DOI 10.20535/2411-1031.2026.14.1.365462
УДК 621.396.94:004.738.5:351.815

ОЛЕКСАНДР ЗАБРУДСЬКИЙ,
ОЛЕГ КОКОТОВ,
ІГОР ГЕПКО,
ІГОР САМОЙЛОВ

ТРАФІК ЗВИЧАЙНИХ КОРИСТУВАЧІВ ПРОТИ ПРОМИСЛОВОГО ТРАФІКУ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ: АНАЛІЗ ДИНАМІКИ ТА ПРОГНОЗ

У статті розглянуто трансформацію структури трафіку в сучасних мобільних мережах, об’єктом дослідження є динаміка співвідношення споживчого та індустріального (IoT/M2M) сегментів у контексті еволюції технологій від 3G до 5G та перспектив 6G. Актуальність роботи зумовлена стрімким зростанням кількості промислових сенсорів і систем управління, що створює безпрецедентне навантаження на радіочастотний ресурс. Метою статті є обґрунтування необхідності реформування системи державного регулювання спектра в Україні для забезпечення потреб цифровізації критичної інфраструктури та промисловості в період післявоєнної відбудови. На основі аналізу прогнозів провідних світових агенцій доведено неминуче домінування індустріального трафіку над споживчим до середини 2030-х років. Встановлено, що традиційні моделі ліцензування є малоефективними для гарантування наднизької затримки та безпеки, яких потребують масові IoT-рішення. У роботі сформульовано комплекс пріоритетних кроків для національного регулятора, зокрема: впровадження механізмів динамічного доступу до спектра, стимулювання розгортання приватних мереж та інтеграція нових протоколів кібербезпеки в архітектуру мереж наступних поколінь. На відміну від існуючих досліджень, що фокусуються переважно на технічних аспектах пропускної здатності, ця робота вперше комплексно поєднує аналіз структурних змін трафіку з конкретними регуляторними викликами України в контексті Індустрії 4.0. Новизна полягає у запропонованій концепції “гнучкого управління спектром” як інструменту забезпечення технологічного суверенітету, що враховує специфіку відновлення національної економіки. Реалізація запропонованих заходів дозволить створити конкурентоспроможне середовище для розвитку критичних індустріальних систем та гарантувати надійність підключення в умовах цифрової трансформації.

Ключові слова: регуляторна політика, радіочастотний спектр, індустріальний IoT (IIoT), мобільні мережі 5G/6G, Індустрія 4.0, критична інфраструктура, технологічний суверенітет.

Постановка проблеми. Радіочастотний спектр є стратегічним, обмеженим та суспільно значимим ресурсом, від ефективного управління яким залежить розвиток цифрової економіки, національної безпеки та обороноздатності держави [1]. Сучасна еволюція мобільних мереж, зокрема перехід до технологій мобільного зв’язку 5G та наступних поколінь, суттєво змінює парадигму використання спектра: від забезпечення послуг зв'язку для населення до функціонування складних машинно-орієнтованих екосистем, що становлять основу Індустрії 4.0 [2].

Аналіз останніх досліджень і публікацій. Актуальність цього дослідження зумовлена двома ключовими факторами. По-перше, світова тенденція до експоненційного зростання кількості підключених промислових пристроїв (Internet of Things, IoT, Machine-to-Machine, M2M) та обсягів даних, що ними генеруються, неминуче призводить до зміни структури навантаження на мережі [3], [4].

По-друге, для України, що переживає складну гуманітарну та економічну ситуацію і готується до масштабної повоєнної відбудови, актуальність полягає у формуванні прозорої, передбачуваної та інноваційно орієнтованої регуляторної політики у сфері управління спектром. Відбудова країни має ґрунтуватися не на відтворенні застарілих інфраструктур, а на створенні сучасної, стійкої та безпечної цифрової основи для економіки майбутнього [5].

Формулювання цілей статті. Метою цієї роботи є аналіз динаміки та прогнозу співвідношення трафіку звичайних користувачів і промислового трафіку задля обґрунтування необхідності адаптації державної регуляторної політики у сфері користування радіочастотним спектром в контексті повоєнної відбудови України.

Завданнями дослідження є:

1. Проаналізувати історичну динаміку споживчого та промислового трафіку в епохи 3G, 4G і 5G.
2. З'ясувати прогнозні показники зростання обох сегментів трафіку мобільного зв’язку.
3. Визначити ключові виклики для регуляторної політики, пов'язані з масовим впровадженням промислового IoT.
4. Розробити рекомендації щодо пріоритетних напрямів адаптації політики управління спектром в Україні з урахуванням потреб відбудови.

Виклад основного матеріалу дослідження. Порівняння трафіку звичайних (споживчих) та промислових (IoT/M2M) користувачів – це аналіз двох абсолютно різних моделей зростання трафіку мереж мобільного зв’язку. Споживчий трафік домінував протягом десятиліть, але промисловий сегмент має вибуховий потенціал, який фундаментально змінить ландшафт мобільних мереж і вимоги до радіочастотного спектра, який вони використовують.

