https://doi.org/10.31891/2307-5732-2026-363-54
УДК 004.056:004.738.5:631.171

ДЬОМІНА ВІКТОРІЯ
Державний біотехнологічний університет
https://orcid.org/0000-0001-6467-5021
e-mail: 0667217120@btu.kharkov.ua
ЯРУТА ВІКТОР
Харківський національний автомобільно-дорожній університет
https://orcid.org/0000-0002-4410-2792
e-mail: victor_yaruta@ukr.net
САМОЙЛЕНКО АНТОН
Державний біотехнологічний університет
https://orcid.org/0009-0001-5905-691X
e-mail: antonsamoylenko42@gmail.com
ШАБЕЛЬНІКОВ ВОЛОДИМИР
Державний біотехнологічний університет
https://orcid.org/0009-0004-9844-196X
e-mail: vsabelnikov48@gmail.com

ІНФОРМАЦІЙНА БЕЗПЕКА ТА РИЗИКИ ФУНКЦІОНУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ У СИСТЕМАХ МОНІТОРИНГУ МОЛОЧНОЇ ФЕРМИ НА ОСНОВІ МОДЕЛЕЙ ДОВІРИ

У статті розглянуто проблематику забезпечення інформаційної безпеки та управління ризиками функціонування бездротових сенсорних мереж (БСМ) у системах моніторингу молочної ферми в умовах цифровізації тваринництва. Показано, що широке впровадження сенсорних вузлів для контролю просторової активності, фізіологічного стану тварин, параметрів мікроклімату та технологічних процесів підвищує ефективність управління виробництвом, водночас збільшуючи вразливість до кіберзагроз і ризиків порушення цілісності, доступності та достовірності даних. Особливу увагу приділено внутрішнім загрозам, зумовленим компрометацією окремих вузлів, нестабільною поведінкою сенсорів, обмеженими обчислювальними ресурсами та динамічною топологією мережі. Проаналізовано основні класи ризиків інформаційної безпеки WSN у молочному тваринництві, зокрема ризики несанкціонованого доступу, вибіркового переспрямування трафіку, маніпуляції даними, зниження якості сервісу та деградації мережевих характеристик у критичних виробничих періодах. Обґрунтовано доцільність використання моделей довіри як інструменту зниження зазначених ризиків за рахунок динамічного оцінювання надійності сенсорних вузлів і мережевих маршрутів на основі поведінкових, мережевих та подієвих ознак. Показано, що підходи на основі методів довіри доповнюють традиційні механізми захисту, зокрема криптографічні методи та системи виявлення вторгнень, і є більш придатними для ресурсно обмежених середовищ БСМ. Запропоновано узагальнену концептуальну схему інтеграції моделей довіри в архітектуру систем моніторингу молочної ферми з урахуванням ієрархії «сенсорні вузли – шлюзи – рівень обробки даних». Визначено ключові обмеження моделей довіри, пов'язані з масштабованістю, чутливістю до змін поведінки вузлів і необхідністю адаптації моделей до реальних виробничих умов. Отримані результати можуть бути використані як науково-методична основа для подальших досліджень і розроблення практичних рішень у сфері безпечного функціонування БСМ у системах цифрового моніторингу молочного тваринництва.

Ключові слова: *інформаційна безпека; бездротові сенсорні мережі; моделі довіри; оцінювання ризиків; системи моніторингу молочної ферми; хибнопозитивні та хибнонегативні спрацьовування.*

DYOMINA VIKTORIIA
State Biotechnological University
YARUTA VIKTOR
Kharkiv National Automobile and Highway University
SAMOILENKO ANTON, SHABELNIKOV VOLODYMYR
State Biotechnological University

INFORMATION SECURITY AND OPERATIONAL RISKS OF WIRELESS SENSOR NETWORKS IN DAIRY FARM MONITORING SYSTEMS BASED ON TRUST MODELS

The article focuses on information security and operational risk management of wireless sensor networks (WSNs) in dairy farm monitoring systems based on trust models. It is shown that the intensive digitalization of dairy farming, including the deployment of sensor nodes for monitoring animal location and activity, behavioral and physiological indicators, microclimate parameters, and technological processes, significantly improves management efficiency but simultaneously increases the vulnerability of WSNs to cyber threats. Particular attention is paid to internal threats arising from compromised, unstable, or malfunctioning sensor nodes that may continue to participate in data transmission and distort monitoring results under conditions of limited computational and energy resources. The study emphasizes trust models as a core mechanism for reducing information security risks in WSN-based dairy farm monitoring systems. Trust-based approaches are analyzed as methods for dynamic assessment of node and route reliability using behavioral, network-level, and event-driven features. It is demonstrated that trust models complement traditional security mechanisms, such as cryptographic protection and intrusion detection systems, while being more suitable for resource-constrained WSN environments. The integration of trust estimation into a hierarchical architecture of "sensor nodes – gateways – data processing layer" is considered as a means to improve resilience against selective forwarding, data manipulation, and long-term exploitation of compromised nodes. Special attention is devoted to the balance between false positive and false negative decisions in trust-based security mechanisms. Excessively strict trust thresholds may increase false positives, leading to unjustified exclusion of legitimate sensor nodes and disruption of continuous monitoring, whereas overly permissive thresholds raise the risk of false negatives and prolonged use of compromised nodes. The article substantiates the need for adaptive trust threshold adjustment that accounts for technological regimes of the dairy farm, biological activity periods of animals, and dynamic network

conditions. The presented results provide a scientific and methodological basis for the development of secure and reliable trust-based WSN monitoring systems in modern dairy farming.

Keywords: *information security; wireless sensor networks; trust models; risk assessment; dairy farm monitoring systems; false positive and false negative errors*.

Стаття надійшла до редакції / Received 18.02.2026
Прийнята до друку / Accepted 06.03.2026
Опубліковано / Published 26.03.2026

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

В умовах сучасного розвитку людства роль аграрного сектору неминуче посилюватиметься, оскільки постає проблема забезпечення продовольством населення планети, чисельність якого, за прогнозами, сягне піку 10,3 млрд осіб у 2084 році. [1]. Одночасно зростатиме урбанізація [2], і сільське населення зменшуватиметься з 45% до 32%.. Оскільки відбувається випереджальне зростання частки та рівня споживання продуктів тваринного походження, яке може збільшитися на 6% протягом наступного десятиліття – виникає гостра необхідність підвищення ефективності тваринницьких господарств, зокрема в молочній галузі, де продуктивність, стабільність виробництва та якість сировини безпосередньо визначають продовольчу безпеку й економічну стійкість аграрного сектору [3].

Історично підвищення продуктивності в тваринництві супроводжується інтенсифікацією виробництва та укрупненням виробничих одиниць, що корелює зі зростанням показників продуктивності на одну тварину, зокрема, надоїв на корову і підвищенням продуктивності праці [4]. Паралельно в сучасних продовольчих ланцюгах посилюється корпоративна концентрація, що сприяє більш тісній координації та інтеграції сегментів агропродовольчих систем. Водночас традиційні практики індивідуального догляду та спостереження стають менш застосовними в умовах зміни організації праці й зростання складності виробничих процесів, це підвищує ризик того, що добробут тварин може підпорядковуватися лінійній логіці підвищення ефективності, що за відсутності валідованих показників і науково обґрунтованої оцінки впливу технологій автоматизовані підходи можуть зміщувати акценти з індивідуального стану тварин на суто виробничі показники [5]. Моніторинг добробуту тварин при цьому потребує систематичних довготривалих вимірювань і інтеграції множини індикаторів (поведінкових, фізіологічних, середовищних) з урахуванням їх варіабельності впродовж життєвого циклу [6]. У молочній галузі це безпосередньо пов'язано з використанням бездротових сенсорних мереж (БСМ) для збору даних про стан тварин і параметрів середовища.

