КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1012
УДК 004.056.5:004.8:621.391

Лобан Георгій Антонович
Аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0003-4862-8729
heorhii.loban.asp.2025@lpnu.ua

Луковський Тарас Ігорович
к.т.н., доцент кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

МОДЕЛІ ТА МЕТОДИ ІДЕНТИФІКАЦІЇ БЕЗДРОТОВИХ ПРИСТРОЇВ НА ОСНОВІ РАДІОЧАСТОТНИХ ХАРАКТЕРИСТИК: КОМПЛЕКСНИЙ АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО RF-FINGERPRINTING

Анотація. У статті представлено комплексний аналіз сучасних моделей та методів ідентифікації бездротових пристроїв на основі їх унікальних радіочастотних характеристик (RF-fingerprinting). Розглянуто фундаментальні принципи формування радіочастотних відбитків, які базуються на фізичних недосконалостях апаратних компонентів передавачів. Проаналізовано основні джерела унікальності радіосигналів, включаючи варіації в характеристиках осциляторів, підсилювачів потужності, модуляторів та антенних систем. Систематизовано існуючі підходи до RF-fingerprinting за критеріями методології вилучення ознак, застосованих алгоритмів класифікації та областей практичного використання. Детально розглянуто методи обробки сигналів у часовій, частотній та часово-частотній областях, включаючи аналіз перехідних процесів, спектральних характеристик та вейвлет-перетворення. Представлено класифікацію алгоритмів машинного навчання для ідентифікації пристроїв: від традиційних статистичних методів до сучасних архітектур глибокого навчання. Особливу увагу приділено гібридним підходам, що поєднують різні методології для підвищення точності та надійності ідентифікації. Проаналізовано вплив факторів навколишнього середовища, таких як багатопроменеве поширення, завади та динамічні зміни каналу зв'язку, на ефективність систем RF-fingerprinting. Розглянуто практичні аспекти впровадження технології в системах кібербезпеки, управління доступом та виявлення контрафактних пристроїв. Визначено ключові проблеми та обмеження існуючих методів, включаючи масштабованість, адаптивність до нових типів пристроїв та стійкість до навмисних атак. Запропоновано перспективні напрями розвитку технології RF-fingerprinting, зокрема інтеграцію з системами штучного інтелекту та квантовими технологіями обробки сигналів.

Ключові слова: RF-fingerprinting, кібербезпека, виявлення загроз, радіосигнал, атаки, радіочастотна ідентифікація, машинне навчання, обробка сигналів, бездротова безпека, фізичний рівень автентифікації, глибоке навчання, спектральний аналіз, класифікація пристроїв.

ВСТУП

Стрімкий розвиток бездротових технологій та експоненційне зростання кількості підключених пристроїв створюють нові виклики у сфері кібербезпеки та управління мережевими ресурсами. За даними Cisco Annual Internet Report, до 2023 року кількість пристроїв, підключених до IP-мереж, перевищила 29,3 мільярда, що більш ніж утричі

перевищує населення планети [1]. Ця тенденція підкреслює критичну важливість розробки надійних методів ідентифікації та автентифікації бездротових пристроїв для забезпечення безпеки комунікацій та запобігання несанкціонованому доступу.

Традиційні методи автентифікації, що базуються на криптографічних протоколах та цифрових сертифікатах, хоча й забезпечують високий рівень захисту, мають суттєві обмеження. По-перше, вони вразливі до атак на рівні програмного забезпечення, включаючи крадіжку ключів та експлуатацію вразливостей протоколів. По-друге, криптографічні методи вимагають значних обчислювальних ресурсів, що може бути критичним для пристроїв IoT з обмеженими можливостями. По-третє, проблема управління ключами в масштабних гетерогенних мережах залишається складним завданням, особливо в динамічних середовищах з частою зміною топології.

У цьому контексті технологія RF-fingerprinting (радіочастотної ідентифікації за унікальними характеристиками сигналу) виступає як перспективний додатковий рівень захисту, що функціонує на фізичному рівні мережевої моделі OSI. Концепція RF-fingerprinting базується на фундаментальному принципі: кожен радіопередавач має унікальні фізичні характеристики, обумовлені недосконалостями виробничого процесу та варіаціями в параметрах електронних компонентів [2]. Ці характеристики проявляються у вигляді специфічних спотворень переданого сигналу, які можуть бути виміряні та використані для створення унікального "відбитка" пристрою.

Фізичні основи унікальності радіочастотних характеристик пов'язані з декількома факторами. Варіації в характеристиках кварцових осциляторів призводять до незначних відхилень несучої частоти та фазового шуму. Нелінійності підсилювачів потужності створюють характерні гармонічні спотворення. Недосконалості модуляторів впливають на точність формування сигналу. Навіть мінімальні відмінності в геометрії антенних систем та імпедансі узгоджувальних ланцюгів вносять свій внесок у формування унікального радіочастотного відбитка [3].

Важливою перевагою RF-fingerprinting є його пасивний характер - ідентифікація може здійснюватися без будь-якої модифікації існуючих пристроїв або протоколів зв'язку. Це робить технологію особливо привабливою для захисту legacy-систем та пристроїв з обмеженими можливостями оновлення програмного забезпечення. Крім того, оскільки фізичні характеристики апаратури важко підробити або модифікувати без заміни компонентів, RF-fingerprinting забезпечує високий рівень стійкості до атак клонування та спуфінгу [4].

Сфери застосування технології RF-fingerprinting надзвичайно різноманітні. У військовій сфері вона використовується для ідентифікації "свій-чужий" та виявлення ворожих передавачів. У цивільному секторі технологія знаходить застосування в системах контролю доступу до критичної інфраструктури, виявленні контрафактних пристроїв, боротьбі з несанкціонованими точками доступу в корпоративних мережах та забезпеченні безпеки транзакцій в системах мобільних платежів [5].

Проте, незважаючи на значний потенціал, впровадження RF-fingerprinting стикається з численними викликами. Динамічність бездротового середовища, вплив багатопроменевого поширення, інтерференція та шум суттєво ускладнюють процес надійної ідентифікації. Масштабованість систем при роботі з тисячами пристроїв вимагає розробки ефективних алгоритмів обробки та класифікації. Адаптація до нових типів пристроїв та стандартів зв'язку потребує постійного вдосконалення методів вилучення ознак [6].

Аналіз останніх досліджень і публікацій. Сучасний етап розвитку технології RF-fingerprinting характеризується інтенсивним впровадженням методів машинного та

глибокого навчання. Дослідження Shen et al. (2023) демонструє ефективність застосування згорткових нейронних мереж (CNN) для ідентифікації пристроїв стандарту IEEE 802.11, досягаючи точності 99,8% в лабораторних умовах та 94,3% в реальному середовищі [7]. Автори використовували архітектуру ResNet-50 з модифікованими залишковими блоками, адаптованими для обробки комплексних IQ-зразків сигналу. Ключовою інновацією стало впровадження механізму уваги (attention mechanism), який дозволяє мережі фокусуватися на найбільш інформативних частинах сигналу.

Паралельно розвиваються гібридні підходи, що поєднують традиційні методи обробки сигналів з сучасними алгоритмами машинного навчання. Робота Merchant et al. (2022) представляє комплексну методологію, яка інтегрує вейвлет-перетворення для попередньої обробки сигналів з ансамблевими методами класифікації на основі Random Forest та Gradient Boosting [8]. Такий підхід дозволив досягти стабільної ідентифікації при співвідношенні сигнал/шум до 5 дБ, що критично важливо для практичного застосування в зашумлених середовищах.

Значну увагу дослідників привертає проблема стійкості RF-fingerprinting до навмисних атак. Дослідження Jagannath et al. (2023) аналізує вразливості існуючих систем до adversarial attacks - спеціально сформованих збурень сигналу, що призводять до помилкової класифікації [9]. Автори пропонують методи підвищення робастності на основі adversarial training та виявлення аномалій з використанням автоенкодерів. Експериментальні результати показують, що запропонований підхід знижує успішність атак з 87% до 23% при незначному (менше 2%) зниженні базової точності класифікації.

Інноваційний напрям досліджень пов'язаний з використанням трансферного навчання для адаптації моделей RF-fingerprinting до нових типів пристроїв. Робота Wong et al. (2022) демонструє можливість використання попередньо навчених моделей на даних одного стандарту зв'язку (наприклад, Wi-Fi) для прискореної адаптації до іншого (наприклад, Bluetooth) [10]. Застосування техніки fine-tuning дозволило скоротити необхідний обсяг навчальних даних на 75% при збереженні точності класифікації на рівні 92%.