Етап 1: Ера 3G (2000 – теперішній час) – Зародження мобільних даних. В епоху 3G концепція “промислового трафіку” в мобільних мережах була практично відсутня. Вся інфраструктура та бізнес-моделі були орієнтовані на одного кінцевого користувача – людину, що відповідало загальній архітектурі мобільних мереж того часу [6].

Споживчий трафік:

Драйвери: поява перших смартфонів, можливість перегляду веб-сторінок, завантаження електронної пошти та зображень. Цей попит стимулював операторів розгортати мережі та пропонувати перші тарифні плани для передачі даних [7].

Динаміка: повільне, але впевнене зростання. Трафік був незначним за сьогоднішніми мірками, вимірювався в мегабайтах на користувача на місяць.

Частка: практично 100% усього мобільного трафіку даних.

Промисловий трафік (M2M – Machine-to-Machine):

Драйвери: дуже нішеві застосування, такі як SMS-інформування від банкоматів, найпростіша телеметрія (наприклад, відстеження вантажівок) через GPRS. Ці рішення були першими кроками до концепції “Інтернету речей”, але ще не сформували окремого ринку [8].

Динаміка: мінімальне зростання. Трафік був настільки малим, що у глобальних звітах його практично не виділяли в окрему категорію [7].

Частка: менше 1%.

Висновок по ері 3G. Повне домінування споживчого сегмента. Промислове використання було радше експериментом, який заклав теоретичні основи для майбутнього розвитку M2M-комунікацій [8].

Етап 2: Ера 4G/LTE (2010 – теперішній час) – Вибухове зростання відео та початок IoT. Мережі 4G були створені для швидкої передачі великих обсягів даних, що стало каталізатором для споживчого трафіку та заклало фундамент для майбутнього зростання IoT.

Споживчий трафік:

Драйвери: масове поширення смартфонів і планшетів, екосистеми додатків (App Store, Google Play) і, найголовніше, відеострімінг (YouTube, Netflix) та соціальні мережі. Якість відео зростала від Standard Definition – відео зі стандартною роздільною здатністю до High Definition

– відео високої чіткості та 4K (Ultra High Definition) – відео надвисокої роздільної здатності. Саме відео стало основним драйвером, частка якого в мобільному трафіці наприкінці десятиліття перевищила 60% [9].

Динаміка: експоненційне зростання. Середнє споживання трафіку на одного користувача злетіло з сотень мегабайт до десятків гігабайт на місяць [10].

Частка: залишалася домінуючою, становлячи $\sim 95-98\%$ усього мобільного трафіку на кінець десятиліття.

Промисловий трафік (IoT):

Драйвери: з'явилися стандарти для "масового" Інтернету речей (LTE-M, NB-IoT), які були розроблені консорціумом 3GPP спеціально для підключення мільйонів датчиків з низьким енергоспоживанням та невеликими обсягами передачі даних [11]. Сфери застосування: розумні лічильники (ЖКГ), датчики в сільському господарстві, носимі пристрої, логістика.

Динаміка: почалося швидке зростання кількості підключень, але не обсягу трафіку. Типовий IoT-пристрій генерує кілобайти або мегабайти на місяць, тоді як смартфон – гігабайти. Згідно з прогнозами Cisco того періоду, до 2022 року M2M-модулі мали скласти більше половини всіх підключених до мобільних мереж пристроїв, але їхня частка в трафіку залишалася в межах $3-5\%$ [10].

Ключова відмінність: мільярди пристроїв генерували менше трафіку, ніж мільйони людей, які дивилися відео [9], [10].

Висновок по ері 4G. Споживчий трафік досяг гігантських обсягів, зміцнивши своє домінування. Промисловий сегмент почав зростати за кількістю пристроїв, але його вплив на загальний обсяг трафіку був мінімальним, що чітко розділило динаміку зростання підключень від динаміки зростання трафіку.

Етап 3: Ера 5G (Сьогодення та майбутнє) – Прискорення IoT та початок конвергенції. Мережі 5G – перший стандарт, який від початку проєктувався з урахуванням потреб промисловості [1]. Це змінює правила гри, оскільки вперше технологічні можливості (низькі затримки, висока надійність, масивне підключення) напряму орієнтовані на машинні комунікації.

Споживчий трафік:

Драйвери: подальше зростання якості відео (4K/8K), хмарний геймінг, додатки доповненої та віртуальної реальності (AR/VR).

Динаміка: зростання триває, але його темпи (у відсотках) починають сповільнюватися. База вже величезна. Згідно з Ericsson, середньомісячний трафік на смартфон у світі досягне $2 \sim 50$ ГБ до 2028 року [2].

Річний темп зростання (CAGR – Compound Annual Growth Rate): Прогнозується на рівні $15-20\%$ на найближчі роки [2], [3].

