https://publica.fraunhofer.de/handle/publica/390535 (дата звернення: 23.10.2026).
2. Miller C., Valasek C. Remote Exploitation of an Unaltered Passenger Vehicle. IOActive Whitepaper. 2015. URL: https://ioactive.com/remote-exploitation-of-an-unaltered-passenger-vehicle (дата звернення: 23.10.2026).
3. Oh Deere: Farm hardware jailbroken to run Doom. The Register. 2022. 16 Aug. URL: https://www.theregister.com/2022/08/16/john_deere_doom (дата звернення: 23.10.2026).

УДК 004.056.5:656.13/.2:621.3

Кустов В. Ф.

к.т.н., доцент, доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, Український державний університет залізничного транспорту

КІБЕРСТІЙКІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ КЕРУВАННЯ ТРАНСПОРТОМ В УМОВАХ НАВМИСНИХ І НЕНАВМИСНИХ ЕЛЕКТРОМАГНІТНИХ ВПЛИВІВ

Анотація. Розглянуто електромагнітні впливи як фізичний канал порушення кіберстійкості комп'ютерних систем керування автомобільним і залізничним транспортом. Показано, що відповідність типовим нормам електромагнітної сумісності не гарантує працездатність системи за локальних рівнів завад, не охоплених нормативною моделлю, або за навмисних електромагнітних впливів. Запропоновано розділяти ненавмисні впливи реального середовища та IEMI-атаки (навмисні електромагнітні завади), але оцінювати їх наслідки в єдиному контурі кіберстійкості. Обґрунтовано потребу поєднати вимірювання електромагнітної обстановки, випробування стійкості, функціональну безпечність, кібербезпеку, виявлення подій та відновлення функцій.

Ключові слова: кіберстійкість, електромагнітна сумісність, IEMI, транспортні системи, функціональна безпечність, інтелектуальні транспортні системи.

Постановка проблеми. Сучасні системи керування транспортом є кіберфізичними системами: програмно-апаратні засоби отримують дані про об'єкти і середовище, обмінюються ними, приймають рішення та формують керувальні дії. Конкретні технології змінюються, але функції керування, контролю, зв'язку та безпеки руху залежать від коректної роботи електронних вузлів і каналів передавання даних.

Порушення роботи таких систем може бути спричинене не лише програмними чи мережевими атаками. Електромагнітна енергія може впливати на датчики, лінії зв'язку, живлення, процесорні модулі та пам'ять, спричиняючи спотворення даних, перезавантаження, хибні спрацювання або втрату доступності. Тому її вплив є фізичним каналом загрози кіберстійкості – здатності системи протистояти порушенню, зберігати критичні функції та відновлюватися.

Мета роботи полягає у формуванні спільного підходу до оцінювання навмисних і ненавмисних електромагнітних впливів на комп'ютерні системи керування транспортом та у визначенні обмежень, які виникають, коли кіберстійкість підміняють лише фактом відповідності обладнання стандартним вимогам електромагнітної сумісності (EMC).

Ненавмисні електромагнітні впливи та межі нормативної моделі. Випробування на EMC відтворюють визначені стандартом явища, частотні діапазони, рівні та критерії функціонування. Це забезпечує відтворюваність сертифікації, але не описує кожне місце експлуатації, де обстановка залежить від параметрів і відстані до джерел, конфігурації кабелів, заземлення, екранів, живлення, комутацій та резонансів конструкції.

Для транспортної інфраструктури особливо важливі локальні джерела: службовий і аварійний радіозв'язок, базові та мобільні станції, силові перетворювачі й комутації, перехідні процеси бортової мережі, імпульсні перенапруги та електростатичні розряди. Ризик підвищують близькість передавачів, щільне розміщення електронних блоків і протяжні кабельні мережі, що можуть діяти як антени. В Україні вимоги до емісії завад і несприйнятливості сигнальної та телекомунікаційної апаратури визначає ДСТУ EN 50121-4:2019 [1], також побудований на нормативній моделі середовища.

Нормативна база оновлюється: після prEN 50121-4:2025 підготовлено FprEN 50121-4:2026 – фінальний проєкт, що до 30.10.2026 перебуває на

формальному голосуванні CENELEC [2, 3]. Проте проєкти залишаються стандартами класичної EMC – установлюють межі емісії, рівні несприйнятливості та критерії функціонування під час випробувань. Вони не формують моделі електромагнітної кіберстійкості життєвого циклу, що охоплює контроль деградації, виявлення аномального або навмисного впливу, реєстрацію події та відновлення. До прийняття нової редакції чинним в Україні залишається ДСТУ EN 50121-4:2019; надалі потрібні її національне впровадження та відповідний додаток.