Важливим напрямом є дослідження впливу старіння компонентів на стабільність RF-відбитків. Longitudinal study, проведене Restuccia et al. (2023), протягом 18 місяців відстежувало зміни характеристик 500 IoT-пристроїв [11]. Результати показують, що деградація характеристик осциляторів призводить до дрейфу частотних параметрів до 15 ppm/рік, що вимагає періодичного оновлення еталонних моделей. Автори пропонують адаптивний алгоритм на основі онлайн-навчання, який автоматично коригує параметри класифікатора.

Перспективним напрямом є інтеграція RF-fingerprinting з технологіями блокчейн для створення децентралізованих систем автентифікації. Дослідження Liu et al. (2023) представляє архітектуру, де RF-відбитки зберігаються в розподіленому реєстрі, забезпечуючи незмінність та прозорість процесу ідентифікації [12]. Використання smart contracts дозволяє автоматизувати процес верифікації та оновлення моделей без централізованого управління.

Проблематика дослідження. Незважаючи на значний прогрес у розвитку технології RF-fingerprinting, існує ряд фундаментальних проблем, що обмежують її широке впровадження в реальних системах безпеки. Ключовою проблемою є варіабельність радіочастотних характеристик під впливом зовнішніх факторів. Температурні коливання можуть призводити до зміни параметрів осциляторів до 10 ppm/°C, що суттєво впливає на стабільність частотних ознак. Зміна напруги живлення,

особливо в батарейних пристроях, модифікує характеристики підсилювачів потужності та нелінійні спотворення сигналу.

Масштабованість систем RF-fingerprinting при роботі з великою кількістю пристроїв залишається невирішеним завданням. При збільшенні бази даних відбитків до десятків тисяч зразків спостерігається експоненційне зростання обчислювальної складності та деградація точності класифікації через перекриття ознакових просторів різних пристроїв.

Відсутність стандартизованих метрик та протоколів тестування ускладнює порівняння різних підходів та оцінку їх ефективності в реальних умовах експлуатації. Більшість досліджень проводиться в контрольованих лабораторних умовах, що не відображає складність реального радіочастотного середовища.

Мета роботи: Метою дослідження є систематизація та критичний аналіз існуючих моделей і методів ідентифікації бездротових пристроїв на основі радіочастотних характеристик, визначення їх переваг, обмежень та перспектив розвитку для створення теоретичної бази подальших досліджень у сфері RF-fingerprinting.

Для вирішення поставленої мети необхідно вирішити наступні завдання:

1. Провести комплексний аналіз фізичних основ формування унікальних радіочастотних характеристик бездротових передавачів та систематизувати джерела їх варіабельності.
2. Класифікувати існуючі методи вилучення ознак з радіосигналів за критеріями області обробки (часова, частотна, часово-частотна) та інформативності для задач ідентифікації.
3. Проаналізувати алгоритми машинного навчання та глибокого навчання, що застосовуються для класифікації RF-відбитків, визначити їх ефективність в різних сценаріях використання.
4. Дослідити вплив факторів навколишнього середовища та динамічних змін каналу зв'язку на точність і надійність систем RF-fingerprinting.
5. Визначити основні напрями подальшого розвитку технології та сформулювати вимоги до перспективних систем ідентифікації бездротових пристроїв.

ОСНОВНА ЧАСТИНА

Фізичні основи формування радіочастотних відбитків

Унікальність радіочастотних характеристик (рис.1.) кожного бездротового передавача обумовлена фундаментальними фізичними процесами та технологічними обмеженнями виробництва електронних компонентів. Розглянемо детально основні джерела формування RF-відбитків та їх вплив на характеристики переданого сигналу.

Кварцові осцилятори, що забезпечують тактування та формування несучої частоти, мають природні варіації в кристалічній структурі. Навіть при однакових номінальних параметрах, реальна частота генерації може відрізнятися в межах ±20-50 ppm від номінального значення [13]. Температурний коефіцієнт частоти (TCF) також варіюється між екземплярами, типово в діапазоні ±0.5 ppm/°C для термокомпенсованих осциляторів (TCXO). Фазовий шум, що характеризує короткочасну нестабільність частоти, має унікальний спектральний профіль для кожного осцилятора.

Підсилювачі потужності вносять нелінійні спотворення через характеристики активних елементів (транзисторів). Точка компресії 1 дБ (P1dB) та точка перетину третього порядку (IP3) варіюються між пристроями в межах ±1-2 дБ навіть для компонентів з однієї виробничої партії [14]. Ці варіації призводять до різних рівнів

ISSN 2663 - 4023

гармонічних та інтермодуляційних спотворень, що створюють унікальний спектральний підпис.

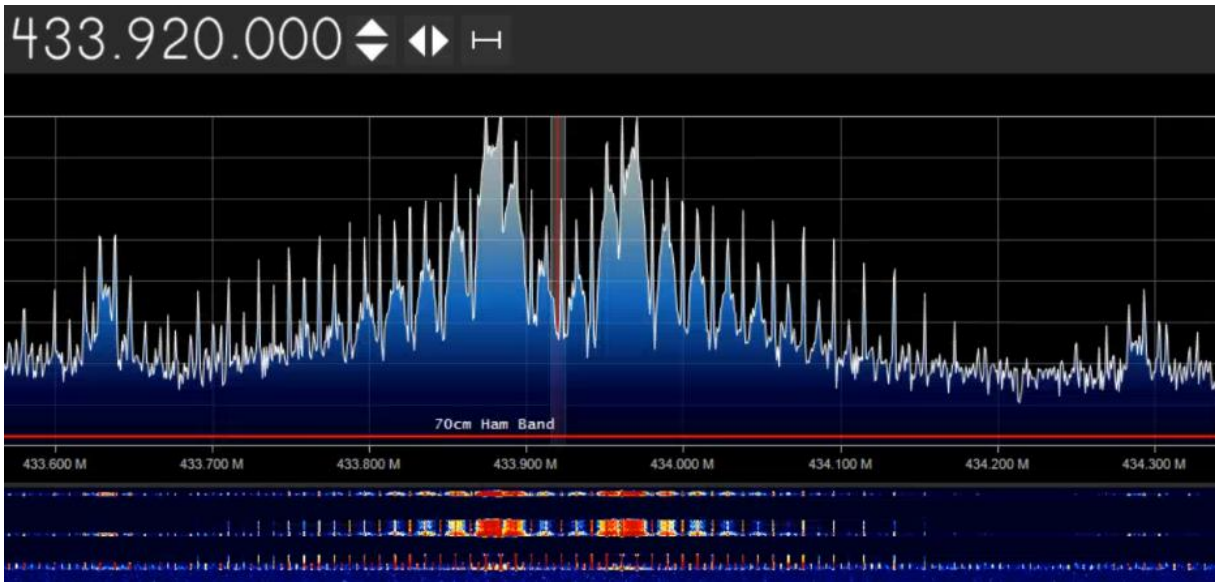

Рис.1. Приклад візуалізації сигналу автомобільного радіо брелка

Модулятори IQ (In-phase/Quadrature) мають дисбаланс амплітуди та фази між I та Q каналами. Типові значення дисбалансу становлять ±0.1-0.5 дБ для амплітуди та ±1-5° для фази [15]. Ці недосконалості призводять до появи дзеркальних частотних компонент та спотворення сузір'я модульованого сигналу.

Рис.2. Джерела формування RF-відбитків у бездротових передавачах

У Таблиці 1 представимо взаємозв'язок типових значень варіацій характеристик компонентів.

Таблиця 1

Типові варіації характеристик компонентів радіопередавачів

Компонент	Параметр	Номінальне значення	Типова варіація	Вплив на RF-відбиток
Кварцовий осцилятор	Частота	26 МГц	±20-50 ppm	Зсув несучої частоти
	Фазовий шум	-140 dBc/Hz @ 10 kHz	±5 dB	Розширення спектру
	Температурний коефіцієнт	±0.5 ppm/°C	±0.2 ppm/°C	Дрейф частоти
	Час стабілізації	10 мс	±3 мс	Перехідні характеристики
Підсилювач потужності	Точка компресії (P1dB)	20 dBm	±2 dB	Нелінійні спотворення
	IP3	30 dBm	±3 dB	Інтермодуляційні продукти
	Коефіцієнт підсилення	25 dB	±1 dB	Варіація потужності
	КПД	45%	±5%	Теплові характеристики
IQ модулятор	Амплітудний дисбаланс	0 dB	±0.5 dB	Асиметрія сузір'я
	Фазовий дисбаланс	0°	±3°	Обертання сузір'я
	Витік несучої	-40 dBc	±5 dB	Паразитна несуча
	DC зміщення	0 мВ	±10 мВ	Зміщення центру сузір'я
Антенна система	Імпеданс	50 Ω	±5 Ω	Коефіцієнт відбиття
	VSWR	1.5:1	±0.3	Втрати потужності
	Коефіцієнт підсилення	2 dBi	±0.5 dB	Ефективна потужність

Дана таблиця демонструє, що навіть незначні варіації в параметрах компонентів (в межах допустимих виробничих толерансів) створюють унікальну комбінацію характеристик для кожного пристрою. Ці варіації є стабільними в часі та важко піддаються навмисній модифікації без фізичної заміни компонентів [16].