Промисловий трафік (Massive & Critical IoT):

Драйвери: 5G поділяє IoT на два ключові напрямки:

1. Massive IoT (mMTC): мільярди низькошвидкісних пристроїв (датчики, лічильники). Вони продовжують домінувати за кількістю підключень, але не за обсягом трафіку [4].
2. Critical & Broadband IoT (URLLC/eMBB): це головне джерело майбутнього зростання трафіку. Сюди належать:

– підключені автомобілі: телеметрія, інфотейнмент (інформаційно-розважальна система) і в майбутньому – обмін даними для автопілота (сотні гігабайт на автомобіль на місяць) [12];

– промислова відеоаналітика: камери на виробництві для контролю якості та безпеки, що передають відеопотоки у високій роздільній здатності [13].

– дрони та робототехніка: управління та передача даних між робототехнічними системами у реальному часі [14].

Динаміка: Вибухове зростання. Кількість пристроїв продовжує зростати на $20-25\%$ на рік [4], але, що важливіше, починає зростати середній трафік на один "просунутий" IoT-пристрій.

Річний темп зростання (CAGR): Прогнозується на рівні $30-40\%$ і вище [3, 15].

Коли промисловий трафік зрівняється зі споживчим? Це ключове питання для регуляторного планування. Незважаючи на вищі темпи зростання, промисловий трафік стартує з дуже низької бази [4], [15]. На сьогоднішній день споживчий трафік перевищує промисловий у десятки разів (орієнтовно 95% проти 5%) [3], [16]. Використовуючи прогнозовані CAGR (17% для споживачів та 35% для промисловості), можна розрахувати точку перетину [2], [3], [15]. Більшість аналітиків сходяться на думці, що в цьому десятилітті (до 2030 року) цього не станеться. Споживчий трафік, завдяки відео, все ще домінуватиме за обсягом [3], [16], [17].

Точка, коли обсяги трафіку зрівняються, залежить від швидкості впровадження "важких" промислових додатків [15], [18]. Прогнозний період, коли трафік промислових користувачів може зрівнятися з трафіком звичайних користувачів, – це середина 2030-х років (орієнтовно 2033-2038 рр.) [3], [17], [19].

Це відбудеться за виконання наступних умов:

– масове впровадження підключених автомобілів із просунутими системами допомоги водієві (ADAS) та автопілотом [12], [20];

– широке використання відеоаналітики на виробництві, в ритейлі та "розумних містах" [13], [21];

– розвиток нових бізнес-моделей, що використовують постійну передачу великих обсягів даних в промислових додатках [1], [18].

Порівняльна характеристика динаміки трафіку для різних категорій споживачів наведена у таблиці 1.

Таблиця 1 – Порівняльна характеристика динаміки трафіку для різних категорій споживачів

Епоха	**Споживчий трафік**	**Промисловий трафік (IoT/M2M)**	**Співвідношення (приблизно)**
3G	Низький (веб-серфінг, пошта)	Майже нульовий (SMS-телеметрія)	99,9% / 0,1%
4G	Величезний (HD-відео, соцмережі)	Низький (зростання кількості датчиків)	95% / 5%
5G	Дуже великий (4K/8K відео, AR/VR)	Вибухове зростання (автомобілі, відео)	Поступове зближення
Прогноз	Сповільнення темпів зростання	Продовження вибухового зростання	Рівність до середини 2030-х

Таким чином, спостерігається суттєва трансформація пріоритетів у сфері мобільних комунікацій. Якщо донедавна мережі будувалися переважно для обслуговування людської комунікації, то в майбутньому їхнє завдання розшириться та трансформується, із поступовим перенесенням центру ваги на забезпечення ефективної комунікації між машинами та пристроями IoT [1], [18]. Незважаючи на те, що обсяги людського трафіку продовжать стрімко

зростати, прогнозоване вибухове зростання трафіку від мільярдів розумних пристроїв зрештою виведе його на перше місце, радикально змінюючи профіль завантаження мереж [17], [19]. Ця зміна вимагає превентивних та продуманих дій з боку національних регуляторів.

Виклики та можливості для регуляторної політики в умовах відбудови України. Прогнозований експоненційний ріст промислового трафіку та його неминуче домінування до середини 2030-х років [2], [3], [15], [17] створюють безпрецедентні виклики та можливості для державного регулювання радіочастотного спектра в Україні. Існуюча модель управління, орієнтована перш за все на послуги зв'язку для населення та аукціонну модель ліцензування, потребує термінової та глибокої адаптації в контексті повоєнної відбудови.

Відбудова України – це історичний шанс створити не просто відновлену, а сучасну, ефективну та стійку цифрову інфраструктуру. У нових умовах радіочастотний спектр є не просто ресурсом для електронних комунікацій, а важливим елементом критичної інфраструктури для національної цифрової економіки, промисловості та безпеки [5], [21].

