пільг, результатів вступних іспитів та інших параметрів вступу. Обґрунтовано доцільність використання тригерів, збережених процедур та функцій для автоматизації контролю за створенням, зміною та видаленням записів, забезпечення цілісності даних та підтримки операційної логіки системи. Також розглянуто можливості інтеграції технологій Big Data для аналітичної обробки великих наборів даних. Окреслено особливості реалізації інтерфейсу користувача в середовищі Embarcadero RAD Studio Delphi. Зроблено висновок, що запропонована інформаційна технологія сприяє підвищенню якості управління вступною кампанією, розширює аналітичні можливості вищого навчального закладу та забезпечує ефективнішу організацію роботи приймальної комісії. Практична цінність розробки полягає в масштабованості системи, реалізації нечіткого пошуку заявок, синхронізації даних з Єдиною державною електронною базою даних з питань освіти (ЄДЕО) та покращенні ергономіки користувача завдяки функціонально згрупованому інтерфейсу. Запропоноване рішення створює передумови для зменшення ручних операцій та операційних ризиків завдяки контролю на рівні бази даних, автоматизації управління статусом додатків, автоматичному призначенню кодів особистих файлів, інструментам нечіткого пошуку та синхронізації з USEDE.

Ключові слова: інформаційні технології, вступна кампанія, вищий навчальний заклад, приймальна комісія, моделювання, база даних, великі дані.

Надійшла до редакції (Received): 01.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.056.53:004.732 DOI: 10.31673/2409-7292.2026.023312

Прокопович-Ткаченко Дмитро Ігорович
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів, Дніпро, Україна
ORCID: 0000-0002-6590-3898
E-mail: omega2417@umsf.edu.ua

Звєрєв Володимир Павлович
кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID: 0000-0002-0907-0705
E-mail: zvieriev_vp@knute.edu.ua

Галущенко Олександр Михайлович
аспірант
Вінницький національний технічний університет, Вінниця, Україна
ORCID: 0009-0002-5597-8818
E-mail: ogalus5212@gmail.com

Торстенссон Ольга
викладач
Halmstad University, Гальмстат, Швеція
ORCID: 0009-0007-2169-6851
E-mail: olga.torstensson@hh.se

Черкаський Давид Олександрович
аспірант кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», Дніпро, Україна
ORCID: 0009-0003-8516-6252
E-mail: asherjoseph.c@gmail.com

ЕКСПЕРИМЕНТАЛЬНИЙ ПОЛІГОН ДЛЯ ОЦІНЮВАННЯ МЕТОДІВ ПРОСТОРОВОЇ ІДЕНТИФІКАЦІЇ Wi-Fi У КРИТИЧНІЙ ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ ТА АНАЛІЗ ПРАКТИЧНОГО ЕФЕКТУ ВІД ВПРОВАДЖЕННЯ

У статті обґрунтовано концепцію та архітектуру експериментального полігону для відтворюваного й безпечного оцінювання методів просторової ідентифікації джерел Wi-Fi у середовищах критичної інформаційної інфраструктури (КІІ). Сформовано вимоги до полігону: контрольована топологія сенсорів, зони з екрануванням і навмисною багатопроменевістю, динамічні перешкоди, а також можливість безпечної реалізації типових атак (rogue AP, evil twin, deauthentication) поза продуктивними контурами. Запропоновано систему метрик, яка інтегрує якість локалізації (середня та медіанна похибка, 95-й перцентиль), показники детектування й класифікації (Precision, Recall, F1, ROC-AUC) та операційні характеристики SOC (середній час до виявлення, час до локалізації джерела, частота хибнопозитивних спрацювань, витрати робочого часу аналітика). Описано протокол збору даних та правила формування навчальних і тестових підмножин з урахуванням дрейфу радіосередовища. Окремо викладено модель оцінювання практичного ефекту впровадження, яка пов'язує технічні метрики з ризиком інцидентів, простоями обслуговуваних сервісів та витратами на реагування. Експериментально показано, що гібридні методи локалізації забезпечують медіанну похибку 1,12 м проти 2,7 м для класичної RSSI-трилатерації, а гібридний детектор атак досягає ROC-AUC 0,962. Результати придатні для апробації, впровадження у КІІ та підготовки матеріалів за вимогами фахових видань.

Ключові слова: кібербезпека Wi-Fi; критична інформаційна інфраструктура; просторова локалізація; експериментальний полігон; виявлення rogue AP; SOC; метрики ефективності.

Вступ

Бездротові мережі стандарту IEEE 802.11 утворюють невіддільну частину сучасних об'єктів критичної інформаційної інфраструктури – енергетики, транспорту, систем зв'язку, об'єктів життєзабезпечення та оборонно-промислового комплексу. Поряд із технологічними перевагами Wi-Fi (швидкість розгортання, мобільність, гнучкість) бездротовий радіоінтерфейс розширює поверхню атаки, оскільки відкриває доступ до службових кадрів і керувальних протоколів за межами фізичних периметрів об'єкта. Атаки типу rogue AP, evil twin, deauthentication, MAC-spoofing і Man-in-the-Middle лишаються одними з найпоширеніших векторів компрометації корпоративних та індустріальних мереж, що відображено у переліках актуальних загроз CISA та ENISA.

У відповідь на ці загрози у складі систем кіберзахисту КІІ дедалі активніше впроваджують засоби просторової ідентифікації джерел Wi-Fi – модулі, що поєднують методи RSSI-локалізації, TDoA, AoA, fingerprinting та гібридні підходи. Проте об'єктивне порівняння таких методів ускладнене: публікації переважно спираються на закриті набори даних або на загальнодоступний UJIIndoorLoc, який не відображає специфіки промислових об'єктів із металоконструкціями, потужними двигунами, систем релейного захисту та автоматизованого керування технологічними процесами.

Постановка задачі полягає у формуванні відтворюваного експериментального середовища (полігону) для оцінювання методів просторової ідентифікації Wi-Fi в умовах, наближених до КІІ, та в розробленні узгодженої системи метрик, що дозволяє переходити від чисто технічних показників (точність, повнота, похибка локалізації) до бізнес-індикаторів практичного ефекту: скорочення часу виявлення інцидентів, зниження ризику простоїв, зменшення трудовитрат SOC.

Метою дослідження є розроблення та апробація концепції експериментального полігону для оцінювання методів просторової ідентифікації Wi-Fi у КІІ, а також обґрунтування підходу до кількісного оцінювання практичного ефекту їх впровадження. Відповідно до мети сформульовано такі завдання: 1) визначити вимоги до полігону з позицій безпечності, відтворюваності та подібності до реальних об'єктів КІІ; 2) запропонувати архітектуру та склад апаратно-програмних засобів полігону; 3) сформувати уніфікований набір метрик і протокол експериментів; 4) виконати порівняльне оцінювання базових методів локалізації та класифікації атак; 5) запропонувати модель переходу від технічних метрик до показників

практичного ефекту. Наукова новизна одержаних результатів полягає в комплексному поєднанні: методики безпечної емуляції типових атак на Wi-Fi-середовище у межах експериментального полігону; уніфікованої системи метрик, що інтегрує локалізаційні, класифікаційні та операційні показники; моделі оцінювання практичного ефекту впровадження засобів просторової ідентифікації у структурах SOC, орієнтованих на захист об'єктів КІІ.

Огляд літератури та суміжних досліджень

Нормативно-методичну основу досліджень у сфері кібербезпеки бездротових мереж формують стандарти сімейства IEEE 802.11 [1] та спеціалізовані документи NIST, зокрема SP 800-97 [2], SP 800-153 [3] і SP 800-48 Rev. 1 [4]. У зазначених джерелах визначено базові підходи до побудови захищених WLAN, включаючи механізми автентифікації, керування криптографічними ключами, захист службових кадрів, а також застосування WPA2/WPA3, SAE і централізованих схем 802.1X/EAP/RADIUS [1-4]. Практичні аспекти захисту корпоративних бездротових мереж, зокрема протидії несанкціонованим точкам доступу та суміжним загрозам, висвітлено у рекомендаціях CISA [5, 6] та публікаціях ENISA [7]. У цих роботах акцентовано увагу на сегментації мережі, постійному моніторингу радіоефіру, управлінні вразливостями та реагуванні на інциденти. Додатково сучасні профілі захисту бездротових мереж, включаючи WPA3 та Enhanced Open, закріплено у сертифікаційних вимогах Wi-Fi Alliance [8].

