International Science Journal of Engineering & Agriculture
2025; 4(3): 125-139
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20250403.11
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Сучасні технології безпровідного зв'язку у задачах автоматизації технологічних процесів

Ірина Воронко
Кафедра автоматизації та комп'ютерно-інтегровані технології транспорту/факультет інфраструктури та рухомого складу залізниць, Державний університет інфраструктури та технологій, м. Київ, Україна
ORCID 0000-0003-3599-6672

Галина Голуб
Кафедра автоматизації та комп'ютерно-інтегровані технології транспорту/факультет інфраструктури та рухомого складу залізниць, Державний університет інфраструктури та технологій, м. Київ, Україна
ORCID 0000-0002-4028-1025

Анотація: в роботі розглянуто існуючі сучасні безпровідні технології зв'язку, які значно розширюють можливості автоматизації виробничих процесів, їх основні можливості та характеристики. Впровадження таких технологій сприяє зниженню витрат на обслуговування кабельних мереж, а також дозволяє підприємствам швидко адаптуватися до змін. Безпровідні технології, такі як Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT та 5G, стають основними інструментами для впровадження розумних систем управління та моніторингу у промислових умовах. Проведений порівняльний аналіз існуючих безпровідних технологій зв'язку. Технологічний прогрес у безпровідних системах зв'язку дозволяє автоматизувати виробничі процеси на новому рівні, підвищуючи ефективність, знижуючи витрати та забезпечуючи надійну роботу обладнання у складних умовах. Розглянуто методологія оцінки ефективності безпровідних технологій. Окрему увагу приділено аспектам кібербезпеки, включаючи аналіз основних загроз (перехоплення трафіку, атаки Man-in-the-Middle, DoS/DDoS, експлуатація вразливостей безпровідних протоколів) та методів їхнього усунення (шифрування WPA3, Zero Trust Security, AI-based cybersecurity). Також розглянуто перспективи інтеграції штучного інтелекту, 6G, квантової криптографії та блокчейн-рішень для підвищення рівня захисту безпровідних мереж. Отримані результати демонструють, що використання гібридних безпровідних рішень, які комбінують різні технології, дозволяє оптимізувати промислові процеси, забезпечити високу продуктивність та мінімізувати кіберризики. Подальші дослідження будуть спрямовані на покращення енергоефективності безпровідних IoT-систем та впровадження новітніх механізмів безпеки у безпровідні промислові мережі.

Ключові слова: безпровідні мережі, Інтернет речей**,** Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT, 5G, захист даних, кібербезпека.

1. Вступ

Сучасні технології безпровідного зв'язку відіграють ключову роль у розвитку інтелектуальних систем управління технологічними процесами. В умовах переходу до Індустрії 4.0 автоматизація набуває нового значення, оскільки від неї вимагається гнучкість, мобільність і висока швидкість реагування на зміну виробничих умов. Актуальність дослідження зумовлена потребою в оптимальному виборі технологій безпровідного зв'язку для різних завдань автоматизації. У статті розглянуто сучасні стандарти безпровідного зв'язку (5G, Wi-Fi 6, ZigBee, LoRaWAN), виявлені їх переваги та обмеження в промислових

умовах. Визначено перспективи подальшого розвитку цих технологій у контексті цифрової трансформації виробництв.

2. Об'єкт і предмет дослідження

Об’єктом дослідження є безпровідні технології зв’язку, що використовуються у промислових системах автоматизації. Предмет дослідження – особливості застосування безпровідних технологій у задачах управління та моніторингу виробничих процесів.

3. Мета та задачі дослідження

Метою дослідження є аналіз можливостей і перспектив використання сучасних технологій безпровідного зв’язку для підвищення ефективності автоматизації технологічних процесів. Для досягнення цієї мети поставлено такі задачі:

– порівняти основні технології бездротового зв’язку за ключовими технічними характеристиками;

– визначити сфери їх оптимального застосування в автоматизованих системах керування.

4. Аналіз літератури

У наукових публікаціях [1–5] розглянуто технологію 5G як перспективне рішення для задач автоматизації, що потребують високої швидкості передачі даних, низької затримки та високої надійності. Автори вказують на здатність 5G забезпечити якісний зв’язок для систем реального часу, робототехніки та мобільних платформ. Наприклад, у [3] детально аналізуються режими URLLC та mMTC, які відповідають вимогам промислового Інтернету речей.

У роботах [6–9] аналізується LoRaWAN як технологія з великою зоною покриття та наднизьким енергоспоживанням, що робить її ефективною для моніторингу розподілених об’єктів та тривалого автономного функціонування сенсорів. Дослідження [7, 8] демонструють приклади застосування LoRaWAN у сільському господарстві та інфраструктурних об’єктах, підкреслюючи переваги технології у гетерогенних середовищах.

Публікації [9–11] присвячено Wi-Fi 6, який забезпечує високу пропускну здатність і ефективну роботу в умовах великої кількості підключень. У [10] аналізуються механізми OFDMA та MU-MIMO, які дозволяють зменшити затримки передачі та підвищити ефективність у насичених мережах.

Джерела [7, 8, 12-14] описують ZigBee як легку й енергоефективну технологію, зручну для розгортання локальних сенсорних мереж. В оглядах підкреслено, що ZigBee зручна для автономних IoT-сценаріїв, однак її пропускна здатність і стійкість до перешкод обмежені.

У згаданих публікаціях переважно подано ізольований аналіз переваг конкретних технологій, однак відсутній системний огляд їх ефективності в умовах реального виробництва. Лише окремі роботи вказують на обмеження певних технологій щодо масштабованості, сумісності з промисловими протоколами або специфіки середовища (наприклад, наявність металевих перешкод). Зокрема, у жодному з проаналізованих джерел не подано комплексного порівняння типових сценаріїв застосування з урахуванням параметрів затримки, енергоспоживання, спектральної ефективності та надійності.

Таким чином, аналіз літератури показує високу зацікавленість наукової спільноти в розвитку безпровідних технологій для автоматизації, однак виявляє відсутність цілісного підходу до вибору технології відповідно до конкретної задачі. Це обґрунтовує актуальність проведення узагальненого дослідження з формалізованим порівнянням характеристик основних технологій у контексті промислового використання. Водночас більшість робіт мають фрагментарний або односторонній характер. Відсутній комплексний підхід до вибору

технології під конкретну задачу автоматизації з урахуванням технічних, організаційних і економічних параметрів. Саме ця прогалина й зумовила необхідність проведення власного системного порівняння технологій у цій статті.