Специфіка українського контексту:

1. ***Вплив війни на сектор електронних комунікацій та перспективи відбудови***. Повномасштабне вторгнення, яке розпочалося в лютому 2022 року, завдало значної шкоди сектору електронних комунікацій України. Станом на 31 грудня 2023 року загальні збитки в галузі оцінювалися в понад $2 млрд, втрати – у $2,27 млрд, а потреби на відновлення – у $4,67 млрд [25].

2. ***Роль електронних комунікацій у післявоєнному відновленні***. Необхідність масштабної відбудови мереж зв'язку створює унікальну можливість для їх модернізації, інтегруючи стандарти 5G/6G та Інтернет речей (IoT). Розвиток інфраструктури електронних комунікацій є важливим чинником післявоєнного становлення економіки, особливо в умовах значних руйнувань фізичної інфраструктури, як-от транспортних магістралей та виробничих потужностей.

Саме електронні комунікації стають каталізатором економічного зростання. Вони забезпечують безперервність бізнес-процесів навіть за відсутності стаціонарних офісів, підтримуючи зв'язок між підприємствами, їхніми постачальниками та клієнтами.

Доступ до мобільного інтернету та послуг зв’язку сприяє підвищенню продуктивності праці, дає співробітникам можливість віддаленої праці, дає змогу швидко отримувати доступ до інформації та приймати управлінські рішення. Мобільний зв’язок також відіграє важливу роль у соціальній інтеграції та доступі до базових послуг (фінансових, освітніх, медичних), що є критично важливим для відновлення стабільності суспільства. З огляду на це, ефективне управління радіочастотним спектром стає фундаментальною передумовою для імплементації цих процесів.

3. ***Безпекові та технологічні виклики пов’язані з захистом критичної інфраструктури та забезпеченням технологічного суверенітету країни***.

Безпековий виклик. Відбудова критичної інфраструктури (енергетики, транспорту, водопостачання) вимагає створення “розумних»”(smart grid, smart city) та надійних систем, захищених від кібератак. Основою цих систем є безпровідні мережі.

Технологічний суверенітет. В умовах розвитку промислових застосувань мобільного зв’язку (наприклад, 5G для Індустрії 4.0, IoT, автоматизації) для України достатньо гостро стоїть проблема диверсифікації постачальників обладнання та технологій. Залежність від одного-двох глобальних виробників створює значні ризики:

– ризики безпеки: можливість технологічного саботажу, кібершпигунства або впровадження прихованих вразливостей в обладнання;

– економічні ризики: обмежена конкуренція призводить до завищення цін, ускладнює переговори та робить Україну вразливою до торговельних обмежень;

– технологічна стагнація: залежність від конкретного вендора може гальмувати впровадження нових, ефективніших рішень.

Для вирішення цих проблем Україна, крім іншого, може розглядати два ключових напряма:

– розширення адоптації відкритих стандартів (Open RAN);
– підтримку національних розробок.

Це дозволить не лише прискорити післявоєнну відбудову, а й закласти основу для довгострокового технологічного суверенітету.

Пріоритети та заходи у сфері користування спектром і регулювання ринку радіообладнання. Аналіз світових трендів свідчить про фундаментальний зсув у структурі мобільного трафіку: від домінування споживчого сегменту до експоненціального зростання промислового (IoT/M2M) трафіку. Ця зміна є визначальною для формування регуляторної політики, оскільки існуючі підходи, переважно орієнтовані на потреби споживчого сегменту (абонентів-людей), стають все більш неефективними для забезпечення потреб машинно-орієнтованої економіки та критичної інфраструктури. Враховуючи ці глобальні тенденції, а також критичну необхідність трансформації, для України процес повоєнної відбудови є унікальним вікном можливостей для створення сучасної, безпечної та інноваційної регуляторної екосистеми управління спектром, інтегрованої в європейський та світовий простір. На основі цих викликів сформовано ключові пропозиції та напрямки, які можуть бути розглянуті національним регулятором як пріоритетні.

Пріоритетні напрямки з удосконалення регулювання:

1) *Використання динамічного розподілу радіочастотного спектра*:

а) Сприяння впровадженню технологій Dynamic Spectrum Sharing (DSS). Регулятор може ініціювати політику, яка заохочуватиме спільне використання спектра (наприклад, між MNO) та динамічний перерозподіл ресурсів у режимі, близькому до реального часу, для задоволення пікових навантажень у промислових кластерах [22], [23]. Це особливо актуально для відновлення промислових зон і створення індустріальних парків.

б) Розгляд питання про виділення відокремлених частот для критичного IoT. Пропонується розглянути питання виділення окремого, захищеного фрагменту спектра (наприклад, у діапазонах 3.7-3.8 ГГц або вище) для ліцензування безпосередньо промисловим підприємствам (енергетика, залізничний транспорт, оборонний комплекс) під критично важливі застосування з особливими вимогами до надійності, затримок та безпеки [12], [22]. Це дозволить уникнути залежності від публічних мереж операторів.