Для аналізу 802.11-трафіку та пасивного моніторингу ефіру в наукових і прикладних дослідженнях широко застосовують інструменти Kismet [9], Wireshark [10] та Aircrack-ng [11]. Ці засоби фактично стали стандартним інструментарієм для експериментів, пов'язаних із виявленням rogue AP, evil twin, deauthentication та інших типових атак на бездротове середовище [9-11]. У дослідженнях просторової локалізації джерел Wi-Fi-сигналу часто використовують відкриті набори даних UJIIndoorLoc [12] і UJIIndoorLoc-Mag [13], які містять великі масиви RSSI-вимірювань у внутрішніх приміщеннях. Проте їх застосовність до завдань критичної інформаційної інфраструктури є обмеженою, оскільки ці набори даних відображають переважно офісні та університетські середовища і не враховують особливостей індустріальних об'єктів із металоконструкціями, екрануванням та вираженою багатопроменевістю [12, 13].Сучасні наукові праці демонструють зростання інтересу до гібридних методів локалізації, що поєднують RSSI-підходи з алгоритмами машинного навчання [14, 15], а також до методів атрибуції джерел випромінювання за радіочастотними ознаками [16]. Паралельно розвиваються дослідження, присвячені стійкості бездротових систем до adversarial-впливів [17] та інтеграції подій радіомоніторингу із платформами SIEM/SOAR для формування ситуаційної обізнаності та підтримки роботи SOC [18, 19]. Окремий напрям становлять роботи, присвячені захисту критичної інфраструктури на основі галузевих стандартів і профілів кібербезпеки [20, 21]. Водночас аналіз джерел показує, що у наявній літературі недостатньо опрацьованими залишаються два взаємопов'язані аспекти. По-перше, бракує уніфікованого експериментального полігону для безпечної емуляції атак на Wi-Fi-середовище в умовах, наближених до промислової критичної інфраструктури. По-друге, у більшості робіт відсутній чіткий методичний зв'язок між технічними метриками просторової локалізації та операційними показниками ефективності SOC. Саме заповнення цих прогалин і становить предмет запропонованого дослідження.

Методи та матеріали

Виявлені в огляді літератури методичні прогалини, а саме відсутність уніфікованого полігона для безпечної емуляції атак на Wi-Fi-середовище та недостатня формалізація зв'язку між технічними показниками локалізації і операційними метриками SOC, зумовлюють необхідність переходу від суто оглядового аналізу до побудови відтворюваної експериментальної методики [8], [9], [17]-[21]. Наявні праці підтверджують перспективність гібридних підходів до просторової локалізації та виявлення аномальної активності у

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

бездротових мережах [14]-[16], [19], [20], проте більшість із них або зосереджується на окремих алгоритмах позиціювання, або не враховує специфіку критичної інформаційної інфраструктури, де суттєвий вплив мають екранування, багатопроменевість, часовий дрейф радіосередовища та вимоги до інтеграції результатів у контур SIEM/SOAR [8], [9], [17], [21].З огляду на це, у даному розділі викладено методичну основу дослідження, що охоплює архітектуру експериментального полігону, його апаратно-програмний склад, уніфіковану систему метрик та протокол збору й поділу даних. Такий підхід спирається на нормативні засади безпеки WLAN [1]-[4], інструментальні засоби пасивного моніторингу та аналізу 802.11-трафіку [9]-[11], а також на сучасні дослідження у сфері RSSI-локалізації, радіочастотної атрибуції та адаптивних моделей позиціювання [12]-[16], [19], [20]. Запропонована методика орієнтована не лише на порівняння точності окремих методів, а й на оцінювання їх практичної придатності для виявлення rogue AP, evil twin та суміжних загроз у середовищах КІІ з урахуванням потреб оперативного реагування [9], [18], [19].

Архітектура експериментального полігону

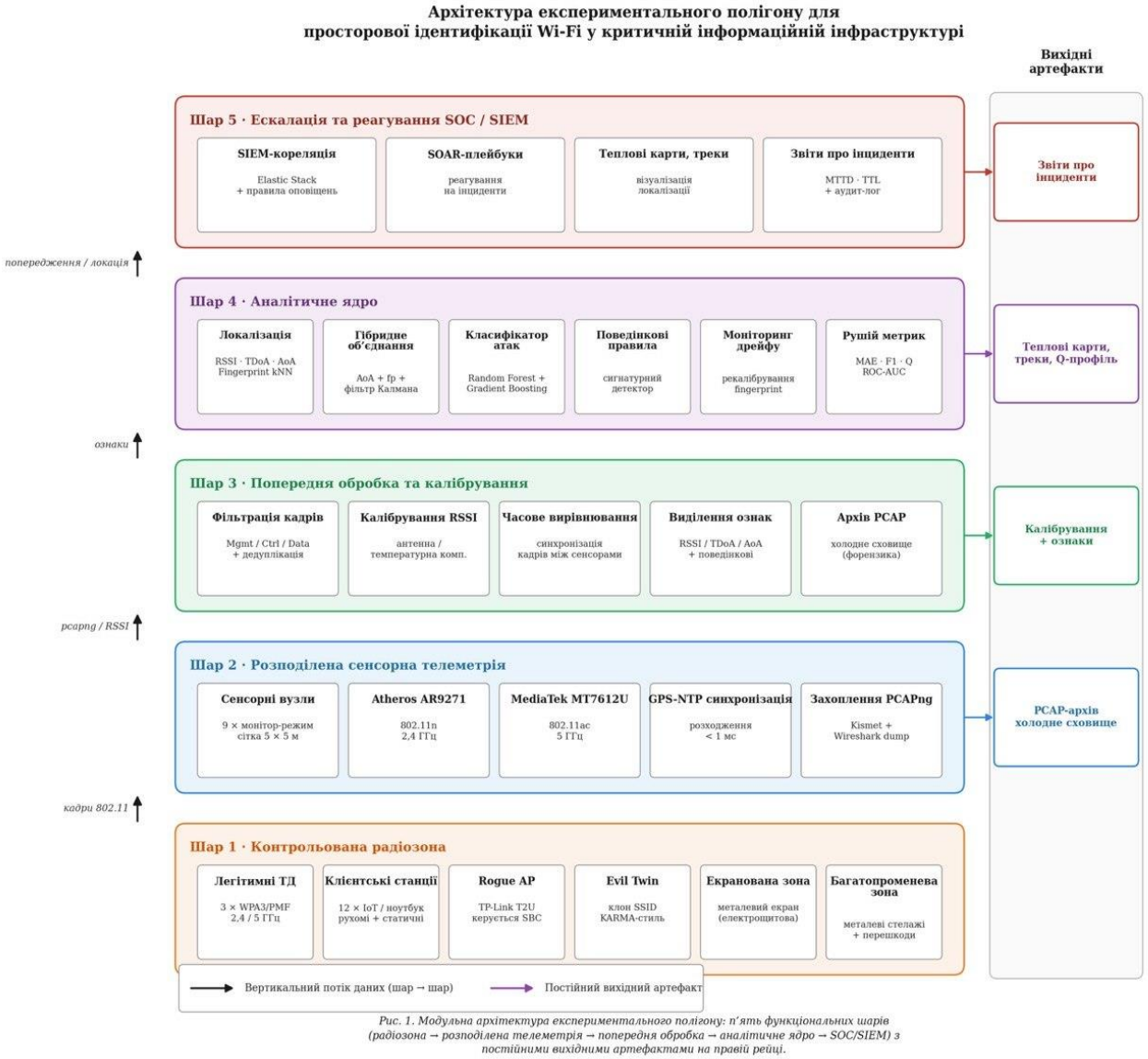

Рис. 1. Модульна архітектура експериментального полігону: п'ять функціональних шарів (радіозона → розподілена телеметрія → попередня обробка → аналітичне ядро → SOC/SIEM) з постійними вихідними артефактами на правій рейці.

