КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1338
УДК 004.054

Дудикевич Валерій Богданович
д.т.н., професор, професор кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0001-8827-9920
valerii.b.dudykevych@lpnu.ua

Микитин Галина Василівна
д.т.н., професор, професор кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0003-4275-8285
halyna.v.mykytyn@lpnu.ua

Мозоль Андрій Іванович
магістрант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0004-0728-5552
andrii.mozol.kb.2022@lpnu.ua

МЕТОДОЛОГІЧНІ ЗАСАДИ ПОБУДОВИ БЕЗПЕЧНОЇ ПЛАТФОРМИ ФУНКЦІОНУВАННЯ ІНТЕРНЕТУ МЕДИЧНИХ РЕЧЕЙ

Анотація. В Україні тривають процеси безпечної інтелектуалізації інфраструктури суспільства. Актуальним сегментом в просторі Індустрії 4.0 та Стратегії кібербезпеки України є медична інфраструктура. Одним з основних сучасних інструментаріїв інтелектуалізації медицини є безпечні кіберфізичні технології, зокрема у частині безпечного Інтернету медичних речей (IoMT). Ефективними механізмами реалізації інтелектуального діагностування стану здоров'я людини є безпечні процеси: відбору біофізичних параметрів функціонування органів і систем пацієнта; передавання медичної інформації безпровідними каналами зв'язку; обробки та аналізу даних про стан організму; прийняття управлінського рішення щодо встановлення діагнозу і, на цій основі, призначення лікування, які є основою функціональної архітектури Інтернету медичних речей. В роботі запропоновано методологію побудови безпечної платформи архітектури IoMT "давачі – сенсорні мережі – хмарна інфраструктура – користувач – конфіденційність та безпека", яка реалізує функціональний алгоритм "відбір – обмін – обробка – аналіз – прийняття рішення" згідно концепції "об'єкт – загроза – захист" та ймовірних зовнішніх випадкових і цілеспрямованих загроз. Представлено системи безпеки складових IoMT: давачів, сенсорних мереж, компонентів хмарної інфраструктури згідно моделі загроз STRIDE та моделі OSI. Розглянуто практичну реалізацію безпечного обміну медичними даними в сенсорній мережі Bluetooth у частині криптографічного захисту інформації на рівні алгоритмічно-програмного забезпечення шифрування повідомлень засобами AES-256-GCM та Python.

Ключові слова: інтелектуалізація, методологія, Інтернет медичних речей, давачі, сенсорні мережі, хмарна інфраструктура, користувачі, зовнішні випадкові і цілеспрямовані загрози, системи безпеки, шифрування повідомлень.

ВСТУП

У рамках Європейської цифрової трансформації, Стратегії розвитку системи охорони здоров'я на період до 2030 року та Концепції розбудови електронної охорони здоров'я в Україні актуальними векторами інтелектуалізації медичної інфраструктури є: 1) впровадження міжнародних стандартів та уніфікованих документів у сфері охорони здоров'я, які стосуються: заходів інформаційної безпеки на рівні Інтернету медичних речей; правил безпеки HIPAA, спрямованих на підвищення рівня захищеності електронної медичної інформації; 2) формування єдиного медичного інформаційного простору хмарної інфраструктури; 3) застосування систем аналітики медичних даних на основі технологій штучного інтелекту (ШІ) та безпровідних мереж на основі єдиних принципів і загальних правил інформаційної взаємодії.

Триває розвиток підходів до вирішення проблеми безпечного функціонування Інтернету медичних речей, у сегменті діагностування стану організму людини на рівні: безпечного відбору біофізичних параметрів функціонування організму людини та їх безпечного збереження; безпечного обміну медичними даними, безпечної обробки та аналізу інформації з метою прийняття управлінського рішення; забезпечення безпеки та конфіденційності інформаційних процесів. Інтернет медичних речей для задач діагностування стану організму людини, системи безпеки складових його архітектури, механізми реалізації захисту інформації за впливу випадкових і цілеспрямованих загроз сьогодні є актуальними векторами Концепції Індустрія 4.0 та Стратегії кібербезпеки України [1, 2].

Постановка проблеми. Інтернет медичних речей є однією з найефективніших технологій 21-го століття у просторі інтелектуалізації сфери охорони здоров'я України, архітектура якого розвивається за векторами: давачі, безпровідні сенсорні мережі, хмарна інфраструктура, користувачі. Безпечна інтелектуалізація об'єктів медичної інфраструктури суспільства передбачає впровадження безпечного IoMT, як одного з ефективних інструментаріїв безпечного відбору медичних даних від організму людини, обробки, аналізу та прийняття управлінського рішення щодо точності діагностування у просторі біофізичних параметрів систем та органів людини і, на цій основі, призначення коректного лікування пацієнта у випадку відхилення медичних даних від їх нормованих значень, які пов'язані з встановленими межами безпечної життєдіяльності.

Безпека IoMT вимагає розвитку методології побудови безпечної платформи "архітектура IoMT – системи безпеки", яка функціонально розгортається на рівні складових IoMT і є підгрунтям практичної реалізації комплексу новітніх технологій протидії випадковим і цілеспрямованим загрозам в сучасному просторі кібервикликів.

Аналіз останніх досліджень і публікацій. Розглянемо сучасні тенденції розвитку архітектури IoMT та безпеки складових на міжнародному рівні та в Україні. Загальні підходи до безпеки IoMT. Серед системних підходів до забезпечення безпеки Інтернету речей актуальною є трирівнева модель безпеки IoT, що у складі кіберфізичних технологій інтелектуалізації інфраструктури суспільства на основі концепції "об'єкт – загроза – захист" [3] . Елементи багатофункціональності Інтернету медичних речей розгортаються в дослідженні [4] на рівні технологій: штучного інтелекту, машинного навчання, глибокого навчання, блокчейн, радіочастотної ідентифікації та Індустрії 5.0. З метою побудови архітектури IoMT, яка охоплює різноманітні пристрої, вразливості та протоколи безпеки і, на цій основі, підсилення рівня кібербезпеки в системах Інтернет медичних речей, в роботі [5] запропонований підхід у просторі моделювання на основі Microsoft CyberBattleSim.

Однією з ключових вимог до створення безпечної архітектури IoMT є реалізація механізмів автентифікації, авторизації та обліку дій користувачів, що цілісно забезпечують контроль доступу до критичних ресурсів і медичних даних [6; 7]. Сучасні методи забезпечення безпеки систем IoMT з точки зору життєвого циклу інформації – відбору, передавання та зберігання даних представлені в статті [8]. Отримали розвиток сучасні методи забезпечення захисту інформації в інтелектуальних системах кібербезпеки з використанням технологій штучного інтелекту та блокчейн [9].

Безпека давачів IoMT і технологій обміну медичними даними. В роботі [10] розглянуто сучасний стан: створення нових і використання існуючих мініатюрних медичних сенсорів, що безпосередньо здійснюють відбір біофізичних параметрів організму пацієнта; мініатюрні інтерфейси для збору та первинної обробки медичних даних, отриманих від сенсорів; засоби обміну даними з віддаленими медичними центрами; автоматизовані засоби дистанційного діагностування.