5. Методи досліджень

Для досягнення мети дослідження використано методи порівняльного аналізу технічних характеристик безпровідних технологій (зокрема пропускної здатності, дальності дії, стійкості до завад, енергоспоживання). Також було застосовано системний аналіз для оцінки доцільності використання кожної технології в типових задачах автоматизації.

6. Результати досліджень

На сьогодні існує багато технологій бездротового зв'язку, які застосовуються для задач автоматизації. Серед них найбільш поширеними є Wi-Fi [1, 2] та Bluetooth [1, 2], які відомі завдяки високим швидкостям передачі даних та широкому використанню в мережах загального користування. Однак, їхнє застосування в промислових умовах має певні обмеження через нестабільність у середовищах з великими перешкодами та високими вимогами до надійності [2, 4].

Більш спеціалізованим рішенням для промислових задач є технології на зразок ZigBee [1-3, 7], яка працює на низьких швидкостях передачі даних, але пропонує надзвичайно низьке енергоспоживання та високу надійність. ZigBee підтримує складні топології мереж і є ідеальним рішенням для розподілених систем керування та моніторингу.

Слід відмітити, що у промислових системах активно розвиваються технології LoRaWAN [7, 8] та NB-IoT [10, 11], що дозволяють здійснювати зв'язок з низьким енергоспоживанням, ідеально підходять для моніторингу обладнання та збирання даних з великих територій.

Розглянемо детальніше застосування безпровідних технологій у сучасній автоматизації для задач управління та моніторингу:

Wi-Fi (802.11) [1-3, 7-9] – технологія, що забезпечує високошвидкісний обмін даними (до кількох Гбіт/с). Стандарти Wi-Fi забезпечують високі швидкості передачі даних, що сягають до 9.6 Гбіт/с (802.11ax) на частотах 2.4 ГГц і 5 ГГц. У промислових умовах Wi-Fi активно використовується для забезпечення бездротового доступу до локальних мереж, передавання відео та великого обсягу даних у реальному часі. Основними перевагами Wi-Fi є [2, 7, 9]:

- Швидкість передачі даних – одна з найвищих серед безпровідних технологій.
- Поширеність – широке впровадження у всіх сферах, простота налаштування.
- Підтримку OFDMA (Orthogonal Frequency Division Multiple Access), що зменшує затримки у мережі, роблячи Wi-Fi придатним для задач реального часу.
- BSS Coloring, що мінімізує взаємні перешкоди між точками доступу в насичених безпровідних середовищах.
- Можливість роботи в діапазонах 2.4 ГГц, 5 ГГц та 6 ГГц (Wi-Fi 6E), що забезпечує більшу пропускну здатність.

Недоліками Wi-Fi для промислових застосувань є:

- Високе енергоспоживання, що обмежує використання у автономних системах.
- Вразливість до перешкод у складних промислових умовах (металеві конструкції, електромагнітні випромінювання).

Bluetooth (5.0, BLE) [1-3, 7, 8] – використовується для короткочасного обміну даними між пристроями на відстані до 100 метрів (Bluetooth 5.0). Остання версія Bluetooth 5.0 підтримує швидкість передачі до 2 Мбіт/с, а також має режим Bluetooth Low Energy (BLE) [7, 8], який значно знижує енергоспоживання, що робить цю технологію ідеальною для пристроїв, що працюють на батареях. Переваги Bluetooth:

- Низьке енергоспоживання у режимі BLE.

- Широка підтримка мобільних пристроїв.

Недоліки:

- Обмежена дальність зв'язку (до 100 метрів).
- Невисока пропускна здатність, що робить його менш придатним для задач, які потребують швидкої передачі великих обсягів даних

ZigBee [1-4, 7, 8]– це енергозберігаюча технологія, що підтримує розгалужені мережі (mesh topology), яка забезпечує високу надійність та безпеку. Швидкість передачі даних сягає 250 кбіт/с, що робить ZigBee ідеальною для систем моніторингу, але не для додатків, що вимагають високої швидкості передачі даних. ZigBee здатен підтримувати зв'язок на відстані до 100 метрів на відкритих територіях, що робить його ідеальним для використання на промислових об'єктах.

Це одна з найбільш надійних і широко використовуваних технологій у промислових системах автоматизації. Технологія дозволяє створювати великі мережі з автоматичною конфігурацією та високою відмовостійкістю. Отже, основними перевагами ZigBee є:

- Низьке енергоспоживання - дозволяє датчикам і виконавчим пристроям працювати протягом тривалого часу без заміни батарей.
- Висока надійність - використання багатоканальної передачі даних забезпечує стійкість до збоїв окремих вузлів.
- Безпека - підтримує шифрування даних за допомогою AES-128 [8], що гарантує захист мережі від несанкціонованого доступу.

Завдяки цим характеристикам ZigBee широко використовується в промислових системах для керування процесами, відстеження стану обладнання та безпеки.

Слід відмітити, що стандарт ZigBee активно застосовується в автоматизованих промислових системах та системах управління енергоресурсами. Він використовується для дистанційного керування промисловими процесами, збору даних з автономних датчиків, впроваджується в системах безпеки, домашній автоматизації та телеметрії. Завдяки своїй надійності та енергоефективності, ZigBee ідеально підходить для забезпечення зв'язку у розподілених мережах з великою кількістю вузлів.

LoRaWAN [7-9] – ця технологія дозволяє здійснювати далекобійний зв'язок на відстані до кількох десятків кілометрів при дуже низькому енергоспоживанні. Вона ідеальна для рішень IoT [5, 6] та моніторингу віддалених об'єктів, інфраструктурних систем або сільськогосподарських угідь. Основні переваги LoRaWAN:

- Дуже низьке енергоспоживання, що дозволяє пристроям працювати до 10 років на одній батареї.
- Велика дальність зв'язку, що робить технологію ідеальною для великих територій.

Недоліки:

- Низька пропускна здатність (до 50 кбіт/с), що обмежує використання для передачі великих обсягів даних.
- Висока затримка при передачі даних, що робить її непридатною для додатків реального часу.

LoRaWAN застосовується для автоматизованого зчитування даних з лічильників води, електроенергії та газу на великих територіях, з мінімальними витратами на обслуговування, у промислових зонах LoRaWAN використовується для відстеження роботи важкодоступного обладнання, контролю температури, вологості, тиску та інших параметрів. Використовується для відстеження місцезнаходження контейнерів, транспортних засобів та вантажів у реальному часі.