БСМ широко використовуються у тваринництві, оскільки забезпечують просторово-розподілене сенсорне спостереження із високою просторовою роздільністю без стаціонарної кабельної інфраструктури, що критично для «мокрих» зон і частих перепланувань у корівниках [7]. Низькоенергетичні стандарти та енергозбирання підтримують тривалу автономну роботу на великій площі; передача вимірювань за фактом події у поєднанні з локальним обчислювальним опрацюванням на периферії мережі зменшують трафік і затримки. Мережі самоорганізуються, підтримують мобільність і гетерогенність (стаціонарні вузли, переносні на тваринах, шлюзи), надають суцільне площинне, вибіркове точкове та лінійно-бар'єрне покриття та підвищують надійність через багатострибкові маршрути й надлишковість за збереження вимог якості та безпеки, адаптованих до обмежених ресурсів. Інтеграція з виробничими IT (наприклад, інтеграція з системами Інтернету речей), диспетчерського нагляду зі збором даних та лабораторного інформаційного менеджменту через легковагові протоколи обміну: MQTT, CoAP і 6LoWPAN забезпечує трасованість і керованість процесів у реальному часі. Економічно це знижує сукупну вартість завдяки дешевим вузлам, відсутності кабельних робіт, модульності та локальній аналітиці. У підсумку БСМ є технологічно адекватною відповіддю на вимоги молочної ферми: енергоефективний, масштабований і гігієнічно безпечний моніторинг і керування [8].

З іншого боку, застосування БСМ має декілька обмежень. Енергетика вузлів і радіопоширення у складному середовищі корівника стикається з високою вологістю, наявністю аміаку (NH_3) та сірководню (H_2S) у повітрі приміщень, їм перешкоджають елементи металоконструкцій, які спричиняють затухання та багатопроменевість, поширюють «сліпі зони» покриття. Все це впливає на затримки та втрати пакетів [9]. Надійність і гігієна сенсорів потребує додаткової уваги, бо газові й кліматичні датчики зазнають корозії, переносні модулі впливають на добробут тварин, а дотримання очисних процедур та регулярне калібрування підвищують експлуатаційні витрати [10]. Додаються ризики пов'язані з кібербезпекою, тому що обмежені ресурси вузлів звужують можливість застосування ресурсоємних криптографічних протоколів, а несинхронність журналів подій на межі між системами SCADA, IoT і системами HACCP призводить до розривів ланцюга трасованості та потенційної невідповідності вимогам аудиту [11].

Аналіз досліджень та публікацій

Застосування бездротових сенсорних мереж у молочному тваринництві з точки зору їх надійності, безпеки та стійкості до викривлення даних у складному виробничо-біологічному середовищі розглядається в багатьох наукових дослідженнях. Зокрема робота [12] присвячена питанням кібербезпеки «розумного» сільського господарства з акцентом на виявлення вторгнень у мережевому трафіку аграрних IoT та БСМ-систем. Технічна реалізація та оцінювання системи автоматизованого інтегрованого моніторингу середовища корівника і поведінки молочної худоби у режимі реального часу описана в статті [13], питання захисту

цифрового тваринництва, виявлення вторгнень в інтелектуальному сільському господарстві з урахуванням мережевих потоків у статті [14].

Надійність графів маршрутизації БСМ з їх властивостями й побудовою формалізовано у [15], приділена увага захисту даних, оцінюванню ризиків і забезпечення довіри до сенсорної інформації. Проблемам розвитку точного тваринництва в екстенсивних системах присвячений огляд [16], автори наголошують на зростаючі поширеності сенсорних технологій для моніторингу поведінки тварин, та якості пасовищ та закликають до проведення додаткових досліджень щодо інтеграції передових методів аналізу даних та технологій дистанційного зондування, включаючи граничні обчислення. У статті [17] з даної проблематики розглянут такий параметр, як аналіз питання утримання тварин у розробці та валідації етичних і достовірних інструментів оцінювання добробуту тварин на основі штучного інтелекту (AI).

Підхід до оцінювання надійності та доступності БСМ у промислових застосуваннях за умов постійних відмов пристроїв запропонований у дослідженні [18]. Автори поєднують дерева відмов з марковським моделюванням для аналізу сценаріїв збоїв і розрахунку показників відмов, що допомагає обґрунтовувати необхідну надлишковість і топологію мережі. Показано, що стійкість до відмов суттєво залежить від критичності вузлів і обраної стратегії резервування, а запропонована методика надає практичні орієнтири для інженерного проєктування БСМ. У статті [19] запропоновано кросрівневу архітектуру безпеки для бездротових мереж персональної зони, яка поєднує машинне навчання для виявлення аномалій та механізми запобігання вторгненням під час передавання медичних даних. Показано, що використання ML-моделей на різних рівнях мережі підвищує точність виявлення атак і зменшує ризик компрометації чутливих фізіологічних даних за наявності ресурсних обмежень сенсорних вузлів.

Ефективності виявлення вторгнень у БСМ присвячена стаття [20], запропонована гібридна модель, що поєднує метод синтетичного збільшення вибірки міноритарного класу на основі K-середніх та методів зменшення розмірності. У роботі [21] добір гіперпараметрів реалізується за допомогою алгоритму машинного навчання під назвою «випадковий ліс», що призводить до зменшення частоти хибнопозитивних спрацювань порівняно з базовими методами машинного навчання за умов обмежених обчислювальних ресурсів сенсорних вузлів. Загрози інформаційної безпеки у БСМ розглянуто у дослідженні [22], а стаття [23] корисна насамперед як архітектурно-функціональний шаблон побудови підсистеми безпеки для системи управління БСМ. Запропонована функціональна модель підсистеми безпеки дає підстави формалізувати склад і взаємодію базових функцій захисту (ідентифікація та автентифікація, контроль доступу, моніторинг подій, виявлення інцидентів, забезпечення цілісності та керування політиками) на рівні керування мережею, а не лише на рівні окремих вузлів.

У статті [24] запропоновано динамічну модель оцінювання довіри для БСМ, що базується на методах машинного навчання та враховує змінну поведінку вузлів у часі. Підкреслюється, що за високих показників якості алгоритмів їх ефективність у реальному часі в умовах гетерогенних мережевих середовищ залишається обмеженою. Середовище молочної ферми критично до таких зауважень, бо кількість вузлів (мітки, датчики в приміщеннях, шлюзи) і подій (переміщення, годівля, доїння) швидко зростає. Застосування кластеризації k-середніх повинно зменшити розмірність, але такі зміни розподілів даних у часі підвищує ризик деградації якості. У статті [25] розглянуто підхід до маршрутизації в бездротових сенсорних мережах, у якому довіра до вузлів використовується як ключовий параметр прийняття маршрутних рішень**.** Автори пропонують механізм оцінювання надійності сенсорних вузлів на основі їхньої поведінки та інтегрують цей показник у процес вибору маршрутів для підвищення цілісності й достовірності переданих даних. Серед основних недоліків підходу слід відзначити додаткові обчислювальні та комунікаційні витрати, пов’язані з постійним обчисленням і поширенням показників довіри між вузлами. Крім того, модель є чутливою до on–off-атак і атак змови, за яких шкідливі вузли можуть тимчасово поводитися коректно або взаємно підтверджувати довіру. Крім того, у роботі недостатньо висвітлено вплив хибнопозитивних і хибнонегативних рішень на прикладні наслідки, що ускладнює оцінювання ризиків у реальних динамічних умовах експлуатації БСМ.

Формулювання цілей статті

Метою роботи є розроблення та наукове обґрунтування підходів до забезпечення інформаційної безпеки й зниження ризиків функціонування бездротових сенсорних мереж у системах моніторингу молочної ферми шляхом використання моделей довіри та методів машинного навчання з урахуванням ресурсних обмежень сенсорних вузлів і динамічних виробничо-біологічних умов.

Виклад основного матеріалу

Робота БСМ молочної ферми будується як багаторівнева система, що складається з сенсорних вузлів, голов кластерів, маршрутизаторів та шлюзів передавання даних до рівня обробки. Об’єднання сенсорних вузлів у кластери за просторовою локалізацією та функціональним призначенням забезпечує зменшення енергетичних витрат і мережевого трафіку. (рис. 1). Кластеризація забезпечує локальну агрегацію даних, скорочує кількість прямих передавань до шлюзу та підвищує масштабованість мережі. Така архітектура створює передумови для зниження ризиків порушення цілісності та достовірності даних, а також для підвищення рівня кібербезпеки мережі за рахунок локалізації загроз і контролю обміну даними на рівні кластерів, що є особливо важливим в умовах динамічного аграрного середовища.