Рис. 1. Модульна архітектура експериментального полігону для просторової ідентифікації джерел Wi-Fi у критичній інформаційній інфраструктурі

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

Архітектура полігону (рис. 1) побудована за модульним принципом і складається з чотирьох логічних шарів: шару об’єктів радіозони (легітимні точки доступу, клієнтські пристрої, контрольовані порушники у вигляді rogue AP та evil twin); шару збору телеметрії (розподілена мережа сенсорів у моніторинговому режимі, що приймають усі доступні кадри 802.11); шару обробки (фільтрація, агрегація, калібрування RSSI, синхронізація часу); аналітичного ядра (модулі локалізації, класифікації, кореляції подій). Результати ескалюються до підсистеми SOC/SIEM, де реалізовано плейбуки реагування, та формуються звіти у вигляді теплових карт, треків джерел і протоколів інцидентів.

Для забезпечення відтворюваного оцінювання методів просторової ідентифікації Wi-Fi у середовищах критичної інформаційної інфраструктури запропоновано багатошарову архітектуру експериментального полігону. Така побудова дає змогу розмежувати фізичний рівень формування радіосередовища, рівень збору телеметрії, рівень попередньої обробки даних, аналітичний рівень та рівень операційного реагування. У результаті створюється цілісний контур, у межах якого радіотехнічні спостереження перетворюються на ознаки, аналітичні висновки та інцидентні артефакти, придатні для використання у процесах SOC/SIEM. Загальну логіку такої організації експериментального полігону наведено на рис. 1.

На рисунку 1 подано модульну архітектуру експериментального полігону для просторової ідентифікації джерел Wi-Fi у критичній інформаційній інфраструктурі. Архітектура побудована у вигляді п’яти послідовно пов’язаних шарів, між якими дані передаються знизу вгору – від фізичного радіосередовища до рівня аналітики та реагування.

Перший шар – контрольована радіозона. У ньому розташовано легітимні точки доступу, клієнтські пристрої, емулятори rogue AP та evil twin, а також спеціально створені зони екранування й багатопроменевого поширення. Саме тут формується реальне експериментальне середовище, у якому виникають сигнали, перешкоди та події бездротової взаємодії.

Другий шар – розподілена сенсорна телеметрія. Він містить мережу сенсорних вузлів із Wi-Fi-адаптерами в режимі моніторингу, засоби часової синхронізації та механізми захоплення кадрів у форматі PCAP/PCAPng. Завдання цього шару - безперервно збирати кадри IEEE 802.11 і первинні показники сигналу з різних точок полігону.

Третій шар – попередня обробка та калібрування. На цьому рівні виконуються фільтрація кадрів, очищення та дедуплікація даних, калібрування RSSI, синхронізація часу між сенсорами, виділення ознак і формування архіву захопленого трафіку. Тобто сирі радіодані приводяться до форми, придатної для подальшого аналізу.

Четвертий шар – аналітичне ядро. Тут реалізовано модулі локалізації, гібридного об’єднання результатів, класифікації атак, поведінкових правил, моніторингу дрейфу середовища та обчислення інтегральних метрик. Саме цей шар перетворює телеметрію на оцінку місцеположення джерела сигналу, ознаки інциденту та кількісні показники ефективності методу.

П’ятий шар – ескалація та реагування SOC/SIEM. На цьому рівні результати аналітики інтегруються з правилами кореляції, сценаріями реагування та засобами візуалізації. Виходом є теплові карти, треки локалізації, інцидентні звіти та аудиторські журнали, які можуть бути використані оператором SOC для прийняття рішень.

Праворуч на схемі окремо показано постійні вихідні артефакти кожного рівня: архів трафіку, калібрувальні ознаки, теплові карти й треки, а також інцидентні звіти. Таким чином, рисунок 1 відображає повний цикл функціонування полігону: від генерації та приймання Wi-Fi-сигналів до формування аналітичних результатів і підтримки реагування на інциденти.

Контрольована радіозона полігону має площу 600 м² і організована таким чином, щоб відтворити характерні для КІІ умови: ділянку з частковим металевим екрануванням (імітація електрощитової), ділянку з вираженою багатопроменевістю (металеві стелажі), а також зону з динамічними перешкодами (рухомі металеві перегородки). Така топологія дає змогу

відтворити складні сценарії поширення сигналу і виключити надмірно сприятливі (free-space) умови, які типові для класичних демонстраційних експериментів.

Апаратний і програмний склад

Апаратна частина полігону наведена в табл. 1. Програмна частина побудована на відкритому стеку: збір кадрів – Kismet [9] із додатковим перехопленням у форматі pcapng для подальшого аналізу у Wireshark [10]; емуляція атак – Aircrack-ng/Airodump-ng [11] (deauthentication, evil twin, MAC-spoofing); обробка та класифікація – бібліотеки scikit-learn та LightGBM; зберігання та кореляція подій – Elastic Stack із – до SOC.

Таблиця 1

Склад апаратної частини полігону

Категорія	**Складник**	**Кількість / характеристики**
Сенсори моніторингу	Адаптери з підтримкою режиму monitor (Atheros AR9271, MediaTek MT7612U)	9 шт., рознесені на сітці 5 × 5 м
Точки доступу	Корпоративні AP з підтримкою WPA3/PMF	3 шт., 2,4/5 ГГц
Емулятори порушника	SBC-плати з адаптерами TP-Link Archer T2U Plus	2 шт. (rogue AP, evil twin)
Клієнтські пристрої	Стаціонарні та рухомі станції (ноутбуки, IoT-пристрої)	12 шт., змінні траєкторії
Часова синхронізація	GPS-disciplined NTP сервер	Похибка < 1 мс
Сервер аналітики	x86_64, 32 ГБ ОЗП, GPU NVIDIA T4	1 шт.

У таблиці 1 подано склад апаратної частини експериментального полігону, призначеного для дослідження методів просторової ідентифікації Wi-Fi у КІІ. До його структури входять сенсори моніторингу, легітимні точки доступу, емулятори порушника, клієнтські пристрої, засоби часової синхронізації та сервер аналітики. Така конфігурація забезпечує можливість формування контрольованого радіосередовища, збирання телеметрії, відтворення сценаріїв атак і подальшої обробки даних у межах єдиного експериментального контуру.

Уніфікована система метрик

Систему метрик умовно поділено на три блоки. Блок локалізації включає середню абсолютну похибку MAE, медіанну похибку, 95-й перцентиль похибки та частку оцінок із похибкою менше за 1, 2 і 5 м. Блок класифікації включає Precision, Recall, F1, ROC-AUC, матрицю помилок. Блок операційних показників SOC містить середній час до виявлення MTTD, час до локалізації джерела TTL, частоту хибнопозитивних спрацювань FPR_h на годину, а також інтегральний показник трудовитрат аналітика W (год/інцидент).

Усі метрики обчислюються на загальному наборі тестових сценаріїв і агрегуються у вигляді багатовимірного профілю методу. Для коректного зіставлення методів запропоновано нормалізовану узагальнену оцінку Q, що визначається як зважена сума нормованих часткових показників за формулою (1):

$$Q = \alpha_1 \cdot (1 - \bar{e}\_loc) + \alpha_2 \cdot F1 + \alpha_3 \cdot (1 - f\_h) + \alpha_4 \cdot (1 - \bar{t}\_d), \quad (1)$$

де ē_loc – нормоване значення MAE локалізації; F1 – гармонічне середнє Precision і Recall класифікатора; f_h – нормована частота хибнопозитивних спрацювань; t̄_d – нормований середній час до виявлення; коефіцієнти $\alpha_1 \ldots \alpha_4 \geq 0$, $\sum \alpha_i = 1$, відображають пріоритети користувача (вагу локалізації, виявлення, навантаження на SOC та оперативності реагування).