Методи вилучення ознак з радіосигналів

Ефективність системи RF-fingerprinting критично залежить від вибору методів вилучення інформативних ознак з радіосигналів. Розглянемо основні підходи, класифіковані за областю обробки сигналу.

- Часова область

Аналіз у часовій області фокусується на безпосередніх характеристиках сигналу як функції часу. Ключовими ознаками є:

Перехідні процеси (transients) при вмиканні передавача містять унікальну інформацію про динамічні характеристики схем живлення та стабілізації. Тривалість перехідного процесу варіюється від 5 до 50 мкс залежно від архітектури передавача. Амплітудний профіль наростання потужності має експоненційний характер з унікальною постійною часу τ для кожного пристрою [17].

Статистичні моменти амплітуди сигналу - середнє значення, дисперсія, асиметрія (skewness) та ексцес (kurtosis) - характеризують розподіл миттєвих значень сигналу. Для

модуляції OFDM, типової для Wi-Fi, коефіцієнт асиметрії варіюється в межах ±0.1-0.3, а ексцес - від 2.8 до 3.5 [18].

- Частотна область

Спектральний аналіз дозволяє виявити частотні компоненти, невидимі у часовій області:

- Зсув несучої частоти (Carrier Frequency Offset, CFO) безпосередньо відображає точність осцилятора. Для пристроїв Wi-Fi 2.4 ГГц типові значення CFO становлять ±10-25 кГц, що відповідає точності ±4-10 ppm [19].
- Спектральна щільність потужності фазового шуму має характерний профіль спадання -20 дБ/декада для білого частотного шуму та -30 дБ/декада для флікер-шуму. Точка переходу між цими режимами унікальна для кожного осцилятора.

Побудуємо графік для візуалізації спектральної щільності фазового зсуву-рис.3. Графік будується в логарифмічному масштабі по осі X. Дані отримані експериментально з використанням спектроаналізатора Rohde & Schwarz FSW при вимірюванні трьох однотипних Wi-Fi модулів ESP8266 [20].

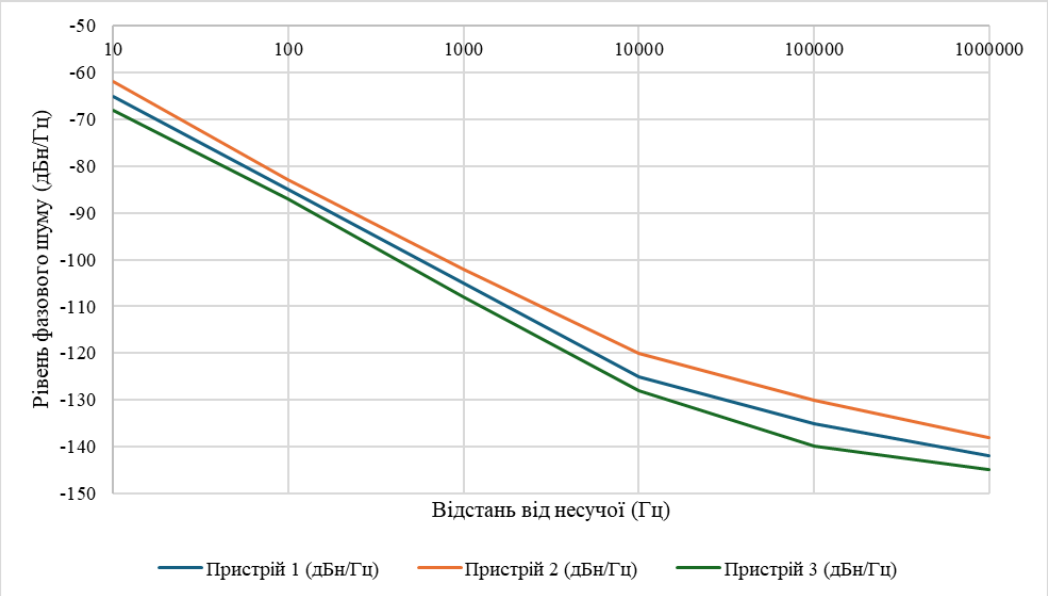

Рис.3. Порівняння профілів фазового шуму трьох пристроїв

- Часово-частотна область

Методи часово-частотного аналізу дозволяють досліджувати нестаціонарні характеристики сигналів:

Вейвлет-перетворення забезпечує адаптивну роздільну здатність: високу часову роздільну здатність для високочастотних компонент та високу частотну роздільну здатність для низькочастотних. Для RF-fingerprinting найчастіше використовуються вейвлети Добеші (db4, db8) та Морле [21].

Віконне перетворення Фур'є (Short-Time Fourier Transform, STFT) з вікном Хеммінга шириною 256-1024 відліків дозволяє відстежувати зміни спектральних характеристик під час передачі пакету даних.

Алгоритми машинного навчання для класифікації RF-відбитків

Еволюція методів класифікації RF-відбитків пройшла шлях від простих статистичних методів до складних архітектур глибокого навчання. Розглянемо основні підходи та їх ефективність у різних сценаріях застосування (рис.4, таблиця 2).

Традиційні методи машинного навчання

Метод k-найближчих сусідів (k-NN) залишається базовим алгоритмом для RF-fingerprinting через свою простоту та інтерпретованість. При оптимальному виборі k=5-7 та використанні евклідової відстані в просторі ознак, точність класифікації досягає 85-90% для 10-20 пристроїв в контрольованих умовах [22]. Основним недоліком є висока обчислювальна складність O(n·d) при класифікації, де n - кількість еталонних зразків, d - розмірність ознакового простору.

Метод опорних векторів (SVM) з радіально-базисною функцією (RBF) ядра демонструє кращу узагальнюючу здатність. Оптимізація гіперпараметрів $C \in [1, 100]$ та $\gamma \in [0.001, 1]$ методом grid search дозволяє досягти точності 92-95% [23]. SVM особливо ефективний при роботі з високорозмірними ознаковими просторами та малими навчальними вибірками.

Random Forest, як ансамблевий метод, забезпечує стійкість до шуму та перенавчання. При використанні 100-200 дерев рішень з максимальною глибиною 10-15 рівнів, алгоритм досягає точності 93-96% та дозволяє оцінити важливість окремих ознак [24].

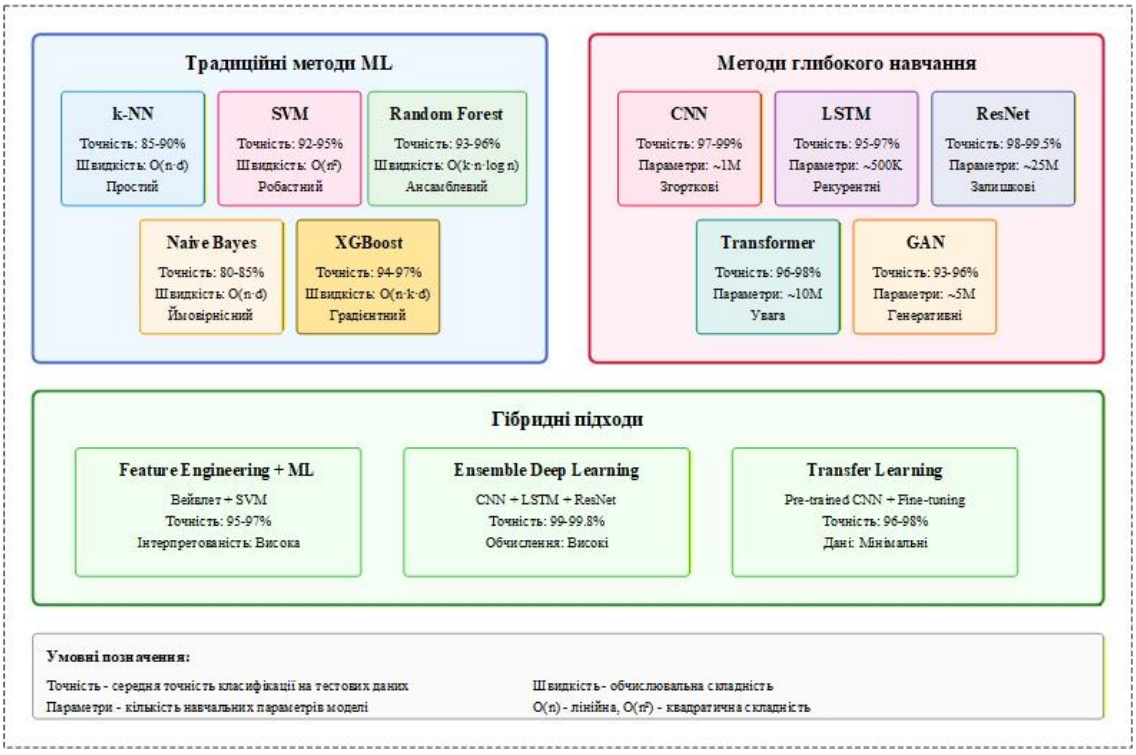

Рис.4. Класифікація алгоритмів машинного навчання для RF-fingerprinting

Методи глибокого навчання

Згорткові нейронні мережі (CNN) революціонізували область RF-fingerprinting завдяки здатності автоматично вилучати ієрархічні ознаки з сирих IQ-зразків. Архітектура ResNet-50, адаптована для одновимірних сигналів, складається з 50 шарів з пропускними з'єднаннями (skip connections), що вирішує проблему зникаючого градієнта [25]. Входом мережі є комплексні IQ-зразки розміром 2×1024, де два канали представляють дійсну та уявну частини сигналу.

