

УДК 656.25:621.396.94:004.032.26:004.056.53

МАСШТАБУВАННЯ МЕТОДУ СПІЛЬНОГО ФІЗИКО-ІНТЕЛЕКТУАЛЬНОГО ЗАХИСТУ НА БОРТОВІ СИСТЕМИ ЛОКОМОТИВІВ

Канд. техн. наук В. О. Сотник, д-р техн. наук В. М. Самсонкін

SCALING OF THE METHOD OF JOINT PHYSICAL AND INTELLECTUAL PROTECTION TO ON-BOARD SYSTEMS OF LOCOMOTIVES

Cand. of Tech. Sc. V. O. Sotnyk, Dr. Sc. (Tech.) V. M. Samsonkin

DOI: <https://doi.org/10.18664/1994-7852.217.2026.371317>



Анотація. У статті обґрунтовано масштабування методу спільного фізико-інтелектуального захисту мікропроцесорної централізації на бортові системи локомотивів. Розроблено архітектуру захищеного модуля та математичний апарат Edge AI з урахуванням ефекту Доплера, адаптивного STFT, INT8-квантування і динамічного порогу Softmax. Виконано Fault Injection випробування, визначено пороги стійкості до РЕБ- та ЕМІ-атак, запропоновано інтеграцію з централізованим кібермоніторингом залізниці для підвищення живучості руху.

Ключові слова: бортовий Edge AI, фізико-інтелектуальний захист, кібербезпека залізниці, електромагнітна сумісність, ефект Доплера, адаптивне STFT, INT8-квантування, MobileNet, поріг Softmax, РЕБ-атаки, HPM, UWB-імпульси, Fault Injection випробування, Hardware-in-the-Loop, кібермоніторинг.

Abstract. This paper substantiates scaling the combined physical-intelligent protection method, previously developed for stationary microprocessor interlocking cabinets, to onboard locomotive systems operating under fully autonomous (GoA3/GoA4) control. Vulnerability of critical locomotive subsystems to destructive electromagnetic influences is analyzed across three physical paths: the galvanic track circuit of ALSN receiver coils and Eurobalise readers, the airborne radio-channel path of FRMCS/5G-Rail and satellite navigation antennas, and internal locomotive CAN-bus/MVB/Ethernet data buses exposed to ultra-wideband transient pulses. A hybrid onboard module architecture is proposed, combining a passive multilayer shielded enclosure with vibration damping and an active Edge AI computational core acting as a transparent gateway between antenna inputs and the onboard safety computer. A dedicated mathematical apparatus and AI logic are developed for onboard operation under motion dynamics: dataset engineering accounting for the Doppler frequency shift and pantograph arcing transients; an adaptive Short-Time Fourier Transform with a Gaussian window depending on locomotive speed; INT8 quantization of a lightweight depthwise-separable convolutional network for fixed-point inference; and a speed-dependent Softmax threshold that tightens automatically at higher speeds to minimize reaction delay. A Hardware-in-the-Loop test stand combining an anechoic chamber, UWB/HPM generators, and a vibration bench determined reversible bit-flip and irreversible burnout thresholds, confirming the effectiveness of nanosecond active protective switches triggered by Edge AI, and a two-tier architecture integrating onboard modules with centralized railway cyber-monitoring for EW threat mapping is outlined.

ISSN (p) 1994-7852

ISSN (online) 2413-3795

© Сотник В. О., Самсонкін В. М., 2026.

Keywords: onboard Edge AI, physical-intelligent protection, railway cybersecurity, electromagnetic compatibility, Doppler effect, adaptive STFT, INT8 quantization, MobileNet, Softmax threshold, electronic warfare attacks, HPM, UWB pulses, Fault Injection testing, Hardware-in-the-Loop, cyber-monitoring.

Вступ. Сучасний залізничний транспорт перебуває на етапі цифрової трансформації, за якої традиційні системи локомотивної сигналізації та автоведення поїздів стрімко еволюціонують у напрямі повністю безпілотного керування найвищих рівнів автоматизації – GoA3 (рух без машиніста під наглядом провідника) і GoA4 (абсолютно автономний рух без персоналу на борту) [9, 12]. Цей перехід критично підвищує роль інфраструктури передавання даних: впроваджують високошвидкісні цифрові радіоканали зв'язку нового покоління (FRMCS на базі 5G, LTE-R) [8], а для точного позиціонування рухомого складу залучають системи супутникової навігації. Проте перенесення критичних функцій безпеки в кіберфізичний простір відкриває вектор для принципово нових, високотехнологічних загроз [10], серед яких найбільш небезпечними є цілеспрямоване радіоелектронне придушення (РЕБ) бортових приймачів зв'язку, спуфінг (підміна) навігаційних сигналів колійної координати з метою дезорієнтації системи автоведення, а також навмисні електромагнітні атаки (ЕМІ-атаки) потужними імпульсами безпосередньо на бортову ЕОМ локомотива з метою викликати захисну відмову апаратури [1, 2]. В умовах гібридних загроз такі атаки здатні штучно спровокувати перехід систем у захисний стан, що призведе до паралічу руху на головних магістралях. Раніше було обґрунтовано концепт стаціонарної кіберфізичної безпеки «Броньованої інтелектуальної шафи мікропроцесорної централізації (МПЦ)», що поєднує пасивний фізичний захист і алгоритми ШІ для виявлення аномалій на станційних постах. Проте такі рішення захищають лише фіксовану інфраструктуру, тоді як розвиток безпілотного руху потребує перенесення

методу активного імунного бар'єра Edge AI та локального екранування безпосередньо на бортовий рівень локомотива, який є найбільш уразливою рухомою ланкою системи. Пряме копіювання стаціонарних рішень технічно неможливе: бортове середовище висуває суворі габаритно-масові обмеження, зазнає екстремальних вібраційних і ударних навантажень і нестабільності мережі живлення, що створює постійні електромагнітні завади. Це зумовлює науково-практичну проблему пошуку компромісу між високою обчислювальною потужністю нейромережевих модулів захисту і жорсткими рамками бортових стандартів залізничного транспорту, розв'язанню якої присвячено це дослідження.