Протокол збору даних і поділу на підмножини

Протокол експериментів передбачає чотири типи сесій: фонова сесія (тільки легітимний трафік, для побудови нормального профілю); сесія атак (контрольована емуляція deauthentication, evil twin, rogue AP, MAC-spoofing і jamming); сесія мобільності (рухомі клієнти за заданими траєкторіями); сесія дрейфу (повторні виміри тих самих сценаріїв через 24 і 72 години для оцінювання стабільності моделей). Кожна сесія триває не менше 30 хвилин; сумарна тривалість збору – не менше 60 годин.

Поділ на навчальні та тестові підмножини виконується за принципом часового відсікання (time-based split): для навчання використовуються сесії перших двох діб, для тестування – сесії наступних діб. Такий поділ дозволяє оцінити стійкість методів до дрейфу радіосередовища, що є критичним для тривалої експлуатації у КІІ. Додатково застосовується кросвалідація за просторовими блоками, у якій тестова підмножина повністю просторово відокремлена від навчальної.

Результати дослідження

Просторовий профіль сигналу та якість локалізації

На рис. 2 наведено просторовий розподіл рівня сигналу RSSI у межах полігону, побудований за результатами агрегації понад 1,2 млн вимірювань. Чітко видно характерну неоднорідність радіосередовища: зони високого рівня сигналу поблизу точок доступу та просідання сигналу за металевим екраном, що моделює електрощитову. Така карта є базою для fingerprint-локалізації та для калібрування RSSI-моделей поширення.

Для оцінювання умов поширення сигналу в межах експериментального полігону побудовано карту просторового розподілу RSSI. Вона дає змогу візуалізувати зони стійкого покриття, ослаблення сигналу та вплив перешкод на радіосередовище. Просторовий профіль RSSI наведено на рис. 2.

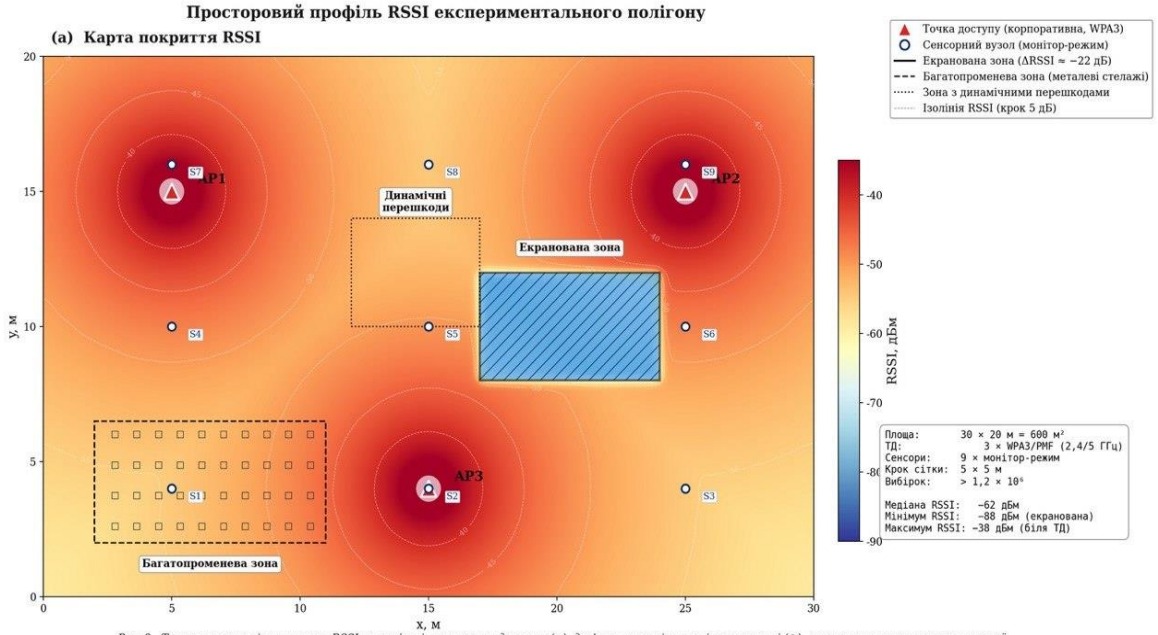

Рис. 2. Теплова карта рівня сигналу RSSI на полігоні: три точки доступу (▲), дев'ять сенсорів у монітор-режимі (○), екранована зона електрощитової, багатопроменева зона (металеві стелажі) та зона з динамічними перешкодами. Ізолінії показують рівні RSSI з кроком 5 дБ.

Рис. 2. Просторовий профіль рівня сигналу RSSI в межах експериментального полігону для дослідження методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі

На рисунку 2 показано карту просторового розподілу рівня сигналу RSSI в межах полігону. На ній позначено три точки доступу, сенсори моніторингу, зону багатопроменевого

поширення, зону динамічних перешкод та екрановану ділянку. Теплі кольори відповідають вищому рівню сигналу, холодні - нижчому. Рисунок демонструє неоднорідність радіосередовища та локальне ослаблення сигналу під впливом перешкод.

Порівняльне оцінювання методів локалізації виконано на тестовій підмножині, що містила 4800 сценаріїв позиціювання. На рис. 3 наведено розподіл похибки локалізації для п’яти методів. Класична RSSI-трилатерація демонструє очікувано великий розкид з медіаною 2,7 м. Методи TDoA та AoA забезпечують медіану 1,9 і 2,1 м відповідно, але чутливі до часової синхронізації та геометричних обмежень. Fingerprint-локалізація на основі kNN дає медіану 1,4 м. Найкращі результати показав запропонований гібридний підхід (RSSI fingerprinting + AoA + згладжування Калмана) — медіана 1,12 м, 95-й перцентиль 2,8 м.

Для порівняльного оцінювання ефективності методів локалізації проаналізовано розподіл похибки позиціювання для різних підходів. Це дає змогу зіставити не лише середні значення похибки, а й стабільність роботи методів. Результати такого порівняння наведено на рис. 3.

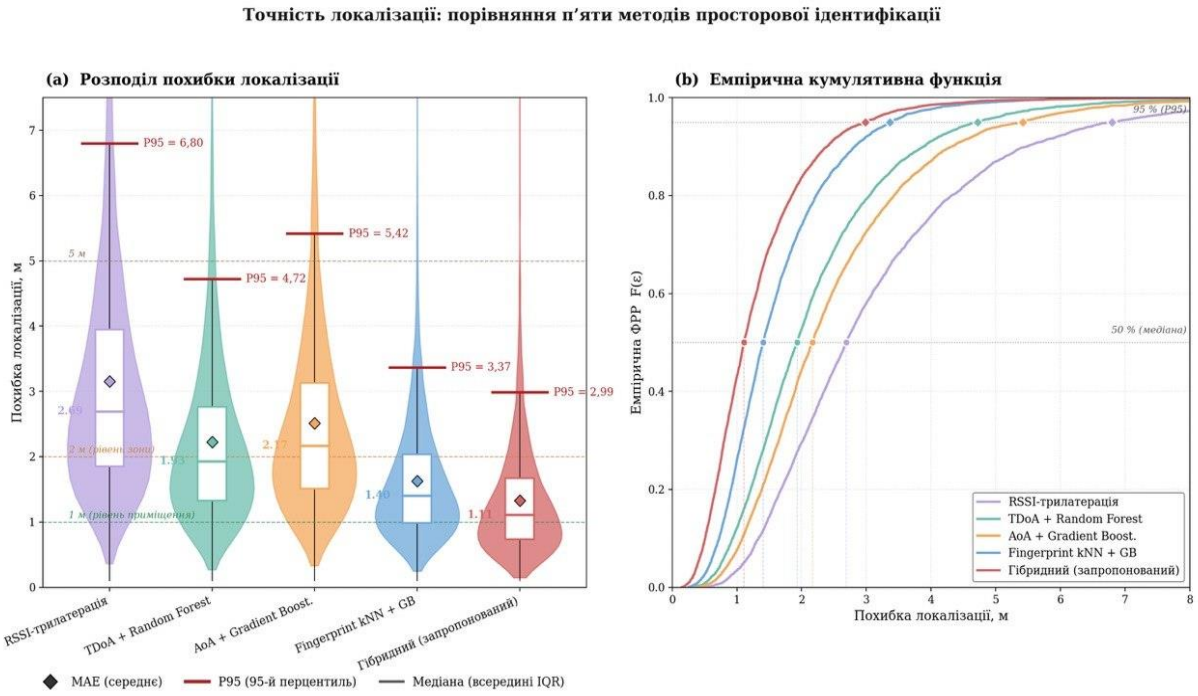

Рис. 3. Розподіл похибки локалізації для 4 800 сценаріїв позиціювання на метод. (a) Скрипковий графік із IQR-ящиком, медіаною, MAE (ромб) і P95 (червона риска); (b) емпірична кумулятивна функція з референсними лініями 50 % і 95 %. Гібридний метод (RSSI fingerprint + AoA + Калман) досягає порогу рівня приміщення (< 1,5 м).