У роботі [11] розглядаються питання: медичних даних, стратегії багатоетапної оцінки прогнозних показників та алгоритмів машинного навчання. Застосування інтелектуальних безпровідних давачів для системи моніторингу стану здоров'я людини з використанням когнітивних радіомереж передбачає комунікаційні зв'язки між шлюзами WBAN, сервером та наносенсорами, що робить систему вразливою до ймовірних атак. У цьому контексті в дослідженні [12] пропонується новий алгоритм шифрування на основі ДНК для забезпечення безпеки обміну медичними даними між сенсорними пристроями та центральним сховищем, якому властиві менші обчислювальні витрати під час аутентифікації, шифрування та дешифрування.

Для безпечної архітектури IoMT актуальним завжди залишається безпека сенсорних мереж. В цьому напрямку в праці [13] розглянуто інформаційну безпеку сенсорних мереж Zigbee, Wi-Fi та Bluetooth згідно моделі OSI у просторі "рівень OSI – функції – протоколи" на основі концепції "об'єкт – загроза – захист" та нормативного забезпечення, які системно створюють підхід до побудови комплексних систем безпеки сенсорного безпровідного комунікаційного середовища IoMT у складі кіберфізичних систем за профілями конфіденційність – цілісність – доступність. Як технологія протидії несанкціонованому доступу та фальсифікації конфіденційних даних в праці [14] представлена блокчейн-орієнтована система кібербезпеки для класифікації сигналів електрокардіограми (ЕКГ) на основі

машинного навчання, основна функція якої полягає у забезпеченні безпечного зв'язку між пристроями IoMT. Цікавими є підходи до забезпечення кібербезпеки інтелектуальних технологій, зокрема у частині виявлення програм-вимагачів та захисту безпровідних мереж на основі штучного інтелекту [15].

У інтелектуальних системах охорони здоров'я в комунікаційному просторі найбільше застосовуються технології Bluetooth, відповідно дуже актуальним є питання їх безпеки. В дослідженні [16] представлено децентралізований, прогнозний процес на основі глибокого навчання, призначений для автономного виявлення та блокування зловмисного трафіку, а також забезпечення комплексного захисту від мережевих атак на пристрої IoMT. Під час обміну медичними даними в процесі медичного діагностування/лікування важливим є забезпечення безпеки зв'язку між пристроями IoMT, зокрема на рівні безпровідної мережі тіла WBAN. Відповідно у цьому контексті в праці [17] запропоновано безпечний протокол аутентифікації та узгодження ключів для безпровідної мережі тілесної зони на базі Інтернету речей.

Безпека компонентів хмарної інфраструктури IoMT. З метою забезпечення конфіденційності медичних даних пацієнтів, зокрема у частині МРТ-зображень, в праці [18] розгорнуто специфіку методів криптографічного захисту даних на рівні безпечної автоматизованої системи класифікації МРТ-зображень, яка інтегрує методи шифрування з гібридними моделями глибокого навчання.

Цікавими є аналітичні дослідження у сегменті методів захисту даних за профілем конфіденційності в медичних інформаційних системах [19]: криптографічні методи, засоби контролю доступу, методи анонімізації та псевдоанонімізації, технології блокчейн для збереження цілісності даних, а також інструменти машинного навчання для виявлення аномалій у мережевому трафіку. В дослідженні [20] запропоновано метод зберігання медичних даних на основі блокчейну та реляційної бази даних, що реалізує механізм підвищення захисту цілісності даних в реляційній базі за рахунок їх верифікації в блокчейні, без розкриття вмісту цих даних.

З метою забезпечення конфіденційності інформації технічні заходи безпеки доповнюються заходами фізичної, особистої та організаційної безпеки медичних даних пацієнтів у просторі комплексу методів анонімізації [21]. У просторі забезпечення захисту та конфіденційності інформації прогресивними є сучасні технології децентралізованих баз даних, а також методи аутентифікації та авторизації [22]. У просторі захисту персональних і медичних даних в українській електронній системі охорони здоров'я впроваджують технології протидії заволодінню персональними даними пацієнтів, зокрема на рівні тестування систем захисту від фішингових атак [23].

Систематизацію сучасних методів захисту баз даних в умовах сучасних кіберзагроз та війни розглянуто в роботі [24], де авторами запропоновано алгоритм, що передбачає аудит інформаційних активів, впровадження багатофакторної автентифікації, організацію резервного копіювання, використання сучасних методів шифрування, навчання персоналу, моніторинг подій безпеки та формування комплексної політики захисту даних.

У дослідженні [25] представлено нові рішення перспективних підходів до підвищення заходів безпеки та стандартизованих протоколів для цілісного захисту медичних даних пацієнтів: алгоритми машинного навчання, технологія блокчейн та периферійні обчислення. Для захисту кібернетичного середовища хмарної інфраструктури на практиці використовуються брандмауери IoMT. У цьому відношенні в роботі [26] представлено дворівневу архітектуру системи безпеки MEDIotWALL для середовищ охорони здоров'я: система поєднує розподілений моніторинг трафіку в режимі реального часу з генерацією правил на основі штучного інтелекту.

Безпека веб-додатків. У дослідженні [27] проаналізовано загрози автентифікації, механізми та технології захисту і, на цій основі, створено системну модель безпечної багатофакторної автентифікації у ВЕБ-застосунку на основі концепції "об'єкт – загроза – захист" за структурою "ВЕБ-сторінка – ВЕБ-сервер – база даних". Розроблено алгоритмічно-програмну реалізацію системи безпечної багатофакторної автентифікації у ВЕБ-застосунку на основі застосування криптографічної хеш-функції SHA-1 та симетричного алгоритму шифрування повідомлень AES засобами мови програмування JavaScript. В роботі [28] представлено сучасні методики та підходи до моделювання загроз, які допомагають забезпечити безпеку веб-додатків, а також розглянуто методики моделювання загроз: Threat Modeling, Security Testing, Risk Assessment, Penetration Testing, Security Audits, STRIDE, DREAD, VAST, PASTA, Trike, PTA, на основі яких запропоновано оновлені і вдосконалені основні принципи безпеки веб-додатків.

Мета статті. Метою роботи є – розроблення методології побудови безпечної платформи функціонування Інтернету медичних речей для задач діагностування стану організму людини згідно зі структурою "архітектура IoMT – системи безпеки", яка реалізує конструктивний алгоритм її безпечного функціонування на основі концепції "об'єкт – загроза – захист" та уможливлює забезпечення безпеки та конфіденційності медичних даних пацієнтів новітніми технологіями: шифрування повідомлень при

передаванні; аутентифікації користувачів як протидія несанкціонованому доступу; моніторингу мережі для виявлення аномалій/вторгнень.

Завданням дослідження є:

1. Створити платформу безпечної архітектури Інтернету медичних речей для задач медичного діагностування стану організму людини у функціональному просторі “відбір – обробка – аналіз – управління”;
2. Побудувати зовнішні системи безпеки складових IoMT за впливу комплексу випадкових і цілеспрямованих загроз на рівні: давачів, сенсорних мереж, компонентів хмарної інфраструктури, інформаційних процесів;
3. Розробити алгоритмічно-програмне забезпечення криптографічного захисту медичних даних в сенсорній безпровідній мережі Bluetooth на основі симетричного блокового алгоритму шифрування AES-256 в режимі GCM засобами мови програмування Python.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Методологія побудови безпечної платформи IoMT для задач діагностування. Усталена структура Інтернету медичних речей охоплює такі складові: пристрої та давачі; безпровідні технології обміну даними; хмарні платформи для зберігання та обробки даних; інтерфейси користувачів; технології безпеки та конфіденційність.