2) *Забезпечення технологічного суверенітету та інтероперабельності*:

а) Формування національних профілів стандартів для промислового IoT. Активна участь у міжнародних органах стандартизації (CEPT, MCE, ETSI) з метою просування національних інтересів та розробка національних вимог до обладнання, що використовується в критичній інфраструктурі, для забезпечення його безпеки, сумісності та стійкості [21], [24].

б) Стимулювання розвитку приватних та віртуальних мереж (Private Networks). Спрощення процедур ліцензування та виділення спектра (за аналогією з діапазоном CBRS у США) для підприємств, що прагнуть до розгортання відокремлених мереж (наприклад, на відбудованих підприємствах гірськодобувної або металургійної галузі). Це підвищить гнучкість, продуктивність і безпеку промислових рішень [13], [22].

3) *Безпека та стійкість*:

а) Посилення уваги до кібербезпеки мереж IoT. Впровадження обов'язкових сертифікацій та процедур аудиту безпеки для промислових IoT-пристроїв і мережевої інфраструктури, що використовуються на критично важливих об'єктах [21], [24]. Це залишається пріоритетом номер один після досвіду збитків від кібератак на інфраструктуру.

б) Вдосконалення національної системи радіочастотного моніторингу. Розгортання сучасних систем для безперервного контролю використання спектра (радіочастотний моніторинг) з метою оперативного виявлення завад, несанкціонованого використання (зокрема, пов'язаного з можливою диверсійною діяльністю) та кібератак на промислову інфраструктуру [24].

4) *Економічна політика та стимулювання інновацій*:

а) Перегляд фіскальної політики щодо спектра. Зміщення акценту з разових платежів за ліцензії на довгострокові стимули для операторів та промислових підприємств, що інвестують у розвиток мереж для критичного IoT [18], [21]. Наприклад, зниження ліцензійних зборів за умови інвестування у відновлення інфраструктури певних регіонів.

б) Створення так званих "регуляторних пісочниць" (regulatory sandboxes). Надання тимчасових експериментальних ліцензій для тестування нових технологій та бізнес-моделей в обмежених географічних зонах (порти, індустріальні парки, "розумні" міста) [22], [23]. Це дозволить Україні стати пілотним майданчиком для інновацій в регіоні та навіть у світі.

Висновки з даного дослідження та перспективи подальших досліджень. Запропоновані пріоритети національного регулювання в галузі користування спектром (перехід до гнучкого розподілу спектра, розвиток приватних мереж, посилення кібербезпеки) спрямовані на забезпечення технологічного суверенітету, стимулювання інвестицій та створення безпечного середовища для розгортання критичної інфраструктури майбутнього.

Для державного регулятора настання ери промислового IoT означає необхідність еволюції від звичайного "адміністратора" радіочастотного спектра до активного архітектора цифрової екосистеми країни. Успішне управління цим переходом визначить конкурентоспроможність національної промисловості, стійкість критичної інфраструктури та технологічний суверенітет держави в повоєнний період. Запізнення з адаптацією нормативно-правової бази призведе до дефіциту радіочастотного спектра для перспективних галузей економіки, зниження рівня національної безпеки та технологічного відставання [3], [15], [17].

За результатами проведеного аналізу розвитку мереж мобільного зв'язку та відповідних регуляторних викликів, подальші дослідження будуть спрямовані на розробку математичних моделей спільного використання спектра в умовах стрімкого зростання кількості радіообладнання та випромінювальних пристроїв у промислових зонах і містах. Це дозволить реалізувати концепції спільного доступу до спектра (Spectrum Sharing) та динамічного управління ним для українських підприємств у межах впровадження стандартів Industry 5.0.

Внесок авторів:

– Олександр Забрудський – концептуалізація; обґрунтування методики дослідження;

– Олег Кокотов – формування ідеї; критичний аналіз міжнародних регуляторних практик; формулювання висновків;

– Ігор Гепко – аналіз та систематизація джерел, розробка теоретичного базису дослідження; наукове редагування тексту;

– Ігор Самойлов – збір і верифікація первинних даних, порівняльний аналіз споживчого та промислового трафіку.

Декларація про штучний інтелект. Під час підготовки цієї роботи автори використовували інструменти на основі штучного інтелекту (Gemini 3 Flash) виключно з метою покращення мовного стилю, перевірки граматики й орфографії, перекладу термінології та технічного оформлення бібліографічних джерел згідно зі стандартом IEEE. Після використання цих інструментів автори перевірили та відредагували контент, беручи на себе повну відповідальність за зміст статті та відсутність фактичних помилок.

Конфлікт інтересів. Автори заявляють про відсутність будь-якого конфлікту інтересів. Підтверджується, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових або особистих зв'язків, які могли б бути розцінені як такі, що здатні вплинути на

результати дослідження чи їх інтерпретацію. Робота виконана з дотриманням принципів академічної доброчесності, етичних норм наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, Recommendation -R M.2083-0, ITU, Sept. 2015. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/r-rec-m.2083-0-201509-i!!pdf-e.pdf. Accessed on: Dec. 21, 2025.