NB-IoT (Narrowband IoT) [10, 11] – технологія, що використовує вузькосмуговий зв'язок і є частиною стільникових мереж 4G і 5G. Вона забезпечує покриття у важкодоступних місцях та довгий термін служби батареї при передачі невеликих обсягів даних. NB-IoT використовується для моніторингу в розумних містах, системах обліку енергії, а також для інших IoT-рішень. Переваги NB-IoT:

- Широке покриття завдяки використанню стільникових мереж.
- Низьке енергоспоживання, що робить NB-IoT придатною для довгострокової роботи пристроїв.

Недоліки:

- Низька пропускна здатність (до 100 кбіт/с).
- Відносно висока затримка (до 1 секунди), що робить її непридатною для додатків реального часу

5G [12] – останнє покоління мобільних мереж, яке пропонує високі швидкості (до 10 Гбіт/с) та низьку затримку (< 1 мс), що ідеально підходить для критичних промислових додатків. Основні переваги 5G – можливість підключення мільйонів пристроїв одночасно, що є ключовим для Інтернету речей. Водночас впровадження цієї технології вимагає значних інвестицій у нову інфраструктуру.

Технологія 5G є революційною в промисловій автоматизації завдяки своїм високим показникам продуктивності. Висока пропускна здатність і мінімальні затримки роблять її ідеальною для автоматизованих систем управління, де потрібна обробка великих обсягів даних у реальному часі. Завдяки підтримці мільйонів підключених пристроїв на квадратний кілометр, 5G відкриває нові можливості для масштабованих розумних виробництв та автономних транспортних систем [12].

У порівнянні з попередніми поколіннями зв'язку, 5G забезпечує:

- Дуже низькі затримки (менше 1 мілісекунди), що дозволяє забезпечити реальний час управління технологічними процесами.
- Високі швидкості передачі даних (до 1 Тбіт/с), що значно прискорює обмін інформацією між пристроями.
- Масштабованість дозволяє одночасно підключати велику кількість пристроїв, що є критично важливим для промислового Інтернету речей.

Завдяки цим характеристикам 5G активно впроваджується у виробничі процеси для автоматизованого управління роботизованими системами, відстеженням стану обладнання та впровадженням розумних заводів.

З порівняльного аналізу (таблиця 1) видно, що кожна технологія має свої переваги та недоліки, залежно від вимог до дальності, пропускної здатності, енергоспоживання та затримки та від сфери застосування. Для задач із низькими вимогами до пропускної здатності, але високими вимогами до енергоспоживання, ідеальними є ZigBee та LoRaWAN. Для критичних додатків, які потребують передачі даних у реальному часі, найкращим вибором буде 5G, а в майбутньому 6G. Важливо, щоб підприємства обирали технологію, яка найкраще відповідає їхнім вимогам щодо надійності, швидкості та енергоспоживання. Однак у всіх випадках важливим аспектом залишається кібербезпека та захист промислових мереж.

Таблиця 1. Порівняльний аналіз технологій безпровідного зв’язку.

Технологія	Дальність	Пропускна здатність	Енергоспоживання	Затримка	Застосування
Wi-Fi (802.11)	До 100 м	До 9.6 Гбіт/с	Високе	20-30 мс	Промисловий моніторинг, передача відеоданих
Bluetooth 5.0	До 100 м	До 2 Мбіт/с	Низьке (BLE)	<50 мс	Взаємодія пристроїв, коротка дистанційна комунікація
ZigBee	До 100 м	До 250 кбіт/с	Дуже низьке	30-50 мс	Промисловий моніторинг, енергоефективні системи

Продовження таблиці 1

LoRaWAN	До 20 км	До 50 кбіт/с	Дуже низьке	Висока (сотні мс)	Віддалений моніторинг, екосистеми IoT
NB-IoT	До 10 км	До 100 кбіт/с	Низьке	<1 сек	Розумне місто, системи моніторингу, охорона
5G	До 1 км (мм-хвилі)	До 10 Гбіт/с	Відносно низьке	<1 мс	Промислова автоматизація, роботи, управління в реальному часі

Методологія оцінки ефективності безпровідних технологій. Дослідження ефективності різних безпровідних технологій у промислових умовах базується на комплексному підході, а саме багатофакторний аналіз, що включає математичне моделювання, яке дозволяє оцінити ключові параметри мережі за аналітичними виразами, порівняльний аналіз характеристик, що передбачає зіставлення пропускної здатності, затримок, надійності та енергоспоживання різних технологій, імітаційне моделювання, яке використовується для прогнозування поведінки мереж у реальних умовах експлуатації. Для оцінки ефективності безпровідних технологій використовуються такі основні показники [7, 13-20]:

1. Пропускна здатність (C), що визначає максимальну швидкість передачі даних у мережі.
2. Затримка (D), яка оцінює час доставки пакета даних від передавача до приймача.
3. Енергоспоживання (E), що є критичним фактором для автономних IoT-пристроїв.
4. Надійність (R), яка оцінюється як ймовірність безпомилкової передачі даних.
5. Коефіцієнт використання спектру (η), що визначає ефективність використання доступного радіочастотного діапазону.

Для оптимізації мереж застосовуються математичні моделі пуассонівських потоків та теорії марковських процесів, що дозволяють описати навантаження на бездротову мережу та прогнозувати її продуктивність. [13 - 15].

Пропускна здатність мережі (1) визначається за рівнянням [16, 17]:

$$\mathrm{C} = \mathrm{B} \cdot \log 2(1 + \mathrm{SNR}), \quad (1)$$

де B – ширина спектру (МГц), SNR – відношення сигнал/шум у каналі.

Для оцінки ефективності безпровідних технологій у промисловості проводять порівняльний аналіз основних параметрів:

- Wi-Fi 6 – висока пропускна здатність, але залежність від перешкод.
- 5G – висока швидкість та низька затримка.
- LoRaWAN – низьке енергоспоживання, але обмежена пропускна здатність.

Для різних безпровідних технологій значення B і SNR відрізняються. Так, Wi-Fi 6 має ширину каналу до 160 МГц і високий рівень SNR, що забезпечує високу пропускну здатність, а LoRaWAN використовує вузький канал (до 125 кГц) і працює при низькому SNR, що обмежує швидкість передачі, тоді як 5G використовує міліметрові хвилі (24-100 ГГц), що значно збільшує пропускну здатність.

