УДК 004.85:004.056:61:004.77 DOI: 10.31673/2412-9070.2026.318110

І. М. СРІБНА, д-р техн. наук, доцент;
ORCID: 0000-0001-9242-2021
К. О. ТРЕНЬОВА, PhD;
ORCID: 0009-0005-9729-2373
О. С. ЧУДАКОВ, студент,
ORCID: 0009-0006-6667-1335
Державний університет інформаційно-комунікаційних технологій, Київ

МОДЕЛІ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ТА ЗАХИСТУ ДАНИХ У СИСТЕМАХ МЕДИЧНОГО АДМІНІСТРУВАННЯ НА ОСНОВІ IoT

У статті розглянуто застосування моделей машинного навчання (ML) для аналізу та захисту даних в автоматизованих системах медичного адміністрування, що функціонують на основі технологій Інтернету речей (IoT). Сучасні медичні заклади все частіше впроваджують IoT-пристрої для моніторингу пацієнтів, управління апаратурою та оптимізації організаційних процесів. Це призводить до різкого зростання обсягів даних і складності їх обробки, а також створює додаткові ризики, пов'язані з кібербезпекою та стабільністю комунікацій.

У роботі досліджено можливості використання алгоритмів Decision Tree та Random Forest для класифікації, прогнозування і виявлення аномалій у потоках медичних даних. Запропоновано концептуальну модель інтеграції ML-модулів у багаторівневу систему медичного адміністрування, що сприяє підвищенню точності аналізу, ефективності управління та рівня захисту інформації.

Ключові слова: IoT, машинне навчання, медицина, аналіз даних, кібербезпека, автоматизація, Decision Tree, Random Forest.

Вступ

Постановка проблеми. Активна цифровізація охорони здоров'я призводить до масового впровадження пристроїв Інтернету речей (IoT) та автоматизованих систем управління, які використовуються для спостереження за станом пацієнтів, керування медичною апаратурою, обліком ресурсів та оптимізацією процесів. Ці системи генерують значні обсяги даних у режимі, наближеному до реального часу. Дані часто є нерегулярними, містять пропуски або шум, що ускладнює їх аналіз традиційними методами. Одночасно середовище IoT є вразливим до кіберзагроз: несанкціонованого доступу, підміни інформації, нестабільності з'єднань та апаратних збоїв. У цих умовах виникає потреба у впровадженні інтелектуальних аналітичних методів, здатних швидко виявляти порушення, прогнозувати потенційні відхилення та підвищувати ефективність управлінських рішень. Завдяки своїй здатності працювати з великими обсягами даних і виявляти приховані закономірності, алгоритми Decision Tree та Random Forest є перспективними для побудови систем аналітики та безпеки у медичних IoT-інфраструктурах.

Аналіз останніх досліджень і публікацій. Сучасні наукові дослідження демонструють **стійке зростання інтересу до інтеграції технологій Інтернету речей (IoT)** із методами **машинного навчання (ML)** у медичних інформаційних системах. Збільшення кількості підключених пристроїв призводить до формування масивів неоднорідних даних — як клінічних, так і технічних, — які потребують автоматизованої обробки, зберігання та аналізу у режимі, наближеному до реального часу [1]. Традиційні аналітичні методи часто не справляються з обсягом і швидкістю оновлення інформації, що зумовлює потребу у використанні **інтелектуальних ML-алгоритмів,** здатних адаптивно навчатися на потокових даних та виявляти приховані закономірності.

Алгоритми **Decision Tree** забезпечують прозору та інтерпретовану логіку ухвалення рішень, що робить їх особливо зручними для медичних фахівців. Ці моделі дозволяють візуалізувати процес класифікації станів пацієнтів, аналізувати фактори ризику та прогнозувати результати лікування [2]. У контексті клінічного прийняття рішень Decision Tree використовуються для створення експертних систем, які здатні пояснювати свої рекомендації, що відповідає сучасним вимогам **пояснюваного штучного інтелекту (Explainable AI, XAI)** у медицині.