З метою безпечного відбору біофізичних параметрів стану організму людини у просторі “контроль – обробка – аналіз – прийняття рішення” розглянемо основні технічні характеристики: давачів моніторингу біофізичних параметрів організму людини та давачів безпеки пацієнта (табл. 1.1-1.2); сенсорних мереж Wi-Fi, Bluetooth (табл. 2.1-2.2).

Таблиця 1.1

Технічні характеристики давачів IoMT: моніторинг біофізичних параметрів організму людини

Давачі	Модель		Технічні характеристики
Давач серцевого ритму	Wellue DuoEK Portable ECG Monitor		Портативний ECG-давач для безперервного моніторингу серцевого ритму. Діапазон вимірювання – 30-250 уд./хв. Bluetooth-передавання даних, синхронізація зі смартфоном, автономна робота до 20 годин.
Пульсоксиметр	Contec CMS50D		Пульсоксиметр для вимірювання рівня сатурації крові та пульсу. Діапазон SpO_2 – 70-100%, точність ±2%, OLED-дисплей, відображення показників пульсу в реальному часі.
Тонометр	Omron M7 Intelli IT		Автоматичний тонометр для контролю артеріального тиску. Діапазон вимірювання – 40-260 мм рт. ст.; пам’ять результатів. Bluetooth-синхронізація, система індикації аритмії та високої точності вимірювання.
Глюкометр	Accu-Chek Instant		Глюкометр для контролю рівня глюкози в крові. Діапазон вимірювання – 1.1-33.3 ммоль/л. Bluetooth-синхронізація зі смартфоном, висока точність вимірювання, автоматичне збереження результатів.
Давач частоти дихання	Polar H10		Нагрудний давач моніторингу дихання та активності пацієнта. Передавання даних через Bluetooth Low Energy, безперервний моніторинг 24/7, висока точність вимірювання частоти дихання та серцевого ритму.
Давач температури тіла	CORE Body / Temperature Sensor		Wearable-давач для безперервного контролю температури тіла. Діапазон вимірювання – 32-42°C, точність ±0.1°C, передавання даних через Bluetooth, моніторинг у режимі реального часу.

Таблиця 1.2

Технічні характеристики давачів IoMT: безпека пацієнта

Давачі	Модель	Технічні характеристики
Давач падіння пацієнта	Smart Caregiver FallGuard 	Автоматичне виявлення падіння, акселерометр + гіроскоп, час спрацювання до 1 с, передавання даних через Bluetooth Low Energy
Система контролю доступу	ZKTeco SpeedFace V5L 	Система контролю доступу з RFID/NFC та біометричною ідентифікацією персоналу. Підтримує журнал доступу, багатофакторну автентифікацію та віддалене адміністрування
Система відеоспостереження	Hikvision DS-2CD2043G2-I 	IP-камера відеоспостереження. Роздільна здатність – 4 Мп, FullHD/2K відео, нічне бачення до 40 м, віддалений моніторинг, PoE-живлення, підтримка запису подій та виявлення руху
Система сигналізації	Honeywell EBI Nurse Call System 	Інтелектуальна система сигналізації та виклику медперсоналу. Підтримує звукове й світлове оповіщення, централізований моніторинг палат, інтеграцію з медичною інформаційною системою та автоматичне передавання тривожних повідомлень у режимі реального часу
Давач руху пацієнта	Securitas Healthcare Silent Knight Motion Sensor 	Давач моніторингу активності пацієнта. Діапазон виявлення – до 5 м, кут огляду – 120, передавання даних через Wi-Fi/BLE, підтримка виявлення руху та падіння пацієнта.

Таблиця 2.1

Технічні характеристики безпровідної сенсорної мережі Wi-Fi

Характеристики	Параметри
Стандарт	IEEE 802.11ax
Протоколи	TCP/IP, HTTPS, MQTT
Частота	2.4 / 5 ГГц
Швидкість	до 9.6 Гбіт/с
Дальність	до 100 м
Безпека	WPA3, TLS
Призначення	Сервери, шлюзи, IoMT

Таблиця 2.2

Технічні характеристики безпровідної сенсорної мережі Bluetooth

Характеристики	Параметри
Стандарт	Bluetooth 5.0 BLE
Протоколи	GATT, ATT
Частота	2.4 ГГц
Швидкість	до 2 Мбіт/с
Дальність	10-30 м
Безпека	AES-128, Pairing
Призначення	Медичні сенсори

На основі розглянутих характеристик давачів і безпровідних сенсорних мереж Wi-Fi та Bluetooth відповідно запропоновано платформи безпечної архітектури IoMT (рис. 1-2), а також алгоритм функціонування IoMT (рис. 3) та фази інформаційних процесів IoMT (рис. 4), які цілісно спрямовані на забезпечення захисту і конфіденційності медичних даних пацієнта, отриманих при відборі, обробці, аналізі, прийнятті діагностичного рішення щодо стану організму людини.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

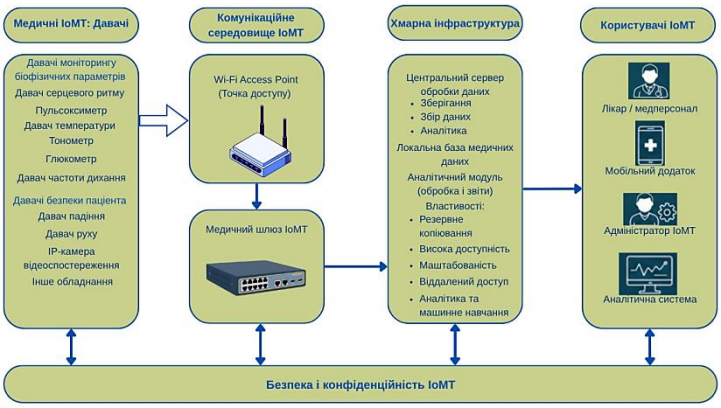

Рис. 1. Платформа безпечної архітектури IoMT на основі безпровідної сенсорної мережі WI-FI

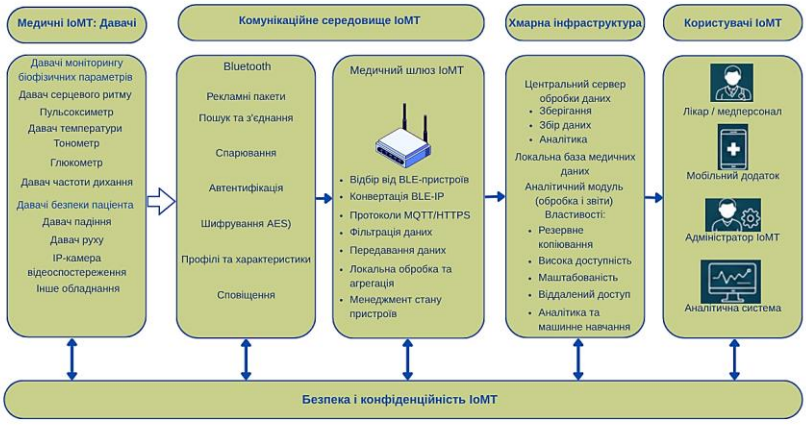

Рис. 2. Платформа безпечної архітектури IoMT на основі безпровідної сенсорної мережі Bluetooth