Таким чином, для високошвидкісних рішень найкраще підходять Wi-Fi 6 і 5G, а для енергоефективних IoT-рішень – LoRaWAN і NB-IoT.

Затримка в безпровідних мережах (2) складається з часу передачі пакета (Tt), часу обробки пакета (Tp), часу очікування в черзі (Tq), часу розповсюдження (Td) та визначається рівнянням [18, 19]:

$$D = Tt + Tp + Tq + Td, \quad (2)$$

- Wi-Fi 6 має низьке Tt, але високе Tq через колізії у завантаженій мережі.
- 5G мінімізує всі складові D, забезпечуючи затримку менше 1 мс.
- LoRaWAN має високе Td, оскільки використовує низьку швидкість передачі.

Отже, для критичних промислових систем, де потрібна мінімальна затримка, найкращими технологіями є 5G та Wi-Fi 6.

Енергоспоживання безпровідної технології [15, 17-19] визначається формулою (3):

$$E = Pt \cdot T, \quad (3)$$

де Pt – середня потужність передавача, T – час передачі.

Для IoT-систем важливо мінімізувати E, що досягається використанням LoRaWAN, NB-IoT та BLE. Наприклад, LoRaWAN-пристрої працюють до 10 років на батареї завдяки низькій частоті передачі даних. З іншого боку, Wi-Fi та 5G споживають більше енергії, тому вони менш ефективні для автономних IoT-рішень.

Надійність мережі (2) визначається ймовірністю безпомилкової передачі даних (Pr) [20]:

$$Pr = 1 - Pe, \quad (4)$$

де Pe – ймовірність помилки передачі, залежить від співвідношення сигнал/шум.

Для високонадійних рішень потрібні технології з високими механізмами корекції помилок, 5G та Wi-Fi 6 мають низьке Pe завдяки адаптивній модуляції, а LoRaWAN та NB-IoT використовують FEC-кодування для підвищення надійності. Таким чином, для критичних застосувань (автономний транспорт, промислові системи керування) 5G є найкращим вибором.

Для оцінки ефективності безпровідних технологій у промисловості використовують імітаційне моделювання в середовищах Matlab, NS3 та Cisco Packet Tracer. Основні параметри, які аналізуються під час моделювання це кількість активних пристроїв у мережі, середній час відповіді мережі, втрати пакетів під час передачі даних.

Одним із важливих критеріїв ефективності мережі є коефіцієнт використання спектру, тобто **с**пектральна ефективність (η) [7, 16, 18], що визначається як (5):

$$\eta = \frac{C}{B}, \quad (5)$$

де C – пропускна здатність, а B – ширина каналу.

Порівняння різних технологій:

- 5G має найвищу спектральну ефективність (~10 біт/с/Гц).
- Wi-Fi 6 – до 8 біт/с/Гц.
- NB-IoT – 0.1-0.5 біт/с/Гц, оскільки працює у вузькому спектрі.

Чим вище значення η, тим ефективніше використовується частотний ресурс. Таким чином**,** 5G та Wi-Fi 6 є найбільш ефективними для високошвидкісних промислових рішень**.**

Отже, чим вища спектральна ефективність, тим краще технологія використовує частотний ресурс, що критично для розгорнутих промислових мереж.

Слід зазначити що методи підвищення ефективності мережі включають оптимізацію топології розташування точок доступу, використання AI-алгоритмів для розподілу ресурсів, застосування технологій SDN (Software-Defined Networking) для динамічного керування мережею.

Подальший розвиток методів оцінки ефективності безпровідних технологій передбачає розширення математичних моделей з урахуванням параметрів кібербезпеки, інтеграцію механізмів машинного навчання для адаптивного управління трафіком та застосування гібридних рішень для забезпечення оптимального балансу між швидкістю передачі даних, енергоефективністю та надійністю безпровідних мереж у промислових умовах.

Інтеграція безпровідних систем у промислову автоматизацію. Зі стрімким розвитком Industry 4.0 та підготовкою до Industry 5.0 [5, 6] підприємства активно переходять до гнучких, адаптивних виробничих систем, де безпровідні технології відіграють центральну роль. Використання розумних сенсорів, автономних виконавчих механізмів та безпровідних комунікацій дозволяє підвищити швидкість обміну даними, зменшити витрати на кабельні мережі та створити самоорганізовані системи управління виробничими процесами.

Крім того, сучасні рішення на основі хмарних технологій дозволяють забезпечити централізоване управління та моніторинг виробничих процесів з будь-якої точки світу. Такі рішення дозволяють оптимізувати роботу обладнання, знижувати енергоспоживання та підвищувати ефективність виробництва.

Іншою тенденцією є інтеграція безпілотних літальних апаратів (БПЛА або дронів) [21] для моніторингу важкодоступних об'єктів або великих територій. Дрони, оснащені бездротовими сенсорами та камерами високої роздільної здатності, дозволяють оперативно оцінювати технічний стан обладнання, контролювати роботу об’єктів великої площі (наприклад, нафто- і газопроводів, електростанцій, або ж залізничних колій чи складів) та проводити автоматизовані інспекції. Інтеграція дронів із бездротовими мережами 5G та технологіями Edge Computing забезпечує обробку отриманих даних у режимі реального часу та швидке реагування на потенційні загрози, аварійні ситуації або відхилення у роботі обладнання.

Одним із ключових напрямів є повна автоматизація логістичних процесів за допомогою безпровідних промислових мереж (IIoT – Industrial Internet of Things) [7, 22, 23]. Завдяки інтеграції Wi-Fi 6, Bluetooth 5.3, LoRaWAN та 5G підприємства отримують можливість відстежувати переміщення матеріалів та готової продукції в реальному часі, покращуючи управління ланцюгами постачання та мінімізуючи ризики людського фактора.

Окрім логістики, автоматизовані транспортні системи все частіше використовують ультрашвидкісний бездротовий зв'язок 5G та Wi-Fi 6E, що дозволяє керувати автономними навантажувачами, роботизованими складськими системами та транспортом на виробництвах.

Ще одним важливим напрямом є розумне управління енергоспоживанням, де безпровідні мережі дозволяють здійснювати:

- Безперервний моніторинг електроспоживання у всіх виробничих зонах.
- Аналіз енерговитрат та виявлення неефективних процесів.
- Автоматичне налаштування режимів роботи обладнання для мінімізації витрат електроенергії.