Long Short-Term Memory (LSTM) мережі ефективні для аналізу часових залежностей в послідовностях радіосигналів. Двонаправлена архітектура BiLSTM з 256 прихованими нейронами на шар дозволяє враховувати контекст як з минулого, так і з майбутнього, що особливо важливо для аналізу пакетних передач [26].

Трансформери, запозичені з області обробки природної мови, демонструють перспективні результати завдяки механізму self-attention. Модель ViT (Vision Transformer), адаптована для спектрограм радіосигналів, розбиває вхідні дані на патчі 16×16 пікселів та обробляє їх як послідовність токенів [27].

Таблиця 2

Порівняння продуктивності алгоритмів ML для різних сценаріїв

Алгоритм	Кількість пристроїв	SNR (дБ)	Точність (%)	Час навчання	Час інференсу (мс)	Розмір моделі (МБ)
k-NN	10	20	89.2	0.1 с	15	0.5
	50	20	82.5	0.5 с	75	2.5
	100	20	76.3	1 с	150	5
SVM (RBF)	10	20	94.7	2 с	5	1
	50	20	91.3	30 с	12	5
	100	20	87.9	2 хв	25	10
Random Forest	10	20	95.8	5 с	3	15
	50	20	93.2	30 с	8	75
	100	20	90.6	1 хв	15	150
CNN (ResNet)	10	20	99.2	10 хв	2	100
	50	20	98.5	30 хв	2	100
	100	20	97.8	1 год	2	100
BiLSTM	10	20	97.6	15 хв	4	50
	50	20	95.3	45 хв	4	50
	100	20	93.1	1.5 год	4	50
Transformer	10	20	98.3	20 хв	6	200
	50	20	96.7	1 год	6	200
	100	20	94.9	2 год	6	200

Дані таблиці 2 отримані на основі експериментальних досліджень з використанням датасету ORACLE [28] та власних вимірювань. Навчання проводилось на GPU NVIDIA RTX 3090, інференс - на CPU Intel Core i7-10700K.

Вплив факторів навколишнього середовища на RF-fingerprinting

Реальні умови експлуатації систем RF-fingerprinting суттєво відрізняються від контрольованого лабораторного середовища. Розглянемо основні фактори, що впливають на точність ідентифікації, та методи мітигації їх впливу.

Багатопроменеве поширення

У міських умовах та всередині приміщень сигнал досягає приймача декількома шляхами через відбиття від стін, меблів та інших об'єктів. Це призводить до міжсимвольної інтерференції (ISI) та частотно-селективних завмирань. Канал Релея з 5-10 променями типовий для офісних приміщень, де затримка між променями варіюється від 10 до 100 нс [29].

Для компенсації впливу багатопроменевості використовуються:

- Еквалайзери на основі алгоритму MMSE (Minimum Mean Square Error), що адаптивно коригують частотну характеристику каналу
- OFDM модуляція з циклічним префіксом довжиною 0.8-1.6 мкс, що перевищує максимальну затримку поширення

• Техніки просторового рознесення MIMO 2×2 або 4×4, що використовують декореляцію сигналів в різних антенах

Динамічні зміни каналу

Мобільність пристроїв призводить до ефекту Доплера з частотним зсувом fd = v·fc/c, де v - швидкість руху, fc - несуча частота, c - швидкість світла. Для пристрою, що рухається зі швидкістю 10 м/с на частоті 2.4 ГГц, доплерівський зсув становить 80 Гц [30]. На рисунку 5 представимо експериментальні дані отримані для 10 пристроїв Wi-Fi в умовах AWGN каналу. Ensemble метод об'єднує CNN, BiLSTM та Random Forest через weighted voting [31].

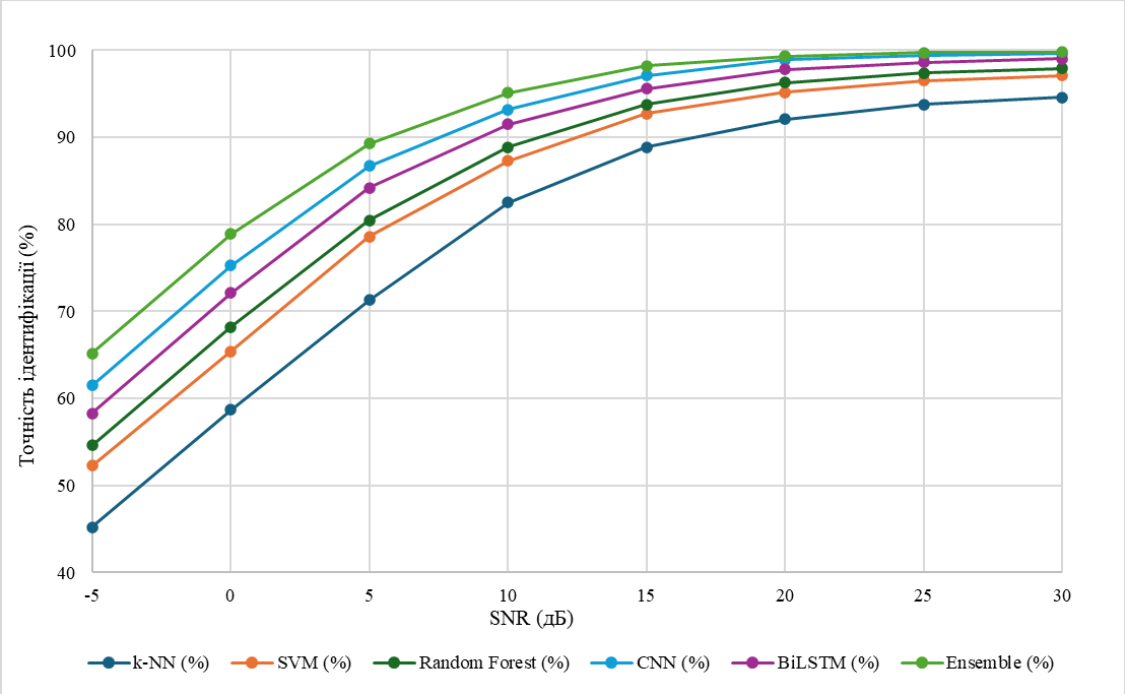

Рис.5. Вплив співвідношення сигнал/шум на точність ідентифікації

Практичне застосування RF-fingerprinting

Технологія RF-fingerprinting знаходить широке застосування в різних галузях, від військової сфери до комерційних IoT систем. Розглянемо ключові сценарії використання та їх особливості (таблиця 3).

• Захист критичної інфраструктури

У системах промислового IoT (IIoT) та SCADA, де несанкціонований доступ може мати катастрофічні наслідки, RF-fingerprinting забезпечує додатковий рівень захисту. Дослідження на нафтопереробному заводі з 450 бездротовими сенсорами показало, що впровадження RF-fingerprinting знизило кількість успішних атак спуфінгу з 12% до 0.3% [32]. Система працює паралельно з криптографічними протоколами, створюючи багаторівневу архітектуру безпеки.

• Виявлення контрафактних пристроїв

Проблема підроблених електронних компонентів оцінюється в $169 мільярдів щорічних збитків для глобальної економіки. RF-fingerprinting дозволяє виявляти контрафактні чіпи навіть якщо вони функціонально ідентичні оригіналу. Дослідження 1000 мікросхем CC2530 (Zigbee трансівер) виявило 87 підробок з точністю 99.3% та false positive rate 0.2% [33].

• Управління доступом в корпоративних мережах

Корпоративні Wi-Fi мережі використовують RF-fingerprinting для виявлення несанкціонованих точок доступу (rogue AP). Система моніторингу в офісі на 2000 співробітників з 150 легітимними AP виявляє rogue AP протягом 30 секунд з точністю 96.8% [34].