Водночас чинний в Україні ДСТУ IEC/TR 61000-5-6:2012 ідентичний IEC/TR 61000-5-6:2002 [4]. IEC 61000-5-6:2024 уже охоплює IEMI та електромагнітну стійкість, включно з виявленням потужних впливів і відновленням [5]. Станом на 17.09.2026 його не впроваджено як ДСТУ, тому чинна національна редакція ще не відображає ці положення.

Позитивний результат типового випробування підтверджує стійкість лише в межах прийнятої нормативної моделі. Він не доводить стійкість до вищого локального рівня поля, іншої частоти, не передбаченого виду кондуктивної завади або несприятливої комбінації впливів. Для критичних транспортних систем базові стандарти слід доповнювати вимогами, що враховують національне радіочастотне використання та умови конкретних об’єктів. Цю функцію можуть виконувати національні додатки, профілі середовища й об’єктові програми випробувань; потребу такого доповнення для завад поїзного радіозв’язку 2,13 і 2,15 МГц обґрунтовано в [6].

Окремою проблемою є збереження стійкості в часі. Сертифікація характеризує обладнання на момент перевірки, тоді як волога, старіння та інші чинники надалі можуть деградувати елементи захисту і змінити канали проникнення завад [7]. Отже, підтверджена сьогодні відповідність не гарантує збереження початкового запасу завадостійкості протягом життєвого циклу.

Навмисні електромагнітні впливи. Навмисні електромагнітні

впливи (Intentional Electromagnetic Interference, IEMI) – це цілеспрямоване генерування електромагнітної енергії для введення завад або сигналів в електронні системи та порушення їх роботи. На відміну від звичайної електромагнітної обстановки, частота, форма сигналу, місце, відстань і тривалість IEMI-атаки можуть добиратися для використання вразливості системи. IEC 61000-4-36:2020 встановлює підходи до визначення рівнів та методів випробувань обладнання і систем на стійкість до IEMI [8]. IEC 61000-5-6:2024 розглядає захист установок від зовнішніх електромагнітних впливів, включно з радіопередавачами, HEMP та IEMI, і пов'язує технічні засоби захисту з ширшим поняттям електромагнітної стійкості [5].

Для транспортних систем потенційними об'єктами впливу є бездротові канали, антенно-фідерні тракти, кабелі датчиків, лінії живлення та корпусні отвори. Дослідження залізничного радіозв'язку показало, що навіть малопотужні радіочастотні подавлювачі можуть створювати небезпечний вплив на наземно-поїзний канал, а зниження вразливості потребує спеціальних методів виявлення і протидії [9]. Для автомобільних ITS аналогічна логіка поширюється на супутникову навігацію (GNSS), стільниковий зв'язок, бездротові канали передавання даних і дорожню телематику, однак конкретні рівні та критерії мають визначатися за результатами аналізу загроз і функцій системи.

Спільна модель наслідків для транспортної системи. Походження ненавмисного EMI та IEMI різне, але ланцюг наслідків може бути однаковим: електромагнітний вплив порушує фізичний сигнал або роботу електронного вузла; програмне забезпечення отримує хибні, несвоєчасні чи відсутні дані; функція керування деградує; система переходить у безпечний стан, втрачає доступність або, за недостатньої діагностики, формує небезпечну команду. Отже, оцінювання має охоплювати не тільки факт збою пристрою, а й системний наслідок для руху, безпечності та відновлення.

Для обох класів впливів спочатку визначають критичні функції, інтерфейси й допустиму деградацію. Для реального середовища потрібні вимірювання, статистика рівнів, урахування національних частот і режимів обладнання; для IEMI – модель порушника, доступність об’єкта та можливості джерела. Обидві гілки мають завершуватися перевіркою системної реакції, а не лише електричного параметра на порту пристрою.

Напрями забезпечення кіберстійкості. Перший напрям – адекватна характеристика електромагнітного середовища: обстеження місця встановлення, виявлення близьких передавачів і силових джерел, прогнозування змін радіочастотного використання, а для рухомих об’єктів – визначення типових і граничних сценаріїв маршруту.

Другий напрям – багаторівневий захист: екранування і зонування; фільтрація та обмеження перенапруг; належне прокладання, симетрування і заземлення кабелів; резервування без спільної електромагнітної вразливості; контроль правдоподібності даних; безпечна деградація функцій. IEC 61000-5-6:2024 рекомендує розглядати захист на рівні установки, де взаємодіють будівля, кабельні вводи, екрани та обладнання [5].

Третій напрям – виявлення та відновлення. На відміну від класичного критерію EMC, кіберстійкість вимагає визначити, як система розпізнає аномальний електромагнітний вплив, відрізняє його від несправності, фіксує подію, локалізує порушену функцію та відновлюється без прихованого пошкодження даних. Дані сенсорів електромагнітної обстановки доцільно корелювати з журналами контролерів, мережевими подіями і станом функціональної безпечності.