Системи, що використовують NB-IoT та LoRaWAN, можуть підключати тисячі датчиків без значних витрат на інфраструктуру, що робить їх ідеальними для віддаленого моніторингу енергомереж, систем опалення та вентиляції.

Перспективи інтеграції безпровідних технологій із 6G та штучним інтелектом. Наступним кроком у розвитку промислових безпровідних мереж стане впровадження технологій 6G, які забезпечать:

- Швидкість передачі даних понад 100 Гбіт/с.
- Інтеграцію квантових комунікацій для підвищеної безпеки.
- Застосування штучного інтелекту для автономного управління мережами.

Уже сьогодні розробляються цифрові двійники (Digital Twins) [24], що працюють на основі безпровідних технологій та штучного інтелекту. Вони дозволяють створювати віртуальні копії виробничих процесів, тестувати нові підходи без фізичних змін на виробництві та прогнозувати поведінку обладнання.

Слід відмітити, що в сучасній промисловій автоматизації відбувається злиття безпровідних мереж з технологіями штучного інтелекту та машинного навчання. Ці технології допомагають ефективно управляти мережевими ресурсами, прогнозувати аварії на виробництві та оптимізувати процеси.

Отже, сучасні безпровідні системи відкривають нові можливості для автоматизації виробничих процесів, оптимізації ресурсів та підвищення рівня безпеки. Завдяки поєднанню технологій IoT, 5G, AI та хмарних обчислень підприємства отримують гнучкі, масштабовані рішення, що забезпечують високу продуктивність та адаптивність до динамічних умов ринку. Подальші дослідження у сфері 6G, інтегрованих нейромереж та квантових комунікацій створять нові перспективи для розвитку індустрії майбутнього.

Кібербезпека та захист безпровідних мереж. З розвитком безпровідних технологій зв'язку та широким впровадженням їх у промислові процеси питання кібербезпеки [23, 25] стає надзвичайно актуальним. Оскільки безпровідні мережі використовуються для передачі критично важливих даних, вони є цілями для кібератак, які можуть спричинити фінансові втрати, порушення роботи виробництва та компрометацію конфіденційної інформації. Їхня відкритість до радіочастотних атак робить їх вразливими до різноманітних кіберзагроз. Основні загрози безпеці безпровідних мереж включають перехоплення даних, атаки на доступність, підроблені точки доступу, маніпуляції з трафіком та експлуатацію вразливостей протоколів зв'язку.

1. Перехоплення даних (Eavesdropping) [26]. Оскільки безпровідні сигнали передаються через відкриті радіоканали, зловмисники можуть здійснювати перехоплення трафіку за допомогою спеціальних пристроїв (анализаторів пакетів, SDR – Software-Defined Radio [27]). Основними ризиками є використання незашифрованих або слабко зашифрованих протоколів (наприклад, WEP у Wi-Fi, старі версії Bluetooth), атаки на недостатньо захищені IoT-пристрої, які передають важливі дані у відкритому вигляді, використання відкритих або публічних мереж Wi-Fi, які легко можуть бути скомпрометовані. Застосовуються наступні методи захисту [28]:

- Використання сучасних алгоритмів шифрування (AES-256, WPA3, TLS 1.3).
- Налаштування VPN (Virtual Private Network) для шифрування трафіку.
- Відключення відкритих мереж Wi-Fi та налаштування WPA3-Enterprise для корпоративного середовища.

2. Атаки «Man-in-the-Middle» (MitM) [29, 30]. Цей тип атак передбачає перехоплення, зміну або підробку даних під час їхньої передачі між двома пристроями. Основні методи MitM є Rogue Access Point, коли зловмисники створюють Wi-Fi-мережу з таким самим ім'ям (SSID), що і штатна мережа, змушуючи пристрої підключитися до неї; ARP Spoofing та DNS Spoofing це маніпуляція таблицями маршрутизації та підміна DNS-запитів для скеровування трафіку через шкідливий сервер; Bluetooth Sniffing – атаки на пристрої, які використовують Bluetooth для передачі конфіденційних даних. Застосовані методи захисту:

- Використання шифрування E2E (End-to-End Encryption), яке унеможливлює читання трафіку навіть при його перехопленні.
- Налаштування сертифікованих точок доступу (802.1X, EAP-TLS).
- Використання детекторів фальшивих точок доступу (Wireless IDS/IPS).

3. Атаки на доступність: DoS та DDoS [31]. Зловмисники можуть перевантажити бездротову мережу, створюючи перешкоди на частотах або надсилаючи величезний обсяг непотрібного трафіку. Основні варіанти таких атак є Jamming (перешкоди у радіочастотному спектрі), тобто використання потужних передавачів для заглушення Wi-Fi, Bluetooth або ZigBee; Deauthentication Attack [32] це примусове відключення пристроїв від мережі Wi-Fi

через надсилання підроблених пакетів «відключення»; Beacon Flooding – атака на Wi-Fi, яка створює велику кількість підроблених SSID, змушуючи клієнти перевантажуватися при спробах підключення. Методи захисту:

- Використання динамічного вибору частот (DFS – Dynamic Frequency Selection).
- Впровадження автоматичного перемикання каналів у разі виявлення перешкод.
- Використання фільтрації MAC-адрес та списків довірених пристроїв.

4. Підроблені точки доступу та атаки Evil Twin [33, 34]. Атака Evil Twin передбачає створення фальшивої Wi-Fi-мережі з такою ж назвою (SSID), як у штатної точки доступу, що змушує користувачів підключатися до неї. Це дозволяє атакуючому виконувати перехоплення трафіку та крадіжку конфіденційних даних, використовувати автоматичний перехоплювач логінів та паролів через підроблені сторінки авторизації, впроваджувати вредоносний код або шпигунське ПЗ на пристрої користувачів. Методи захисту включають:

- Використання сертифікованих VPN-з'єднань для шифрування трафіку.
- Заборона підключення до відкритих Wi-Fi-мереж без додаткової перевірки.
- Використання протоколу WPA3 та автентифікації EAP-TLS.

5. Експлуатація вразливостей безпровідних протоколів. Старі та небезпечні протоколи, такі як WEP, WPA1, Bluetooth 2.0, мають критичні вразливості, які дозволяють зловмисникам легко розшифрувати передані дані. Деякі популярні атаки [35]: KRACK (Key Reinstallation Attack) це атака на WPA2, яка дозволяє розшифровувати трафік без знання пароля; BlueBorne атака на вразливості Bluetooth, що дозволяє отримати контроль над пристроєм без авторизації; BLE Spoofing – підміна BLE-пристроїв для отримання контролю над "розумними" пристроями IoT. Основні методи захисту:

- Відмова від використання застарілих стандартів шифрування (WEP, WPA1).
- Регулярне оновлення прошивок та використання патчів безпеки.
- Впровадження багатофакторної автентифікації для IoT-пристроїв.