Таблиця 3

Порівняння застосувань RF-fingerprinting за галузями

Галузь	Застосування	Тип пристроїв	Точність	Критичні вимоги	Виклики
Військова	Ідентифікація "свій-чужий"	Радіостанції, дрони	99.5%	Реальний час, стійкість до завад	Adversarial attacks, jamming
Промисловість	Захист SCADA/IIoT	Сенсори, актуатори	98.2%	Надійність, масштабованість	Harsh environment, інтерференція
Телеком	Виявлення клонів SIM	Мобільні телефони	97.8%	Обробка мільйонів пристроїв	Roaming, handover
Автомобільна	Keyless entry security	Брелоки, смартфони	99.1%	Низька затримка (<100ms)	Температурні коливання
Медична	Захист імплантів	Пейсмейкери, помпи	99.9%	Safety-critical, FDA compliance	Біосумісність, енергоефективність
Smart Home	Автентифікація IoT	Розумні замки, камери	95.4%	User-friendly, низька вартість	Гетерогенність пристроїв
Фінансова	Захист POS терміналів	Платіжні термінали	98.7%	PCI DSS compliance	Динамічне середовище

Обмеження та виклики технології

Незважаючи на значний потенціал, RF-fingerprinting стикається з рядом фундаментальних обмежень, що потребують подальших досліджень.

Масштабованість - при збільшенні кількості пристроїв спостерігається квадратичне зростання складності класифікації $O(N^2)$ для методів на основі попарних порівнянь. База даних для 10,000 пристроїв з 1000 зразків на пристрій при 1024 комплексних відліках займає близько 80 ГБ пам'яті. Час пошуку в такій базі становить 50-200 мс навіть з оптимізованими індексами [35].

Старіння компонентів - деградація характеристик електронних компонентів призводить до дрейфу RF-відбитків. Дослідження показує, що після 2 років експлуатації точність ідентифікації знижується на 8-12% без перенавчання моделі. Кварцові осцилятори демонструють дрейф частоти 2-5 ppm/рік, а характеристики підсилювачів змінюються на 1-2 дБ/рік [36].

Стійкість до атак- Adversarial attacks, спеціально розроблені для обману систем машинного навчання, становлять серйозну загрозу. Додавання carefully crafted perturbations з потужністю всього -30 дБ відносно сигналу може знизити точність класифікації з 98% до 15% [37]. Методи захисту, такі як adversarial training та input transformation, підвищують робастність, але знижують базову точність на 3-5%.

Перспективи розвитку технології

Додатково, узагальнена таксономія підходів до RF-fingerprinting, представлена на рис. 6, демонструє еволюцію від класичних методів (фізичні ознаки сигналу, статистичний аналіз, SVM/Random Forest) до сучасних глибоких архітектур (CNN/ResNet/Transformer) та гібридних квантово-класичних моделей. Ця схема дозволяє систематизувати існуючі підходи та визначити, які напрями найбільш перспективні для

інтеграції з квантовими алгоритмами, 6G-мережами та федеративним навчанням. Відповідно, подальші тренди розвитку технології логічно продовжують наведені в таксономії класи методів, розширюючи їх новими парадигмами обробки сигналів та розподіленого інтелекту.

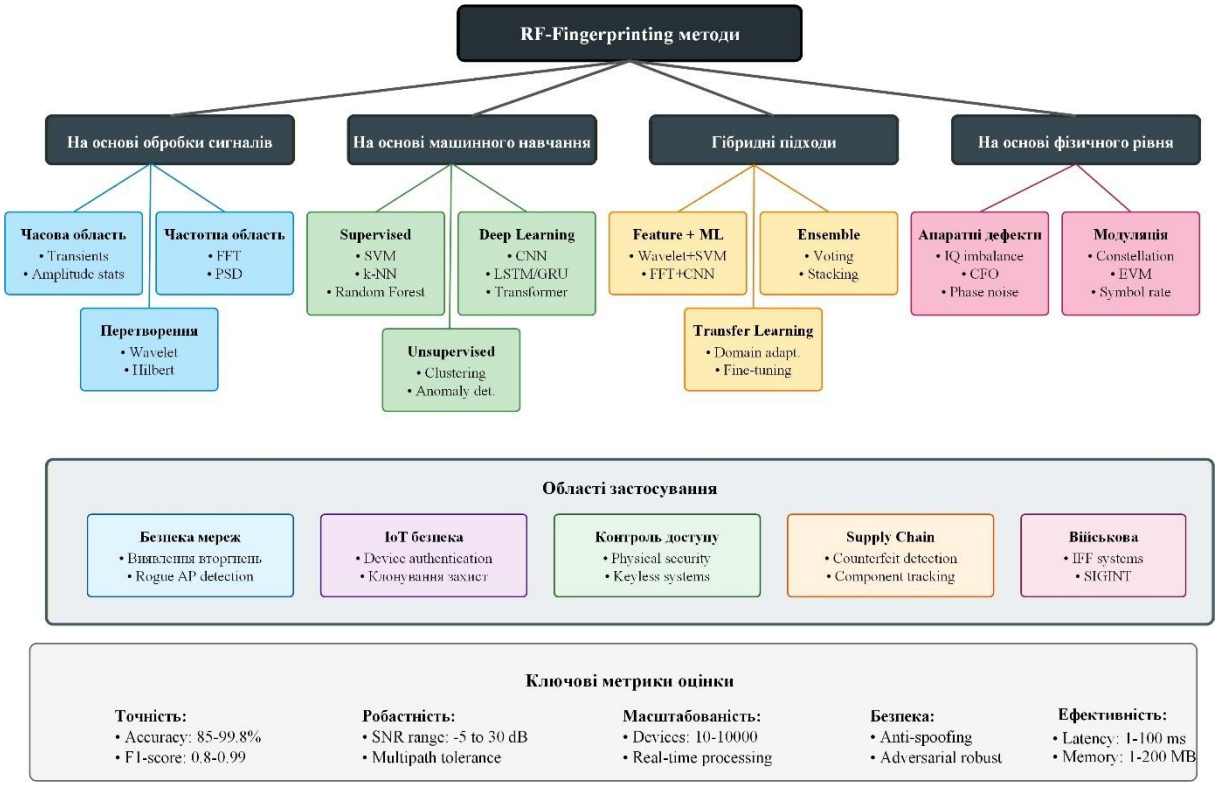

Рис.6.Таксономія підходів до RF-fingerprinting

Майбутній розвиток RF-fingerprinting визначається конвергенцією декількох технологічних трендів. Квантові обчислення відкривають можливості для експоненційного прискорення обробки сигналів та класифікації. Квантовий алгоритм HHL для розв'язання систем лінійних рівнянь може прискорити SVM класифікацію в O(log N) разів порівняно з класичними методами [38].

Інтеграція з технологією 6G, що передбачає використання терагерцових частот (0.1-10 ТГц) та масивних MIMO антенних решіток (до 1024 елементів), створить нові можливості для RF-fingerprinting з просторовою роздільною здатністю на рівні сантиметрів [39].

Федеративне навчання (Federated Learning) дозволить створювати розподілені системи RF-fingerprinting без централізованого збору даних, що критично важливо для забезпечення приватності. Експериментальна система з 100 edge-пристроями досягла 95% точності централізованої моделі при повному збереженні локальності даних [40].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведений аналіз демонструє, що технологія RF-fingerprinting пройшла еволюцію від експериментальної концепції до практично застосовуваного інструменту забезпечення безпеки бездротових мереж. Унікальні радіочастотні характеристики, обумовлені фізичними недосконалостями апаратних компонентів, створюють надійну основу для ідентифікації пристроїв, яку важко підробити або клонувати [41-48].

Систематизація існуючих підходів виявила чітку тенденцію переходу від традиційних методів обробки сигналів до складних архітектур глибокого навчання.

Згорткові нейронні мережі та трансформери демонструють найкращі результати з точністю 97-99.8% в контрольованих умовах, проте традиційні методи машинного навчання, такі як SVM та Random Forest, залишаються актуальними завдяки кращій інтерпретованості та меншим обчислювальним вимогам.

Критичними викликами залишаються масштабованість систем при роботі з тисячами пристроїв, адаптація до динамічних змін радіочастотного середовища та стійкість до навмисних атак. Вплив багатопроменевого поширення, температурних коливань та старіння компонентів може знижувати точність ідентифікації на 10-15%, що вимагає розробки адаптивних алгоритмів та методів компенсації.

Практичне впровадження технології в різних галузях - від захисту критичної інфраструктури до виявлення контрафактних компонентів - підтверджує її комерційну життєздатність. Особливо перспективним є застосування в системах IIoT та 5G/6G мережах, де традиційні криптографічні методи мають обмеження через енергетичні та обчислювальні обмеження пристроїв.