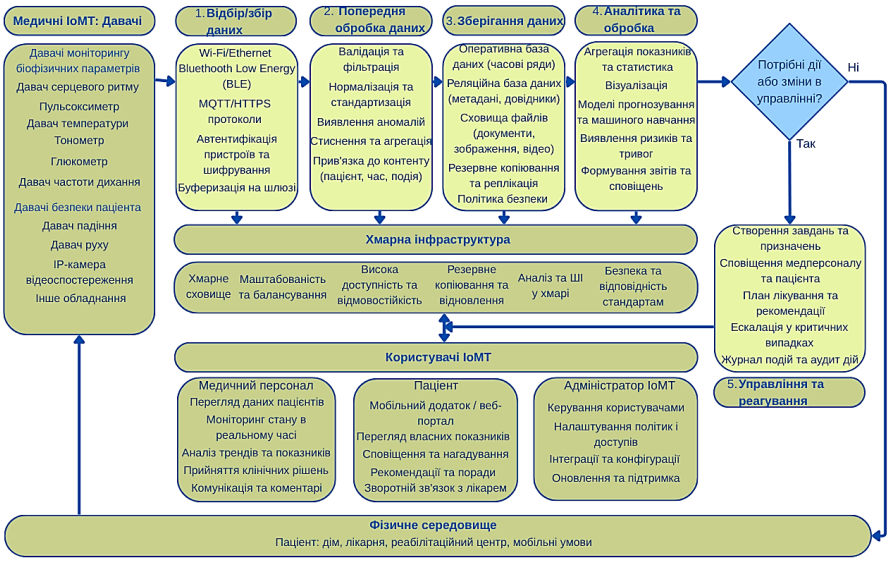

Рис. 3. Алгоритм функціонування IoMT

Рис. 4. Фази інформаційних процесів в IoMT

Системи безпеки складових IoMT: зовнішні загрози. Об'єктом дослідження інтелектуальної медицини є – сегмент Інтернету медичних речей, функціональна архітектура якого об'єднує: медичні давачі, безпровідні сенсорні мережі, хмарну інфраструктуру (серверне обладнання та програмне забезпечення, аналітику даних на основі ШІ) та забезпечує безперервний контроль біофізичних параметрів організму людини, передавання, обробку та аналіз медичних даних у режимі реального часу і, на цій основі, прийняття рішення про встановлення діагнозу і призначення подальшого лікування пацієнта. Предметом дослідження є – системи безпеки основних складових архітектури IoMT на основі концепції "об'єкт – загроза – захист", моделі загроз STRIDE та моделі відкритих систем OSI.

Критично важливим для забезпечення безпеки інтелектуальної медицини є захист IoMT від зовнішніх загроз, оскільки порушення функціонування медичних давачів або витік медичних даних може призвести до неточного відбору біофізичних параметрів систем організму людини, відповідно до неточності медичного діагностування, а значить встановлення неправильного діагнозу, компрометації персональних медичних даних пацієнта та ймовірної загрози життю людини. Основними векторами зовнішніх загроз для архітектури IoMT є:

- несанкціонований доступ до пристроїв і давачів Інтернету медичних речей;
- перехоплення або модифікація медичних даних про стан здоров'я людини під час передавання безпровідними каналами зв'язку;
- атаки типу DoS/DDoS на сервери та мережеву інфраструктуру IoMT;
- підміна показників біофізичних параметрів медичних давачів;
- компрометація Wi-Fi та BLE-з'єднань;
- шкідливе програмне забезпечення та ransomware-атаки;
- витік конфіденційної медичної інформації;
- фізичне пошкодження або відключення медичних давачів або пристроїв.

Розглянемо системи безпеки основних складових IoMT на рівні комплексу зовнішніх загроз.

Система безпеки давачів IoMT побудована на основі концепції "об'єкт – загроза – захист" згідно моделі STRIDE і представлена в табл. 3.

Таблиця 3

Система безпеки давачів IoMT: моніторинг біофізичних параметрів, безпека пацієнта

Давачі	Модель загроз STRIDE	Загрози		Технології протидії загрозам	
		Випадкові	Цілеспрямовані	Випадковим	Цілеспрямованим
Моніторинг біофізичних параметрів ECG Sensor	S (автентичність)	Збій сенсора, втрата сигналу Помилка калібрування Перепади живлення	Підміна медичного пристрою Spoofing ECG-даних Несанкціонова не підключення	Резервне живлення UPS Автоматичне калібрування сенсора Дублювання каналів передавання даних Система моніторингу стану пристрою	Багатофакторна автентифікація Цифрові сертифікати, TLS/AES-шифрування Журналювання доступу Контроль MAC-адрес

Пульсоксиметр (SpO_2)	T (цілісність)	Некоректне зчитування через рух пацієнта Розряд батареї Нестабільне BLE-з'єднання	Модифікація показників сатурації Підробка медичних даних	Резервне джерело живлення Автоматична перевірка коректності показників Контроль стабільності сигналу Повторне зчитування даних	Контроль цілісності даних AES-шифрування Цифровий підпис медичних записів IDS/IPS моніторинг
Глюкометр	R (авторство)	Помилка вимірювання Нестабільна робота сенсора Пошкодження тест-смужок	Підміна показників глюкози Модифікація медичних записів	Автоматична перевірка сенсора Журналювання результатів Резервне збереження даних	Цифровий підпис даних Аудит дій користувачів Контроль версій записів Шифрування медичної інформації
Безпека пацієнта Система контролю доступу	I (авторизація)	втрата RFID-картки Збій системи зчитування	Клонування NFC/RFID Несанкціонований доступ	Резервні контролери доступу Дублювання бази користувачів Журнал подій Резервне живлення	Біометрична автентифікація MFA Обмеження кількості спроб входу Шифрування ідентифікаційних даних
Давач падіння пацієнта	D (доступність)	Помилкове спрацювання Відмова сенсора	Блокування Глушіння сигналу BLE	Автоматична перевірка працездатності сенсора Резервний канал зв'язку Система самодіагностики	IDS/IPS захищений BLE-канал Контроль активності пристрою Виявлення аномальної поведінки
Система відеоспостереження	E (конфіденційність)	Втрата мережевого з'єднання Збій живлення Помилки запису відео	Перехоплення відеопотоку Несанкціонований доступ до камер Підміна відео	Резервне копіювання відео UPS-живлення Дублювання серверів зберігання Контроль стабільності мережі	VPN, WPA3 Сегментація мережі VLAN Шифрування відеопотоку Контроль доступу RBAC

Система безпеки комунікаційного середовища IoMT побудована на основі концепції "об'єкт – загроза – захист" згідно моделі OSI і представлена в табл. 4.