Для роботи зі складними, багатовимірними й «шумними» даними ефективно зарекомендували себе **ансамблеві методи,** зокрема **Random Forest**. Завдяки комбінуванню рішень великої кількості дерев, ці моделі досягають високої точності навіть при неповних або некоректних даних, характерних для IoT-середовищ. Random Forest активно застосовується для задач прогнозування серцево-судинних подій, аналізу електрокардіограм, оцінки життєвих показників пацієнтів у режимі моніторингу, а також для виявлення технічних збоїв у медичному обладнанні [3].

Значна кількість публікацій останніх років присвячена **питанням кібербезпеки медичних IoT-систем,** де методи машинного навчання використовуються для аналізу мережевого трафіку, виявлення вторгнень, класифікації аномалій та оцінки ризиків несанкціонованого доступу [4], [8]. Поєднання ML-алгоритмів з класичними засобами шифрування дозволяє створювати **багаторівневі моделі безпеки,** у яких поведінковий аналіз пристроїв і користувачів виступає додатковим бар'єром для виявлення атак типу «нульового дня».

У сфері **eHealth та "розумних лікарень"** (Smart Healthcare) машинне навчання розглядається як інструмент підвищення ефективності адміністрування: моделі прогнозують навантаження на персонал, допомагають оптимізувати графіки прийому пацієнтів, скорочують час очікування і раціоналізують використання ресурсів клініки [5], [6]. Такі підходи поєднують **аналітику часових рядів,** кластеризацію поведінкових даних пацієнтів і алгоритми прогнозування для систем підтримки прийняття управлінських рішень.

Крім того, у світовій практиці активно розвиваються дослідження щодо **інтеграції ML, IoT і блокчейн-технологій** для створення захищених платформ зберігання медичних даних [7]. Поєднання розподілених реєстрів і машинного навчання дозволяє досягти вищого рівня довіри, оскільки дані про пацієнтів можуть аналізуватись без порушення їх конфіденційності.

Узагальнення результатів наявних робіт підтверджує, що застосування методів машинного навчання в IoT-орієнтованих медичних системах відкриває нові можливості для **прогнозної аналітики, персоналізованої медицини** та **активного кіберзахисту.** Водночас наукова спільнота наголошує на необхідності стандартизації форматів даних, підвищення етичності використання ML-рішень та забезпечення їх сумісності з національними системами eHealth.

Мета статті. Розроблення концептуальної моделі використання методів машинного навчання для аналізу, інтелектуальної обробки та захисту даних у системах медичного адміністрування на базі технологій IoT.

Завдання дослідження:

1. Обґрунтувати архітектуру IoT-орієнтованої системи медичного адміністрування;
2. Визначити роль і можливості ML-моделей у класифікації, прогнозуванні та виявленні аномалій;
3. Продемонструвати приклади інтеграції ML-модулів у процеси управління медичним центром.

Основна частина

Архітектуру системи медичного адміністрування на основі IoT зручно розглядати як набір взаємопов'язаних рівнів, кожен з яких відповідає за свою частину роботи: збір даних, їх передавання, обробку та використання результатів для управлінських рішень. Такий підхід зараз фактично став стандартом для "розумних" медичних систем [1], [5].

Перший рівень - це IoT-пристрої. До нього належать датчики життєвих показників, монітори пацієнтів, RFID-мітки для відстеження обладнання, сенсори температури, вологості, відкриття дверей тощо. Вони постійно формують потоки телеметрії: показники стану пацієнтів, події у приміщеннях, технічні параметри апаратури. Частина цих пристроїв працює авто-

номно, частина під керуванням центральної системи, яка може змінювати частоту вимірювань, порогові значення спрацювання або режими роботи через конфігураційні повідомлення.