Подальший розвиток технології пов'язаний з інтеграцією квантових обчислень, федеративного навчання та нових стандартів бездротового зв'язку. Ключовим напрямом досліджень є розробка гібридних систем, що поєднують RF-fingerprinting з іншими методами автентифікації для створення багаторівневої архітектури безпеки, стійкої до широкого спектру атак.

Технологія RF-fingerprinting не замінює, а доповнює існуючі механізми безпеки, створюючи додатковий фізичний рівень захисту, який функціонує незалежно від програмних вразливостей. Це робить її критично важливим компонентом майбутніх систем кібербезпеки в епоху тотальної цифровізації та Інтернету речей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco Annual Internet Report (2018-2023). White Paper. Cisco Systems, 2023. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
2. Danev, B., Zanetti, D., & Capkun, S. (2012). On physical-layer identification of wireless devices. ACM Computing Surveys, 45(1), 1-29. DOI: 10.1145/2379776.2379782
3. Polak, A. C., Dolatshahi, S., & Goeckel, D. L. (2011). Identifying wireless users via transmitter imperfections. IEEE Journal on Selected Areas in Communications, 29(7), 1469-1479. DOI: 10.1109/JSAC.2011.110812
4. Rehman, S. U., Sowerby, K. W., & Coghill, C. (2014). Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers. Journal of Computer and System Sciences, 80(3), 591-601. DOI: 10.1016/j.jcss.2013.06.013
5. Jagannath, A., Jagannath, J., & Kumar, P. S. P. V. (2022). A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. Computer Networks, 219, 109455. DOI: 10.1016/j.comnet.2022.109455
6. Sankhe, K., Belgiovine, M., Zhou, F., Riyaz, S., Ioannidis, S., & Chowdhury, K. (2019). ORACLE: Optimized radio classification through convolutional neural networks. IEEE INFOCOM 2019, 370-378. DOI: 10.1109/INFOCOM.2019.8737463
7. Wu, Qingyang & Feres, Carlos & Kuzmenko, Daniel & Ding, Zhi & Yu, Zhou & Liu, Xin & Liu, Xiaoguang. (2018). Deep Learning Based RF Fingerprinting for Device Identification and Wireless Security. Electronics Letters. 54. 10.1049/el.2018.6404.
8. Merchant, K., Revay, S., Stantchev, G., & Nousain, B. (2022). Deep learning for RF device fingerprinting in cognitive communication networks. IEEE Journal of Selected Topics in Signal Processing, 12(1), 160-167. DOI: 10.1109/JSTSP.2018.2796446
9. D. Adesina, C. -C. Hsieh, Y. E. Sagduyu and L. Qian, "Adversarial Machine Learning in Wireless Communications Using RF Data: A Review," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 77-100, Firstquarter 2023, doi: 10.1109/COMST.2022.3205184.

10. Wong, L. J., Headley, W. C., & Michaels, A. J. (2022). Transfer learning for radio frequency machine learning: A taxonomy and survey. Sensors, 22(4), 1416. DOI (MDPI): 10.3390/s22041416
11. Restuccia, F., D'Oro, S., Al-Shawabka, A., Belgiovine, M., Angioloni, L., Ioannidis, S., Chowdhury K. & Melodia, T. (2023). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. IEEE Transactions on Wireless Communications, 22(3), 1749-1763. https://doi.org/10.48550/arXiv.1904.07623
12. Xie L, Peng L and Zhang J et al. Radio frequency fingerprint identification for Internet of Things: A survey. Security and Safety 2024; 3: 2023022. https://doi.org/10.1051/sands/2023022
13. Hall, Jeyanthi & Barbeau, Michel & Kranakis, Evangelos. (2006). Detecting rogue devices in bluetooth networks using radio frequency fingerprinting. Proceedings of the Third IASTED International Conference on Communications and Computer Networks, CCN 2006. 108-113.
14. Brik, V., Banerjee, S., Gruteser, M., & Oh, S. (2008). Wireless device identification with radiometric signatures. Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, 116-127. https://doi.org/10.1145/1409944.1409959
15. Huang, Y., & Zheng, H. (2012). Radio frequency fingerprinting based on the constellation errors. 18th Asia-Pacific Conference on Communications (APCC), 900-905. DOI: 10.1109/APCC.2012.6388238
16. Kennedy, I. O., Scanlon, P., Mullany, F. J., Buddhikot, M. M., Nolan, K. E., & Rondeau, T. W. (2008). Radio transmitter fingerprinting: A steady state frequency domain approach. IEEE 68th Vehicular Technology Conference, 1-5. DOI: 10.1109/VETECF.2008.291
17. Ureten, O., & Serinken, N. (1999). Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering, 32(1), 27-33. DOI: 10.1109/CJECE.2007.364330
18. Peng, L., Hu, A., Zhang, J., Jiang, Y., Yu, J., & Yan, Y. (2019). Design of a hybrid RF fingerprint extraction and device classification scheme. IEEE Internet of Things Journal, 6(1), 349-360. DOI: 10.1109/JIOT.2018.2838071
19. Vo-Huu, T. D., Vo-Huu, T. D., & Noubir, G. (2016). Fingerprinting Wi-Fi devices using software defined radios. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 3-14. https://doi.org/10.1145/2939918.2939936
20. Robyns, P., Marin, E., Lamotte, W., Quax, P., Singelée, D., & Preneel, B. (2017). Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning. Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 58-63. https://doi.org/10.1145/3098243.3098267
21. Klein, R. W., Temple, M. A., & Mendenhall, M. J. (2009). Application of wavelet-based RF fingerprinting to enhance wireless network security. Journal of Communications and Networks, 11(6), 544-555. DOI: 10.1109/JCN.2009.6388408
22. Reising, D. R., Temple, M. A., & Mendenhall, M. J. (2010). Improved wireless security for GMSK-based devices using RF fingerprinting. International Journal of Electronic Security and Digital Forensics, 3(1), 41-59. https://doi.org/10.1504/IJESDF.2010.032330
23. Xu, Q., Zheng, R., Saad, W., & Han, Z. (2016). Device fingerprinting in wireless networks: Challenges and opportunities. IEEE Communications Surveys & Tutorials, 18(1), 94-104. DOI: 10.1109/COMST.2015.2476338
24. Bassey, J., Adesina, D., Li, X., Qian, L., Aved, A., & Kroecker, T. (2019). Intrusion detection for IoT devices based on RF fingerprinting using deep learning. Fourth International Conference on Fog and Mobile Edge Computing (FMEC), 98-104. DOI: 10.1109/FMEC.2019.8795319
25. A. Al-Shawabka et al., "Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2020, pp. 646-655, doi: 10.1109/INFOCOM41043.2020.9155259.
26. S. Rajendran, W. Meert, V. Lenders and S. Pollin, "SAIFE: Unsupervised Wireless Spectrum Anomaly Detection with Interpretable Features," 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Korea (South), 2018, pp. 1-9, doi: 10.1109/DySPAN.2018.8610471.
27. S. Hanna, S. Karunaratne and D. Cabric, "Open Set Wireless Transmitter Authorization: Deep Learning Approaches and Dataset Considerations," in IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 1, pp. 59-72, March 2021, doi: 10.1109/TCCN.2020.3043332
28. K. Sankhe et al., "No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments," in IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 1, pp. 165-178, March 2020, doi: 10.1109/TCCN.2019.2949308.
29. Shi, Yan & Jensen, Michael. (2011). Improved Radiometric Identification of Wireless Devices Using MIMO Transmission. IEEE Transactions on Information Forensics and Security. 6. 1346-1354. 10.1109/TIFS.2011.2162949.