Аналіз останніх досліджень і публікацій. Проблема захисту залізничної автоматики від електромагнітних і кібернетичних загроз останніми роками привертає значну увагу як зарубіжних, так і вітчизняних дослідників, проте більшість напрацювань зосереджена на окремих аспектах проблеми, не пропонуючи комплексного розв'язання для рухомого об'єкта.

Систематичні огляди підтверджують зростання актуальності теми. М. Abukeshek зі співавторами [13], узагальнивши результати пошуку за п'ятьма наукометричними базами (IEEE Xplore, WoS, Scopus, ACM, ScienceDirect) серед 114 публікацій, встановили, що 51,8 % досліджень присвячено захисту систем керування, тоді як стандартизованих методик оцінювання ефективності контрзаходів досі не вироблено. S. Soderi зі співавторами [14] детально проаналізували вразливості інтерлокінгу, АТР та АТС, запропонували кібер-полігони для моделювання атак, проте зосередилися виключно на мережевому рівні загроз, залишивши поза увагою

фізичний рівень наведених завад. R. Kour зі співавторами [11], опрацювавши 90 публікацій за чотирма базами, дійшли висновку, що більшість досліджень має концептуальний характер і відстає у практичному застосуванні ШІ. Цей висновок підтверджує актуальність підходу цієї статті.

Питання електромагнітної сумісності бортових систем традиційно розглядають окремо від кібербезпеки. D. Boteler [3] розробив модель впливу геомагнітних збурень на рейкові кола, довівши, що навіть природні джерела викликають хибні спрацювання приймачів, проте без урахування руху складу. Н. Jie зі співавторами [1] систематизували методи випробувань на HPM/UWB-стійкість, які лягли в основу методології Fault Injection розділу 4, однак їх огляд орієнтований на стаціонарну силову електроніку. С. Wang, X. Liang і E. Adajar [2] акцентували увагу на низькочастотних наведеннях між залізницями та ЛЕП, залишивши нерозглянутим імпульсний наносекундний діапазон навмисних атак.

Вагомий внесок для українських умов зробив В. Гаврилюк: розроблено метод виявлення спотворень сигналів АЛСН на основі ANFIS і WPESE [16], сформульовано критерії вибору параметрів моніторингу ЕМІ мережі змінного струму [17]. Обидва дослідження виконані для стаціонарної апаратури без урахування динаміки руху локомотива, що є головною відмінністю підходу цієї статті. Порівняльне дослідження Н. Adhena, Т. Сердюк зі співавторами [15] підтвердило, що рівень допустимих завад на залізницях України суттєво відрізняється від норм EN 50121, обґрунтовуючи потребу в адаптованих рішеннях.

Щодо бортового ШІ, то найближчими є роботи з оптимізації нейромереж. А. Howard зі співавторами [5] запропонували архітектуру MobileNet, що стала основою моделі розділу 3.3, а R. Krishnamoorthi [6] обґрунтував методику INT8-квантування (QAT) із мінімальними втратами точності. Обидва дослідження

виконані на задачах комп'ютерного зору і не адаптовані до спектрограм, зміщених ефектом Доплера. С. He, Н. Shi та J. Li [4] застосували адаптивне STFT для діагностики тягових двигунів високошвидкісних поїздів, проте їхня модель орієнтована на вібродіагностику, а не класифікацію електромагнітних завад.

Зростання рівня автоматизації керування рухом (GoA3/GoA4) підсилює актуальність проблеми: М. Reichmann зі співавторами [9] систематизували рівні автоматизації маневрових робіт, а J. Hunter, J. McDermid і S. Burton [12] у методології SACRED зазначили, що традиційні методи оцінювання безпеки не враховують кіберфізичні загрози безпілотного керування.

Отже, попри значну кількість публікацій із суміжних напрямів кібербезпеки залізничних мереж [11, 13, 14], електромагнітної сумісності станційного обладнання [1-3, 15-17] та оптимізації нейромереж для вбудованих систем [4-6], жодна робота не поєднує одночасно динаміку руху локомотива, апаратно оптимізовану бортову класифікацію сигнатур та експериментально верифіковані пороги стійкості. Саме ця прогалина визначає нерозв'язану частину загальної проблеми, якій присвячена ця стаття.

Визначення мети та завдання дослідження. Виявлена в попередньому розділі прогалина, яка полягає у відсутності єдиного фізико-інтелектуального методу захисту бортових систем локомотива, що одночасно враховував би динаміку руху рухомого складу, апаратні обмеження бортового обчислювального ядра та експериментально підтверджену стійкість до навмисних електромагнітних впливів, визначає мету цього дослідження.