[2] Ericsson Mobility Report November 2023, Ericsson, Nov. 2023. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2023. Accessed on: Dec. 21, 2025.

[3] Cisco Annual Internet Report (2018–2023) White Paper, Cisco, Mar. 2023. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed on: Dec. 21, 2025.

[4] The Mobile Economy 2023, GSMA Intelligence, Mar. 2023. [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf. Accessed on: Dec. 21, 2025.

[5] *Угода про фінансування заходу "Підтримка ЄС для електронного урядування та цифрової економіки в Україні"*, Feb. 11, 2020. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/984_001-20#Text. Дата звернення: Dec. 21, 2025.

[6] H. Holma, and A. Toskala, *WCDMA for UMTS: HSPA Evolution and LTE, 5th ed*. Chichester, U.K.: Wiley, 2011.

[7] Ericsson Mobility Report June 2015, Ericsson, June 2015. [Online]. Available: https://www.epressi.com/media/userfiles/13896/1433253550/ericsson_mobility_report_2015_06.pdf. Accessed on: Dec. 21, 2025.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "*Internet of Things (IoT): A vision, architectural elements, and future directions*", *Future Gen. Comp. Sys.*, vol. 29, no. 7, pp. 1645-1660, Sept. 2013. doi: http://dx.doi.org/10.1016/j.future.2013.01.010.

[9] Ericsson Mobility Report June 2019, Ericsson, June 2019. [Online]. Available: https://www.ericsson.com/49da94/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf. Accessed on: Dec. 21, 2025.

[10] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast, 2017–2022 White Paper, Cisco, Feb. 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed on: Dec. 21, 2025.

[11] 3GPP Low Power Wide Area Technologies White Paper, GSMA, May 2018. [Online]. Available: www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2018/05/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf. Accessed on: Dec. 21, 2025.

[12] C-V2X Use Cases and Service Level Requirements Volume II, 5G Automotive Association (5GAA), Sept. 2022. 2026. [Online]. Available: https://5gaa.org/news/c-v2x-use-cases-volume-ii/. Accessed on: Dec. 21, 2025.

[13] Factory of the Future: 10 Industry 4.0 Dimensions, SmarterChains, 2023. [Online]. Available: https://www.smarterchains.com/industry-40-dimensions. Accessed on: Dec. 21, 2025.

[14] Verizon 5G Ultra Wideband and the future of robotics, Verizon, 2023. [Online]. Available: https://www.verizon.com/about/our-company/5g/verizon-5g-ultra-wideband-and-future-robotics. Accessed on: Dec. 21, 2025.
[15] Worldwide Global DataSphere IoT Device and Data Forecast, 2023-2027, Doc #US51667324, IDC, 2023. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=US51667324. Accessed on: Dec. 21, 2025.
[16] Nokia MBiT Index 2022: Indian mobile broadband traffic trends, Nokia, 2022. [Online]. Available: https://www.nokia.com/about-us/company/worldwide-presence/india/mbit-index-2022/. Accessed on: Dec. 21, 2025.
[17] Global Industry Vision (GIV) 2030, Huawei,2023. [Online]. Available: https://www.huawei.com/en/giv. Accessed on: Dec. 21, 2025.
[18] The Internet of Things: Catching up to an accelerating opportunity, McKinsey & Company, Nov. 2021. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-internet-of-things-catching-up-to-an-accelerating-opportunity. Accessed on: Dec. 21, 2025.
[19] Op-Ed: 5G is too good, Fierce Network, Nov. 2023. [Online]. Available: https://www.fierce-network.com/wireless/5g-too-good. Accessed on: Dec. 21, 2025.
[20] The Rise of the Vehicle of the Future, Intel, 2022. [Online]. Available: https://www.intel.com/content/www/us/en/automotive/overview.html. Accessed on: Dec. 21, 2025.
[21] Smart Factories @ Scale: Seizing the Multi-Trillion-Dollar Prize, Capgemini Research Institute, 2023. [Online]. Available: https://www.capgemini.com/insights/research-library/smart-factories-at-scale/. Accessed on: Dec. 21, 2025.
[22] Enabling wireless innovation through local licensing, Ofcom, Dec. 2022. [Online]. Available: https://www.ofcom.org.uk/manage-spectrum/spectrum-licensing/local-access-licensing. Accessed on: Dec. 21, 2025.
[23] RSPG Report on 6G Strategic Vision, RSPG25-006 FINAL, European Commission, Brussels, Feb. 12, 2025. [Online]. Available: https://radio-spectrum-policy-group.ec.europa.eu/system/files/2025-02/RSPG25-006_final_report_6G_strategic_vision.pdf. Accessed on: Dec. 21, 2025.
[24] A Guide to 5G Network Security 2.0, Ericsson, Sept. 2021. [Online]. Available: https://www.ericsson.com/4a66f8/assets/local/security/09172021-a-guide-to-5g-network-security-2.0.pdf. Accessed on: Dec. 21, 2025.
[25] Ukraine Rapid Damage and Needs Assessment 3 (RDNA3): February 2022 – December 2023, The World Bank, Feb. 2024. Дата звернення: квіт. 2, 2026. [Online]. Available: https://ukraine.un.org/sites/default/files/2024-02/UA%20RDNA3%20report%20EN.pdf. Accessed on: Dec. 21, 2025.