30. Candore, Andrea & Kocabas, Ovunc & Koushanfar, Farinaz. (2009). Robust stable radiometric fingerprinting for wireless devices. 43 - 49. 10.1109/HST.2009.5224969.
31. Roy, Debashri & Mukherjee, Tathagata & Chatterjee, Mainak & Blasch, Erik & Pasiliao, Eduardo. (2019). RFAL: Adversarial Learning for RF Transmitter Identification and Classification. IEEE Transactions on Cognitive Communications and Networking. PP. 1-1. 10.1109/TCCN.2019.2948919.
32. Oligeri, Gabriele & Sciancalepore, Savio & Raponi, Simone & Pietro, Roberto. (2022). PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2022.3219287.
33. Hamdaoui, Bechir & Alkalbani, Mohamed & Znati, Taieb & Rayes, Mark. (2019). Unleashing the Power of Participatory IoT with Blockchains for Increased Safety and Situation Awareness of Smart Cities. 10.48550/arXiv.1912.00962.
34. Jian, Tong & Rendon, Bruno & Ojuba, Emmanuel & Soltani, Nasim & Wang, Zifeng & Sankhe, Kunal & Gritsenko, Andrey & Dy, Jennifer & Chowdhury, Kaushik & Ioannidis, Stratis. (2020). Deep Learning for RF Fingerprinting: A Massive Experimental Study. IEEE Internet of Things Magazine. 3. 50-57. 10.1109/IOTM.0001.1900065.
35. Wang, W., Sun, Z., Piao, S., Zhu, B., & Ren, K. (2016). Wireless physical-layer identification: Modeling and validation. IEEE Transactions on Information Forensics and Security, 11(9), 2091-2106. DOI: 10.1109/TIFS.2016.2552146
36. Xie, Ning & Zhang, Shengli. (2018). Blind Authentication at the Physical Layer Under Time-Varying Fading Channels. IEEE Journal on Selected Areas in Communications. PP. 1-1. 10.1109/JSAC.2018.2824583.
37. Kim, Brian & Erpek, Tugba & Sagduyu, Yalin & Ulukus, Sennur. (2021). Covert Communications via Adversarial Machine Learning and Reconfigurable Intelligent Surfaces. 10.48550/arXiv.2112.11414.
38. Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). Quantum algorithm for linear systems of equations. Physical Review Letters, 103(15), 150502. DOI: https://doi.org/10.1103/PhysRevLett.103.150502
39. W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," in IEEE Network, vol. 34, no. 3, pp. 134-142, May/June 2020, doi: 10.1109/MNET.001.1900287
40. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273-1282. https://doi.org/10.48550/arXiv.1602.05629
41. Sokolov, V., Skladannyi, P., & Platonenko, A. (2022). Video channel suppression method of unmanned aerial vehicles. In *IEEE 41st International Conference on Electronics and Nanotechnology* (pp. 473–477). https://doi.org/10.1109/ELNANO54667.2022.9927105
42. Sokolov, V., Skladannyi, P., & Platonenko, A. (2023). Jump-stay jamming attack on Wi-Fi systems. In *IEEE 18th International Conference on Computer Science and Information Technologies* (pp. 1–5). https://doi.org/10.1109/CSIT61576.2023.10324031
43. Sokolov, V., Skladannyi, P., & Korshun, N. (2023). ZigBee network resistance to jamming attacks. In *IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics* (pp. 161–165). https://doi.org/10.1109/UkrMiCo61577.2023.10380360
44. Sokolov, V., Skladannyi, P., & Astapenya, V. (2023). Bluetooth Low-Energy beacon resistance to jamming attack. In *IEEE 13th International Conference on Electronics and Information Technologies* (pp. 270–274). https://doi.org/10.1109/ELIT61488.2023.10310815
45. Sokolov, V., Skladannyi, P., & Mazur, N. (2023). Wi-Fi repeater influence on wireless access. In *IEEE 5th International Conference on Advanced Information and Communication Technologies* (pp. 33–36). https://doi.org/10.1109/AICT61584.2023.10452421
46. Sokolov, V., Skladannyi, P., & Astapenya, V. (2023). Wi-Fi interference resistance to jamming attack. In *IEEE 5th International Conference on Advanced Information and Communication Technologies* (pp. 1–4). https://doi.org/10.1109/AICT61584.2023.10452687
47. Sokolov, V. (2025). Ensuring the resilience of wireless systems to jamming attacks. *Telecommunications and Information Technologies, 1*(86), 50–60. https://doi.org/10.31673/2412-4338.2025.013623
48. Sokolov, V. (2025). Technology for tracking subscriber movement across the territory of a critical infrastructure enterprise. *Cybersecurity: Education, Science, Technique, 1*(29), 207–222. https://doi.org/10.28925/2663-4023.2025.29.920

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Loban Heorhii
PhD Student, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0003-4862-8729
heorhii.loban.asp.2025@lpnu.ua

Lukovskyy Taras
PhD, Associate Professor, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

MODELS AND METHODS FOR WIRELESS DEVICE IDENTIFICATION BASED ON RADIO FREQUENCY CHARACTERISTICS: A COMPREHENSIVE ANALYSIS OF MODERN RF-FINGERPRINTING APPROACHES

Abstract. This article presents a comprehensive analysis of state-of-the-art models and methods for wireless device identification based on their unique radio frequency characteristics (RF-fingerprinting). The fundamental principles of RF fingerprint formation, which arise from the intrinsic hardware imperfections of transmitter components, are examined in detail. The study analyzes the primary sources of signal uniqueness, including variations in oscillator parameters, power amplifier behavior, modulator nonlinearities, and antenna system characteristics. Existing RF-fingerprinting approaches are systematized according to feature extraction methodology, applied classification algorithms, and practical application domains. Special attention is devoted to signal processing techniques in the time, frequency, and time–frequency domains, including transient behavior analysis, spectral feature characterization, and wavelet transforms. The article provides a structured classification of machine learning algorithms used for device identification, ranging from traditional statistical models to advanced deep learning architectures. Hybrid approaches that combine multiple methodologies to improve identification accuracy and robustness are highlighted. The impact of environmental factors—such as multipath propagation, interference, and dynamic channel variation—on the effectiveness of RF-fingerprinting systems is thoroughly examined. Practical aspects of deploying RF-fingerprinting in cybersecurity systems, access control mechanisms, and counterfeit device detection are discussed. Key challenges and limitations of existing methods are identified, including scalability, adaptability to emerging device types, and resilience to intentional adversarial attacks. Finally, promising directions for the development of RF-fingerprinting technology are proposed, with particular emphasis on integration with artificial intelligence systems and emerging quantum-enabled signal processing methods.

Keywords: RF-fingerprinting, cybersecurity, threat detection, radio signal, attacks, radio-frequency identification, machine learning, signal processing, wireless security, physical-layer authentication, deep learning, spectral analysis, device classification.

REFERENCES

1. Cisco Annual Internet Report (2018-2023). White Paper. Cisco Systems, 2023. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
2. Danev, B., Zanetti, D., & Capkun, S. (2012). On physical-layer identification of wireless devices. ACM Computing Surveys, 45(1), 1-29. DOI: 10.1145/2379776.2379782
3. Polak, A. C., Dolatshahi, S., & Goeckel, D. L. (2011). Identifying wireless users via transmitter imperfections. IEEE Journal on Selected Areas in Communications, 29(7), 1469-1479. DOI: 10.1109/JSAC.2011.110812
4. Rehman, S. U., Sowerby, K. W., & Coghill, C. (2014). Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers. Journal of Computer and System Sciences, 80(3), 591-601. DOI: 10.1016/j.jcss.2013.06.013