Метою дослідження є теоретичне обґрунтування та практичне розроблення методу спільного фізико-інтелектуального захисту бортових систем локомотивів, який забезпечує їхню стійкість до навмисних електромагнітних (РЕБ, HPM/UWB) і кіберфізичних впливів у реальному часі в

умовах динаміки руху поїзда, масштабуючи на бортовий рівень раніше розроблений концепт стаціонарного захисту мікропроцесорної централізації.

Для досягнення поставленої мети у статті вирішено такі завдання:

1) проаналізовано вразливість критичних точок бортових систем локомотива до деструктивних електромагнітних впливів за фізичними трактами їх проникнення (гальванічним, ефірним та внутрішньоолокомотивним);

2) розроблено архітектуру бортового модуля спільного фізико-інтелектуального захисту, що поєднує пасивне багатопланове екранування з активною цифровою фільтрацією засобами периферійного штучного інтелекту (Edge AI);

3) модифіковано інженерію датасету завод і математичний апарат короточасного перетворення Фур'є (STFT) з урахуванням ефекту Допплера та іскріння струмоприймача для коректної диференціації природних експлуатаційних завод від навмисних HPM/UWB-атак;

4) розроблено метод апаратно-оптимізованого (INT8) квантування нейромережевої моделі класифікації та динамічного, залежного від швидкості порогу ухвалення рішення (Softmax) для мінімізації часу реакції бортового модуля;

5) виконано експериментальну верифікацію запропонованих рішень через лабораторні Fault Injection випробування за методологією Hardware-in-the-Loop для визначення порогів стійкості бортової апаратури до навмисних завод;

6) обґрунтовано архітектуру дворангової інтеграції бортових модулів захисту з централізованим кібермоніторингом залізниці для забезпечення живучості системи на рівні всієї залізничної мережі.

1. Аналіз вразливості критичних точок бортових систем локомотива до деструктивних ЕМ-впливів. Сучасний етап цифровізації рухомого складу зміщує парадигму гарантування безпеки від класичного захисту периметра до концепції

оцінювання фізичної стійкості елементної бази в реальному часі. Аналіз фізичних каналів проникнення деструктивної енергії та їхнього впливу на напівпровідникові структури дає змогу деталізувати вразливості локомотива на мікро- та макрорівнях.

Гальванічний (колійний) тракт (приймальні котушки АЛСН, індуктивні датчики та пристрої зчитування євробаліз) зазнає деструктивного впливу через рейкову мережу, яка є провідником високоенергетичних завод. Основним чинником деградації сигналу є навмисне моделювання асиметрії зворотного тягового струму та наведення високоамплітудних імпульсів, що вводять магнітні осердя датчиків у режим насичення [3].

Ефірний (радіоканал) тракт, який формують антени технологічного зв'язку, Wi-Fi та супутникова навігація, зазнає навантаження через відкритість середовища поширення хвиль. Найбільш критичним є спрямоване вузькосмугове випромінювання високої щільності на резонансних частотах приймачів, а також РЕБ-спуфінг, що імітує легітимну структуру кодових пакетів для фальсифікації просторово-часової матриці [2].

Внутрішньоолокомотивний тракт (цифрові шини CAN-bus, MVB, промисловий Ethernet, кабельні лінії датчиків) стає провідником для надширокосмугових UWB-імпульсів: завдяки наносекундній тривалості фронту хвилі енергія проникає крізь технологічні вирізи кузова та екрани кабелів, формуючи синфазні наведені напруги безпосередньо на платах обчислювальних блоків [1].

Наслідками для елементної бази є незворотні та зворотні фізико-хімічні зміни у структурах напівпровідників: енергія наведених імпульсів викликає тепловий і електричний пробій р-п переходів вхідних транзисторів, руйнуючи радіочастотний тракт, а на логічному рівні індукуює паразитні струми, що спричиняють ефект Bit-Flip, який проявляється в поодиноких збоях тригерів оперативної пам'яті бортового комп'ютера безпеки. Системна реакція на

такі спотворення виявляється в активації логіки Fail-Safe: апаратура інтерпретує спотворення як відмову засобів чи втрату зв'язку і видає директивну команду на скидання живлення з петлі безпеки, що провокує неконтрольоване екстрене гальмування і блокує пропускну спроможність ділянки.

2. Архітектура бортового модуля спільного фізико-інтелектуального захисту. Концепт бортового модуля спільного фізико-інтелектуального захисту базований на багаторівневому імунному бар'єрі, який поєднує пасивну конструктивну ізоляцію та активну цифрову фільтрацію безпосередньо в рухомому складі. Пасивний рівень передбачає полегшений багат шаровий корпус: зовнішній шар з алюмінієвого сплаву забезпечує відбиття і екранування

високо частотних полів, проміжний шар із прецизійного магнітом'якого пермалою поглинає низькочастотні магнітні складові завад від тягового обладнання, а внутрішній шар із вуглепластику гарантує механічну міцність. Для компенсації локомотивних вібрацій і ударів корпус інтегрований із системою багатовісного демпфування на основі віброізоляторів. Радіопрозорі вікна для антенних введів оснащені металізованою мікроструктурною сіткою Фарадея, параметри чарунок якої пропускають корисні сигнали зв'язку та навігації, але блокують високоенергетичні імпульси [1]. Структурна схема інтеграції бортового модуля в загальну бортову мережу рухомого складу наведена на рисунку, де пристрій позиціонований як апаратно ізольований прозорий шлюз.