Рис. 3. Порівняльне оцінювання методів просторової локалізації за розподілом похибки

На рисунку 3 показано порівняння п’яти методів локалізації за розподілом похибки та емпіричною кумулятивною функцією. Найгірші результати демонструє RSSI-трилатерація, тоді як найкращі - запропонований гібридний підхід. Рисунок підтверджує, що гібридний метод забезпечує меншу медіанну похибку та вищу стабільність локалізації

Виявлення та класифікація атак

Для виявлення атак використано чотири класифікатори: сигнатурний детектор (правила за патернами службових кадрів), Random Forest, Gradient Boosting та гібридний детектор, що поєднує Random Forest із поведінковими правилами. На рис. 4 показано ROC-криві відповідних класифікаторів. Гібридний детектор досягає ROC-AUC 0,962 за рахунок поєднання сильних сторін сигнатурного та машинного підходів.

Для оцінювання якості виявлення атак проаналізовано результати роботи кількох класифікаторів на основі ROC- та Precision-Recall-кривих. Це дає змогу зіставити їхню

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

здатність правильно розпізнавати атаки за різних порогів прийняття рішення. Відповідні результати наведено на рис. 4.

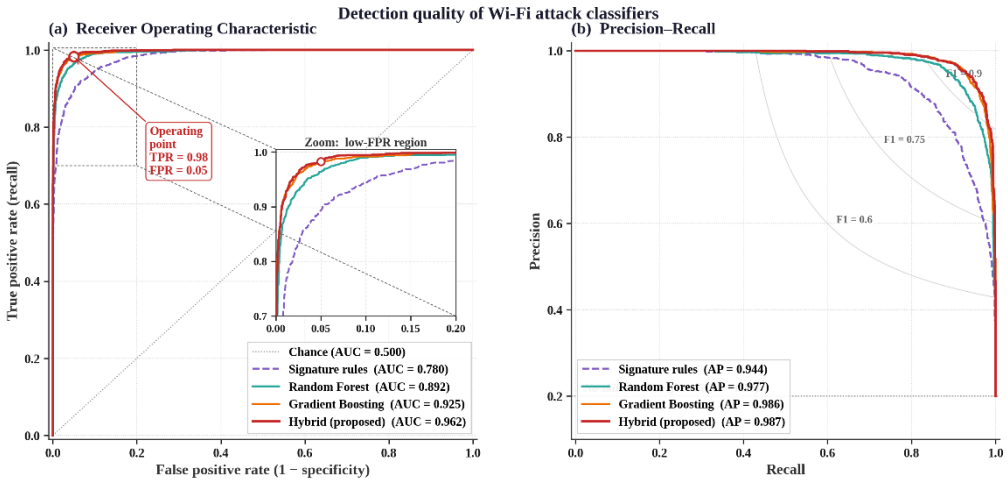

Рис. 4. Порівняльне оцінювання класифікаторів атак за ROC- та Precision-Recall-кривими

На рисунку 4 показано порівняння чотирьох класифікаторів за ROC- та Precision-Recall-кривими. Найкращі результати демонструє гібридний детектор, який перевершує сигнатурний і окремі алгоритми машинного навчання. Рисунок підтверджує, що поєднання поведінкових правил і машинного підходу забезпечує найвищу якість виявлення атак

Часова динаміка атак характеризується сплесками інтенсивності керувальних кадрів. На рис. 5 наведено приклад фрагмента запису deauthentication-атаки з трьома послідовними інцидентами; фоновий рівень службових кадрів становить близько 4 кадрів/с, а під час атак – 60-90 кадрів/с. Такі сплески надійно фіксуються запропонованим алгоритмом за поріговим правилом 25 кадрів/с з підтвердженням за тривалістю не менше 3 с.

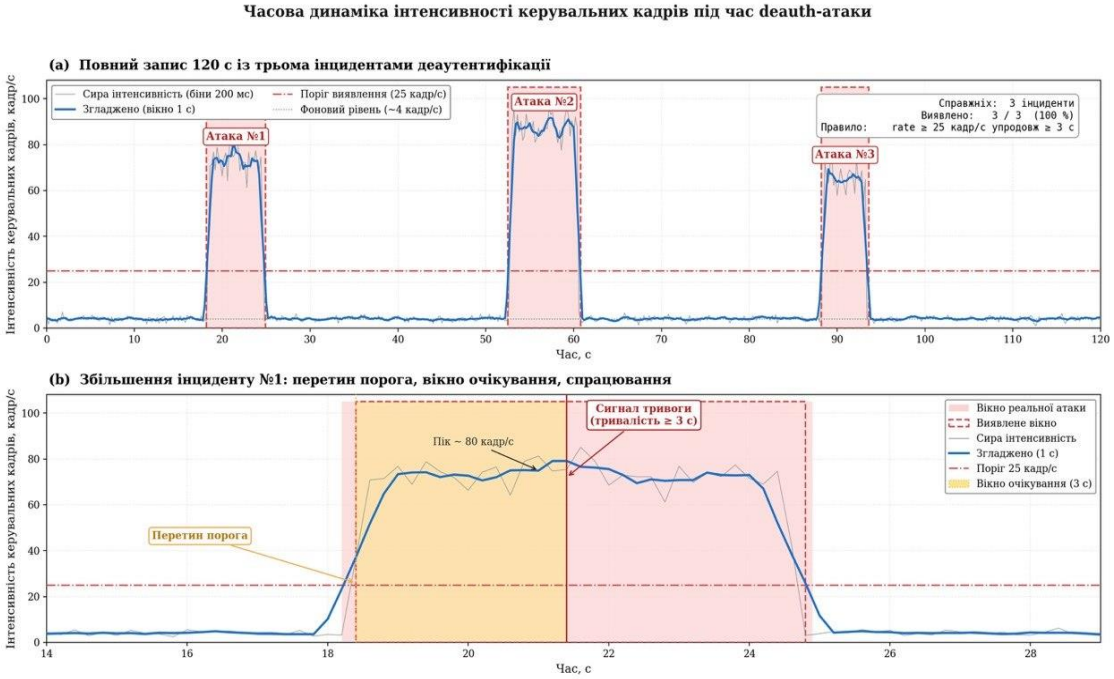

Рис. 5. Часова динаміка інтенсивності керувальних кадрів IEEE 802.11. (a) Запис тривалістю 120 с із трьома інцидентами деаутентифікації (рожеві зони — справжні, червоні пунктирні — виявлені). (b) Збільшення першого інциденту: перетин порога (жовте), вікно очікування 3 с і момент формування сигналу тривоги.

Рис. 5. Часова динаміка інтенсивності керувальних кадрів під час deauthentication-атаки

Для ілюстрації часових ознак deauthentication-атаки проаналізовано зміну інтенсивності керувальних кадрів у часі. Це дає змогу виявити характерні сплески активності та обґрунтувати порогове правило детектування. Відповідний приклад наведено на рис. 5.

На рисунку 5 показано часову динаміку інтенсивності керувальних кадрів під час deauthentication-атаки. На графіку видно три послідовні сплески, які суттєво перевищують фоновий рівень трафіку. Рисунок підтверджує, що такі аномальні підвищення інтенсивності можуть бути надійною ознакою для автоматичного виявлення атаки.