Четвертий напрям – узгодження EMC, кібербезпеки та функціональної безпечності. Перезапуск може відновити доступність, але стерти ознаки атаки; резервний канал може мати ту саму вразливість; повторні переходи пристроїв у безпечний стан – порушити роботу

транспортної мережі. Тому випробування мають перевіряти програмний і апаратний контури за небезпечними та операційними сценаріями.

Практичні пропозиції. Для проєктування і приймання транспортних систем пропонується: 1) вести реєстр ненавмисних і навмисних електромагнітних загроз; 2) порівнювати нормативні рівні з виміряною або прогнозованою обстановкою; 3) призначати об’єктові випробування для неохоплених частот, рівнів і видів впливу; 4) задавати критерії для транспортної функції; 5) перевіряти виявлення, журналювання, безпечну деградацію та відновлення; 6) оновлювати профіль загроз у разі зміни джерел, технологій зв’язку чи конфігурації об’єкта.

Для України потрібні національні й галузеві доповнення до стандартів EMC критичної транспортної інфраструктури, засновані на вимірюваннях, параметрах діючих радіозасобів, досвіді збоїв і вимогах безпечності.

Висновки. Електромагнітний вплив є фізичним каналом порушення транспортних комп’ютерних систем і має враховуватися в оцінюванні кіберстійкості. Ненавмисні EMI та IEMI мають різні моделі загроз, але можуть однаково спотворювати дані, порушувати керування, доступність і безпечність. Для критичних систем базові вимоги EMC слід доповнювати об’єктовою оцінкою середовища, національною конкретизацією, контролем деградації захисних властивостей, аналізом IEMI, багаторівневим захистом та перевіреним відновленням.

Список використаної літератури

1. ДСТУ EN 50121-4:2019 (EN 50121-4:2016, IDT). Залізничний транспорт. Електромагнітна сумісність. Частина 4. Емісія завад і несприйнятливість сигнальної та телекомунікаційної апаратури.
2. prEN 50121-4:2025. Railway applications – EMC – Part 4: Emission and immunity of signalling and telecommunications apparatus. Draft European Standard.
3. FprEN 50121-4:2026. Railway applications – EMC – Part 4: Emission and immunity of signalling and telecommunications apparatus. Final Draft European

Standard. Formal vote, CLC/TC 9X.
4. ДСТУ IEC/TR 61000-5-6:2012. Електромагнітна сумісність. Частина 5-6. Настанови щодо встановлення устаткування та притлумлення завад. Зменшення зовнішнього електромагнітного впливу (IEC/TR 61000-5-6:2002, IDT).
5. IEC 61000-5-6:2024. Electromagnetic compatibility (EMC) – Part 5-6: Mitigation of external EM influences.
6. Кустов В. Ф., Єлізаренко А. О. Нормування і вплив завад поїзного радіозв'язку 2,13 і 2,15 МГц на порти живлення електронних пристроїв СЦБ рівнів SIL 3/4. Зб. наук. пр. УкрДУЗТ. 2026. Вип. 216. С. 289–314. DOI: 10.18664/1994-7852.216.2026.362481.
7. Кустов В. Ф., Прилипко А. А. Вплив вологості на деградацію елементів захисту і параметри каналів проникнення завад: загрози для електромагнітної сумісності і функціональної безпеки систем залізничної автоматики. Інформаційно-керуючі системи на залізничному транспорті. 2025. № 2. С. 144–158.
8. IEC 61000-4-36:2020. Electromagnetic compatibility (EMC) – Part 4-36: IEMI immunity test methods for equipment and systems.
9. Heddebaut M. et al. Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted From a Train. IEEE Trans. Electromagn. Compat. 2017. Vol. 59, No. 3. P. 845–852. DOI: 10.1109/TEMC.2016.2635259.

УДК 656.025.4:004.056

Бойко Андрій Григорович,

аспірант кафедри транспортних технологій Харківського національного автомобільно-дорожнього університету

КЛАСТЕРИЗАЦІЯ ТРАНСПОРТНО-ЛОГІСТИЧНИХ ЦЕНТРІВ У МОДЕЛЯХ КІБЕРСТІЙКОГО УПРАВЛІННЯ ДОСТАВКОЮ ЗАПАСНИХ ЧАСТИН

Анотація. Запропоновано концептуальну модель управління технологією доставки запасних частин на основі динамічної кластеризації транспортно-логістичних центрів. Модель поєднує прогнозування попиту, оцінювання ресурсів центрів і контроль достовірності інформації про замовлення та запаси. Обґрунтовано розділення логістичної кластеризації та перевірки інформаційної надійності, що дає змогу зберігати економічний зміст групування й обмежувати використання непідтверджених даних. Визначено критерій вибору технології доставки, умови переходу до резервного режиму та порядок сценарної перевірки. Очікуване практичне значення полягає у підтримці узгоджених рішень щодо поповнення запасів, консолідації відправлень і перенаправлення замовлень за зміни попиту та порушення інформаційного обміну.

Ключові слова: запасні частини, транспортно-логістичний центр, кластеризація,