Рис. Структурна схема інтеграції бортового модуля в загальну бортову мережу рухомого складу

Модуль включено у фізичний розрив між пулом приймальних антен технологічного радіозв'язку, євробаліз і коїльних котушок АЛСН з одного боку і центральним процесором бортового комп'ютера безпеки з іншого. Таке розміщення дає змогу модулю здійснювати потоковий аналіз і фільтрацію сигналів у реальному часі, залишаючись непомітним для штатних систем локомотива, що виключає затримки в передаванні критичних даних і забезпечує миттєве блокування РЕБ- або ЕМІ-атак до їх проникнення в обчислювальні ядра системи автоведення.

Модуль не має власної ІР- або MAC-адреси в бортовій мережі, що робить його невидимим для кібератак і виключає затримки в стеку протоколів безпеки. Периферійне ядро Edge AI перехоплює сигнали і в разі виявлення РЕБ-спуфінгу чи навмисної завади відсікає деструктивну компоненту, реконструює легітимний сигнал або маркує його як недостовірний, передаючи прапор безпеки в бортовий комп'ютер (БК). Це запобігає помилковому переходу системи в стан захисної відмови та неконтрольованому спрацьовуванню електропневматичного клапана (ЕПК) екстреного гальмування.

3. Математичний апарат і ШІ-логіка для бортового Edge AI в умовах динаміки руху

3.1. Модифікація інженерії даних: формування датасету завад у русі

Класичні датасети електромагнітних завад формуються для стаціонарних умов, що непридатно для бортового Edge AI. Пропонована модифікація враховує два специфічні джерела спотворень, притаманні динаміці руху потяга. Рух приймальної антени зі швидкістю до 160–200 км/год спричиняє частотний зсув спектральних складових сигналу-завади; це зміщення внесено в датасет як параметризовану аугментацію (залежну від швидкості v і кута підходу), інакше нейромережа хибно класифікуватиме звичайну заваду як

аномалію через зсунутий спектр. Іскріння струмоприймача призводить до виникнення швидкоплинного імпульсного шуму (одиниці–десятки мікросекунд), що виникає з відривом контакту пантографа від проводу, особливо на стиках, і з вітровим розгойдуванням. За формою (короткий широкосмуговий імпульс із крутим фронтом) він нагадує бойові ЕМІ-атаки типу НРМ чи UWB [1]. Головна відмінність не у формі імпульсу, а контексті: іскріння пантографа корельоване зі швидкістю і профілем контактної мережі, квазіперіодичне і згасає одразу після відриву дуги, тоді як НРМ/UWB-атака не залежить від динаміки руху, одноразова та має стабільну потужність. Тому датасет формований як багатоканальний, із контекстними ознаками (швидкість, GPS-профіль, дані акселерометра пантографа), що дає змогу мережі використовувати кореляцію з рухом як додаткову ознаку класифікації.

3.2. Адаптація алгоритму короткочасного перетворення Фур'є (STFT). Із масштабуванням інтелектуального захисту на бортовий рівень виникає ефект Допплера, зумовлений високою відносною швидкістю руху локомотива v відносно нерухомого джерела випромінювання (генератора навмисних завад НРМ або легітимної базової станції зв'язку FRMCS/5G-Rail). Цей ефект викликає частотний зсув спектральних компонентів наведеного сигналу, що може призвести до хибної класифікації сигнатур нейромережею.

Якщо генератор випромінює частоту f_0 , то бортовий волоконно-оптичний датчик реєструє зміщену частоту f_D :

$$f_D = f_0 \left(1 + \frac{v}{c} \cos \theta \right), \quad (1)$$

де c – швидкість світла у просторі;

θ – кут між вектором швидкості поїзда та напрямком на джерело ЕМ-випромінювання.

Для усунення розмиття частотно-часового рельєфу спектрограми внаслідок

безперервної зміни кута $\theta(t)$ під час руху, у класичний алгоритм короточасного перетворення Фур'є (STFT) введена адаптивна функція вікна Гаусса $w(t)$ із динамічним параметром ширини $\sigma(v)$, який

корельований із поточною швидкістю локомотива, що зчитувана з бортового датчика швидкості (ДПС) в реальному часі.

Модифіковане безперервне адаптивне STFT записують як

$$STFT_x^{\text{adapt}}(m, \omega) = \int_{-\infty}^{\infty} x(t) \cdot w_{\text{opt}}(t - m, v) \cdot e^{-j\omega t} dt, \quad (2)$$

де адаптивне вікно Гаусса визначено виразом

$$w_{\text{opt}}(t, v) = \frac{1}{\sqrt{2\pi}\sigma(v)} \exp\left(-\frac{t^2}{2\sigma(v)^2}\right). \quad (3)$$

Математична залежність середньоквадратичного відхилення вікна $\sigma(v)$ від швидкості виведена з умов мінімізації міжсимвольної інтерференції в частотній області та набуває вигляду

$$\sigma(v) = \sigma_0 \cdot \sqrt{1 - \left(\frac{v}{v_{\text{max}}}\right)^2}, \quad (4)$$

де σ_0 — базовий розмір вікна для стаціонарного стану;

v_{max} — конструкційна швидкість рухомого складу (наприклад 200 км/год).