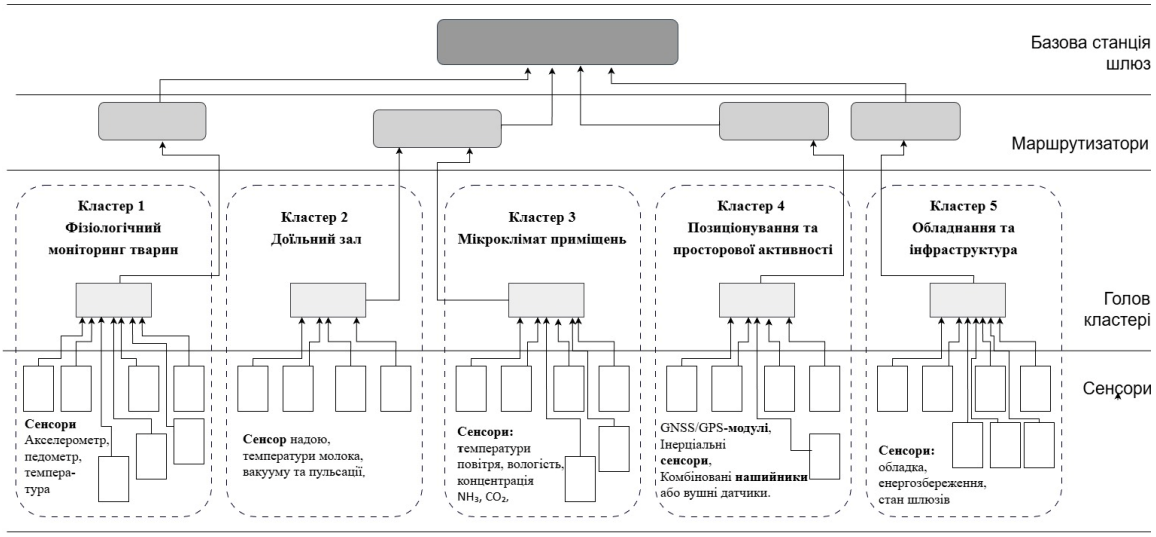

Рис. 1. Ієрархічна структура бездротової сенсорної мережі молочної ферми

Функціональна кластеризація БСМ молочної ферми дає змогу локалізувати потоки даних і тим самим знизити ризики масового викривлення інформації або поширення наслідків атак у межах усієї мережі. Виокремлення кластерів фізіологічного моніторингу тварин, контролю мікроклімату приміщень, доїльного залу та технологічної інфраструктури підвищує керованість безпеки, оскільки дозволяє враховувати специфіку загроз і критичність даних для кожної функціональної підсистеми. Такий підхід забезпечує підвищення загальної надійності БСМ за рахунок диференційованого застосування механізмів контролю та моніторингу, підвищує можливість вчасного реагування на аномальну поведінку вузлів.

У кластері фізіологічного моніторингу тварин використовуються сенсори активності, температури тіла та поведінкових параметрів, які формують часові послідовності даних, що мають надмірну чутливість до спотворення показників та порушення часової синхронізації [26]. Кластери мікроклімату, доїльного залу та інфраструктури оперують переважно телеметричними даними (показники температури, вологості, газового складу повітря, параметри доїння та стану обладнання), для яких визначальними є цілісність, узгодженість і своєчасність передавання в межах БСМ [27]. Нестабільні радіоумови та фізичні перешкоди аграрного середовища збільшують імовірність комунікаційних збоїв у БСМ, тим самим створюючи додаткові кіберризики для систем моніторингу молочної ферми [28].

Кіберзагрози для БСМ у молочному скотарстві охоплюють не тільки атаки на дані, які спотворюють вимірювання, а і атаки на мережеві сервіси для порушення зв'язку, що безпосередньо впливає на якість моніторингу та керованість виробничих процесів. До базових класів атак можна віднести ін'єкцію хибних даних, коли сенсорні вузли передають навмисно некоректні показники, а також on–off-атаки, у яких зловмисник чергує нормальну й шкідливу поведінку, знижуючи ймовірність своєчасного виявлення. Окрему групу становлять атаки на ідентичність і колективну довіру – Sybil-атаки та атаки змови, коли один вузол імітує множинні ідентичності або кілька вузлів узгоджено підтримують неправдиві дані. DoS-атаки (denial of service – відмова в обслуговуванні) спрямовані на деградацію доступності мережі через перевантаження каналів або вузлів, що підвищує ризики втрат пакетів і критичних затримок у передаванні даних.

Ризики порушення цілісності та достовірності даних у БСМ молочної ферми мають кластерно-залежний характер і визначаються типом сенсорів, частотою вимірювань і критичністю інформації для управлінських рішень. У кластері фізіологічного моніторингу тварин викривлення або підміна даних активності й температури можуть призводити до хибної діагностики стану здоров'я та несвоєчасного реагування, що робить цей кластер особливо чутливим до атак ін'єкції хибних даних і on–off-атак. Для кластера мікроклімату основними ризиками є поступове накопичення помилок або повільна зміна характеристик сенсорів у часі, які спотворюють уявлення про умови утримання та можуть залишатися непоміченими протягом тривалого часу. У доїльному залі порушення достовірності даних про надої та параметри доїння безпосередньо впливають на економічні показники та технологічні процеси, тоді як у кластері інфраструктури викривлення телеметрії обладнання підвищує ризик прихованих відмов і аварійних ситуацій.

Порушення цілісності та достовірності даних у БСМ, породжують хибні рішення, що можуть призводити до неправильного оцінювання стану здоров'я тварин і, як наслідок, до несвоєчасного лікування або необґрунтованих ветеринарних втручань. У технологічних процесах молочної ферми викривлені дані здатні спричиняти неефективне керування доїнням, мікрокліматом і використанням ресурсів, що негативно впливає на продуктивність і якість молока. З часом, накопичення таких помилок підвищує операційні витрати та знижує стабільність виробничих процесів. Крім того, систематичні помилкові рішення можуть підривати довіру до автоматизованих систем моніторингу та ускладнювати їх подальше впровадження на фермах.

Ключовими показниками для оцінювання ефективності механізмів безпеки в аграрних БСМ є FPR (false positive rate – частота хибнопозитивних рішень) і FNR (false negative rate – частота хибнонегативних рішень),

оскільки вони безпосередньо відображають баланс між чутливістю та надійністю виявлення загроз [21]. Високі значення FPR призводять до помилкового виключення коректних сенсорних вузлів, що знижує повноту даних і може порушувати безперервність моніторингу на фермі. Натомість підвищений FNR означає пропуск шкідливих або скомпрометованих вузлів, що створює ризик тривалого використання викривлених даних у процесах управління стадом і технологічними операціями. Таким чином, мінімізація FNR за прийнятного рівня FPR є критичною вимогою для забезпечення надійності та безпеки БСМ у молочному скотарстві.

Під час вибору методів забезпечення безпеки даних у бездротових сенсорних мережах доцільно враховувати обмеження традиційних криптографічних і сигнатурних підходів, ефективність яких суттєво знижується в умовах наявності внутрішніх загроз або компрометованих сенсорних вузлів. У таких випадках формальна коректність протокольної взаємодії не гарантує достовірності переданих даних, що зумовлює необхідність застосування поведінково орієнтованих механізмів безпеки. Моделі динамічної оцінки довіри, ґрунтуючись на аналізі фактичної поведінки вузлів у процесі їх взаємодії, дозволяють виявляти аномальні та потенційно шкідливі відхилення навіть за відсутності явних порушень протоколів. Це є особливо актуальним для БСМ молочної ферми, де сенсорні пристрої функціонують у змінному виробничо-біологічному середовищі, мають обмежені обчислювальні ресурси та можуть бути фізично доступними для втручання. Таким чином, оцінювання довіри формує адаптивну й ресурсоефективну основу для зниження ризиків викривлення даних і підвищення надійності функціонування кластеризованої сенсорної мережі.