Таблиця 4

Система безпеки безпровідного комунікаційного середовища

Технологія / стандарт	Рівень моделі OSI	Загрози		Технології безпеки
		Випадкові	Цілеспрямовані	
Wi-Fi (IEEE 802.11)	Фізичний	Інтерференція сигналу від іншого обладнання Нестабільне	Jamming-атаки (глушіння сигналу) Фізичне викрадення або	Використання UPS та резервного живлення Фізичний захист точок доступу

		живлення точки доступу Фізичне пошкодження роутера або мережевого кабелю Перебої передавання даних Неправильне розміщення точки	заміна IoMT-пристрою Підключення несанкціонованої точки доступу (Rogue AP) DoS-атаки Перехоплення Wi-Fi сигналу Несанкціонований фізичний доступ до мережевого обладнання	Резервування мережевого обладнання IDS/IPS моніторинг Сегментація мережі VLAN VPN для захищеного передавання даних Постійний моніторинг підключень Контроль рівня сигналу Використання захищених приміщень для серверного та мережевого обладнання
Wi-Fi (IEEE 802.11)	Канальний рівень	Помилки передавання кадрів Нестабільна робота Wi-Fi адаптера Конфлікти MAC-адрес Перевантаження безпровідного каналу Втрата пакетів даних Неправильна конфігурація точки доступу Помилки автентифікації пристроїв	Підміна MAC-адрес (MAC Spoofing) Атаки на WPA2/WPA3 Brute-force атаки на пароль Wi-Fi Перехоплення пакетів передавання даних Spoofing IoMT-пристроїв Replay-атаки; підключення неавторизованих клієнтів до мережі	Використання WPA3/WPA2-Enterprise AES-шифрування EAP-TLS автентифікація MAC-фільтрація Контроль доступу 802.1X WIPS/WIDS системи виявлення атак Сегментація мережі VLAN Регулярна зміна ключів доступу Журналювання підключень та активності користувачів
Wi-Fi (IEEE 802.11)	Мережевий рівень	Втрата мережевого з'єднання Помилки маршрутизації Перевантаження мережі Нестабільне передавання медичних даних Конфлікти IP-адрес Помилки DNS Затримки передавання пакетів	MITM-атаки DoS/DDoS-атаки ARP Spoofing; DNS Spoofing Перехоплення медичних даних Підміна IP-адрес Несанкціонована маршрутизація трафіку Мережеве сканування та флуд-атаки	VPN та IPsec для захищеного передавання даних Firewall; IDS/IPS системи Сегментація мережі VLAN Контроль маршрутизації; моніторинг мережевого трафіку DNS-захист Багаторівнева автентифікація Шифрування TLS/AES; обмеження доступу до мережевих сервісів
Bluetooth Low Energy (BLE)	Фізичний рівень	Розряд батареї wearable-пристрою Нестабільний BLE-сигнал Електромагнітні перешкоди Фізичне пошкодження сенсора Перебої передавання даних Відключення IoMT-пристрою	Jamming BLE-сигналу Фізичне викрадення медичного сенсора Підключення несанкціонованого BLE-пристрою Перехоплення сигналу Блокування роботи wearable-сенсора	Резервне живлення та контроль заряду батареї Моніторинг активності BLE-пристроїв Захищене розміщення IoMT-пристроїв IDS/IPS моніторинг Контроль рівня сигналу Фізичний захист медичних сенсорів Резервний канал передавання даних
Bluetooth Low Energy	Канальний рівень	Помилки pairing-процесу	BLE Spoofing Replay-атаки	Secure BLE Pairing AES-шифрування

(BLE)		Нестабільна синхронізація пристроїв Конфлікти адрес BLE-пристроїв Втрата пакетів даних Помилки автентифікації Нестабільна робота wearable-сенсорів	Перехоплення пакетів передавання даних Brute-force атаки на pairing Несанкціоноване підключення до медичного сенсора Підміна BLE-пристрою	Багатофакторна автентифікація Whitelist BLE-пристроїв Контроль MAC/BLE-адрес Регулярне оновлення ключів автентифікації Журналювання підключень Системи виявлення аномальної активності
Bluetooth Low Energy (BLE)	Мережевий рівень	Втрата мережевого з'єднання між IoMT-пристроями Затримки передавання медичних даних Помилки маршрутизації через gateway Перевантаження мережевого шлюзу Нестабільна синхронізація з сервером	MITM-атаки Перехоплення медичних даних Підміна IP/BLE Gateway DoS-атаки на gateway Несанкціоноване передавання даних Мережеве сканування IoMT-пристроїв	VPN та TLS-шифрування Захищений IoT Gateway Firewall IDS/IPS системи Сегментація IoMT-мережі Контроль маршрутизації Моніторинг мережевого трафіку Автентифікація gateway-пристроїв Шифрування медичних даних AES-256

Система безпеки хмарної інфраструктури IoMT побудована на основі концепції "об'єкт – загроза – захист" згідно моделі STRIDE і представлена в табл. 5.

Таблиця 5

Система безпеки хмарної інфраструктури IoMT

Хмарна інфра-структура	Модель STRIDE	Загрози		Протидія загрозам	
		Випадкові	Цілеспрямовані	Підходи	Технології безпеки
Локальна база медичних даних	S (автен-тичність)	Втрата або пошкодження облікових даних медперсоналу Збій сервісу автентифікації Помилки конфігурації доступу до БД	Phishing медичного персоналу Credential stuffing / brute force SQL-injection для обходу автентифікації Session hijacking адміністратора БД	Журналювання входів Резервування сервісів автентифікації Моніторинг активних сесій IDS/IPS контроль	MFA автентифікація TLS/mTLS шифрування RBAC модель доступу IAM контроль привілеїв Захист API-token
	T (ціліс-ність)	Пошкодження медичних записів через збій сервера Помилки синхронізації IoMT-пристроїв Некоректне оновлення даних пацієнта	Telemetry tampering медичних показників Модифікація результатів аналізів SQL-injection для зміни даних Видалення критичних записів пацієнта	RAID та backup-системи Контроль цілісності БД Автоматичне відновлення транзакцій Моніторинг змін записів	Цифровий підпис медичних записів Контроль hash-сум Database activity monitoring (DAM) SIEM-моніторинг IDS/IPS захист
	R (автор-ство)	Втрата журналів аудиту Помилки	Підробка авторства медичних записів Фальсифікація журналів подій	Архівування журналів Резервне копіювання логів	Цифрові підписи SIEM та audit logging Контроль версій