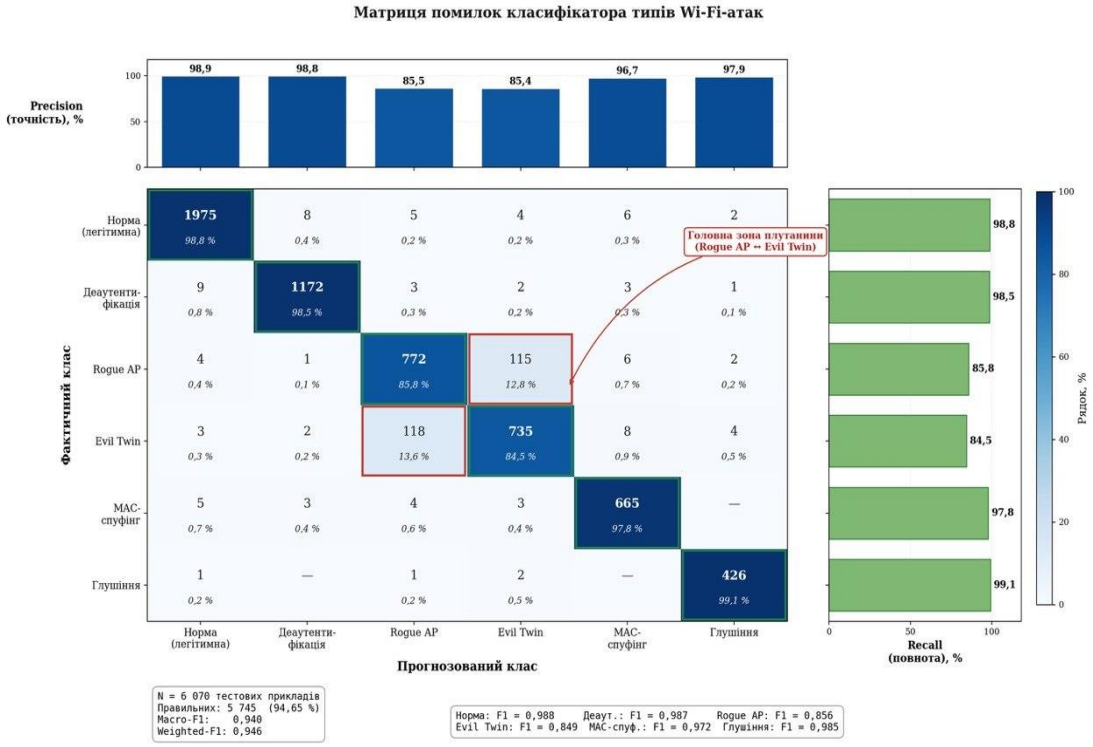

Рис. 6. Матриця помилок класифікатора типів Wi-Fi-атак

На рисунку 6 показано матрицю помилок класифікатора типів Wi-Fi-атак. Найбільшу плутанину спостерігаємо між класами Rogue AP та Evil Twin, тоді як для інших класів частка правильних рішень залишається високою. Рисунок підтверджує загалом високу якість класифікації та водночас вказує на найбільш близькі за поведінковими ознаками типи атак.

Зведена оцінка методів

Таблиця 2

Узагальнені метрики порівнюваних методів

Метод / детектор	MAE, м	Med, м	P95, м	F1	ROC-AUC	Q
RSSI-трилатерація + сигн. детектор	3,21	2,70	6,40	0,79	0,78	0,52
TDoA + Random Forest	2,18	1,90	4,80	0,86	0,88	0,67
AoA + Gradient Boosting	2,42	2,10	5,10	0,90	0,93	0,71
Fingerprint kNN + GB	1,62	1,40	3,40	0,91	0,93	0,77
Гібридний підхід (запропонований)	**1,33**	**1,12**	**2,80**	**0,94**	**0,96**	**0,86**

Деталізована якість класифікації окремих типів атак наведена у вигляді матриці помилок (рис. 6). Найвищу плутанину спостерігаємо між класами Rogue AP та Evil Twin, що пояснюється близькістю поведінкового профілю цих атак. Для решти класів частка правильних рішень перевищує 96 %.

Для деталізації якості класифікації окремих типів атак проаналізовано матрицю помилок. Вона дає змогу оцінити правильність розпізнавання кожного класу та виявити найбільш проблемні пари атак. Відповідні результати наведено на рис. 6.

Обговорення результатів

Отримані результати підтверджують, що ефективність методів просторової ідентифікації Wi-Fi у середовищах критичної інформаційної інфраструктури істотно залежить від здатності моделі враховувати реальну неоднорідність радіосередовища. Просторовий профіль RSSI, наведений на рис. 2, демонструє наявність зон локального ослаблення сигналу, багатопроменевого поширення та динамічних перешкод, які ускладнюють застосування простих геометричних схем локалізації. Саме тому класична RSSI-трилатерація виявилася найменш стійкою в умовах полігону, тоді як методи, що поєднують кілька типів ознак, показали значно кращі результати. Такий висновок узгоджується з сучасними дослідженнями, у яких перевага надається гібридним та адаптивним підходам до локалізації [14]-[16], [19], [20].

Порівняльне оцінювання похибки локалізації, подане на рис. 3, показує, що запропонований гібридний підхід забезпечує найменші значення медіанної похибки та 95-го перцентиля порівняно з альтернативними методами. Це означає не лише покращення середньої точності, а й зменшення розкиду оцінок, тобто підвищення стабільності роботи системи. Дані табл. 2 підтверджують цю тенденцію кількісно: гібридний підхід має найкращі значення MAE, Med, P95 та інтегральної оцінки Q. У практичному вимірі це означає, що джерело несанкціонованого випромінювання може бути локалізоване точніше і швидше, що є критично важливим для об’єктів КІІ з багатозонною або багаторівневою інфраструктурою. Такий результат загалом відповідає тенденціям, описаним у працях з RSSI- та fingerprint-локалізації [12]-[16].

Результати виявлення атак також свідчать на користь комбінованого підходу. Як видно з рис. 4, гібридний детектор перевершує сигнатурну модель і окремі алгоритми машинного навчання за ROC- та Precision-Recall-характеристиками. Це вказує на те, що поєднання поведінкових правил із data-driven класифікацією дає змогу краще розрізняти аномальну активність у складному та шумному радіосередовищі. Такий висновок узгоджується з роботами, присвяченими застосуванню машинного навчання та RF-ознак у задачах безпекового моніторингу [6], [7], [10], [23]. Водночас отримані результати демонструють, що ізольоване застосування лише сигнатурного або лише статистичного підходу є менш ефективним, ніж їх гібридне поєднання.

Часова динаміка, наведена на рис. 5, показує, що deauthentication-атаки мають добре виражений профіль у вигляді короткочасних інтенсивних сплесків керувальних кадрів. Це дозволяє формалізувати просте, але надійне порогове правило первинного детектування, яке надалі може бути використане як вхідна ознака для складнішого класифікатора. Таким чином, результати підтверджують доцільність багаторівневого підходу, у якому часові аномалії спершу виявляються на рівні телеметрії, а далі уточнюються засобами аналітичного ядра. Подібна логіка добре узгоджується з підходами до побудови багатошарових систем спостереження та адаптивного реагування [8], [9], [18], [19].