У динамічних бездротових сенсорних мережах рівень довіри до вузлів не є сталим і має коригуватися з урахуванням часового згасання попередніх взаємодій за відрізок часу $[t_1, t_2]$. Застосування механізмів часового згасання дозволяє зменшувати вплив застарілих спостережень і підвищувати чутливість моделі до актуальної поведінки сенсорних вузлів, що є особливо важливим для виявлення on–off-атак. Адаптивне зважування взаємодій передбачає динамічну зміну ваг окремих спостережень $w_m, m = 1,2, \dots, N^w$, де $N^w -$ кількість спостережень) залежно від їхньої надійності, частоти та контексту функціонування кластера. Поєднання цих підходів забезпечує баланс між стабільністю оцінювання довіри та здатністю моделі оперативно реагувати на зміни поведінки вузлів у БСМ молочної ферми.

Інтегральний показник довіри вузла формується шляхом поєднання прямих і непрямих оцінок довіри з урахуванням їх часової актуальності та надійності джерел [24]. Для цього окремі компоненти довіри агрегуються з використанням адаптивних ваг, що дозволяє враховувати специфіку функціонування кластера та інтенсивність взаємодій.

$$C_{p,q}(t) = w_m^1(t) \cdot C_{p,q}^{tr}(t) + w_m^2(t) \cdot C_{p,q}^{rep}(t), \quad (1)$$

де $C_{p,q}(t)$– інтегральний показник довіри між вузлами u_p та u_q у момент часу $t\epsilon[t_1, t_2]$; $C_{p,q}^{tr}(t)$– пряма довіра, сформована на основі власних спостережень; $C_{p,q}^{rep}(t)$ – непряма довіра (репутація), отримана шляхом агрегування рекомендацій інших вузлів або головних вузлів, кластерів; $w_m^1(t)$ – невід'ємна вага прямої довіри; $w_m^2(t)$ – невід'ємна вага непрямої довіри, причому сума цих адаптивних коефіцієнтів підпорядковується рівнянню $w_m^1(t) + w_m^2(t) = 1$; t – поточний момент часу, $t\epsilon[t_1, t_2]$.

Адаптивний коефіцієнт $w_m^1(t)$ може змінюватися залежно від кількості доступних прямих спостережень або стабільності взаємодій і, наприклад, задаватися у вигляді:

$$w_m^1(t) = \frac{M_{p,q}^{tr}(t)}{M_{p,q}^{tr}(t)+\tau},$$

де $M_{p,q}^{tr}(t)$ – кількість прямих взаємодій між вузлами u_p та u_q до моменту часу $t\epsilon[t_1, t_2]$, $\tau > 0$ – параметр згладжування, що запобігає домінуванню прямої довіри за малої кількості спостережень.

У БСМ молочної ферми така формалізація дозволяє адаптивно змінювати структуру довіри: у кластерах з інтенсивними локальними взаємодіями (фізіологічний моніторинг тварин, доїльний зал) переважає пряма довіра, тоді як у розподілених або менш активних кластерах зростає роль непрямої довіри. Подальший аналіз зосередимо на їх окремому моделюванні з метою збереження інтерпретованості та адаптивності моделі. Для розрахунку прямої довіри між вузлами p та q визначається на основі власних спостережень вузла p за поведінкою вузла q під час їхніх попередніх взаємодій у мережі. Кожна взаємодія між вузлами p та q у момент часу $t_k\epsilon[t_1, t_2]$оцінюється за допомогою показника якості/надійності:

$$Q\left(C_{p,q}^{tr}(t_k)\right) = \begin{cases} 1, \text{надійнав заємодія}, \\ 0, \text{підозріла взаємодія}, \end{cases} \quad (2)$$

де:$C_{p,q}^{tr}(t_k)$– пряма довіра, сформована на основі власних спостережень; t_k – час k-ї взаємодії.

Застосуємо експоненційну функцію згасання для підсилення ваги останніх взаємодій:

$$\xi_k = e^{-\lambda(t-t_k)},$$

де: t – поточний момент часу; t_k – час k-ї взаємодії; $\lambda > 0$ – коефіцієнт часового згасання.

Пряма довіра визначається як нормалізоване зважене середнє:

$$C_{p,q}^{tr}(t) = \frac{\sum_{k=1}^{N_\vartheta} e^{-\lambda(t-t_k)} \cdot Q\left(C_{p,q}^{tr}(t_k)\right)}{\sum_{k=1}^{N_\vartheta} e^{-\lambda(t-t_k)}}, \quad (3)$$

де $C_{p,q}^{tr}(t)$ – пряма довіра вузла p до вузла q; $Q\left(C_{p,q}^{tr}(t_k)\right)$– оцінка якості k-ї взаємодії (2); N_ϑ – кількість зафіксованих взаємодій; λ – параметр чутливості до змін поведінки, у кластерах з рухомими тваринами значення λ дозволяє балансувати між стійкістю та реактивністю моделі.

Таким чином, пряма довіра $C_{p,q}^{tr}(t)$ обчислюється як зважене середнє оцінок попередніх взаємодій із експоненційним часовим згасанням, що дозволяє враховувати актуальну поведінку сенсорного вузла та зменшувати вплив застарілих спостережень. Якщо сенсор постійно передає коректні дані, $\lim_{t\epsilon[t_1,t_2]} C_{p,q}^{tr}(t) \to 1$, якщо вузол застосовує on–off-атаку, останні аномальні взаємодії знижують значення довіри. Водночас у практичних умовах молочної ферми пряма довіра не завжди забезпечує повну та стабільну картину поведінки сенсорних вузлів через обмежену кількість прямих взаємодій і динамічний характер мережі. Тому доцільним є доповнення моделі механізмами непрямої довіри, які дозволяють враховувати колективний досвід мережі та підвищувати надійність оцінювання поведінки сенсорних вузлів у динамічних умовах молочної ферми.

Нехай V_p – множина вузлів-посередників (сусідніх сенсорних вузлів або головних вузлів (кластерів кластерних голів), з якими вузол p має достатній рівень прямої довіри та які мають власні оцінки вузла q. Тоді непряму довіру (репутацію) визначимо як вираз через рекомендаціях проміжних сенсорних вузлів, що мають попередній досвід взаємодії з обома сторонами:

$$C_{p,q}^{rep}(t) = \frac{\sum_{j=1}^{N_V} C_{p,j}(t) \cdot C_{j,q}(t)}{|V_p|}, \tag{4}$$

де $C_{p,q}^{rep}(t)$– непряма довіра між сенсорним вузлом p та сенсорним вузлом q у момент часу t; p – довіряючий вузол, який оцінює надійність іншого сенсорного вузла в мережі (наприклад, сенсор активності корови); q – оцінюваний вузол, для якого визначається рівень довіри (наприклад, сенсор температури тіла або провідності молока). V_p – множина проміжних вузлів, які мають історію взаємодій як з вузлом p, так і з вузлом q; у кластеризованій БСМ молочної ферми це, як правило, головні вузли (кластери, кластерні голови) або сусідні сенсорні вузли; $|V_p|$ – потужність множини V_p; j – індекс проміжного вузла, що належить множині V_p; $C_{p,j}(t)$ – пряма довіра (між вузлом p та проміжним вузлом q, сформована на основі їхніх попередніх взаємодій (успішність передавання пакетів, стабільність зв'язку тощо); $C_{j,q}(t)$ – пряма довіра між проміжним вузлом j та вузлом q (1); t – поточний момент або часовий інтервал оцінювання, що враховує динамічний характер поведінки сенсорних вузлів. У практичному застосуванні на молочній фермі така формула означає, що надійність сенсора (наприклад, датчика кульгавості або мікроклімату) визначається не лише його прямою взаємодією з іншими вузлами, а й репутацією всередині кластера, накопиченою головою кластера. Це знижує ризик хибних рішень у випадках локальних відмов або порушень коректної роботи окремих сенсорних вузлів.