		логування дій користувачів Некоректна синхронізація часових міток	Перехоплення сесії лікаря Приховування несанкціонованих змін	Синхронізація часу NTP	записів Immutable logs Моніторинг anomalous activity
	I (конфіденційність)	Помилки конфігурації каналів передавання даних Випадковий витік резервних копій Некоректне налаштування прав доступу	Несанкціонований доступ до медичних записів Перехоплення трафіку між IoMT-пристроями та сервером Отримання доступу через вразливості API	Контроль доступу до резервних копій Моніторинг мережевих з'єднань Сегментація мережі VLAN Резервування каналів передавання даних	Шифрування бази даних AES-256 VPN та TLS-захист каналів зв'язку Рольова модель доступу RBAC Система запобігання витоку даних DLP
	D (доступність)	Перевантаження серверів БД Втрата електроживлення Відмова мережевого обладнання Пошкодження storage-систем	DoS/DDoS атаки на сервери БД Ransomware атаки Перевантаження системи авторизації Блокування доступу до медичних записів	Резервне живлення UPS Failover-кластери Backup та disaster recovery Моніторинг навантаження серверів	Anti-DDoS захист Мережеві екрани Firewall Балансування навантаження EDR/XDR захист серверів
	E (авторизація)	Помилки налаштування ролей доступу Некоректне призначення прав користувачів Втрата токенів авторизації	Підвищення привілеїв зловмисником Компрометація облікових записів адміністраторів Викрадення токенів доступу Обхід політик доступу	Регулярний аудит ролей Контроль активних привілеїв Моніторинг змін прав доступу Резервування політик IAM	Багатофакторна автентифікація MFA Рольова та атрибутна модель доступу Система керування привілейованим доступом PAM Автоматичне завершення неактивних сесій
Аналітика даних на основі штучного інтелекту	S (автентичність)	Помилки автентифікації користувачів Збій сервісу IAM Некоректна конфігурація API-доступу Помилки синхронізації облікових запис	Фішинг медичного персоналу Підбір паролів та brute force атаки Перехоплення сесії оператора IAC Підміна API-клієнта Несанкціонований доступ до AI-модуля	Резервування сервісів автентифікації Моніторинг активних сесій Контроль API-підключень Журналювання авторизацій	Багатофакторна автентифікація MFA OAuth2/OpenID Connect TLS/mTLS захист API RBAC/IAM контроль доступу
	T (цілісність)	Помилки обробки медичних	Підміна медичних показників Підробка результатів	Резервне копіювання конфігурацій AI	Цифровий підпис медичних даних Контроль hash-

		даних Збій аналітики даних на основі ШІ при перевантаженні Пошкодження cache або temporary storage	AI-аналізу Впровадження шкідливих даних через API Маніпуляція навчальними даними AI-моделі	Контроль цілісності телеметрії Резервування серверів IAC Моніторинг AI-модулів	сум Перевірка та фільтрація API-запитів SIEM-моніторинг IDS/IPS захист
	R (авторство)	Втрата audit-log файлів Помилки журналювання дій операторів Некоректна синхронізація часових міток	Підробка журналів подій Фальсифікація авторства змін Приховування несанкціонованих дій Компрометація облікового запису оператора	Архівування журналів аудиту Резервне копіювання логів Контроль синхронізації часу Моніторинг активності користувачів	Незмінювані журнали подій Immutable logs SIEM audit monitoring Цифрові підписи подій Контроль версій змін
	I (конфіденційність)	Помилки конфігурації cloud-середовища Випадковий витік медичних даних Некоректні політики доступу API Помилки синхронізації backup-систем	Несанкціонований доступ до медичних записів Перехоплення мережевого трафіку Компрометація хмарного сховища Отримання доступу через вразливості API	Сегментація мережі Контроль доступу до хмарних ресурсів Моніторинг мережевих з'єднань Резервне копіювання даних	Шифрування медичних даних AES-256 VPN та TLS-захист каналів зв'язку Рольова модель доступу RBAC Система запобігання витоку даних DLP
	D (доступність)	Перевантаження аналітики даних на основі ШІ Відмова cloud-сервісів Пошкодження API-gateway Втрата мережевого з'єднання	DoS/DDoS атаки на сервери IAC Шифрування серверів шкідливим ПЗ Перевантаження модулів аналітики даних на основі ШІ Блокування доступу до медичних сервісів	Резервування серверів Балансування навантаження Резервне живлення та backup-системи Моніторинг навантаження IAC	Мережеві екрани Firewall WAF-захист API Системи виявлення атак IDS/IPS Обмеження кількості запитів до API
	E (авторизація)	Помилки налаштування прав доступу Некоректне призначення ролей медперсоналу Втрата access-token	Підвищення привілеїв зловмисником Компрометація облікових записів адміністраторів Викрадення токенів доступу Обхід політик доступу	Аудит ролей та привілеїв Моніторинг змін прав доступу Контроль активних сесій користувачів Резервування політик доступу	Багатофакторна автентифікація MFA Система керування привілейованим доступом PAM Автоматичне завершення неактивних сесій

Система безпеки інформаційних процесів в IoMT побудована на основі концепції "об'єкт – загроза – захист" і представлена в табл. 6.

Таблиця 6

Система безпеки IoMT на рівні інформаційних процесів

Фази ІП в IoMT	Загрози		Протидія загрозам	
	Випадкові	Цілеспрямовані	Підходи	Технології безпеки
Відбір/ Збір медичних даних	Помилки конфігурації IoMT-пристроїв Відмова сенсорів через збій обладнання Некоректна синхронізація телеметрії Втрата даних через нестабільний зв'язок	Підміна показників медичних сенсорів MITM-атаки під час передачі даних Несанкціонований доступ до IoMT-пристроїв DoS/DDoS атаки на канали передачі	Моніторинг стану IoMT-пристроїв Журналювання подій Резервування каналів передавання даних Контроль коректності телеметрії	Шифрування даних AES/TLS VPN-захист каналів зв'язку IDS/IPS моніторинг Багатофакторна автентифікація пристроїв
Передавання та зберігання медичних даних	Втрата пакетів під час передавання Помилки резервного копіювання Відмова cloud-сервісів Пошкодження систем зберігання даних	Перехоплення мережевого трафіку Витік медичних даних Несанкціонований доступ до cloud storage Видалення або шифрування резервних копій	Backup та disaster recovery Моніторинг мережевого трафіку Failover-системи Контроль доступності серверів	VPN/TLS захист каналів Шифрування медичних даних AES-256 DLP-система захисту даних RBAC/IAM контроль доступу
Обробка та аналіз медичних даних на основі ШІ	Перевантаження аналітики даних на основі ШІ Помилки алгоритмів обробки даних Пошкодження тимчасових даних Відмова серверного обладнання	Підробка результатів ШІ-аналізу Впровадження шкідливого коду Маніпуляція навчальними даними ШІ-моделі Ransomware-атаки	Backup конфігурацій на основі ШІ Моніторинг ресурсів системи аналітики даних Резервування серверів Контроль цілісності даних	SIEM та IDS/IPS системи EDR/XDR захист серверів Контроль API-запитів Цифровий підпис результатів аналізу

Криптографічний захист інформації в комунікаційному середовищі IoMT: алгоритм шифрування AES-256-GCM, мова Python. З метою практичної реалізації одного із сегментів системи безпеки комунікаційного середовища IoMT, зокрема у частині безпечного обміну медичної інформації безпровідними сенсорними мережами, розроблено алгоритмічно-програмний механізм криптографічного захисту повідомлень. Як було визначено у моделі загроз STRIDE (табл. 4), передавання медичних даних через Bluetooth Low Energy (BLE) вразливе до перехоплення, підміни та атак повторного відтворення (Replay-атак) на канальному та мережевому рівнях OSI. Для нівелювання цих загроз та забезпечення цілісності й конфіденційності телеметрії застосовано симетричний алгоритм блокового шифрування AES-256 у режимі GCM (Galois/Counter Mode). Програмну реалізацію виконано мовою Python, що забезпечує високу продуктивність криптографічних обчислень, кросплатформеність та ефективну роботу з байтовими масивами медичних даних. Архітектура програмного рішення (файл iomt_crypto.py) базується на об'єктно-орієнтованому підході та охоплює такі ключові компоненти, класи та методи:

Криптографічні модулі (бібліотека cryptography). Залучено класи AESGCM, ec (еліптичні криви) та HKDF для реалізації стійкого криптографічного перетворення. Стандартні модулі os, json та time використано для серіалізації даних, генерації криптографічно стійких псевдовипадкових векторів ініціалізації (Nonce) і фіксації часових міток.