Другий рівень комунікаційний. Його завдання - "донести" дані від великої кількості пристроїв до серверної частини системи. Для цього використовуються легковагові протоколи на кшталт MQTT або CoAP, а також HTTP та інші мережні сервіси. На цьому етапі часто виконується попередня обробка: фільтрація очевидно некоректних значень, агрегація показників, буферизація даних у разі тимчасових збоїв зв'язку. Важливо, щоб навіть за великої кількості підключених пристроїв система не "захлиналася" трафіком і могла працювати близько до реального часу [5].

Третій ключовий елемент - це ядро медичного адміністрування. Тут поєднуються бізнес-логіка медичного закладу, електронні картки пацієнтів, модулі управління чергами, планування розкладу лікарів, обліку ресурсів та обробки інцидентів. Саме на цьому рівні дані з IoT-пристроїв вже не просто "потоки цифр", а контекстуалізована інформація: наприклад, підвищений тиск не абстрактного сенсора, а конкретного пацієнта, який знаходиться у певному відділенні. На основі цих даних система може автоматично формувати завдання персоналу, сповіщення, зміни у розкладі прийомів [7].

Окремо виділяється аналітичний рівень на основі машинного навчання. Він отримує з ядра системи нормалізовані та зібрані в єдиний формат дані: історію спрацювань датчиків, інформацію про навантаження на відділення, час очікування пацієнтів, історію відмов обладнання. На цьому рівні працюють моделі, які аналізують тенденції, виявляють аномалії й формують прогнози. Наприклад, система може заздалегідь "побачити" ризик перевантаження певного відділення або підвищену ймовірність відмови конкретного апарата на основі поведінки його сенсорів [3].

Результати роботи аналітики повертаються назад у систему у вигляді сповіщень, рекомендацій і керуючих впливів. Це можуть бути автоматичні попередження для чергового лікаря, пропозиції змінити розклад, сигнали технічній службі, а в окремих випадках - зміна конфігурації самих IoT-пристроїв. Таким чином, формується замкнуте коло: пристрої генерують дані, система їх аналізує, ухвалює рішення і впливає як на організаційні процеси, так і на поведінку обладнання.

На рис. 1 ця логіка узагальнено показана у вигляді взаємодії чотирьох основних блоків, але важливо, що схема лише візуалізує вже описаний підхід: багато IoT-джерел → надійне передавання даних → медичне адміністрування → аналітика на основі ML → зворотний зв'язок і керування. Саме така архітектура дозволяє поєднати щоденну роботу медичного центру з довгостроковим накопиченням даних і поступовим "навчанням" системи на реальній практиці.

Рис. 1. Узагальнена архітектура IoT-орієнтованої системи медичного центру

Моделі машинного навчання для класифікації та прогнозування медичних даних

У системі медичного адміністрування машинне навчання можна використовувати для того, щоб перетворювати потоки подій на зрозумілі рішення. Наприклад, кого обслуговувати в першу чергу, що можна відкласти, а де потрібна негайна реакція. Найзручнішими для таких задач є моделі на основі Decision Tree. Вони працюють за принципом послідовних "якщо – то" правил, тому їх легко інтерпретувати й пояснити медичному персоналу як вони працюють [2].

Логіку прийняття рішень можна описати через набір ознак: чи є пов'язані IoT-дані, який тип запиту, яка важливість події. Приклад такої формалізації наведено у табл. 1. Критичний запит із підвищеним тиском, зафіксованим датчиком, позначається як високої важливості та автоматично приводить до негайного виклику лікаря. Стандартний запис без додаткової телеметрії сприймається як звичайна черга, а плановий моніторинг може бути перенесений без участі оператора. Такі дані можуть використовуватись і як набір правил, і як тренувальна вибірка для побудови дерева рішень [1].

Таблиця 1

Приклад класифікації запитів пацієнтів у системі адміністрування

Характеристика запиту	Дані IoT	Важливість	Рішення системи
Критичний	Так	Висока	Негайний виклик лікаря
Стандартний запис	Ні	Середня	Додати у чергу
Плановий моніторинг	Так	Низька	Автоматичне перенесення

Коли ознак стає більше, а дані містять шум або пропуски, доцільно застосовувати ансамблеві методи, зокрема Random Forest. Ця модель об'єднує багато дерев рішень і приймає підсумкове рішення за принципом голосування, що підвищує точність і стійкість до помилок вимірювань. У межах медичного центру Random Forest доцільно використовувати для прогнозування завантаженості відділень, оцінки ризику відмов обладнання або виявлення підозрілих патернів у журналах подій [3].