Для прийняття автоматизованих рішень у системі виявлення потенційно небезпечних відхилень у роботі сенсорних вузлів оцінки довіри (1)-(4) потребують подальшої інтеграції в узагальнений опис поведінки сенсорного вузла, який має декілька ознак, усі компоненти якого нормалізовані в інтервалі [0,1]:

$$\Xi_q(t) = \left[C_{p,q}^{tr}(t), C_{p,q}^{rep}(t), CLR_{p,q}(t), CWR_{p,q}(t), CFD_{p,q}(t)\right], \tag{5}$$

де: $\Xi_q(t)$ – інтегральний показник сенсорного вузла q; $C_{p,q}^{tr}(t)$ – оцінка прямої довіри (3); p – вузол спостерігач, який взаємодіє з вузлом q або фіксує його поведінку в межах кластера; $C_{p,q}^{rep}(t)$ – оцінка непрямої довіри (4); $CLR_{p,q}(t)$ – показник просторової узгодженості (відстань, відповідність GPS-координатам); $CWR_{p,q}(t)$ – показник узгодженості багатоадресних взаємодій; $CFD_{p,q}(t)$ – показник частоти, тривалість і надійність кооперативних взаємодій у часі.

У періоди різких погодних коливань та фізіологічних фаз тварин, зокрема під час еструсу або сухостоя, природна варіабельність сенсорних даних істотно зростає, і, як наслідок збільшується частка хибнопозитивних спрацювань. За таких умов етап виявлення аномалій потребує адаптивного налаштування порогу класифікації, що відрізняє надійний сенсорний пристрій від хибного. Для зменшення хибнопозитивних спрацювань без втрати здатності виявляти реальні загрози задамо три класи стану вузла: $\gamma_q \in \{-1; 0; 1\}$, де відповідність між класами та інтервалами довіри задається як

$$\gamma_q = \begin{cases} 1, \Xi_q(t) \in [0{,}8; 1], \text{високонадійний сенсорний пристрій}, \\ 0, \Xi_q(t) \in [\Omega; 0{,}8), \text{легітимний (менш ризиковий) сенсорний пристрій}, \\ -1, \Xi_q(t) \in [0; \Omega), \text{шкідливий (ризиковий) сенсорний пристрій}, \end{cases} \tag{6}$$

де $\Xi_q(t)$ – інтегральний показник сенсорного вузла q; Ω – границя між легітимним та шкідливим сенсорним пристроєм. Тут інтервал $[0{,}8;\ 1]$ інтерпретується як зона високої довіри, для якої не потрібні додаткові захисні дії. Вибір порогу Ω можна пов'язати з мінімізацією хибнонегативних спрацювань для кожного кластера окремо без втрати здатності виявляти реальні загрози. Для розв'язку даної задачі багатокласового зниження ризику пропуску сенсорних вузлів із потенційно шкідливою поведінкою, що передбачає поділ вузлів на декілька станів надійності, можна застосувати метод опорних векторів за схемою One-vs-Rest (OvR) SVM із застосуванням лінійного ядра, для забезпечення коректної класифікації кожного вузла відносно сукупності альтернативних класів і одночасної економії обчислювальних ресурсів [29]. Для кожного класу $\gamma_q \in \{-1;\ 0;\ 1\}$ (6) будується розділювальна функція: $f_k(x) = w_k\phi(x) + b_k$, де $\phi(x)$ – відображення у простір ознак; w_k, b_k – параметри моделі. Стан вузла визначається як:

$$\hat{\gamma}_q = \arg \max_{k\in\{-1;\ 0;\ 1\}} f_k(\Xi_q(t)),$$

де $\hat{\gamma}_q$ – клас сенсорного вузла q у момент часу t, як результат оцінювання; q – сенсорний вузел; t – момент часу оцінювання; $\Xi_q(t)$ – вектор ознак вузла q у момент часу t (5); k – показник належності до одного з трьох класів

стану вузла, $\gamma_q \in \{-1; 0; 1\}$ (6); f_k – класифікуюча функція методу опорних векторів для класу k; $\arg\max$ – оператор вибору класу з максимальним значенням класифікуючої функції. Таким чином, інтегральний вектор ознак сенсорного вузла перетворюється на дискретний стан шляхом вибору того класу, для якого модель SVM формує найбільше значення класифікуючої функції.

Вибір порогового значення Ω у (6) здійснюється таким чином, зоб мінімізувати частку хибнонегативних рішень (FNR) для класу шкідливих сенсорних вузлів, де $\gamma = -1$ на валідаційній вибірці, при цьому потрібно контрольовано обмежити рівень хибнопозитивних спрацювань FPR, що дозволяє знизити ризик пропуску атак без суттєвого погіршення стабільності роботи бездротової сенсорної мережі молочної ферми.

Нехай після застосування методу опорних векторів SVM моделі для вузла q маємо рішення $\widehat{\gamma_q}(t) \in \{-1, 0, 1\}$). Введем індикатор для оцінювання шкідливого стану:

$$\hat{y}_q(t) = \begin{cases} 1, & \hat{\gamma}_q(t) = -1, \\ 0, & \hat{\gamma}_q(t) \in \{0, 1\}. \end{cases}$$

де $\hat{y}_q(t)$ – індикатор, що показує шкідливий вузол q або ні. Потім для обраного порога Ω на валідаційній вибірці можна розрахувати:

$$FNR(\Omega) = \frac{FN(\Omega)}{TP(\Omega) + FN(\Omega)}, FPR(\Omega) = \frac{FP(\Omega)}{TN(\Omega) + FP(\Omega)}, \quad (7)$$

де $FNR(\Omega)$ – частка хибнопозитивних, характеризує ймовірність того, що шкідливий або ризиковий сенсорний вузол буде помилково класифікований як легітимний за порогового значення довіри Ω; $FNR(\Omega)$ – частка хибнонегативних, відображає ймовірність помилкового віднесення легітимного сенсорного вузла до шкідливих при тому самому порозі Ω; $TP(\Omega)$ – кількість правильно ідентифікованих шкідливих (ризикових) сенсорних вузлів, $FP(\Omega)$ – хибно позитивні, кількість легітимних вузлів, помилково класифікованих як шкідливі; $TN(\Omega)$ – істинно негативні, кількість правильно розпізнаних легітимних сенсорних вузлів, $FN(\Omega)$ – хибно негативні, кількість шкідливих вузлів, помилково віднесених до легітимних.

Потрібно зауважити, що для кожного кластера v (наприклад, фізіологічний, доїльний зал) задається власний поріг Ω_v, бо кожен кластер має свій функціонал, і ціна помилки в них різна. Далі вибір порогового значення Ω здійснюється шляхом мінімізації зваженої функції втрат, у якій хибнонегативні та хибнопозитивні рішення мають різну вагу, що дозволяє адаптивно збалансувати вимоги до безпеки та стабільності функціонування бездротової сенсорної мережі молочної ферми залежно від ролі у забезпеченні стійкості системи відповідного кластера. Мінімізуємо FNR під обмеженням на FPR через зважену функцію втрат)

$$\Omega_v = \arg\min_{\Omega \in (0,0.8)} (\alpha_v FNR_v(\Omega) + \beta_v FPR_v(\Omega)) \quad (8)$$

Де $FNR_v(\Omega)$ – частка хибнопозитивних спрацювань у кластері v, $FNR_v(\Omega)$ – частка хибнонегативних спрацювань у кластері v; α_v, β_v – коефіцієнти, $\alpha_v > \beta_v$ у більш важливих кластерах, щоб штраф $FNR_v(\Omega)$ був більше.

Для кожного функціонального кластера q показники $FNR_v(\Omega)$та $FPR_v(\Omega)$ (7) визначаються шляхом аналізу отриманих або змодельованих даних про поведінку сенсорних вузлів, послідовного варіювання порогового значення Ω у заданому діапазоні та обчислення елементів матриці змішувань TP, TN, FP, FN, на основі яких обирається кластерно-специфічне оптимальне значення Ω_v.