Об'єктна модель та базові класи. Програмний код структурно розділений на класи, що є цифровими двійниками реальних пристроїв архітектури IoMT:

- Клас IoMTNode: Базовий криптографічний клас вузла.
  - Метод get_public_key_bytes(): здійснює серіалізацію згенерованого еліптичного публічного ключа (у стандарті форматування DER) для його безпечного передаванння через відкриті канали BLE.

- Метод derive_shared_key(): реалізує фазу узгодження ключів (Pairing). Приймає публічний ключ партнера, виконує обмін за асиметричним протоколом ECDH (крива SECP256R1) та виконує деривацію спільного секрету у 32-байтовий симетричний ключ за допомогою функції HKDF.

- Клас MedicalSensor (нащадок IoMTNode): Моделює давач відбору біофізичних параметрів.
  - Метод send_reading(): відповідає за формування корисного навантаження (Payload). Генерує унікальний 12-байтний вектор ініціалізації за допомогою функції os.urandom(12) та викликає метод encrypt() об'єкта AESGCM для зашифровування масиву медичних даних разом з асоційованими даними (AAD).
- Клас MedicalGateway (нащадок IoMTNode): Імітує мережевий шлюз комунікаційного середовища.
  - Метод receive_reading(): приймає зашифрований BLE-пакет, розділяє його на вектор ініціалізації та шифротекст, після чого викликає метод decrypt(). Також містить логіку верифікації порядкового номера (sequence_number) для відхилення застарілих пакетів.
- Функція visualize_encryption(): Аналітична функція, яка покроково розкладає алгоритм AES-GCM на складові (відкритий текст, Hex-представлення, Nonce, асоційовані дані AAD, шифротекст та тег автентифікації) для забезпечення наочності перетворень.

Функціональні характеристики програмної реалізації.

- Гарантія цілісності (Tampering Protection): На відміну від класичного шифрування, режим AES-GCM паралельно генерує 16-байтовий тег автентифікації (Auth Tag). Якщо зловмисник змінить хоча б один біт зашифрованих показників у радіоефірі, метод decrypt() викличе виняток InvalidTag, і пакет буде заблоковано.
- Захист від атак повторного відтворення (Replay Attacks): Інтеграція часової мітки та інкрементованого параметра sequence_number у метод send_reading() гарантує, що перехоплений пакет не може бути відправлений шлюзу повторно.

Оптимізація криптографічного навантаження (Overhead): Для автономних давачів IoMT критичним є об'єм трафіку. Алгоритм розроблено так, що він додає суворо фіксований розмір криптографічного навантаження — рівно 28 байт (12 байт Nonce та 16 байт Auth Tag) незалежно від об'єму телеметрії, що унеможливлює фрагментацію пакетів у мережі BLE. Для підтвердження коректності роботи алгоритму задіяно функцію visualize_encryption().

На рис. 5 наведено скриншот виконання програми, який демонструє декомпозицію процесу: перетворення відкритого JSON-формату у зашифрований пакет із відокремленням вектора ініціалізації та тегу автентифікації. Враховуючи обмежені апаратні ресурси медичних давачів фізичного простору, проведено оцінку швидкодії запропонованого рішення. Результати стрес-тестування на 5000 ітерацій (рис.6) підтверджують, що обраний стек технологій забезпечує високу пропускну здатність та мінімальні затримки на криптографічні перетворення.

```
[ СИСТЕМА ] Ініціалізація вузлів: Sensor (PT-1045) та Gateway
[ УЗГОДЖЕННЯ ] Алгоритм ECDH + HKDF. Час виконання: 1.55 мс

======================================================================
 [ ВІЗУАЛІЗАЦІЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ (AES-256-GCM) ]
======================================================================
 1. Відкритий текст (JSON): {"patient_id": "PT-1045", "hr": 72, "spo2": 99, "seq": 1, "ts": 1715000000}
 2. Hex-представлення:      7b2270617469656e745f6964223a202250542d3130343...
 3. Вектор ініціалізації:   c67c30d66be39253907169d7 (12 байт)
 4. Асоційовані дані (AAD): 496f4d545f76312e30 ('IoMT_v1.0')
 5. Шифротекст (Payload):   ce21cbc5597c7d9b204230bc1760f095fc847c0f7693e...
 6. Тег автентифікації:     425f3c2c9a738d17c5ad39064a195cc1 (16 байт)
======================================================================
```

Рис.5. Скриншот процесу автентифікованого шифрування медичних даних на основі алгоритму AES-256-GCM

```
[ БЕНЧМАРК ] Запуск стрес-тесту на 5000 ітерацій...

-----------------------------------------------------------------------
 МЕТРИКА ПРОДУКТИВНОСТІ          | ШИФРУВАННЯ (Tx)  | РОЗШИФРУВАННЯ (Rx)
-----------------------------------------------------------------------
 Середній час на 1 пакет (мс)    | 0.0093           | 0.0077
 Швидкодія (операцій/с)          | 107060           | 129869
 Пропускна здатність (МБ/с)      | 7.96             | 9.66
-----------------------------------------------------------------------
```

Рис.6. Скриншот метрики швидкодії криптографічного перетворення в системі IoMT

Отримані кількісні результати підтверджують високу швидкодію алгоритму, що робить запропоновану програмну реалізацію ефективною та енергоощадною для інтеграції в загальну платформу безпечної архітектури IoMT.