Виявлення аномалій у трафіку IoT-систем медичного центру

Коли в медичному центрі працюють десятки або сотні IoT-пристроїв, мережний трафік стає досить складним: постійні заміри, службові повідомлення, оновлення конфігурацій, звернення до серверів тощо. У такому середовищі помітити "дивну" поведінку пристрою або підозрілу активність вручну майже нереально. Дослідження з безпеки медичних IoT-систем показують, що частина атак і збоїв проявляється саме як нетипові зміни трафіку: різкі стрибки кількості запитів, підозрілі звернення до сервісів, спроби частого підключення з невластивих адрес [4], [8].

Щоб автоматизувати виявлення таких ситуацій, у системі доцільно використовувати моделі машинного навчання для аналізу мережних журналів. Один із практичних варіантів – навчити Random Forest або іншу модель класифікації на історичних даних, де для кожної події відомо, чи була вона нормальною, чи пов'язувалась із епізодом збою або інцидентом безпеки. У роботах з аналізу IoT-мереж показано, що ансамблеві методи добре справляються з такими задачами, оскільки враховують одразу багато ознак: частоту запитів, тип протоколу, розмір пакетів, час доби, тип пристрою тощо [3].

У нашій концепції аномалії можуть відслідковуватися на рівні "профілю поведінки" кожного пристрою: система запам'ятовує, як зазвичай поводиться конкретний сенсор або шлюз, а потім порівнює поточну активність із цією моделлю. Якщо інтенсивність трафіку, напрямки запитів або типові шаблони сильно відрізняються від звичних, подія позначається як потенційно небезпечна і передається в модуль медичного адміністрування у вигляді сповіщення. Для

візуалізації таких ситуацій можна використовувати прості графіки зміни навантаження у часі, де аномальні ділянки виділяються окремим кольором (це зручно відобразити на рис. 2). У підсумку адміністратор бачить не сирі мережеві логи, а вже "просіяні" системою сигнали про ризики, на які варто звернути увагу [1].