З огляду на періоди природно-фізіологічних змін, коли ризик хибнопозитивних спрацювань через природні зсуви сигналів зростає, потрібно ввести адаптацію порога шкідливого або годного вузла за контекстом $u(t)$ (режим ферми):

$$\Omega_v(t) = \Omega_v^{(0)} + \Delta\Omega_v \cdot u(t), u(t) \in \{0,1\},$$

де $\Omega_v(t)$ – адаптивне порогове значення інтегральної довіри, що використовується для віднесення сенсорного вузла до шкідливого або легітимного стану в момент часу *t;* $\Omega_v^{(0)}$– базове (номінальне) порогове значення довіри, визначене для стандартних умов функціонування ферми за відсутності аномальних природно-фізіологічних впливів; $\Delta\Omega_v$ – коригувальна складова порогу, що відображає допустиме зміщення межі прийняття рішення з метою зниження частоти хибнопозитивних спрацювань FNR у нестабільних умовах, $\Delta\Omega_v > 0$; v – кластер; $u(t)$ – індикатор контексту період природно-функціональних змін, $u(t) = 1$ у випадках, наприклад, різкого похолодання, спекотного періоду, періоду еструсу або сухостою. При цьому умова на часту хибнонегативних спрацювань FNR контролюється через критерій (8).

Результати багатокласової класифікації сенсорних вузлів залежать віж функціонального призначення кластерів молочної ферми, оскільки однаковий клас стану вузла може мати різні наслідки для управління технологічними та біологічними процесами. Насамперед це стосується різних наслідків для помилок класифікації: у кластерах, пов'язаних із безпосереднім моніторингом фізіологічного стану тварин і процесів доїння, критичним є зниження частки хибнонегативних рішень FNR, тоді як у кластерах контролю мікроклімату допустимим може бути дещо вищий рівень хибнопозитивних спрацювань FPR без істотного ризику для функціонування системи. Адаптивне реагування на реалізацію потенційних ризиків, що проявляються у вигляді порушення цілісності, достовірності або доступності даних у відповідних функціональних кластерах, дозволяє пов'язати формальні метрики якості (хибнопозитивні, FPR та хибнонегативні, FNR) з практичними управлінськими діями в різних функціональних кластерах молочної ферми (табл. 1).

Таблиця 1

Приклади результатів класифікації за кластерами БСМ молочної ферми

Функціональний кластер	Основний ризик	Реалізація ризику	Критичний тип помилки	Потенційні наслідки	Управлінська реакція
Фізіологічний моніторинг тварин	Порушення достовірності даних	Ін'єкція хибних даних про активність	**FNR**	Пропуск патологічних станів, хибні ветеринарні рішення	Ізоляція вузла, зниження ваги даних, додаткова верифікація
Мікроклімат приміщень	Локальні збої або шум вимірювань	Тимчасове відхилення показників температури	**FPR**	Необґрунтоване ігнорування справного сенсора	Повторна перевірка, часовий фільтр, збереження вузла в мережі
Доїльний зал	Спотворення технологічних параметрів	Підміна даних про надій або електропровідність молока	**FNR / FPR (баланс)**	Хибні рішення щодо якості молока або роботи обладнання	Контекстна перевірка, адаптація порогів, порівняння з історичними даними
Інфраструктурний кластер	Порушення стійкості мережі	Sybil-атаки, змова, selective forwarding, DoS	**FNR**	Деградація маршрутизації, втрата цілісності БСМ	Ізоляція вузла, перебудова маршрутів, активація механізмів безпеки

Таким чином, інтерпретація класу шкідливого вузла $\gamma = -1$ у фізіологічному та доїльному кластерах розглядається передусім як сигнал потенційної загрози достовірності даних, що може призвести до хибних управлінських рішень щодо здоров'я тварин або якості молока. Водночас в інфраструктурному кластері така класифікація має системний характер і може бути використана при застосуванні мережевих механізмів реагування, зокрема ізоляції вузла або перебудови маршрутів передавання даних, що в сукупності забезпечує узгодження результатів представленої класифікації з практичними вимогами управління безпекою та надійністю БСМ молочної ферми.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Кількісна оцінка ризиків у бездротовій сенсорній мережі молочної ферми виконувалася шляхом моделювання типових сценаріїв нормальної роботи та порушень функціонування сенсорних вузлів у різних функціональних кластерах, включно з викривленням даних, нестабільною поведінкою та імітацією атак. Параметри мережі відповідали типовій кластеризованій БСМ молочної ферми з урахуванням характеристик передавання даних, затримок, ресурсних обмежень і кластерно-специфічних параметрів довіри, що забезпечило адекватність моделювання реальним умовам експлуатації. Запропонована теоретична модель показала, що поєднання динамічної оцінки довіри з багатокласовою SVM-класифікацією дозволяє знизити частку хибнонегативних рішень порівняно з пороговими підходами та забезпечує надійніше розрізнення легітимної і шкідливої поведінки сенсорних вузлів, особливо у фізіологічному кластері та кластері доїльного залу.

Аналіз хибнопозитивних рішень (FPR) показав, що кластерно-специфічний вибір порогового значення Ω дозволяє обмежити необґрунтоване віднесення справних сенсорів до шкідливого класу, особливо в умовах природних піків біологічної та кліматичної мінливості. У кластері мікроклімату допустимий дещо вищий рівень FPR не призводив до істотного погіршення якості управлінських рішень, тоді як у доїльному та фізіологічному кластерах контроль FPR був необхідним для збереження безперервності моніторингу ключових параметрів. Таким чином, результати моделювання підтвердили доцільність диференційованого підходу до інтерпретації FPR і FNR залежно від функціонального призначення кластера.

Узагальнюючи, отримані результати свідчать, що запропонована модель дозволяє досягти збалансованого компромісу між чутливістю до шкідливої поведінки сенсорних вузлів і стабільністю роботи бездротової сенсорної мережі в цілому. Поєднання динамічної оцінки довіри, кластерно-орієнтованого вибору порогів і SVM-класифікації створює передумови для зниження ризиків порушення цілісності та достовірності даних у реальних умовах експлуатації молочної ферми.

Подальші дослідження доцільно спрямувати на адаптивне розширення запропонованої моделі динамічної оцінки довіри з урахуванням контекстних чинників експлуатації молочної ферми, зокрема сезонних змін, фаз виробничого циклу та фізіологічного стану тварин, що дозволить підвищити точність класифікації сенсорних вузлів. Перспективним напрямом є поєднання методу опорних векторів із іншими підходами машинного навчання та впровадження інкрементального навчання для підвищення стійкості моделі до змін

структури мережі й появи нових типів загроз. Додатково інтеграція моделі з механізмами мережевого управління та кіберзахисту може забезпечити комплексне підвищення надійності, безпеки й ефективності бездротових сенсорних мереж у молочному скотарстві.

Література

1. Lam D. The Next 2 Billion: Can the World Support 10 Billion People? // Population and Development Review. 2025. Vol. 51, No. 1. P. 63-102. DOI: 10.1111/padr.12685.

2. Dash S., Maity R., Maity S. *Population exposure to compound climate extremes: global analysis to identify continent wise age group disparities in a warming world* // Natural Hazards. 2025. Vol. 2. Art. 88. DOI: 10.1038/s44304-025-00145-9.

3. OECD–FAO Agricultural Outlook 2025–2034: Emerging economies will drive growth in animal-source food consumption and production [Electronic resource] // FAO Newsroom. – 15.07.2025. – Available at: https://www.fao.org/newsroom/detail/oecd-fao-agricultural-outlook-2025-2034--emerging-economies-will-drive-growth-in-animal-source-food-consumption-and-production/en (Last accessed: 14.01.2026).

4. Felis A. Dairy's Development and Socio-Economic Transformation: A Cross-Country Analysis // World. 2025. Vol. 6, No. 3. Art. 105. – DOI: 10.3390/world6030105

5. Dawkins M. S. Smart farming and Artificial Intelligence (AI): How can we ensure that animal welfare is a priority? // Applied Animal Behaviour Science. – 2025. – Vol. 262. – Art. 106519. – DOI: 10.1016/j.applanim.2025.106519.

