду спрямованих антен

Тип антени	**Кут огляду, град.**
Панельна	60–90
Типу «Yagi»	20–30
Параболічна	5–10
Секторна	60–120

У випадку, коли немає можливості зменшити потужність передачі чи встановити спрямовану антену, актуальним є використання джаммерів. За допомого джаммерів створюється обмеження КЗ за рахунок блокування сигналу та ізолюються об'єкти, де циркулює інформація з обмеженим доступом (дата-центр, конференц-зали тощо). Потужність джаммерів легко контролювати, що надає велику адаптивність зазначеній технології. Джаммери є потужним інструментом для обмеження зони покриття бездротового сигналу, але його використання потребує обережності, точності налаштувань і дотримання законодавства.

Для побудови КЗ з найкращими показниками безпеки та адаптивності доцільно використовувати комбінований метод формування КЗ, який об'єднує різні типи захисту для підвищення загального рівня захисту. Розглянута методологія захисту при розгортанні ізольованих сегментів у локальні бездротовій мережі включає всі рівні захисних заходів – фізичні, логічні та організаційні (рис. 1).

Рис. 1. Схема формування КЗ у БКМ

Також важливою ланкою системи захисту будь-якої локальної мережі є обізнаність персоналу, який буде користуватися даною мережею. Впровадження організаційних заходів теж є складовою стратегії побудови КЗ.

Висновки та перспективи подальшого дослідження. Було проаналізовано існуючі методи формування КЗ у БКМ, їх переваги та недоліки. Було відмічено, що класичні фізичні та програмні методи зонування мають певні обмеження в гнучкості, зміні зони покриття та введення нових систем кібербезпеки. Використання VLAN, WIDS-моніторингу та новітніх протоколів безпеки дозволяє формувати адаптивні КЗ, але для впровадження кожного методу є певні складнощі. Запропонована схема формування КЗ комбінованого підходу, який включає різні методи в тому числі й організаційні заходи. Подальші дослідження полягають у розробці нових методів формування КЗ, а також у автоматизації систем динамічного управління КЗ. Важливою ланкою майбутніх перспектив є використання штучного інтелекту для забезпечення безпеки та моніторингу мережевих ресурсів. Доцільно дослідити технології SDN/NFV та методи їх інтеграції у структуру БКМ.

Список бібліографічного опису

1.Huang B., Yao H., Wu Q. B. Prediction and evaluation of wireless network data transmission security risk based on machine learning. *Wireless Networks*. 2024. DOI: 10.1007/s11276-024-03773-7.

2.Zhang X. et al. Scalable Power Control/Beamforming in Heterogeneous Wireless Networks with Graph Neural Networks / GLOBECOM 2021 – 2021 IEEE Global Communications Conference, Madrid, Spain, 7–11 December 2021. 2021. DOI: 10.1109/globecom46510.2021.9685457.

3.Зінченко О. В., Вишнівський В. В., Гладких В. М., Прокопов С. В., Звенігородський О. С. Аналітичне моделювання SDN / NFV. *Системи управління, навігації та зв'язку :* зб. наук. праць. 2021. Т. 2, № 64. С. 136–139. DOI: 10.26906/SUNZ.2021.2.136.

4.Zhu C. et al. ADFL: Defending backdoor attacks in federated learning via adversarial distillation. *Computers & Security.* 2023. Vol. 132. P. 103366. DOI: 10.1016/j.cose.2023.103366.

5.Guri M., Zadov B., Elovici Y. ODINI: Escaping Sensitive Data From Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *IEEE Transactions on Information Forensics and Security.* 2020. Vol. 15. P. 1190–1203. DOI: 10.1109/tifs.2019.2938404.

6.Shukla V. Review of electromagnetic interference shielding materials fabricated by iron ingredients. *Nanoscale Advances.* 2019. Vol. 1, no. 5. P. 1640–1671. DOI: 10.1039/c9na00108e.

7.MikroTik hAP (RB951Ui-2nD). Mikrotik.UA. URL: https://www.technotrade.com.ua/Products/MikroTik_RB951Ui-2nD.php (дата звернення: 27.04.2025).

8.WPA and WPA2 4-Way Handshake. URL: https://networklessons.com/wireless/wpa-and-wpa2-4-way-handshake (Last accessed: 27.04.2025).
9.Arikumar K. S., Kumar D., Prathiba S. B., Tamilarasi K., et al. Enhancing the Security of WPA2/PSK Authentication Protocol in Wi-Fi Networks. *Procedia Computer Science*. 2022. Vol. 215. P. 413–421. DOI: 10.1016/j.procs.2022.12.043.
10. Noh J., Kim J., Cho S. Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks. *IEEE Access.* 2018. P. 1–10. DOI: 10.1109/ACCESS.2018.2809614.
11. Опірський І., Максимів Н., Женчур М. Дослідження безпеки стандарту Wi-Fi Protected Access 3 (WPA3). *Ukrainian Scientific Journal of Information Security.* 2023. Т. 29, № 1. С. 21–31. DOI: 10.18372/2225-5036.29.17549.
12. Zanna P., Radcliffe P., Kumar D. WP4: A P4 Programmable IEEE 802.11 Data Plane. 2020 30th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 25–27 November 2020. 2020. DOI: 10.1109/itnac50341.2020.9315141.
13. Bennet K. et al. Implementing AI Bill of Materials (AI BOM) with SPDX 3.0: A Comprehensive Guide to Creating AI and Dataset Bill of Materials. The Linux Foundation, 2024. DOI: doi.org/10.70828/rned4427.
14. Chernyshev M., Baig Z., Doss R. R. M. Towards Large Language Model (LLM) Forensics Using LLM-based Invocation Log Analysis. CCS '24: ACM SIGSAC Conference on Computer and Communications Security, Salt Lake City UT USA. New York, NY, USA, 2023. P. 89–96. DOI: 10.1145/3689217.3690616.
15. Hsu F.-H., Wu M.-H., Hwang Y.-L., Lee C.-H., Wang C.-S., Chang T.-C. WPFD: Active User-Side Detection of Evil Twins. *Applied Sciences*. 2022. Vol. 12, Is. 8088.P. 1–14. DOI: 10.3390/app12168088.
16. Korolkov R., Kutsak S. Received-Signal-Strength-Based Approach for Detection and 2D Indoor Localization of Evil Twin Rogue Access Point in 802.11. *International Journal of Safety and Security Engineering.* 2021. Vol. 11. P. 13–20. DOI: 10.18280/ijsse.110102.
17. Kara İ. Twin Ghosts: Evil Twin Attacks in Wireless Networks and Defense Mechanisms. *Bitlis Eren University Journal of Science and Technology.* 2024. Vol. 14. DOI: 10.17678/beuscitech.1450756.