6. Атаки на промислові безпровідні мережі (IIoT) [9, 12, 22, 36]. У сфері промислової автоматизації безпровідні технології використовуються для керування критичними процесами. Це створює нові ризики і появу атаки на LoRaWAN та NB-IoT, що можуть призвести до маніпуляції даними сенсорів; підміна сигналів у SCADA-системах, що може призвести до збоїв у виробництві; спуфінг GPS та часу, що впливає на автономні промислові системи; зараження безпровідних пристроїв вірусами (Malware, Ransomware), які можуть шифрувати дані або виводити обладнання з ладу. Пропоновані методи захисту:

- Використання фізичних апаратних модулів безпеки (HSM – Hardware Security Module).
- Впровадження AI-систем аналізу трафіку для виявлення аномальної активності.
- Використання сегментованих промислових мереж із мінімальними точками доступу в Інтернет.

Отже, основними методами забезпечення кібербезпеки є шифрування даних, використання надійних протоколів аутентифікації та регулярні оновлення програмного забезпечення. Наприклад, технологія ZigBee забезпечує шифрування даних за допомогою AES-128, що унеможливлює перехоплення інформації третіми особами [7, 8]. Сучасні промислові мережі також все частіше використовують технології блокчейн [37] для підвищення рівня безпеки та захисту даних.

Таким чином, безпека безпровідних мереж є критично важливим аспектом промислової автоматизації. Використання сучасних методів шифрування, аутентифікації та сегментації мереж дозволяє мінімізувати ризики атак. Інтеграція штучного інтелекту та технологій Zero Trust Security [38] підвищує рівень захисту безпровідних інфраструктур, роблячи їх більш стійкими до сучасних кіберзагроз.

У майбутньому з розвитком Wi-Fi7, 6G [17], квантової криптографії та блокчейн-рішень з’являться нові можливості для підвищення безпеки, що стане важливим кроком у створенні стійких до атак промислових безпровідних систем.

Результати досліджень. Аналіз показав, що:

– LoRaWAN найкраще підходить для систем збору телеметричних даних із великої кількості датчиків на великій території при мінімальному енергоспоживанні;

– 5G забезпечує найвищу пропускну здатність та мінімальну затримку, що робить його придатним для систем реального часу;

– Wi-Fi 6 є доцільним у середовищах з високою щільністю пристроїв (наприклад, у цехах), де важливим є баланс між швидкістю та витратами;

– ZigBee та інші технології доцільно застосовувати у локальних мережах з автономними пристроями.

Побудована таблиця відповідності характеристик та сценаріїв використання дозволяє обґрунтувати вибір технології залежно від виробничої задачі.

7. Перспективи подальшого розвитку досліджень

Подальший розвиток безпровідних технологій у промисловій автоматизації буде пов’язаний із впровадженням передових мережевих рішень, спрямованих на підвищення швидкості, безпеки та енергоефективності. Одним із ключових напрямів є впровадження Wi-Fi 7 та 6G у промислові системи зв’язку. Очікується, що Wi-Fi 7 забезпечить швидкість до 30 Гбіт/с завдяки використанню 320 МГц каналів та модуляції 4096-QAM, що дозволить значно підвищити ефективність безпровідних промислових мереж. Водночас 6G зможе використовувати терагерцовий діапазон (0,1–10 ТГц), що забезпечить затримку менше 0,1 мс та інтеграцію з квантовими комунікаціями для підвищення безпеки.

Окрім швидкості передачі даних, ключовою проблемою залишається енергоефективність безпровідних IoT-пристроїв. Подальші дослідження зосередяться на розробці алгоритмів адаптивного енергоспоживання, зокрема Self-Sustaining Wireless Networks (SSWN), що використовують Harvesting Technology. Це дозволить створювати автономні IoT-пристрої, що працюватимуть без потреби в заміні батареї.

Ще одним важливим напрямом є інтеграція квантової криптографії у безпровідні мережі. Сучасні методи шифрування WPA3 та TLS 1.3 ефективні, але не гарантують захисту від атак квантових комп’ютерів. Протоколи Quantum Key Distribution дозволять створити універсальну захищену архітектуру для IoT та промислових безпровідних мереж.

Важливим аспектом також стане використання штучного інтелекту для управління безпровідними мережами. AI-алгоритми будуть застосовуватися для аналізу та прогнозування кіберзагроз у режимі реального часу, автоматичного налаштування частотних ресурсів у динамічних промислових середовищах, оптимізації маршрутизації трафіку для мінімізації затримок та втрат пакетів.

Також перспективним напрямом є впровадження блокчейн-рішень у промислові бездротові системи. Блокчейн дозволить гарантувати автентичність IoT-пристроїв, виключаючи можливість підміни даних, забезпечити децентралізований контроль доступу до виробничих мереж, захистити логістичні та промислові процеси від атак типу MitM.

Таким чином, майбутні дослідження будуть сфокусовані на інтеграції 6G, AI, квантової криптографії та блокчейну для підвищення надійності, безпеки та продуктивності безпровідних промислових мереж.

8. Висновки

Досліджено що, безпровідні технології стають невід'ємною частиною сучасних виробничих процесів, забезпечуючи гнучкість, ефективність та надійність. Технології, такі як ZigBee, 5G та хмарні платформи, дозволяють автоматизувати процеси на високому рівні, знижуючи витрати та підвищуючи продуктивність. Однак важливим аспектом залишається кібербезпека, яка має забезпечувати захист від новітніх загроз у цифровому середовищі. Тому