6. Foris B., Sheng K., Dürnberger C., Oczak M., Rault J.-L. AI for One Welfare: the role of animal welfare scientists in developing valid and ethical AI-based welfare assessment tools // Frontiers in Veterinary Science. 2025. Vol. 12. Art. 1645901. – DOI: 10.3389/fvets.2025.1645901.

7. Provolo G., Brandolese C., Grotto M., Marinucci A., Fossati N., Ferrari O., Beretta E., Riva E. An Internet of Things Framework for Monitoring Environmental Conditions in Livestock Housing to Improve Animal Welfare and Assess Environmental Impact // Animals. – 2025. – Т. 15, № 5. – Art. 644. – DOI: 10.3390/ani15050644.

8. Shafi F.B., Ahamed M.F., Nabi M.F., Khandakar A., Rohouma W., Ayari M.A., Thomas K., Rahman A., Reaz M.B.I., Haq F., Refaat S.S. Review of sensor technologies, DC-DC converters, and power electronics for sustainable monitoring in precision livestock farming // Results in Engineering. – 2025. – Т. 28. – Стаття № 107975. – DOI: 10.1016/j.rineng.2025.107975.

9. Neethirajan S. Digital Twins for Cows and Chickens: From Hype Cycles to Hard Evidence in Precision Livestock Farming // Agriculture. – 2026. – Т. 16, № 2. – Art. 166. – DOI: 10.3390/agriculture16020166.

10. Lorincz J., Levarda K., Čagalj M., Kukuruzović A. A Comprehensive Analysis of LoRa Network Wireless Signal Quality in Indoor Propagation Environments // Journal of Sensor and Actuator Networks. – 2025. – Т. 14, № 6. – Art. 111. – DOI: 10.3390/jsan14060111.

11. Піхота К. В. Потенційні загрози інтернету речей і способи їх подолання : дипломна робота бакалавра : спец. 172 «Телекомунікації та радіотехніка» / К. В. Піхота. – Київ, 2020. – [Електронний ресурс]. – 59 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/39393 (Дата звернення: 18.01.2026).

12. Ferreira R., Bispo I., Rabadão C., Santos L., Costa R. L. de C. Farm-flow dataset: Intrusion detection in smart agriculture based on network flows // Computers and Electrical Engineering. 2025. Vol. 121. Art. 109892. DOI: 10.1016/j.compeleceng.2024.109892.

13. Leliveld L.M.C., Brandolese C., Grotto M., Marinucci A., Fossati N., Lovarelli D., Riva E., Provolo G. Real-time automatic integrated monitoring of barn environment and dairy cattle behaviour: Technical implementation and evaluation on three commercial farms. Computers and Electronics in Agriculture. 2024. Vol. 216. Art. 108499. – DOI: 10.1016/j.compag.2023.108499.

14. Neethirajan S. Safeguarding digital livestock farming – a comprehensive cybersecurity roadmap for dairy and poultry industries // Frontiers in Big Data. – 2025. – Art. 1556157. – DOI: 10.3389/fdata.2025.1556157.

15. Han S., Zhu X., Mok A. K., Chen D., Nixon M. Reliable and Real-time Communication in Industrial Wireless Mesh Networks : preprint / University of Texas at Austin ; Emerson Process Management, 2008. – 15 p.

16. Bernabucci G., Evangelista C., Girotti P., Viola P., Spina R., Ronchi B., Bernabucci U., Basiricò L., Turini L., Mantino A., Mele M., Primi R. Precision livestock farming: an overview on the application in extensive systems // Italian Journal of Animal Science, 2025. – P. 859-884. – DOI: 10.1080/1828051X.2025.2480821.

17. Foris B., Sheng K., Dürnberger C., Oczak M., Rault J.-L. AI for One Welfare: the role of animal welfare scientists in developing valid and ethical AI-based welfare assessment tools // Frontiers in Veterinary Science. – 2025. – Vol. 12. – Art. 1645901. DOI: 10.3389/fvets.2025.1645901.

18. Heidari, A.; Amiri, Z.; Jamali, M. A. J.; Jafari, N. Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults // Concurrency and Computation: Practice and Experience. – 2024. – Vol. 36, No. 27. – Art. e8252. – DOI: 10.1002/cpe.8252.

19. Islam M. M., Shamshuzzoha M. Securing Wireless Body Area Networks data transmission with machine learning: A cross-tier framework for anomaly detection and intrusion prevention // Computer Science & Business Review. – 2025. – Art. 100031. – DOI: 10.1016/j.csbr.2025.100031.

20. Talukder M. A., Rahman M. M., Islam M. R., Hasan M. K. A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction // Scientific Reports. – 2025. – Vol. 15. – Article 87028. – DOI: 10.1038/s41598-025-87028-1.

21. Pandey V. K., Prakash S., Gupta T. K., Sinha P., Yang T., Rathore R. S., Wang L., Tahir S., Bakhsh S. T. Enhancing intrusion detection in wireless sensor networks using a Tabu search-based optimized random forest // Scientific Reports. 2025. Vol. 15, No. 1. Art. 18634. DOI: 10.1038/s41598-025-03498-3.

22. Руденко Н. В., Шрам М. М. Загрози інформаційної безпеки у бездротових сенсорних мережах: моделювання та аналіз // Зв'язок. 2024. № 5. – С. 24-29. – DOI: 10.31673/2412-9070.2024.050729.

23. Артюх С. Г. Функціональна модель підсистеми безпеки системи управління безпроводовими сенсорними мережами військового призначення / С. Г. Артюх // Сучасні інформаційні технології у сфері безпеки та оборони. – 2025. – Т. 52, № 1. – С. 85-92. – DOI: 10.33099/2311-7249/2025-52-1-85-92.

24. Goswami P., Sarkar D., Das S., Pal A., Ghosh A., Chatterjee C., Pal T., Sarkar S. Machine learning based dynamic trust estimation framework for securing wireless sensor networks // Scientific Reports. – 2025. – Vol. 15, No. 1. – Art. 35821. – [Electronic resource]. – DOI: 10.1038/s41598-025-19768-z.

25. Bao F., Chen I.-R., Chang M., Cho J.-H. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection // IEEE Transactions on Network and Service Management. – 2012. – Vol. 9, No. 2. – P. 169-183. – DOI: 10.1109/TNSM.2012.022312.110145.

26. Liu N., Qi J., An X., Wang Y. A Review on Information Technologies Applicable to Precision Dairy Farming: Focus on Behavior, Health Monitoring, and the Precise Feeding of Dairy Cows // Agriculture. – 2023. – Vol. 13, No. 10. – Art. 1858. – DOI: 10.3390/agriculture13101858

27. Ojha A., Gupta B. Evolving landscape of wireless sensor networks: a survey of trends, timelines, and future perspectives // Discover Applied Sciences. – 2025. – Vol. 7. – Art. 825. – DOI: 10.1007/s42452-025-07070-6.

28. Tariq H., Majeed M., Ahmad M. Optimizing SVM performance through combinatorial hyperparameter tuning and model selection // *International Journal of Bioautomation*. – 2025. – Vol. 29, No. 2. – P. 117-144. – DOI: 10.7546/ijba.2025.29.2.000981.

References

1. Lam D. The Next 2 Billion: Can the World Support 10 Billion People? // Population and Development Review. 2025. Vol. 51, No. 1. P. 63-102. DOI: 10.1111/padr.12685.

2. Dash S., Maity R., Maity S. *Population exposure to compound climate extremes: global analysis to identify continent wise age group disparities in a warming world* // Natural Hazards. 2025. Vol. 2. Art. 88. DOI: 10.1038/s44304-025-00145-9.