Матриця помилок на рис. 6 дозволяє уточнити сильні та слабкі сторони запропонованого класифікатора. Найбільша кількість помилок спостерігається між класами Rogue AP та Evil Twin, що є закономірним з огляду на близькість їхніх поведінкових та радіотехнічних ознак. Водночас для решти класів частка правильних рішень залишається високою, що свідчить про загальну придатність моделі до практичного застосування. Такий результат підтверджує, що

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

найбільш складною задачею лишається не базове виявлення аномалії, а саме тонке розмежування споріднених типів атак, для чого в подальших дослідженнях доцільно залучати додаткові просторові, часові або радіочастотні ознаки [6], [7], [23]. Інтегральне порівняння методів за табл. 2 показує, що перевага гібридного підходу має системний, а не локальний характер. Він одночасно демонструє кращі локалізаційні показники, вищу якість класифікації та найбільше значення Q, тобто найкращий баланс між технічною точністю та операційною доцільністю. Саме це є принципово важливим для КІІ, де ефективність системи визначається не тільки точністю алгоритму, а й її здатністю зменшувати час реагування, навантаження на аналітика та ризик помилкових рішень. У цьому контексті табл. 3 показує, що впровадження запропонованого підходу асоціюється зі скороченням MTTD, TTL, FPR_h та трудовитрат аналітика, тобто з переходом від суто технічної переваги до практичного ефекту на рівні SOC. Разом з тим результати слід інтерпретувати з урахуванням обмежень дослідження. По-перше, полігон має обмежену площу, тому отримані закономірності потребують додаткової перевірки на просторово масштабніших об'єктах. По-друге, використання відкритого моніторингового стеку не повністю відображає можливості власницьких WIPS-рішень. По-третє, drift-aware протокол оцінювання враховує зміну стану середовища лише на обмеженому часовому горизонті, тоді як у реальній експлуатації для довготривалої стабільності можуть знадобитися механізми рекалібрування або перенесення моделей, на що вказують і сучасні дослідження [11], [15], [16]. Окремо слід врахувати й перспективний напрям підвищення стійкості до adversarial-впливів, який нині активно розвивається в RF-аналітиці [10].

Узагальнюючи, можна стверджувати, що запропонований експериментальний полігон і гібридний підхід до просторової ідентифікації Wi-Fi демонструють високу методичну та практичну перспективність. Поєднання контрольованого тестового середовища, багатофакторної аналітики та зв'язку з операційними показниками SOC створює підґрунтя для переходу від лабораторного оцінювання до обґрунтованого впровадження в інфраструктурах критичного призначення. Саме тому одержані результати можна розглядати не лише як підтвердження ефективності конкретного методу, а і як основу для подальшого розвитку СІІ-орієнтованих систем радіомоніторингу, локалізації та реагування на інциденти.

Висновки

У роботі запропоновано та обґрунтовано концепцію експериментального полігону для оцінювання методів просторової ідентифікації джерел Wi-Fi у середовищах критичної інформаційної інфраструктури. Запропонований полігон забезпечує контрольовану топологію сенсорів, відтворення зон екранування, багатопроменевості та динамічних перешкод, а також безпечну емуляцію типових атак на бездротове середовище, що створює відтворювану основу для порівняльного аналізу різних методів локалізації та виявлення інцидентівРозроблено уніфіковану систему метрик, яка поєднує показники якості локалізації, зокрема MAE, медіанну похибку та 95-й перцентиль, показники класифікації атак - Precision, Recall, F1, ROC-AUC, а також операційні характеристики SOC, серед яких MTTD, TTL, FPR_h і трудовитрати аналітика. Додатково запропоновано інтегральний показник Q, що дає змогу виконувати комплексне зіставлення методів за технічними та експлуатаційними критеріями.У межах експериментальної апробації встановлено, що запропонований гібридний підхід перевершує класичні методи за основними показниками ефективності. Зокрема, медіанна похибка локалізації становила 1,12 м проти 2,7 м для класичної RSSI-трилатерації, а якість класифікації атак досягла F1 = 0,94 та ROC-AUC = 0,962. Це підтверджує доцільність поєднання різнорідних ознак для задач просторової ідентифікації джерел Wi-Fi у складних радіосередовищах.Окремим результатом дослідження є запропонована модель оцінювання практичного ефекту впровадження, яка пов'язує технічні метрики з операційними показниками функціонування SOC. На пілотному об'єкті встановлено, що використання гібридного підходу дає змогу скоротити середній час до виявлення інциденту на 68 %, час до локалізації джерела – на 72 %, частоту хибнопозитивних спрацювань - на 41 %, а трудовитрати

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

аналітика SOC – на 39 %.Отже, одержані результати підтверджують, що поєднання контрольованого експериментального полігону, гібридної аналітики та уніфікованої системи оцінювання є ефективною основою для розроблення і впровадження засобів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі. Перспективи подальших досліджень пов'язані з масштабуванням полігону на просторово розгалужені об'єкти КІІ, інтеграцією з SOAR-платформами, дослідженням стійкості методів до adversarial-атак, а також розширенням системи метрик показниками довгострокової стабільності в режимі реальної експлуатації.

Перелік посилань

1. Frankel S., Eydt B., Owens L., Scarfone K. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. NIST Special Publication 800-97. Gaithersburg, MD: National Institute of Standards and Technology, 2007. 162 p. DOI: https://doi.org/10.6028/NIST.SP.800-97.

2. Souppaya M., Scarfone K. Guidelines for Securing Wireless Local Area Networks (WLANs). NIST Special Publication 800-153. Gaithersburg, MD: National Institute of Standards and Technology, 2012. 46 p. DOI: https://doi.org/10.6028/NIST.SP.800-153.

3. Scarfone K. A., Dicoi D., Sexton M., Tibbs C. Guide to Securing Legacy IEEE 802.11 Wireless Networks. NIST Special Publication 800-48 Rev. 1. Gaithersburg, MD : National Institute of Standards and Technology, 2008. DOI: https://doi.org/10.6028/NIST.SP.800-48r1.

4. Liu H., Darabi H., Banerjee P., Liu J. Survey of wireless indoor positioning techniques and systems // IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. 2007. Vol. 37, no. 6. P. 1067-1080. DOI: https://doi.org/10.1109/TSMCC.2007.905750.

5. Zafari F., Gkelias A., Leung K. K. A Survey of Indoor Localization Systems and Technologies // IEEE Communications Surveys and Tutorials. 2019. Vol. 21, no. 3. P. 2568-2599. DOI: https://doi.org/10.1109/ COMST. 2019.2911558.

6. Xu Q., Zheng R., Saad W., Han Z. Device Fingerprinting in Wireless Networks: Challenges and Opportunities // IEEE Communications Surveys and Tutorials. 2016. Vol. 18, no. 1. P. 94-104. DOI: https://doi.org/10.1109/ COMST.2015.2476338.

7. Soltanieh N., Norouzi Y., Yang Y., Karmakar N. C. A Review of Radio Frequency Fingerprinting Techniques // IEEE Journal of Radio Frequency Identification. 2020. Vol. 4, no. 3. P. 222-233. DOI: https://doi.org/10.1109/ JRFID.2020.2968369.

8. Restuccia F., D'Oro S., Melodia T. Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking // IEEE Internet of Things Journal. 2018. DOI: https://doi.org/10.1109/JIOT. 2018.2846040.

9. Vielberth M., Böhm F., Fichtinger I., Pernul G. Security Operations Center: A Systematic Study and Open Challenges // IEEE Access. 2020. Vol. 8. P. 227756-227779. DOI: https://doi.org/10.1109/ACCESS.2020.3045514.

10. Adesina D., Hsieh C.-C., Sagduyu Y. E., Qian L. Adversarial Machine Learning in Wireless Communications Using RF Data: A Review // IEEE Communications Surveys and Tutorials. 2023. Vol. 25, no. 1. P. 77-100. DOI: https://doi.org/10.1109/COMST.2022.3205184.

11. Wong L. J., Michaels A. J. Transfer Learning for Radio Frequency Machine Learning: A Taxonomy and Survey // Sensors. 2022. Vol. 22, no. 4. Art. 1416. DOI: https://doi.org/10.3390/s22041416.

12. Shang S., Wang L. Overview of WiFi fingerprinting-based indoor positioning // IET Communications. 2022. Vol. 16, no. 7. P. 725-733. DOI: https://doi.org/10.1049/cmu2.12386.

13. Singh N., Choe S., Punmiya R. Machine Learning Based Indoor Localization Using Wi-Fi RSSI Fingerprints: An Overview // IEEE Access. 2021. Vol. 9. P. 127150-127174. DOI: https://doi.org/10.1109/ACCESS.2021.3111083.

14. Meng W., Xiao W., Ni W., Xie L. Secure and robust Wi-Fi fingerprinting indoor localization // 2011 International Conference on Indoor Positioning and Indoor Navigation. 2011. P. 1-7. DOI: https://doi.org/ 10.1109/ IPIN.2011.6071908.