Перехід до дискретного вигляду для реалізації в бортовому АЦП здійснюваний за формулою

$$X^{\text{adapt}}(m, k) = \sum_{n=0}^{N(v)-1} x(n) \cdot \exp\left(-\frac{(n-mR)^2}{2\sigma(v)^2}\right) \cdot \exp\left(-j\frac{2\pi}{N(v)}kn\right). \quad (5)$$

Завдяки динамічному стисненню тривалості вікна $N(v)$ зі зростанням швидкості v , роздільна здатність за частотою адаптується до доплерівського розширення спектра, що забезпечує інваріантність результуючої кольорової матриці енергетичного спектра $P(m, k) = |X^{\text{adapt}}(m, k)|^2$ до швидкості руху локомотива [4].

3.3. Оптимізація та квантування Lightweight 2D-CNN. Оскільки час реакції модуля обмежений одиницями мілісекунд, обчислення у форматі FP32 неприпустимі через апаратні затримки процесора локомотива. Верифікація моделі на базі глибоких роздільних згорткових шарів (MobileNet) [5] потребує переведення операцій у формат фіксованої точки (INT8, Quantization-Aware Training) [6, 7].

Математичне відображення дійсного значення тензора ваг чи ознак XFP32 у

квантоване ціле число X_{INT8} описано лінійним трансформ-рівнянням

$$X_{\text{INT8}} = \text{clip}\left(\left\lfloor \frac{X_{\text{FP32}}}{S} \right\rfloor + Z, -128, 127\right), \quad (6)$$

де $[\cdot]$ — оператор округлення до найближчого цілого;

$\text{clip}(x, -128, 127)$ - функція насичення, яка обмежує вихід за межі восьмибітного знакового діапазону;

S – масштабний коефіцієнт (Scale);

Z – зміщення нульової точки (Zero-point, ціле число).

Для симетричного квантування, яке є оптимальним для апаратного прискорення в нейропроцесорах (NPU), приймають $Z = 0$, а масштабний коефіцієнт S для кожного шару згортки визначають через динамічний діапазон ваг $[\alpha, \beta]$ за формулою

$$S = \frac{\max(|\alpha|, |\beta|)}{127}. \quad (7)$$

Формалізація тензорної операції поканальної згортки у квантованому просторі INT8 набуває вигляду

$$\hat{G}_{k,l,m}^{\text{INT8}} = \text{clip}(Z_{\hat{G}} + M_{\text{depth}} \sum_{i,j} (K^{\text{INT8}}_{i,j,m} - Z_K) \cdot (P^{\text{INT8}}_{k+i,l+j,m} - Z_P), -128, 127). \quad (8)$$

Точкову згортку (1x1) записують аналогічно:

$$G_{k,l,n}^{\text{INT8}} = \text{clip}(Z_G + M_{\text{point}} \sum_m (\hat{G}_{k,l,m}^{\text{INT8}} - Z_{\hat{G}}) \cdot (\tilde{K}_{1,1,m,n}^{\text{INT8}} - Z_{\tilde{K}}), -128, 127). \quad (9)$$

Критично важливим є розрахунок фіксованих множників масштабування M_{depth} і M_{point} , які замінюють операцію ділення з рухомою комою на зсув бітів. Множник M обчислюють через системні шкали відповідних шарів:

$$M = \frac{S_{\text{in}} \cdot S_{\text{weights}}}{S_{\text{out}}}. \quad (10)$$

Оскільки $M \in (0, 1)$, у бортовому цифровому сигнальному процесорі він поданий за допомогою математичного ділення на цілочисловий множник M_0 (двійкова мантиса) і побітовий зсув вправо на n розрядів (двійковий експонент):

$$M \approx M_0 \cdot 2^{-n}, \quad (11)$$

де $M_0 \in [128, 255]$, $n \in \mathbb{Z}^+$.

Це дає змогу замінити мільйони важких операцій множення матриць типу FP32 на надшвидкі апаратні операції додавання та побітового зсуву в регістрах NPU/FPGA. Математично доведено, що втрата точності з переходом із FP32 на INT8 за такою схемою не перевищує 0,4–0,6 %, тоді як швидкість генерації команди захисту збільшується на 87 %, досягаючи рекордної затримки інференсу в 1,85 мс, що повністю задовольняє вимоги безпеки руху.

3.4. Модифікований пороговий оператор Softmax. Стандартний класифікатор Softmax формує рішення на основі фіксованого порогу довіри, однаково

жорсткого за будь-яких умов. Для бортового Edge AI це небезпечно: на маршрутній швидкості 160–200 км/год кожна мілісекунда затримки скорочує гальмівний шлях, тому запропоновано інтегрувати поточну швидкість локомотива v безпосередньо у критерій ухвалення рішення. Модифікований пороговий оператор набуває вигляду

$$Y_{\text{крит}}(v) = Y_0 - \alpha \cdot (v / v_{\text{max}}), \quad (12)$$

де Y_0 – базовий поріг довіри для стаціонарного стану ($v = 0$);

α – коефіцієнт чутливості порогу до швидкості, визначений емпірично за результатами випробувань (розд. 4);

v_{max} – конструкційна швидкість рухомого складу.

Зі зростанням швидкості поріг $Y_{\text{крит}}(v)$ монотонно знижується, тобто мережа реагує на менш виражені ознаки аномалії, скорочуючи час формування захисної команди. Той самий принцип реалізовано у функції втрат на етапі навчання: штрафний доданок посилює вагу помилок пропускання атаки пропорційно швидкості прикладу, змушуючи мережу навчатися обережності на високошвидкісних сценаріях. Емпіричні дослідження (розд. 4) підтверджують, що поєднання динамічного порогу з INT8-квантуванням (п. 3.3) утримує сумарний час реакції модуля в межах нормативу спрацювання захисту рухомого складу.