3. OECD–FAO Agricultural Outlook 2025–2034: Emerging economies will drive growth in animal-source food consumption and production [Electronic resource] // FAO Newsroom. – 15.07.2025. – Available at: https://www.fao.org/newsroom/detail/oecd-fao-agricultural-outlook-2025-2034--emerging-economies-will-drive-growth-in-animal-source-food-consumption-and-production/en (Last accessed: 14.01.2026).

4. Felis A. Dairy's Development and Socio-Economic Transformation: A Cross-Country Analysis // World. 2025. Vol. 6, No. 3. Art. 105. – DOI: 10.3390/world6030105.

5. Dawkins M. S. Smart farming and Artificial Intelligence (AI): How can we ensure that animal welfare is a priority? // Applied Animal Behaviour Science. – 2025. – Vol. 262. – Art. 106519. – DOI: 10.1016/j.applanim.2025. 106519.

6. Foris B., Sheng K., Dürnberger C., Oczak M., Rault J.-L. AI for One Welfare: the role of animal welfare scientists in developing valid and ethical AI-based welfare assessment tools // Frontiers in Veterinary Science. 2025. Vol. 12. Art. 1645901. – DOI: 10.3389/fvets.2025.1645901.

7. Provolo G., Brandolese C., Grotto M., Marinucci A., Fossati N., Ferrari O., Beretta E., Riva E. An Internet of Things Framework for Monitoring Environmental Conditions in Livestock Housing to Improve Animal Welfare and Assess Environmental Impact // Animals. – 2025. – T. 15, № 5. – Art. 644. – DOI: 10.3390/ani15050644.

8. Shafi F.B., Ahamed M.F., Nabi M.F., Khandakar A., Rohouma W., Ayari M.A., Thomas K., Rahman A., Reaz M.B.I., Haq F., Refaat S.S. Review of sensor technologies, DC-DC converters, and power electronics for sustainable monitoring in precision livestock farming // Results in Engineering. – 2025. – T. 28. – Стаття № 107975. – DOI: 10.1016/j.rineng.2025.107975

9. Neethirajan S. Digital Twins for Cows and Chickens: From Hype Cycles to Hard Evidence in Precision Livestock Farming // Agriculture. – 2026. – T. 16, № 2. – Art. 166. – DOI: 10.3390/agriculture16020166.

10. Lorincz J., Levarda K., Čagalj M., Kukuruzović A. A Comprehensive Analysis of LoRa Network Wireless Signal Quality in Indoor Propagation Environments // Journal of Sensor and Actuator Networks. – 2025. – T. 14, № 6. – Art. 111. – DOI: 10.3390/jsan14060111.

11. 11. Pikhota K. V. Potentsiini zahrozy internetu rechei i sposoby yikh podolannia : dyplomna robota bakalavra : spets. 172 «Telekomunikatsii ta radiotekhnika» / K. V. Pikhota. – Kyiv, 2020. – [Elektronnyi resurs]. – 59 s. – Rezhym dostupu: https://ela.kpi.ua/handle/123456789/39393 (Data zvernennia: 18.01.2026).

12. Ferreira R., Bispo I., Rabadão C., Santos L., Costa R. L. de C. Farm-flow dataset: Intrusion detection in smart agriculture based on network flows // Computers and Electrical Engineering. 2025. Vol. 121. Art. 109892. DOI: 10.1016/j.compeleceng.2024.109892.

13. Leliveld L.M.C., Brandolese C., Grotto M., Marinucci A., Fossati N., Lovarelli D., Riva E., Provolo G. Real-time automatic integrated monitoring of barn environment and dairy cattle behaviour: Technical implementation and evaluation on three commercial farms. Computers and Electronics in Agriculture. 2024. Vol. 216. Art. 108499. – DOI: 10.1016/j.compag.2023.108499.

14. Neethirajan S. Safeguarding digital livestock farming – a comprehensive cybersecurity roadmap for dairy and poultry industries // Frontiers in Big Data. – 2025. – Art. 1556157. – DOI: 10.3389/fdata.2025.1556157.

15. Han S., Zhu X., Mok A. K., Chen D., Nixon M. Reliable and Real-time Communication in Industrial Wireless Mesh Networks : preprint / University of Texas at Austin ; Emerson Process Management, 2008. – 15 p.

16. Bernabucci G., Evangelista C., Girotti P., Viola P., Spina R., Ronchi B., Bernabucci U., Basiricò L., Turini L., Mantino A., Mele M., Primi R. Precision livestock farming: an overview on the application in extensive systems // Italian Journal of Animal Science, 2025. – P. 859-884. – DOI: 10.1080/1828051X.2025.2480821.

17. Foris B., Sheng K., Dürnberger C., Oczak M., Rault J.-L. AI for One Welfare: the role of animal welfare scientists in developing valid and ethical AI-based welfare assessment tools // Frontiers in Veterinary Science. – 2025. – Vol. 12. – Art. 1645901. DOI: 10.3389/fvets.2025.1645901.

18. Heidari, A.; Amiri, Z.; Jamali, M. A. J.; Jafari, N. Assessment of reliability and availability of wireless sensor networks in industrial applications by considering permanent faults // Concurrency and Computation: Practice and Experience. – 2024. – Vol. 36, No. 27. – Art. e8252. – DOI: 10.1002/cpe.8252.

19. Islam M. M., Shamshuzzoha M. Securing Wireless Body Area Networks data transmission with machine learning: A cross-tier framework for anomaly detection and intrusion prevention // Computer Science & Business Review. – 2025. – Art. 100031. – DOI: 10.1016/j.csbr.2025.100031.

20. Talukder M. A., Rahman M. M., Islam M. R., Hasan M. K. A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction // Scientific Reports. – 2025. – Vol. 15. – Article 87028. – DOI: 10.1038/s41598-025-87028-1.

21. Pandey V. K., Prakash S., Gupta T. K., Sinha P., Yang T., Rathore R. S., Wang L., Tahir S., Bakhsh S. T. Enhancing intrusion detection in wireless sensor networks using a Tabu search-based optimized random forest // Scientific Reports. 2025. Vol. 15, No. 1. Art. 18634. DOI: 10.1038/s41598-025-03498-3.

22. Rudenko N. V., Shram M. M. Zahrozy informatsiinoi bezpeky u bezdrotovykh sensornykh merezhakh: modeliuvannia ta analiz [Electronic resource] // Zv'iazok. 2024;(5): 24-29. doi:10.31673/2412-9070.2024.050729.

23. Artiukh S. H. Funktsionalna model pidsystemy bezpeky systemy upravlinnia bezprovodovymy sensornymy merezhamy viiskovoho pryznachennia // Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony. 2025;52(1):85-92. doi:10.33099/2311-7249/2025-52-1-85-92.

24. Goswami P., Sarkar D., Das S., Pal A., Ghosh A., Chatterjee C., Pal T., Sarkar S. Machine learning based dynamic trust estimation framework for securing wireless sensor networks // Scientific Reports. – 2025. – Vol. 15, No. 1. – Art. 35821. – [Electronic resource]. – DOI: 10.1038/s41598-025-19768-z.

25. Bao F., Chen I.-R., Chang M., Cho J.-H. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection // IEEE Transactions on Network and Service Management. – 2012. – Vol. 9, No. 2. – P. 169-183. – DOI: 10.1109/TNSM.2012.022312.110145.

26. Liu N., Qi J., An X., Wang Y. A Review on Information Technologies Applicable to Precision Dairy Farming: Focus on Behavior, Health Monitoring, and the Precise Feeding of Dairy Cows // Agriculture. – 2023. – Vol. 13, No. 10. – Art. 1858. – DOI: 10.3390/agriculture13101858

27. Ojha A., Gupta B. Evolving landscape of wireless sensor networks: a survey of trends, timelines, and future perspectives // Discover Applied Sciences. – 2025. – Vol. 7. – Art. 825. – DOI: 10.1007/s42452-025-07070-6.

28. Tariq H., Majeed M., Ahmad M. Optimizing SVM performance through combinatorial hyperparameter tuning and model selection // *International Journal of Bioautomation*. – 2025. – Vol. 29, No. 2. – P. 117-144. – DOI: 10.7546/ijba.2025.29.2.000981.