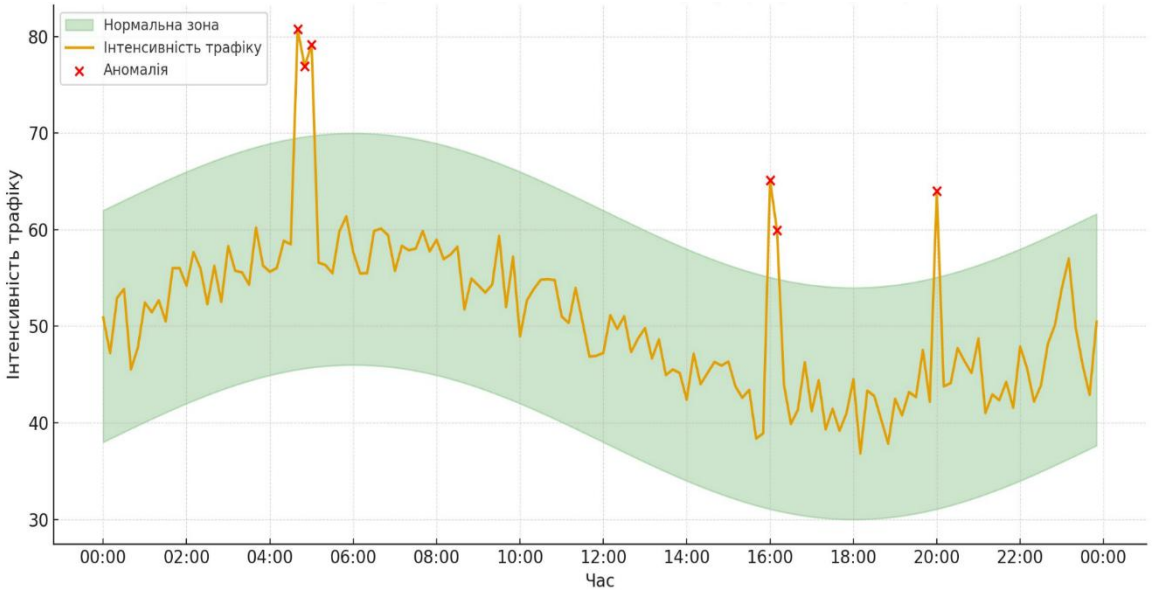

Рис. 2. Діаграма виявлення аномалій у трафіку IoT-пристроїв

Інтеграція ML-модулів у процеси адміністративного управління медичним центром

Коли моделі машинного навчання вже навчені на історичних даних, їхня реальна цінність починається тоді, коли вони вбудовані у щоденну роботу медичного центру. Ідея проста: ML-модулі працюють "за лаштунками" системи медичного адміністрування і постійно підказують, де можуть виникнути проблеми, а де є резерви. Для цього вони отримують інформацію з електронних медичних записів, журналів подій IoT-пристроїв, розкладів лікарів та статистики відвідувань [5].

Практично це можна розбити на кілька окремих модулів. Наприклад, модуль прогнозування навантаження оцінює, скільки пацієнтів очікується в певний день або зміну і пропонує збільшити або зменшити кількість лікарів. Модуль контролю технічного стану обладнання аналізує телеметрію від апаратури й сигналізує про підозрілі тенденції ще до фактичної відмови [6]. Інший модуль може відслідковувати, як користувачі працюють із системою і виявляти нетипову активність, пов'язану з можливими порушеннями доступу [7]. Узагальнений перелік таких модулів та їхній вплив зручно подати у вигляді таблиці.

Таблиця 2

Функції ML-модулів у медичному центрі

Модуль	Опис	Інформаційний ефект
Прогнозування навантаження	Працює на основі часових рядів	Розвантаження черг
Діагностика обладнання	Аналіз IoT-даних про роботу пристроїв	Попередження відмов
Виявлення аномалій	Аналіз мережного трафіку	Захист даних
Аналіз поведінки	Оцінка активності користувачів	Підвищення кіберзахисту

Важливий момент - результати ML не повинні “жити окремо”. Вони мають повертатися у ядро медичного адміністрування у вигляді зрозумілих підказок: зміна статусу пацієнта в черзі, попередження для чергового лікаря, автоматичне створення заявки для технічної служби чи рекомендація переглянути розклад. Тоді машинне навчання не виглядає як абстрактна аналітика “для звіту”, а стає частиною реального робочого процесу, допомагаючи приймати більш обґрунтовані рішення на щодень [5], [6].

Приклад застосування аналітичного модуля на основі Random Forest

Щоб показати, як саме аналітичний модуль може працювати у реальній системі медичного адміністрування, розглянемо спрощений приклад використання моделі Random Forest для виявлення підозрілих подій у журналах IoT-пристроїв.

Для цього формується вибірка з журналів подій за певний період (наприклад, 3–6 місяців). Кожен запис описує одну подію: тип пристрою, час доби, кількість запитів за невеликий інтервал, тип протоколу, наявність помилок, статус відповіді тощо. Додатково для частини подій вказується клас: “норма” або “інцидент” (збій, підозріла активність, спрацювання служби безпеки). Подібний підхід до підготовки даних використовується і в роботах, присвячених виявленню аномалій в IoT-мережах [3], [4].

Далі вибірка ділиться на тренувальну й тестову частини, після чого на тренувальних даних навчається модель Random Forest з фіксованою кількістю дерев. Після навчання модель перевіряється на тестовій вибірці: оцінюється точність класифікації, повнота та частка хибних спрацювань. У нашій концепції така модель використовується не як “остаточний вирок”, а як фільтр: усі події, які класифікуються як потенційно аномальні, передаються в систему медичного адміністрування у вигляді сповіщень для адміністратора або служби безпеки. Це дає змогу зосередити увагу не на сирих логах, а на невеликій кількості справді підозрілих ситуацій [3], [8].