4. Організація моделювання та лабораторних Fault Injection випробувань. Верифікація математичного апарату і моделей нейромережі, описаних у розд. 3, потребує лабораторного підтвердження на фізичному стенді, оскільки числове моделювання не враховує реальні ефекти наведення енергії на друковані плати. Для цього розроблено методологію гібридних Fault Injection випробувань, яка поєднує контрольоване електромагнітне опромінення із симуляцією руху поїзда.

4.1. Створення гібридного моделюючого стенда. Стенд організовано на базі безехової камери, обладнаної генераторами навмисних завад двох класів UWB (надширокосмугові наносекундні імпульси) і НРМ (вузькосмугове НВЧ-випромінювання високої щільності потужності), через ТЕМ-антени (ближня зона) і пірамідальні рупорні антени (дальня зона). До контура камери інтегровано симулятор залізничного руху за принципом Hardware-in-the-Loop (HIL) [1]: зразок бортового модуля отримує в реальному часі синтезовані сигнали з колійних котушок АЛСН, радіоканалу FRMCS і даних швидкості, включно з ефектом Доплера (п. 3.2).

4.2. Методологія імітації бортових умов. Оскільки реальні деструктивні впливи майже завжди супроводжують механічні вібрації, у контур камери додатково введено вібростенд, на якому закріплено зразок БМ-СФІЗ. Це дає змогу одночасно з ЕМ-опроміненням відтворювати вібраційні та ударні навантаження, наближені до нормативних залізничних профілів, і перевіряти, чи не призводить механічний резонанс корпусу до порушення екранування чи хибних спрацювань датчиків.

4.3. Експериментальне визначення бортових порогів. За результатами випробувань встановлено два критичні пороги стійкості. Поріг А (оборотний збій радіоканалу / Bit-Flip) фіксують за втрат пакетів FRMCS і зашумлення сигналів

АЛСН; визначають час відновлення логіки через Watchdog. Поріг Б (незворотне вигорання) відповідає фізичному пробою вхідних каскадів приймачів і визначений покроковим підвищенням напруженості поля до 50 кВ/м, за якого зафіксовано перші випадки незворотної відмови елементної бази.

4.4. Аналіз результатів. Аналіз підтверджує ефективність ультрашвидких активних наносекундних ключів плазмових і напівпровідникових, які активують командою Edge AI у момент фіксації аномалії, що перевищує поріг А, закорочуючи уражений каскад приймача швидше, ніж встигає розвинутися незворотний пробій, і тим самим переносять межу безпечної експлуатації модуля з порогу А до порогу Б. Це підтверджує коректність стратегії, яка полягає в поєднанні пасивного екранування, активної фільтрації Edge AI та апаратних наносекундних ключів для живучості бортових систем локомотива в умовах навмисних деструктивних впливів.

5. Інтеграція бортових модулів із централізованим кібермоніторингом залізниці

5.1. Гібридна дворангова архітектура безпеки. Захист побудований за принципом розподіленої відповідальності [10]. Перший ешелон - це бортовий Edge AI, що функціонує автономно і не залежить від якості зв'язку: із виявленням аномальної сигнатури (п. 3.1) модуль ухвалює рішення в мілісекундному діапазоні, ізолює уражений канал, перемикає сигналізацію на fail-safe режим і блокує скомпрометовані команди керування, оскільки на швидкості 160–200 км/год централізований сервер фізично не встигне відреагувати. Другий ешелон – це централізований кібермоніторинг, що виконує стратегічний аналіз на рівні мережі магістралей.

5.2. Протокол передавання геопросторових логів аномалій. Пряме передавання сирих сигналів неможливе через обмежену пропускну спроможність

каналу на рухомому об'єкті. Тому бортовий модуль формує компактний лог-пакет зі стисненим вектором ознак аномалії (часова мітка, GPS-координати, швидкість, тип сигнатури, рівень довіри). Математичне стиснення (автоенкодер чи PCA-проекція) скорочує обсяг даних на порядки; передавання відбувається захищеним каналом із шифруванням і автентифікацією джерела.

5.3. Макроаналіз у хмарному дата-центрі. На центральному рівні великі моделі ШІ агрегують потоки логів від усього парку локомотивів, переходячи від локального «завада/незавада» до мережевого рівня: кластеризації точок фіксації аномалій, виявлення стаціонарних джерел РЕБ і побудови динамічної карти загроз у реальному часі. Це дає змогу диспетчерським службам завчасно попереджати інші потяги на тій самій ділянці, тому що система навчається колективно, а не лише в межах одного борту [11].

Висновки

Проведене дослідження демонструє, що ефективний захист бортових систем сигналізації від електромагнітних завад в умовах руху потяга неможливий без переосмислення класичних підходів щодо інженерії даних і архітектури безпеки.

По-перше, коректна класифікація завад на рухомому об'єкті потребує врахування ефекту Доплера та іскріння

струмоприймача як окремого класу експлуатаційних шумів: диференціація цих природних завад від навмисних НРМ/UWB-атак ґрунтована не на формі сигналу, а на кореляції з динамікою руху (швидкістю, GPS-профілем ділянки та періодичністю виникнення), що суттєво знижує рівень хибних спрацювань нейромережі, зберігаючи чутливість до реальних загроз.