References

1.Huang B., Yao H., Wu Q. B. Prediction and evaluation of wireless network data transmission security risk based on machine learning. *Wireless Networks*. 2024. DOI: 10.1007/s11276-024-03773-7.
2.Scalable Power Control/Beamforming in Heterogeneous Wireless Networks with Graph Neural Networks / X. Zhang et al. GLOBECOM 2021 - 2021 IEEE Global Communications Conference, Madrid, Spain, 7–11 December 2021. 2021. DOI: 10.1109/globecom46510.2021.9685457.
3.Zinchenko O. V., Vyshnivskyi V. V., Hladkykh V. M., Prokopov S. V., Zvenihorodskyi O. S. Analytical Modeling of SDN / NFV. *Control, Navigation and Communication Systems* : Collection of Scientific Papers. 2021. Vol. 2, No. 64. P. 136–139. DOI: 10.26906/SUNZ.2021.2.136 [In Ukrainian].
4.Zhu C. et al. ADFL: Defending backdoor attacks in federated learning via adversarial distillation. *Computers & Security.* 2023. Vol. 132. P. 103366. DOI: 10.1016/j.cose.2023.103366.
5.Guri M., Zadov B., Elovici Y. ODINI: Escaping Sensitive Data From Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *IEEE Transactions on Information Forensics and Security.* 2020. Vol. 15. P. 1190–1203. DOI: 10.1109/tifs.2019.2938404 (Last accessed: 26.04.2025).
6.Shukla V. Review of electromagnetic interference shielding materials fabricated by iron ingredients. *Nanoscale Advances.* 2019. Vol. 1, No. 5. P. 1640–1671. DOI: 10.1039/c9na00108e.
7.MikroTik hAP (RB951Ui-2nD). Mikrotik.UA. URL: https://www.technotrade.com.ua/Products/MikroTik_RB951Ui-2nD.php (Last accessed: 27.04.2025) [In Ukrainian].
8.WPA and WPA2 4-Way Handshake. URL: https://networklessons.com/wireless/wpa-and-wpa2-4-way-handshake (Last accessed: 27.04.2025).
9.Arikumar K. S., Kumar D., Prathiba S. B., Tamilarasi K., et al. Enhancing the Security of WPA2/PSK Authentication Protocol in Wi-Fi Networks. *Procedia Computer Science*. 2022. Vol. 215. P. 413–421. DOI: 10.1016/j.procs.2022.12.043.
10. Noh J., Kim J., Cho S. Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks. *IEEE Access.* 2018. P. 1–10. DOI: 10.1109/ACCESS.2018.2809614.
11. Opirskyi I., Maksymiv N., Zhenchur M. Security research of Wi-Fi Protected Access 3 (WPA3). *Ukrainian Scientific Journal of Information Security.* 2023. T. 29, № 1. C. 21–31. DOI: 10.18372/2225-5036.29.17549 [In Ukrainian].
12. Zanna P., Radcliffe P., Kumar D. WP4: A P4 Programmable IEEE 802.11 Data Plane. 2020 30th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 25–27 November 2020. 2020. DOI: 10.1109/itnac50341.2020.9315141.
13. Bennet K. et al. Implementing AI Bill of Materials (AI BOM) with SPDX 3.0: A Comprehensive Guide to Creating AI and Dataset Bill of Materials. The Linux Foundation, 2024. DOI: 10.70828/rned4427.
14. Chernyshev M., Baig Z., Doss R. R. M. Towards Large Language Model (LLM) Forensics Using LLM-based Invocation Log Analysis. CCS '24: ACM SIGSAC Conference on Computer and Communications Security, Salt Lake City UT USA. New York, NY, USA, 2023. P. 89–96. DOI: 10.1145/3689217.3690616.
15. Hsu F.-H., Wu M.-H., Hwang Y.-L., Lee C.-H., Wang C.-S., Chang T.-C. WPFD: Active User-Side Detection of Evil Twins. *Applied Sciences*. 2022. Vol. 12, Is. 8088.P. 1–14. DOI: 10.3390/app12168088.
16. Korolkov R., Kutsak S. Received-Signal-Strength-Based Approach for Detection and 2D Indoor Localization of Evil Twin Rogue Access Point in 802.11. *International Journal of Safety and Security Engineering.* 2021. Vol. 11. P. 13–20. DOI: 10.18280/ijsse.110102.
17. Kara İ. Twin Ghosts: Evil Twin Attacks in Wireless Networks and Defense Mechanisms. *Bitlis Eren University Journal of Science and Technology.* 2024. Vol. 14. DOI: 10.17678/beuscitech.1450756.