Схему роботи такого модуля зручно подати у вигляді окремого рисунка: вхідні журнали подій → попередня обробка та формування ознак → модель Random Forest → класифікація подій як “норма/аномалія” → сповіщення та реєстрація інцидентів у системі медичного адміністрування. У результаті ML-модуль органічно вбудовується в архітектуру медичного центру та підсилює існуючі механізми контролю й безпеки [1], [5].

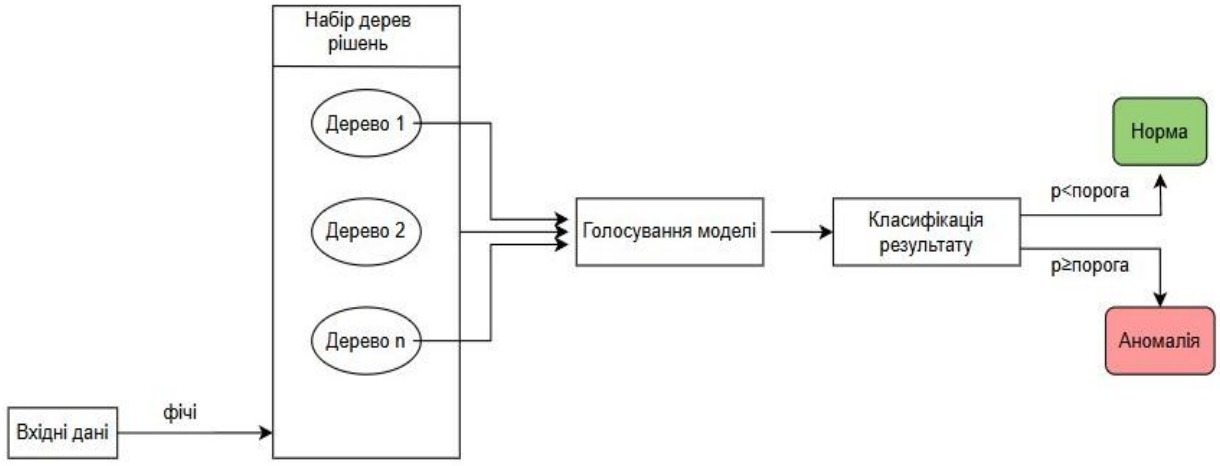

Рис. 3. Схема роботи Random Forest у системі адміністрування

Висновки

У статті запропоновано концепцію побудови IoT-орієнтованої системи медичного адміністрування з інтегрованими модулями машинного навчання.

Розроблена архітектура включає рівні збору даних, комунікацій, адміністрування та аналітики, що забезпечує ефективну обробку телеметрії й автоматизовану підтримку управлінських рішень.

Доведено, що моделі Decision Tree та Random Forest є доцільними для вирішення задач класифікації, прогнозування навантаження і виявлення аномалій у медичних інформаційних

потоках. Їх застосування підвищує точність аналізу, своєчасність реагування на інциденти та рівень кіберзахисту.

Практичне значення дослідження полягає у можливості інтеграції запропонованих ML-модулів у реальні системи eHealth для зниження ризику технічних та інформаційних збоїв.

Перспективи подальших досліджень - розширення спектру моделей (Gradient Boosting, SVM), побудова поведінкових профілів пристроїв і користувачів, а також створення адаптивних систем безпеки на основі самооновлюваних ML-модулів.

Внесок авторів

Ірина СРІБНА – формування концепції дослідження, дослідження можливостей використання моделей машинного навчання для аналізу та захисту медичних даних, підготовка первинного рукопису статті; Катерина ТРЕНЬОВА – реалізація та дослідження алгоритмів Decision Tree і Random Forest, проведення експериментальних досліджень, обробка та візуалізація отриманих результатів; Олег ЧУДАКОВ – оцінка ефективності застосування моделей машинного навчання, редагування та наукове доопрацювання статті, підготовка висновків.