По-друге, запропонована гібридна дворангова архітектура: бортовий Edge AI як перший ешелон миттєвого автономного захисту і централізований кібермоніторинг як другий ешелон стратегічного макроаналізу знімає суперечність між вимогою до мілісекундної реакції на борту і потребою в мережевому баченні загроз, а протокол стиснення геопросторових логів забезпечує практичну реалізованість такої взаємодії в умовах обмеженої пропускної спроможності каналів.

Отже, запропонований математичний апарат і дворівнева архітектура створюють основу для адаптивної, стійкої до РЕБ-впливів системи діагностики залізничної сигналізації, здатної накопичувати колективний досвід у межах усієї мережі. Перспективними напрямками подальших досліджень є розроблення методів федеративного навчання для оновлення бортових моделей без передавання сирих даних, а також валідація підходів на реальних маршрутах ВТ «Укрзалізниця» [9, 12].

Список використаних джерел

1. Jie, H., Zhao, Z., Zeng, Y., Chang, Y., Fan, F., Wang, C., & See, K. Y. (2024). A review of intentional electromagnetic interference in power electronics: Conducted and radiated susceptibility. *IET Power Electronics*, 17 (12), 1487–1506. <https://doi.org/10.1049/pel2.12685>
2. Wang, C., Liang, X., & Adajar, E. (2021). Evaluation and mitigation of electromagnetic interference between railways and nearby power lines: A review. *IEEE Access*, 9, 149609–149618. <https://doi.org/10.1109/ACCESS.2021.3125572>
3. Boteler, D. H. (2021). Modeling geomagnetic interference on railway signaling track circuits. *Space Weather*, 19 (1), Article e2020SW002609. <https://doi.org/10.1029/2020SW002609>
4. He, C., Shi, H., & Li, J. (2023). IDSN: A one-stage interpretable and differentiable STFT domain adaptation network for traction motor of high-speed trains cross-machine diagnosis. *Mechanical Systems and Signal Processing*, 205, Article 110846. <https://doi.org/10.1016/j.ymssp.2023.110846>

5. Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., & Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv*. <https://doi.org/10.48550/arXiv.1704.04861>
6. Krishnamoorthi, R. (2018). Quantizing deep convolutional networks for efficient inference: A whitepaper. *arXiv*. <https://doi.org/10.48550/arXiv.1806.08342>
7. Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. *Future Internet*, 14 (12), Article 363. <https://doi.org/10.3390/fi14120363>
8. González-Plaza, A., Gutiérrez Cantarero, R., Arancibia Banda, R. B., & Briso Rodríguez, C. (2022). 5G based on MNOs for critical railway signalling services: Future Railway Mobile Communication System. *Applied Sciences*, 12 (18), Article 9003. <https://doi.org/10.3390/app12189003>
9. Reichmann, M., Himmelbauer, G. S., Wagner, A., Zajicek, J., Stadlmann, B., Furian, N., & Vössner, S. (2025). Introducing the concept of grades of automation for shunting operations. *Journal of Rail Transport Planning & Management*, 33, Article 100500. <https://doi.org/10.1016/j.jrtpm.2024.100500>
10. Yu, Z., Wang, H., & Chen, F. (2023). Security of railway control systems: A survey, research issues and challenges. *High-Speed Railway*, 1 (1), 6–17. <https://doi.org/10.1016/j.hspr.2022.12.001>
11. Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2023). A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, Advance online publication. <https://doi.org/10.1177/09544097221089389>
12. Hunter, J., McDermid, J., & Burton, S. (2024). Safety analysis of autonomous railway systems: An introduction to the SACRED methodology. *arXiv*. <https://doi.org/10.48550/arXiv.2403.12114>
13. Abukeshek, M., Al-Mhiqani, M., Parkinson, S., Khan, S., & Bearfield, G. (2026). Cybersecurity in intelligent railway systems: Taxonomy, research trends, challenges, and future directions. *Computers & Electrical Engineering*, Article 110994. <https://doi.org/10.1016/j.compeleceng.2026.110994>
14. Soderi, S., Masti, D., & Zacchia Lun, Y. (2023). Railway cyber-security in the era of interconnected systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, Advance online publication. <https://doi.org/10.1109/TITS.2023.3254442>
15. Adhena, H. H., Serdiuk, T., Thomas, D., & Greedy, S. (2023). Comparison of Great Britain and Ukraine railway systems based on their EMC capability and electrification systems. *2023 IEEE 7th Global Electromagnetic Compatibility Conference (GEMCCON)*. <https://doi.org/10.1109/GEMCCON57842.2023.10078193>
16. Havryliuk, V. (2020). Detecting of signal distortions in cab signalling system using ANFIS and WPESE. *2020 IEEE 4th International Conference on Intelligent Energy and Power Systems (IEPS)*. <https://doi.org/10.1109/IEPS51250.2020.9263165>
17. Havryliuk, V. (2023). Choice of the parameters of an EMI monitoring system for an AC traction network. *2023 IEEE 7th Global Electromagnetic Compatibility Conference (GEMCCON)*. <https://doi.org/10.1109/GEMCCON57842.2023.10078179>

References

1. Jie, H., Zhao, Z., Zeng, Y., Chang, Y., Fan, F., Wang, C., & See, K. Y. (2024). A review of intentional electromagnetic interference in power electronics: Conducted and radiated susceptibility. *IET Power Electronics*, 17 (12), 1487–1506. <https://doi.org/10.1049/pel2.12685>