5. Jagannath, A., Jagannath, J., & Kumar, P. S. P. V. (2022). A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. Computer Networks, 219, 109455. DOI: 10.1016/j.comnet.2022.109455
6. Sankhe, K., Belgiovine, M., Zhou, F., Riyaz, S., Ioannidis, S., & Chowdhury, K. (2019). ORACLE: Optimized radio classification through convolutional neural networks. IEEE INFOCOM 2019, 370-378. DOI: 10.1109/INFOCOM.2019.8737463
7. Wu, Qingyang & Feres, Carlos & Kuzmenko, Daniel & Ding, Zhi & Yu, Zhou & Liu, Xin & Liu, Xiaoguang. (2018). Deep Learning Based RF Fingerprinting for Device Identification and Wireless Security. Electronics Letters. 54. 10.1049/el.2018.6404.
8. Merchant, K., Revay, S., Stantchev, G., & Nousain, B. (2022). Deep learning for RF device fingerprinting in cognitive communication networks. IEEE Journal of Selected Topics in Signal Processing, 12(1), 160-167. DOI: 10.1109/JSTSP.2018.2796446
9. D. Adesina, C. -C. Hsieh, Y. E. Sagduyu and L. Qian, "Adversarial Machine Learning in Wireless Communications Using RF Data: A Review," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 77-100, Firstquarter 2023, doi: 10.1109/COMST.2022.3205184.
10. Wong, L. J., Headley, W. C., & Michaels, A. J. (2022). Transfer learning for radio frequency machine learning: A taxonomy and survey. Sensors, 22(4), 1416. DOI (MDPI): 10.3390/s22041416
11. Restuccia, F., D'Oro, S., Al-Shawabka, A., Belgiovine, M., Angioloni, L., Ioannidis, S., Chowdhury K. & Melodia, T. (2023). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. IEEE Transactions on Wireless Communications, 22(3), 1749-1763. https://doi.org/10.48550/arXiv.1904.07623
12. Xie L, Peng L and Zhang J et al. Radio frequency fingerprint identification for Internet of Things: A survey. Security and Safety 2024; 3: 2023022. https://doi.org/10.1051/sands/2023022
13. Hall, Jeyanthi & Barbeau, Michel & Kranakis, Evangelos. (2006). Detecting rogue devices in bluetooth networks using radio frequency fingerprinting. Proceedings of the Third IASTED International Conference on Communications and Computer Networks, CCN 2006. 108-113.
14. Brik, V., Banerjee, S., Gruteser, M., & Oh, S. (2008). Wireless device identification with radiometric signatures. Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, 116-127. https://doi.org/10.1145/1409944.1409959
15. Huang, Y., & Zheng, H. (2012). Radio frequency fingerprinting based on the constellation errors. 18th Asia-Pacific Conference on Communications (APCC), 900-905. DOI: 10.1109/APCC.2012.6388238
16. Kennedy, I. O., Scanlon, P., Mullany, F. J., Buddhikot, M. M., Nolan, K. E., & Rondeau, T. W. (2008). Radio transmitter fingerprinting: A steady state frequency domain approach. IEEE 68th Vehicular Technology Conference, 1-5. DOI: 10.1109/VETECF.2008.291
17. Ureten, O., & Serinken, N. (1999). Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering, 32(1), 27-33. DOI: 10.1109/CJECE.2007.364330
18. Peng, L., Hu, A., Zhang, J., Jiang, Y., Yu, J., & Yan, Y. (2019). Design of a hybrid RF fingerprint extraction and device classification scheme. IEEE Internet of Things Journal, 6(1), 349-360. DOI: 10.1109/JIOT.2018.2838071
19. Vo-Huu, T. D., Vo-Huu, T. D., & Noubir, G. (2016). Fingerprinting Wi-Fi devices using software defined radios. Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 3-14. https://doi.org/10.1145/2939918.2939936
20. Robyns, P., Marin, E., Lamotte, W., Quax, P., Singelée, D., & Preneel, B. (2017). Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning. Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 58-63. https://doi.org/10.1145/3098243.3098267
21. Klein, R. W., Temple, M. A., & Mendenhall, M. J. (2009). Application of wavelet-based RF fingerprinting to enhance wireless network security. Journal of Communications and Networks, 11(6), 544-555. DOI: 10.1109/JCN.2009.6388408
22. Reising, D. R., Temple, M. A., & Mendenhall, M. J. (2010). Improved wireless security for GMSK-based devices using RF fingerprinting. International Journal of Electronic Security and Digital Forensics, 3(1), 41-59. https://doi.org/10.1504/IJESDF.2010.032330
23. Xu, Q., Zheng, R., Saad, W., & Han, Z. (2016). Device fingerprinting in wireless networks: Challenges and opportunities. IEEE Communications Surveys & Tutorials, 18(1), 94-104. DOI: 10.1109/COMST.2015.2476338
24. Bassey, J., Adesina, D., Li, X., Qian, L., Aved, A., & Kroecker, T. (2019). Intrusion detection for IoT devices based on RF fingerprinting using deep learning. Fourth International Conference on Fog and Mobile Edge Computing (FMEC), 98-104. DOI: 10.1109/FMEC.2019.8795319

25. A. Al-Shawabka et al., "Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2020, pp. 646-655, doi: 10.1109/INFOCOM41043.2020.9155259.
26. S. Rajendran, W. Meert, V. Lenders and S. Pollin, "SAIFE: Unsupervised Wireless Spectrum Anomaly Detection with Interpretable Features," 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Seoul, Korea (South), 2018, pp. 1-9, doi: 10.1109/DySPAN.2018.8610471.
27. S. Hanna, S. Karunaratne and D. Cabric, "Open Set Wireless Transmitter Authorization: Deep Learning Approaches and Dataset Considerations," in IEEE Transactions on Cognitive Communications and Networking, vol. 7, no. 1, pp. 59-72, March 2021, doi: 10.1109/TCCN.2020.3043332
28. K. Sankhe et al., "No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments," in IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 1, pp. 165-178, March 2020, doi: 10.1109/TCCN.2019.2949308.
29. Shi, Yan & Jensen, Michael. (2011). Improved Radiometric Identification of Wireless Devices Using MIMO Transmission. IEEE Transactions on Information Forensics and Security. 6. 1346-1354. 10.1109/TIFS.2011.2162949.
30. Candore, Andrea & Kocabas, Ovunc & Koushanfar, Farinaz. (2009). Robust stable radiometric fingerprinting for wireless devices. 43 - 49. 10.1109/HST.2009.5224969.
31. Roy, Debashri & Mukherjee, Tathagata & Chatterjee, Mainak & Blasch, Erik & Pasiliao, Eduardo. (2019). RFAL: Adversarial Learning for RF Transmitter Identification and Classification. IEEE Transactions on Cognitive Communications and Networking. PP. 1-1. 10.1109/TCCN.2019.2948919.
32. Oligeri, Gabriele & Sciancalepore, Savio & Raponi, Simone & Pietro, Roberto. (2022). PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2022.3219287.
33. Hamdaoui, Bechir & Alkalbani, Mohamed & Znati, Taieb & Rayes, Mark. (2019). Unleashing the Power of Participatory IoT with Blockchains for Increased Safety and Situation Awareness of Smart Cities. 10.48550/arXiv.1912.00962.
34. Jian, Tong & Rendon, Bruno & Ojuba, Emmanuel & Soltani, Nasim & Wang, Zifeng & Sankhe, Kunal & Gritsenko, Andrey & Dy, Jennifer & Chowdhury, Kaushik & Ioannidis, Stratis. (2020). Deep Learning for RF Fingerprinting: A Massive Experimental Study. IEEE Internet of Things Magazine. 3. 50-57. 10.1109/IOTM.0001.1900065.
35. Wang, W., Sun, Z., Piao, S., Zhu, B., & Ren, K. (2016). Wireless physical-layer identification: Modeling and validation. IEEE Transactions on Information Forensics and Security, 11(9), 2091-2106. DOI: 10.1109/TIFS.2016.2552146
36. Xie, Ning & Zhang, Shengli. (2018). Blind Authentication at the Physical Layer Under Time-Varying Fading Channels. IEEE Journal on Selected Areas in Communications. PP. 1-1. 10.1109/JSAC.2018.2824583.
37. Kim, Brian & Erpek, Tugba & Sagduyu, Yalin & Ulukus, Sennur. (2021). Covert Communications via Adversarial Machine Learning and Reconfigurable Intelligent Surfaces. 10.48550/arXiv.2112.11414.
38. Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). Quantum algorithm for linear systems of equations. Physical Review Letters, 103(15), 150502. DOI: https://doi.org/10.1103/PhysRevLett.103.150502
39. W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," in IEEE Network, vol. 34, no. 3, pp. 134-142, May/June 2020, doi: 10.1109/MNET.001.1900287
40. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 1273-1282. https://doi.org/10.48550/arXiv.1602.05629
41. Sokolov, V., Skladannyi, P., & Platonenko, A. (2022). Video channel suppression method of unmanned aerial vehicles. In *IEEE 41st International Conference on Electronics and Nanotechnology* (pp. 473–477). https://doi.org/10.1109/ELNANO54667.2022.9927105
42. Sokolov, V., Skladannyi, P., & Platonenko, A. (2023). Jump-stay jamming attack on Wi-Fi systems. In *IEEE 18th International Conference on Computer Science and Information Technologies* (pp. 1–5). https://doi.org/10.1109/CSIT61576.2023.10324031
43. Sokolov, V., Skladannyi, P., & Korshun, N. (2023). ZigBee network resistance to jamming attacks. In *IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics* (pp. 161–165). https://doi.org/10.1109/UkrMiCo61577.2023.10380360
44. Sokolov, V., Skladannyi, P., & Astapenya, V. (2023). Bluetooth Low-Energy beacon resistance to jamming attack. In *IEEE 13th International Conference on Electronics and Information Technologies* (pp. 270–274). https://doi.org/10.1109/ELIT61488.2023.10310815

45. Sokolov, V., Skladannyi, P., & Mazur, N. (2023). Wi-Fi repeater influence on wireless access. In *IEEE 5th International Conference on Advanced Information and Communication Technologies* (pp. 33–36). https://doi.org/10.1109/AICT61584.2023.10452421
46. Sokolov, V., Skladannyi, P., & Astapenya, V. (2023). Wi-Fi interference resistance to jamming attack. In *IEEE 5th International Conference on Advanced Information and Communication Technologies* (pp. 1–4). https://doi.org/10.1109/AICT61584.2023.10452687
47. Sokolov, V. (2025). Ensuring the resilience of wireless systems to jamming attacks. *Telecommunications and Information Technologies, 1*(86), 50–60. https://doi.org/10.31673/2412-4338.2025.013623
48. Sokolov, V. (2025). Technology for tracking subscriber movement across the territory of a critical infrastructure enterprise. *Cybersecurity: Education, Science, Technique, 1*(29), 207–222. https://doi.org/10.28925/2663-4023.2025.29.920