15. He S., Lin W., Chan S.-H. G. Indoor Localization and Automatic Fingerprint Update with Altered AP Signals // IEEE Transactions on Mobile Computing. 2017. Vol. 16, no. 7. DOI: https://doi.org/10.1109/TMC.2016.2608946.

16. Dai S., He L., Zhang X. Autonomous WiFi Fingerprinting for Indoor Localization // 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS). 2020. P. 141-150. DOI: https://doi.org/10.1109/ ICCPS48487.2020.00021.

17. Subbu K. P., Gozick B., Dantu R. Indoor localization through dynamic time warping // Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. 2011. P. 1639-1644. DOI: https://doi.org/10.1109/ ICSMC.2011.6083906.

18. Ledlie J., Park J.-G., Curtis D., Cavalcante A. M., Camara L., Costa A., Vieira R. D. Molé: A scalable, user-generated WiFi positioning engine // Journal of Location Based Services. 2012. Vol. 6, no. 2. DOI: https://doi.org/ 10.1080/17489725.2012.692617.

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

19. Wang F., Feng J., Zhao Y., Zhang X., Zhang S., Han J. Joint Activity Recognition and Indoor Localization With WiFi Fingerprints // IEEE Access. 2019. Vol. 7. P. 80058-80068. DOI: https://doi.org/10.1109/ ACCESS.2019. 2923743.

20. Zhang Z., Lee M., Choi S. Deep-Learning-Based Wi-Fi Indoor Positioning System Using Continuous CSI of Trajectories // Sensors. 2021. Vol. 21, no. 17. Art. 5776. DOI: https://doi.org/10.3390/s21175776.

21. Feng X., Nguyen K. A., Luo Z. WiFi Access Points Line-of-Sight Detection for Indoor Positioning Using the Signal Round Trip Time // Remote Sensing. 2022. Vol. 14, no. 23. Art. 6052. DOI: https://doi.org/10.3390/rs14236052.

22. Chang R. Y., Liu S.-J., Cheng Y.-K. Device-Free Indoor Localization Using Wi-Fi Channel State Information for Internet of Things // 2018 IEEE Global Communications Conference (GLOBECOM). 2018. P. 1-7. DOI: https://doi.org/10.1109/GLOCOM.2018.8647261.

23. Bassey J., Adesina D., Li X., Qian L., Aved A., Kroecker T. Intrusion Detection for IoT Devices based on RF Fingerprinting using Deep Learning // 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC). 2019. P. 98-104. DOI: https://doi.org/10.1109/FMEC.2019.8795319.

24. Song X., Fan X., He X., Xiang S., Chen K. CNNLoc: Deep-Learning Based Indoor Localization with WiFi Fingerprinting // 2019 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Internet of People and Smart City Innovation. 2019. P. 589-595. DOI: https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00139.

25. Jiang H., Peng C., Sun J. Deep Belief Network for Fingerprinting-Based RFID Indoor Localization // ICC 2019 - 2019 IEEE International Conference on Communications. 2019. DOI: https://doi.org/10.1109/ICC.2019.8761800.

Dmytro Prokopovych-Tkachenko
Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies
University of Customs and Finance, Dnipro, Ukraine
ORCID: 0000-0002-6590-3898
E-mail: omega2417@umsf.edu.ua

Volodymyr Zvieriev
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID: 0000-0002-0907-0705
E-mail: zvieriev_vp@knute.edu.ua

Oleksandr Halushchenko
аспірант
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID: 0009-0002-5597-8818
E-mail: ogalus5212@gmail.com

Olha Torstensson
викладач
Halmstad University, Halmstad, Sweden
ORCID: 0009-0007-2169-6851
E-mail: olga.torstensson@hh.se

Davyd Cherkaskyi
Postgraduate student, Department of Information Security and Telecommunications
National Technical University "Dnipro Polytechnic", Dnipro, Ukraine
ORCID: 0009-0003-8516-6252
E-mail: asherjoseph.c@gmail.com

EXPERIMENTAL TERMINAL FOR EVALUATION OF Wi-Fi SPATIAL IDENTIFICATION METHODS IN CRITICAL INFORMATION INFRASTRUCTURE AND ANALYSIS OF THE PRACTICAL EFFECT OF IMPLEMENTATION

The article substantiates the concept and architecture of an experimental polygon for reproducible and safe evaluation of spatial identification methods for Wi-Fi sources in critical information infrastructure (CII) environments. The requirements for the polygon are formulated: controlled sensor topology, zones with shielding and intentional

© Прокопович-Ткаченко Д.І., Звєрєв В.П., Галущенко О.М., Торстенссон О., Черкаський Д.О. Експериментальний полігон для оцінювання методів просторової ідентифікації Wi-Fi у критичній інформаційній інфраструктурі та аналіз практичного ефекту від впровадження. Сучасний захист інформації, 2(66), 138–152. https://doi.org/10.31673/2409-7292.2026.023312

multipath, dynamic interference, as well as the possibility of safe implementation of typical attacks (rogue AP, evil twin, deauthentication) outside productive contours. A system of metrics is proposed that integrates localization quality (mean and median error, 95th percentile), detection and classification indicators (Precision, Recall, F1, ROC-AUC) and SOC operational characteristics (mean time to detection, time to source localization, false positive rate, analyst working time). The data collection protocol and rules for forming training and test subsets taking into account the drift of the radio environment are described. Separately, a model for assessing the practical effect of implementation is presented, which links technical metrics with the risk of incidents, downtime of services and response costs. It is experimentally shown that hybrid localization methods provide a median error of 1.12 m versus 2.7 m for classical RSSI trilateration, and the hybrid attack detector achieves ROC-AUC of 0.962. The results are suitable for testing, implementation in the CII and preparation of materials according to the requirements of professional publications.

Keywords: Wi-Fi cybersecurity; critical information infrastructure; spatial localization; experimental polygon; rogue AP detection; SOC; performance metrics.

Надійшла до редакції (Received): 03.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.056.5:623.746-519 DOI: 10.31673/2409-7292.2026.028613

Ткач Юлія Миколаївна
доктор педагогічних наук, кандидат технічних наук, професор, завідувач кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка», Чернігів, Україна
ORCID: 0000-0002-8565-0525
E-mail: tkachym79@gmail.com

Дюба Ігор Миколайович
аспірант кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка», Чернігів, Україна
ORCID: 0009-0007-3669-6424
E-mail: idyuba@gmail.com

БАГАТОШАРОВИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ КІБЕРФІЗИЧНИХ СИСТЕМ НА ПРИКЛАДІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У статті досліджено комплексний характер уразливостей сучасних безпілотних літальних апаратів (БпЛА) як класу кіберфізичних систем (КФС). Авторами теоретично обґрунтовано та деталізовано концепцію «вакууму безпеки» – системної незахищеності архітектури дронів, що виникає внаслідок стрімкої інтеграції обчислювальних алгоритмів та фізичних процесів за ігнорування базових критеріїв захищеності. У межах теоретико-керівного підходу (Control-Theoretic Approach) проведено пошаровий декомпозиційний аналіз трьох критичних рівнів архітектури БпЛА: навігаційного, мережевого та інформаційного. Математично та емпірично доведено, що відкритість цивільних сигналів GNSS у поєднанні з апаратною архітектурою з однією антеною (Single-Receiver) робить КФС беззахисною перед прихованими атаками ін'єкції помилкових даних (False Data Injection). Досліджено механізми компрометації каналів керування через вразливості протоколу MAVLink за допомогою атак повтору (Replay Attacks). Особливу увагу приділено інформаційному рівню, де продемонстровано можливість деанонімізації стратегії використання системи через аналіз профілю зашифрованого трафіку (Side-Channel Attacks). На основі аналізу провідних світових досліджень сформульовано закон мультиплікативності ризиків КФС та запропоновано системні рекомендації щодо переходу до парадигми Security by Design.

Ключові слова: кіберфізичні системи (КФС), безпілотні літальні апарати (БпЛА), вакуум безпеки, GPS-спуфінг, джаммінг, протокол MAVLink, атака повтору (Replay Attack), ін'єкція хибних даних (FDI), аналіз сторонніх каналів, мультиплікативність ризиків, Security by Design.