REFERENCES

[1] IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, Recommendation -R M.2083-0, ITU, Sept. 2015. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/r-rec-m.2083-0-201509-i!!pdf-e.pdf. Accessed on: Dec. 21, 2025.
[2] Ericsson Mobility Report November 2023, Ericsson, Nov. 2023. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2023. Accessed on: Dec. 21, 2025.

[3] Cisco Annual Internet Report (2018–2023) White Paper, Cisco, Mar. 2023. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed on: Dec. 21, 2025.

[4] The Mobile Economy 2023, GSMA Intelligence, Mar. 2023. [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf. Accessed on: Dec. 21, 2025.

[5] *Financing Agreement for the "EU Support to E-Government and the Digital Economy in Ukraine"*, Feb. 11, 2020. [Online]. Available: https://zakon.rada.gov.ua/laws/show/984_001-20#Text. Accessed on: Dec. 21, 2025.

[6] H. Holma, and A. Toskala, *WCDMA for UMTS: HSPA Evolution and LTE, 5th ed*. Chichester, U.K.: Wiley, 2011.

[7] Ericsson Mobility Report June 2015, Ericsson, June 2015. [Online]. Available: https://www.epressi.com/media/userfiles/13896/1433253550/ericsson_mobility_report_2015_06.pdf. Accessed on: Dec. 21, 2025.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "*Internet of Things (IoT): A vision, architectural elements, and future directions*", *Future Gen. Comp. Sys.*, vol. 29, no. 7, pp. 1645-1660, Sept. 2013. doi: http://dx.doi.org/10.1016/j.future.2013.01.010.

[9] Ericsson Mobility Report June 2019, Ericsson, June 2019. [Online]. Available: https://www.ericsson.com/49da94/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf. Accessed on: Dec. 21, 2025.

[10] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast, 2017–2022 White Paper, Cisco, Feb. 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed on: Dec. 21, 2025.

[11] 3GPP Low Power Wide Area Technologies White Paper, GSMA, May 2018. [Online]. Available: www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2018/05/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf. Accessed on: Dec. 21, 2025.

[12] C-V2X Use Cases and Service Level Requirements Volume II, 5G Automotive Association (5GAA), Sept. 2022. 2026. [Online]. Available: https://5gaa.org/news/c-v2x-use-cases-volume-ii/. Accessed on: Dec. 21, 2025.

[13] Factory of the Future: 10 Industry 4.0 Dimensions, SmarterChains, 2023. [Online]. Available: https://www.smarterchains.com/industry-40-dimensions. Accessed on: Dec. 21, 2025.

[14] Verizon 5G Ultra Wideband and the future of robotics, Verizon, 2023. [Online]. Available: https://www.verizon.com/about/our-company/5g/verizon-5g-ultra-wideband-and-future-robotics. Accessed on: Dec. 21, 2025.

[15] Worldwide Global DataSphere IoT Device and Data Forecast, 2023-2027, Doc #US51667324, IDC, 2023. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=US51667324. Accessed on: Dec. 21, 2025.

[16] Nokia MBiT Index 2022: Indian mobile broadband traffic trends, Nokia, 2022. [Online]. Available: https://www.nokia.com/about-us/company/worldwide-presence/india/mbit-index-2022/. Accessed on: Dec. 21, 2025.

[17] Global Industry Vision (GIV) 2030, Huawei,2023. [Online]. Available: https://www.huawei.com/en/giv. Accessed on: Dec. 21, 2025.