2. Wang, C., Liang, X., & Adajar, E. (2021). Evaluation and mitigation of electromagnetic interference between railways and nearby power lines: A review. *IEEE Access*, 9, 149609–149618. <https://doi.org/10.1109/ACCESS.2021.3125572>
3. Boteler, D. H. (2021). Modeling geomagnetic interference on railway signaling track circuits. *Space Weather*, 19 (1), Article e2020SW002609. <https://doi.org/10.1029/2020SW002609>
4. He, C., Shi, H., & Li, J. (2023). IDSN: A one-stage interpretable and differentiable STFT domain adaptation network for traction motor of high-speed trains cross-machine diagnosis. *Mechanical Systems and Signal Processing*, 205, Article 110846. <https://doi.org/10.1016/j.ymssp.2023.110846>
5. Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., & Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv*. <https://doi.org/10.48550/arXiv.1704.04861>
6. Krishnamoorthi, R. (2018). Quantizing deep convolutional networks for efficient inference: A whitepaper. *arXiv*. <https://doi.org/10.48550/arXiv.1806.08342>
7. Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. *Future Internet*, 14 (12), Article 363. <https://doi.org/10.3390/fi14120363>
8. González-Plaza, A., Gutiérrez Cantarero, R., Arancibia Banda, R. B., & Briso Rodríguez, C. (2022). 5G based on MNOs for critical railway signalling services: Future Railway Mobile Communication System. *Applied Sciences*, 12 (18), Article 9003. <https://doi.org/10.3390/app12189003>
9. Reichmann, M., Himmelbauer, G. S., Wagner, A., Zajicek, J., Stadlmann, B., Furian, N., & Vössner, S. (2025). Introducing the concept of grades of automation for shunting operations. *Journal of Rail Transport Planning & Management*, 33, Article 100500. <https://doi.org/10.1016/j.jrtpm.2024.100500>
10. Yu, Z., Wang, H., & Chen, F. (2023). Security of railway control systems: A survey, research issues and challenges. *High-Speed Railway*, 1 (1), 6–17. <https://doi.org/10.1016/j.hspr.2022.12.001>
11. Kour, R., Patwardhan, A., Thaduri, A., & Karim, R. (2023). A review on cybersecurity in railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, Advance online publication. <https://doi.org/10.1177/09544097221089389>
12. Hunter, J., McDermid, J., & Burton, S. (2024). Safety analysis of autonomous railway systems: An introduction to the SACRED methodology. *arXiv*. <https://doi.org/10.48550/arXiv.2403.12114>
13. Abukeshek, M., Al-Mhiqani, M., Parkinson, S., Khan, S., & Bearfield, G. (2026). Cybersecurity in intelligent railway systems: Taxonomy, research trends, challenges, and future directions. *Computers & Electrical Engineering*, Article 110994. <https://doi.org/10.1016/j.compeleceng.2026.110994>
14. Soderi, S., Masti, D., & Zacchia Lun, Y. (2023). Railway cyber-security in the era of interconnected systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, Advance online publication. <https://doi.org/10.1109/TITS.2023.3254442>
15. Adhena, H. H., Serdiuk, T., Thomas, D., & Greedy, S. (2023). Comparison of Great Britain and Ukraine railway systems based on their EMC capability and electrification systems. *2023 IEEE 7th Global Electromagnetic Compatibility Conference (GEMCCON)*. <https://doi.org/10.1109/GEMCCON57842.2023.10078193>
16. Havryliuk, V. (2020). Detecting of signal distortions in cab signalling system using ANFIS and WPESE. *2020 IEEE 4th International Conference on Intelligent Energy and Power Systems (IEPS)*. <https://doi.org/10.1109/IEPS51250.2020.9263165>

17. Havryliuk, V. (2023). Choice of the parameters of an EMI monitoring system for an AC traction network. *2023 IEEE 7th Global Electromagnetic Compatibility Conference (GEMCCON)*. <https://doi.org/10.1109/GEMCCON57842.2023.10078179>

Сотник Василь Олександрович, кандидат технічних наук, доцент, Український державний університет залізничного транспорту, 61050, м. Харків, майдан Феєрбаха, 7. Тел.: +3 80 67 573 90 25. E-mail: sotnyk.va@gmail.com. ORCID: 0000-0002-8039-1392.

Самсонкін Валерій Миколайович, доктор технічних наук, професор кафедри технологій транспорту та управління процесами перевезень, Державний університет інфраструктури та технологій, вул. Кирилівська, 9, м. Київ, Україна, 04071. E-mail: samsonkin1520mm@gmail.com. ORCID: <http://orcid.org/0000-0002-1521-2263>. Тел.: +38067-466-14-47.

Sotnyk Vasyl Oleksandrovych, Cand. of Tech. Sc., Associate Professor, Ukrainian State University of Railway Transport, Feuerbach Square, 7, Kharkiv, 61050. Tel.: +3 80 67 573 90 25. E-mail: sotnyk.va@gmail.com. ORCID: 0000-0002-8039-1392.

Samsonkin Valery Mykolayovych, Doctor of technical sciences, professor Department of transport technologies and management of transportation processes, State University of Infrastructure and Technologies, St. 9 Kyrylivska St., Kyiv, Ukraine, 04071. E-mail: samsonkin1520mm@gmail.com. ORCID: <http://orcid.org/0000-0002-1521-2263>. Tel.: +38067-466-14-47.

Дата надходження статті: 25.07.2026 р.

Дата прийняття статті до друку: 04.09.2026 р.

Дата публікації (оприлюднення) статті: 16.10.2026 р.

Стаття поширюється на умовах ліцензії Creative Commons Attribution License International CC-BY