окрему увагу приділено аспектам кібербезпеки, включаючи аналіз загроз (перехоплення трафіку, атаки MitM, DoS/DDoS, експлуатація уразливостей протоколів) та ефективних методів захисту (шифрування WPA3, AI-based cybersecurity, Zero Trust Security). Проведений аналіз показує, що впровадження гібридних безпровідних рішень дозволяє зменшити витрати на інфраструктуру, покращити надійність зв'язку та мінімізувати кіберризики. У порівнянні з дротовими технологіями, безпровідні рішення пропонують швидшу інтеграцію, масштабованість та адаптивність, що є критичним для Industry 4.0 та Industry 5.0. У результаті дослідження методології оцінки ефективності безпровідних технологій визначено, що комплексний підхід, який включає математичне моделювання, порівняльний аналіз характеристик та імітаційне моделювання, є найбільш ефективним для оцінки продуктивності та надійності безпровідних мереж у промислових умовах. Встановлено, що основними критеріями оцінки є пропускна здатність, затримка, енергоспоживання, надійність та спектральна ефективність, кожен з яких має критичне значення для різних сценаріїв використання. Перспективи розвитку включають саме оптимізацію енергоспоживання IoT-пристроїв у промислових безпровідних мережах; подальше впровадження 6G, квантової криптографії та блокчейн-рішень для підвищення безпеки; розвиток AI-алгоритмів для автономного управління мережею та кіберзахисту. Встановлено, що перспективи подальших досліджень у цій галузі полягають у покращенні інтеграції безпровідних технологій із системами штучного інтелекту та підвищенні рівня безпеки для захисту виробничих процесів від кібератак.

Список літератури:

1) Danbatta S.J., Varol A. (2019). Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.

2) Naidu, G.A., & Kumar, J. (2019). Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi. *Lecture Notes in Networks and Systems. Innovations in Electronics and Communication Engineering*, 229-239.

3) Lee J. S., Su Y. W., Shen C.C. (2007) A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi, *IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society*, Taipei, Taiwan, 46-51, doi:10.1109/IECON.2007.4460126.

4) Gupta M., Singh S. (2021). A Survey on the ZigBee Protocol, It's Security in Internet of Things (IoT) and Comparison of ZigBee with Bluetooth and Wi-Fi. *Applications of Artificial Intelligence in Engineering*, 473-482.

5) Das L., Raman R., Chandan, P. Kaur A., Singh A., Rana B. D. (2023) Shivhare, Advancements in Wireless Network Technologies for Enabling the (IoT): A Comprehensive Review, *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, Gautam Buddha Nagar, India, 807-814, doi:10.1109/IC3I59117.2023.10397952.

6) Voronko, I. (2024). The security of IoT systems in railway transport. *Transport Systems and Technologies*, (43), 90–99. https://doi.org/10.32703/2617-9059-2024-43-7

7) Baronti P., Pillai P., Chook V.W.C., Chessa S., Gotta A., Fun Hu Y. (2007) Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards, *Computer Communications,* 30 (7), 1655-1695.

8) Kumar N.V., Bhuvana C., Anushya S. (2017). Comparison of ZigBee and Bluetooth wireless technologies-survey. *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, 1-4.

9) Mandanna C.M., Mrs. Suman, H., Aiyanna T. (2021). LoRaWAN: an evolution of wi-fi from short range to long range. *EPRA IJRD*, 6 (7), 611-616.

10) LTE-M vs NB-IoT – A Guide Exploring the Differences between LTE-M and NB-IoT, URL: https://iot.telenor.com/iot-insights/lte-m-vs-nb-iot-guide-differences

11) Lin H., Jung C., Huang T., Hendrick H., Wang Z. (2020). NB-IoT Application on Decision Support System of Building Information Management. *Wireless Personal Communications, 114*, 711 - 729.

12) Kengesbayeva S., Taissariyeva K., Jobalayeva G. (2023). Evaluation of the Effectiveness of IoT Implementation Based on the 5G Network. *Trudy Universiteta, 92 (3)*, 434-438.

13) Li T. at el. (2006) A new MAC scheme for very high-speed WLANs / T. Li, Q. Ni, D. Malone, D. Leith, Y. Xiao, T. Turletti / *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Buffalo-NY, USA, June 2006*, 171-180.

14) Litvinov A. L. (2018) Teoriya sistem masovogo obslugovuvannya /*HarkIv:* HNUMG im. O. M. Beketova, 141 s. [in Ukranian]

15) Zaharchenko M.V ta in. (2010) Matematichns osnovi optimizatsiyi telekomunikatsiynih sistem: pidruchnik / *Zaharchenko M.V., Gorohov S.M., Balan M.M., Gadzhiev M.M., Korchinskiy V.V., Lozhkovskiy A.G. Odesa: ONAZ im. O.S. Popova*, 240 s. [in Ukranian]

16) Lazebniy V.S. ta in. (2018) Doslidzhennya realnoyi propusknoyi spromozhnosti bezprovodovoyi informatslynoyi merezhi spetsifikatsiyi IEEE 802.11n/ *Lazebniy V.S., In Chenlyan, Omelyanets O.O. / Vcheni zapiski Tavriyskogo natsionalnogo universitetu im. V.I.Vernadskogo Seriya: Tehnichni nauki*, 29 (68). No.5 Chastina 1, 155-160. [in Ukranian]

17) ITU-T, FG NET-2030 Technical Report on Network 2030. (2020) *Additional Representative Use Cases and Key Network Requirements for Network 2030 (June 2020).* URL: www.itu.int/dms_pub/itu-t/opb/fg/T-FG-NET2030-2020-SUB.G1-PDF-E.pdf

18) 18) Zhurakovskiy B. Yu., Zeniv I.O. (2020) Komp'yuterni merezhi: *navch. posib*. Kiyiv: KPI im. Igorya SIkorskogo, 336 s. [in Ukranian]

19) Krivchenkov A., Sedykh D.(2015) Analysis Of Packets Delay In Wireless Data Networks / *Transport and Telecommunication*, 16(4), 330–340.

20) Laktionov, I., Zhabko, O., Diachenko, G. (2024). Rezultaty analizu efektyvnosti bezdrotovykh tekhnolohii obminu danymy pid chas pobudovy informatsiinykh system ahromonitorynhu. *Computer Science, Software Engineering and Cyber Security*, 3, 108–115, DOI: https://doi.org/10.32782/IT/2024-3-11

21) Sakovskiy A.A. ta In. (2022) Osoblivosti zastosuvannya bezpilotnih litalnih aparatIv organami ta pidrozdilami politsiyi / A.A. Sakovskiy, S.M. Naumenko, S.I. Kravchenko, I. M. EfImenko ta in. Kiyiv: Nats. akad. vnutr. sprav, 72 s. [in Ukranian]

22) Zhurakovskiy B. Yu. Zeniv I.O. (2021). Tehnologiyi internetu rechey: navch. posib. Kiyiv: KPI im. Igorya SIkorskogo, 271 s. [in Ukranian]

23) Jhanjhi N., Humayun M., Almuayqil S.N. (2021). Cyber security and privacy issues in Industrial Internet of Things. *Computer Systems Science and Engineering*, 37(3), 361-380. DOI: https://doi.org/10.32604/csse.2021.015206.