Декларація про штучний інтелект

Автори не використовували штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System / W. Li et al. Mobile Networks and Applications. 2021. URL: https://doi.org/10.1007/s11036-020-01700-6

2. Abdulqader H. A., Abdulazeez A. M. Review on Decision Tree Algorithm in Healthcare Applications. Indonesian Journal of Computer Science. 2024. Vol. 13, no. 3. URL: https://doi.org/10.33022/ijcs.v13i3.4026

3. Khalid H. Anomaly Detection in IoT Networks Using Machine Learning Techniques. Dijlah Journal of Engineering Science. 2025. Vol. 2, no. 3. P. 127–136. URL: https://doi.org/10.13140/RG.2.2.31076.44164

4. Chacko A., Hayajneh T. Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology. 2018. P. 155079. URL: https://doi.org/10.4108/eai.13-7-2018.155079

5. Alshehri F., Muhammad G. A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. IEEE Access. 2021. Vol. 9. P. 3660–3678. URL: https://doi.org/10.1109/access.2020.3047960

6. Gomes M. A. S., Silva V. L. d., Rodrigues J. F. TECHNOLOGY TRANSFER IN HEALTHCARE: LEVERAGING PREDICTIVE MODELS TO OPTIMIZE MEDICAL OUTCOMES. International Journal of Professional Business Review. 2024. Vol. 9, no. 12. P. e05168. URL: https://doi.org/10.26668/businessreview/2024.v9i12.5168

7. Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment for Pandemic Preparedness, Challenges, and Solutions / M. Imran et al. Electronics. 2021. Vol. 10, no. 20. P. 2501. URL: https://doi.org/10.3390/electronics10202501

8. Health IoT Threats: Survey of Risks and Vulnerabilities / S. Madanian et al. Future Internet. 2024. Vol. 16, no. 11. P. 389. URL: https://doi.org/10.3390/fi16110389

I. Sribna, K. Trenova, O. Chudakov

MACHINE LEARNING MODELS FOR DATA ANALYSIS AND PROTECTION IN IOT-BASED HEALTHCARE ADMINISTRATION SYSTEMS

The article examines the application of machine learning models for the analysis and protection of data within automated medical administration systems operating on the basis of Internet of Things technologies. Modern healthcare institutions increasingly integrate IoT devices for patient monitoring, equipment control, environmental data collection, and optimization of administrative processes. As a result, the volume, heterogeneity, and dynamic nature of medical and infrastructural data continue to grow, which complicates their processing and significantly increases the number of potential vulnerabilities. At the same time, IoT-enabled infrastructures introduce additional risks associated with cybersecurity threats, unstable communication channels, device malfunctions, and various anomalies in data streams that may negatively affect the reliability of medical services.

This work analyzes the capabilities of Decision Tree and Random Forest algorithms in addersing classification, prediction, and anomaly detection tasks in medical information systems. Both methods demonstrate high interpretability and accuracy, which is crucial for decision-making processes in the healthcare domain. A conceptual architecture for integrating machine learning models into a multi-level medical administration system is proposed, detailing the roles of data acquisition, communication, analytical, and administrative layers. The implementation of machine learning modules enhances data quality assessment, strengthens system security through behavioral analysis of IoT traffic, and supports intelligent decision-making for resource planning and operational management in medical centers.

The presented examples demonstrate the practical potential of ML-based solutions for improving the reliability, stability, and security of IoT-oriented healthcare infrastructures. The study confirms that the combined use of IoT and machine learning technologies significantly increases the efficiency of medical administration processes and opens new opportunities for the development of intelligent clinical and organizational support systems.

Keywords: IoT, machine learning, medicine, data analysis, cybersecurity, automation, Decision Tree, Random Forest.

Надійшла до редакції: 10.03.2026
Прийнята до друку: 28.04.2026
Опубліковано: 29.06.2026