[18] The Internet of Things: Catching up to an accelerating opportunity, McKinsey & Company, Nov. 2021. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-internet-of-things-catching-up-to-an-accelerating-opportunity. Accessed on: Dec. 21, 2025.
[19] Op-Ed: 5G is too good, Fierce Network, Nov. 2023. [Online]. Available: https://www.fierce-network.com/wireless/5g-too-good. Accessed on: Dec. 21, 2025.
[20] The Rise of the Vehicle of the Future, Intel, 2022. [Online]. Available: https://www.intel.com/content/www/us/en/automotive/overview.html. Accessed on: Dec. 21, 2025.
[21] Smart Factories @ Scale: Seizing the Multi-Trillion-Dollar Prize, Capgemini Research Institute, 2023. [Online]. Available: https://www.capgemini.com/insights/research-library/smart-factories-at-scale/. Accessed on: Dec. 21, 2025.
[22] Enabling wireless innovation through local licensing, Ofcom, Dec. 2022. [Online]. Available: https://www.ofcom.org.uk/manage-spectrum/spectrum-licensing/local-access-licensing. Accessed on: Dec. 21, 2025.
[23] RSPG Report on 6G Strategic Vision, RSPG25-006 FINAL, European Commission, Brussels, Feb. 12, 2025. [Online]. Available: https://radio-spectrum-policy-group.ec.europa.eu/system/files/2025-02/RSPG25-006_final_report_6G_strategic_vision.pdf. Accessed on: Dec. 21, 2025.
[24] A Guide to 5G Network Security 2.0, Ericsson, Sept. 2021. [Online]. Available: https://www.ericsson.com/4a66f8/assets/local/security/09172021-a-guide-to-5g-network-security-2.0.pdf. Accessed on: Dec. 21, 2025.
[25] Ukraine Rapid Damage and Needs Assessment 3 (RDNA3): February 2022 – December 2023, The World Bank, Feb. 2024. Дата звернення: квіт. 2, 2026. [Online]. Available: https://ukraine.un.org/sites/default/files/2024-02/UA%20RDNA3%20report%20EN.pdf. Accessed on: Dec. 21, 2025.

OLEKSANDR ZABRUDSKYI,
OLEG KOKOTOV,
IHOR HEPKO,
IHOR SAMOILOV

CONSUMER VS. INDUSTRIAL TRAFFIC IN MOBILE COMMUNICATION NETWORKS: ANALYSIS OF DYNAMICS AND FORECASTING

Subject and Object of Research. The article examines the transformation of traffic structures in modern mobile networks. The object of the study is the dynamics of the ratio between consumer and industrial (IoT/M2M) segments during the evolution of 3G, 4G, and 5G technologies, including 6G perspectives.

Problem and Goal. The relevance of this work is driven by the rapid proliferation of industrial sensors and control systems, which creates unprecedented pressure on the radio frequency spectrum. The goal of the article is to substantiate the need for reforming the state spectrum management system in Ukraine to meet the digitalization needs of critical infrastructure and industry during the post-war reconstruction period. Based on forecasts from leading global research agencies, the inevitable dominance of industrial traffic over consumer traffic by the mid-2030s is proven.

Research Results. The authors found that traditional licensing models are inefficient in guaranteeing the ultra-low latency and high security required by massive IoT solutions. The paper formulates a set of priority steps for the national regulator, including: implementing dynamic spectrum access (DSA) mechanisms, stimulating the deployment of private (niche) networks, and integrating new cybersecurity protocols into next-generation network architectures.

Scientific Novelty. Unlike existing studies that focus primarily on technical throughput aspects, this paper is the first to comprehensively link the structural shift in traffic with specific regulatory challenges for Ukraine in the context of Industry 4.0. The novelty lies in the proposed "flexible spectrum management" concept as a tool for ensuring technological sovereignty, taking into account the specifics of national economic recovery. The implementation of these measures will create a competitive environment for the development of critical industrial systems and ensure connection reliability under digital transformation.

Keywords: regulatory policy, radio frequency spectrum, Industrial IoT (IIoT), 5G/6G mobile networks, Industry 4.0, critical infrastructure, technological sovereignty.

Забрудський Олександр Васильович, кандидат економічних наук, директор з адміністративних питань, Український державний центр радіочастот, Київ, Україна, ORCID 0009-0001-9540-8409, centre@ucrf.gov.ua.

Кокотов Олег Вікторович, кандидат технічних наук, доцент, начальник відділу, науково-методичний департамент, Український державний центр радіочастот, Київ, Україна, ORCID 0009-0008-3654-5121, kokotov@ucrf.gov.ua.

Гепко Ігор Олександрович, доктор технічних наук, професор, начальник відділу, науково-методичний департамент, Український державний центр радіочастот, Київ, Україна, ORCID 0000-0002-4138-021X, gepko@ucrf.gov.ua.

Самойлов Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8251-9257, samoilov1966igor@gmail.com.

Zabrudskyi Oleksandr, candidate of economic sciences, director of administrative affairs, Ukrainian state centre of radio frequencies, Kyiv, Ukraine.

Kokotov Oleh, candidate of technical sciences, associate professor, head of department, scientific and methodological department, Ukrainian state centre of radio frequencies, Kyiv, Ukraine.

Hepko Ihor, doctor of technical sciences, professor, head of department, scientific and methodological department, Ukrainian state centre of radio frequencies, Kyiv, Ukraine.

Samoilov Ihor, candidate of technical sciences, associate professor, associate professor at the department of security of state information resources, Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Стаття надійшла до редакції 08.05.2026.
Стаття прийнята до друку після рецензування 26.05.2026.
Дата оприлюднення: 26.06.2026.