24) Digital Twins. URL: https://www.it.ua/knowledge-base/technology-innovation/cifrovoj-dvojnik-digital-twin.

25) He D., Chan S., Guizani M. (2017). Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring. *IEEE Wireless Communications, 24*, 98-103.

26) Gorbenko I. D. in. (2011) Metodi perehoplennya informatsiyi u sistemah kvantovoyi kriptografiyi / *I. D. Gorbenko, E. V. Ivanchenko, S. V. Karpenko, S. O. Gnatyuk / Zahist Informatsiyi*, 2, 121-129. [in Ukranian]

27) Definitions of software-defined radio (SDR) and cognitive radio system (CRS). *ITU*. URL: https://www.itu.int/pub/R-REP-SM.2152.

28) Bezdrotove shifruvannya. Viznachennya Shifruvannya BezprovIdnih Merezh. [in Ukranian] URL: https://www.vpnunlimited.com/ua/help/cybersecurity/wireless-encryption?srsltid=AfmBOorV0Ckm5GfdmfHiL9d8rKUSWW7K3R7wk6uFM6SgIH82EUrtLkgx.

29) Understanding Man-In-The-Middle Attacks. Part 3: Session Hijacking. TechGenix. URL: https://techgenix.com/understanding-man-in-the-middle-attacks-arp-part3/.

30) Kozel V. (2019) Klasifikatsiya ta rekomendatsiyi zahistu vid MITM atak / Problemi Informatsiynih tehnologIy, 25, 58-65. [in Ukranian]

31) DoS I DDoS Ataka: Zagrozi ta Zahist. [in Ukranian] URL: https://cyberset.com.ua/network/attacks-vs-defense/dos-ddos-ataka-zahist.

32) Korolkov R., Kutsak S., Voskoboinyk V.(2021) Analysis of deauthentication attack in IEEE 802.11 networks and a proposal for its detection *Visnik Harkivskogo natsionalnogo universitetu im. V. N. Karazina seriya «Matematichne modelyuvannya. Informatsiyni tehnologiyi. Avtomatizovani sistemi upravlinnya», 50*, 58-70. DOI: 10.26565/2304-6201-2021-50-06.

33) Korolkov R.Yu.,. Laptev S.O (2022) Naturne modelyuvannya ataki «WAR DRIVING» na bezdrotovu merezhu. *Kiberbezpeka: osvIta, nauka, tehnika*, 2 (18), 99-107. [in Ukranian] DOI: 10.28925/2663-4023.2022.18.99107.

34) Korolkov R.Yu. (2021) Stsenariy ataki z vikoristannyam nesanktsionovanoyi tochki dostupu u merezhah IEEE 802.11 *Kiberbezpeka: osvIta, nauka, tehnIka,* 3(11), 144-154. [in Ukranian] DOI: 10.28925/2663-4023.2021.11.144154

35) Skidan, D. Galchinskiy, L. (2024). Otsinka rivnya zahischenosti protokoiIv bezpeki dlya bezprovidnih merezh. *Collection of Scientific Papers «SCIENTIA», (June 7, 2024; Antwerp, Belgium)*, 113–117. [in Ukranian] URL: https://previous.scientia.report/index.php /archive/article/view/1893.

36) Shabala E., Korniychuk B. (2024). Metodologiya otsinyuvannya bezpeki IoT na promislovih ob'ektah. Upravlinnya rozvitkom skladnih sistem (60), 146–155. DOI: https://doi.org/10.32347/2412-9933.2024.60.146-155 [in Ukranian]

37) William P., Rai A.K., Madan P., Kumar C.P., Shrivastava A., Rana, A. (2023). Analysis of Blockchain Technology to Protect Data Access Using Intelligent Contract Mechanism for 5G Networks. *2023 6th International Conference on Contemporary Computing and Informatics (IC3I), 6*, 1651-1657.

38) Vorohob M., Kirichok R., Yaskevich V., Dobrishin Yu., Sidorenko S. (2023). Suchasni perspektivi zastosuvannya kontseptsiyi ZERO TRUST pri pobudovi politiki informatsIynoyi bezpeki pidpriemstva. *Kiberbezpeka: osvita, nauka, tehnika,* 1(21), 223-233. [in Ukranian] DOI: https://doi.org/10.28925/2663-4023.2023.21.223233.

Modern wireless communication technologies in the tasks of automation of technological processes

Iryna Voronko
Department of Automation and Computer-Integrated Transport Technologies/Faculty of Infrastructure and Railway Rolling Stock, State University of Infrastructure and Technologies, Kyiv, Ukraine
ORCID 0000-0003-3599-6672

Galyna Holub
Department of Automation and Computer-Integrated Transport Technologies/Faculty of Infrastructure and Railway Rolling Stock, State University of Infrastructure and Technologies, Kyiv, Ukraine
ORCID 0000-0002-4028-1025

Abstract: The paper examines existing modern wireless communication technologies that significantly expand the possibilities of automation of production processes, their main capabilities and characteristics. Implementing such technologies helps reduce the cost of maintaining cable networks and allows enterprises to adapt to changes quickly. Wireless technologies such as Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT, and 5G are the primary tools for implementing intelligent control and monitoring systems in industrial environments. A comparative analysis of existing wireless communication technologies is conducted. Technological progress in wireless

communication systems allows the automation of production processes at a new level, increasing efficiency, reducing costs, and ensuring reliable equipment operation under challenging conditions. Special attention is paid to aspects of cybersecurity, including an analysis of the main threats (traffic interception, Man-in-the-Middle attacks, DoS/DDoS, exploitation of wireless protocol vulnerabilities) and methods for their elimination (WPA3 encryption, Zero Trust Security, AI-based cybersecurity). The prospects for integrating artificial intelligence (AI), 6G, quantum cryptography, and blockchain solutions to improve the security of wireless networks are also considered. The results demonstrate that using hybrid wireless solutions that combine different technologies can optimize industrial processes, ensure high productivity, and minimize cyber risks. Further research will be aimed at improving the energy efficiency of wireless IoT systems and implementing advanced security mechanisms in wireless industrial networks.

Keywords: Wireless networks, Internet of Things, Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT, 5G, data security, cybersecurity.