ВИСНОВКИ

В роботі запропоновано методологію побудови безпечного Інтернету медичних речей для діагностування стану організму людини, яку розгорнуто 1) платформою безпечної архітектури IoMT "давачі – безпровідні сенсорні мережі – хмарна інфраструктура – безпека та конфіденційність" за впливу комплексу зовнішніх загроз; 2) системами безпеки складових IoMT згідно: концепції "об'єкт – загроза – захист"; моделі STRIDE для давачів та аналітики даних на основі штучного інтелекту; моделі OSI безпровідних мереж Wi-Fi, Bluetooth; 3) алгоритмічно-програмним забезпеченням практичної реалізації механізму захисту медичної інформації в безпровідній сенсорній мережі Bluetooth на основі симетричного блокового шифрування AES-256 в режимі GCM засобами мови програмування Python , що є розвитком системних підходів до безпечного діагностування стану організму людини в умовах сучасних загроз в кіберпросторі і впровадження систем раннього запобігання та реагування на рівні кібердіалогу. Запропонована платформа безпечного функціонування Інтернету медичних речей "архітектура IoMT – системи безпеки" передбачає розвиток підходів до побудови систем безпеки складових IoMT за впливу комплексу внутрішніх загроз на апаратному і програмному рівнях у просторі заходів кібердіалогу Україна – ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Association of Industrial Automation Enterprises of Ukraine. (2018). Industry 4.0 development strategy [In Ukrainian].
2. National Security and Defense Council of Ukraine. (2021). Cybersecurity strategy of Ukraine for 2021–2025 [In Ukrainian].
3. Vasylyshyn, S., Opirskyy, I., Susukailo, V., Mykhaylova, O., Harasymchuk, O., Sovyn, Y., Tyshyk, I., Dudykevych, V., Mykytyn, H., Bobalo, Y., & Stosyk, T. (2025). Advancements in cybersecurity next-generation systems and applications: Collective monograph. CRC Press.
4. Mathkor, D. M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., & Haque, S. (2024). Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. Journal of Infection and Public Health, 17(4), 559–572. https://doi.org/10.1016/j.jiph.2024.01.013
5. Nadhir, A. M., Mounir, B., Abdelkader, L., & Hammoudeh, M. (2025). Enhancing cybersecurity in healthcare IoT systems using reinforcement learning. Transportation Research Procedia, 84, 113–120. https://doi.org/10.1016/j.trpro.2025.03.053
6. Maksymovych, V., Nyemkova, E., Justice, C., Shabatura, M., Harasymchuk, O., Lakh, Y., & Rusynko, M. (2022). Simulation of authentication in information-processing electronic devices based on Poisson pulse sequence generators. Electronics, 11(13), Article 2039. https://doi.org/10.3390/electronics11132039
7. Shevchuk, D., Harasymchuk, O., Partyka, A., & Korshun, N. (2023). Designing secured services for authentication, authorization, and accounting of users. CEUR Workshop Proceedings, 207–225.
8. Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a secure and sustainable internet of medical things (IoMT): Requirements, design challenges, security techniques, and future trends. Sustainability, 15(7), Article 6177. https://doi.org/10.3390/su15076177
9. Harasymchuk, O., Opirskyy, I., et al. (2025). Modern methods of ensuring information protection in cybersecurity systems using artificial intelligence and blockchain technology: Collective monograph. Technology Center PC. https://doi.org/10.15587/978-617-8360-12-2
10. Mintser, O. P., Romanov, V. O., Haleliuka, I. B., & Voronenko, O. V. (2020). Artificial intelligence technologies in medical practice [In Ukrainian]. Medical Informatics and Engineering, (2), 17–27. https://doi.org/10.11603/mie.1996-1960.2020.2.11171
11. Hupalo, & Melnyk, A. (2021). Acquisition and processing of data in CPS for remote monitoring of the human functional state. Advances in Cyber-Physical Systems, 6(1), 14–20. https://doi.org/10.23939/acps2021.01.014
12. Jabeen, T., Jabeen, I., Ashraf, H., Ullah, A., Jhanjhi, N. Z., Ghoniem, R. M., & Ray, S. K. (2023). Smart wireless sensor technology for healthcare monitoring system using cognitive radio networks. Sensors, 23(13), Article 6104. https://doi.org/10.3390/s23136104
13. Bobalo, Yu. Ya., Dudykevych, V. B., & Mykytyn, H. V. (2020). Strategic security of the "object–information technology" system: Monograph [In Ukrainian]. Lviv Polytechnic Publishing House.
14. Ameen, A. H., Mohammed, M. A., & Rashid, A. N. (2024). Enhancing security in IoMT: A blockchain-based cybersecurity framework for machine learning-driven ECG signal classification. Fusion: Practice & Applications, 14(1), 221–251. https://doi.org/10.54216/FPA.140117

15. Harasymchuk, O., Opirskyy, I., Banakh, R., et al. (2025). Intelligent cyber defence systems: Detection of ransomware and protection of wireless networks based on artificial intelligence technologies: Collective monograph. Technology Center PC. https://doi.org/10.15587/978-617-8360-22-1
16. Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., Hammoudeh, M., & Qadir, J. (2022). Secure Bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. Sensors, 22(21), Article 8280. https://doi.org/10.3390/s22218280
17. Soni, M., & Singh, D. K. (2022). LAKA: Lightweight authentication and key agreement protocol for internet of things based wireless body area network. Wireless Personal Communications, 127, 1067–1084. https://doi.org/10.1007/s11277-021-08565-2
18. Rezk, N. G., Alshathri, S., Sayed, A., Hemdan, E. E. D., & El-Behery, H. (2025). Secure hybrid deep learning for MRI-based brain tumor detection in smart medical IoT systems. Diagnostics, 15(5), Article 639. https://doi.org/10.3390/diagnostics15050639
19. Tokar, P. Yu. (2025). Methods for protecting the confidentiality of patient data in medical information systems: An analytical review [In Ukrainian]. Scientific Works of Vinnytsia National Technical University, (3), 133–137. https://doi.org/10.31649/2307-5376-2025-3-133-137
20. Baryshev, Yu. V., & Lanova, V. S. (2023). A method for secure storage of medical data based on a relational database and blockchain [In Ukrainian]. Scientific Works of Vinnytsia National Technical University, (3), 9–17. https://doi.org/10.31649/2307-5376-2023-3-9-17
21. Havrysh, B. M., Tymchenko, O. V., & Kustra, N. O. (2023). Methods for anonymizing medical databases [In Ukrainian]. Scientific Papers, 1(66), 68–79. https://doi.org/10.32403/1998-6912-2023-1-66-68-79
22. Petriv, P., Opirskyy, I., & Mazur, N. (2024). Modern technologies of decentralized databases, authentication, and authorization methods. In Proceedings of the Workshop “Cybersecurity Providing in Information and Telecommunication Systems II” (Vol. 3826, pp. 60–71). CEUR-WS.
23. Opirskyy, I., Lys, S., & Shakh, V. (2026). Analysis and testing of systems countering phishing and social engineering attacks at the corporate level. International Journal of Information Security, 25(2), Article 69.
24. Drozdova, Ye., & Kozel, V. (2025). Modern methods of database protection under cyber threats and wartime conditions [In Ukrainian]. Bulletin of Kherson National Technical University, 2(3), 177–185. https://doi.org/10.35546/kntu2078-4481.2025.3.2.22
25. Dzamesi, L., & Elsayed, N. (2025). A review on the security vulnerabilities of the IoMT against malware attacks and DDoS. In Proceedings of the 2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI) (pp. 1–8). IEEE. https://doi.org/10.48550/arXiv.2501.07703
26. Gosálvez-White, I., Rodríguez-Martín, N., Barajas-García, N., Mena-Gallardo, C., & García-Teodoro, P. (2025). MEDIotWALL: Securing smart healthcare environments through IoT firewalls. Sensors, 25(19), Article 6235. https://doi.org/10.3390/s25196235
27. Dudykevych, V. B., Mykytyn, H. V., Nasylevskyi, V. P., & Fihurniak, V. R. (2023). On the issue of secure authentication in web applications [In Ukrainian]. Information Protection, 25(2), 76–82.
28. Boskin, O. O., Kornilovska, N. V., Polishchuk, V. M., & Sarafannikova, N. V. (2023). Web application security and hacker attacks [In Ukrainian]. Bulletin of Kherson National Technical University, 3(86), 83–92. https://doi.org/10.35546/kntu2078-4481.2023.3.11

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Valerii Dudykevych
Doctor of Technical Sciences, Professor,
Professor of the Department of Information Protection,
Lviv Polytechnic National University, Lviv, Ukraine
ORCID:0000-0001-8827-9920
valerii.b.dudykevych@lpnu.ua

Halyna Mykytyn
Doctor of Technical Sciences, Professor,
Professor of the Department of Information Protection,
Lviv Polytechnic National University, Lviv, Ukraine
ORCID:0000-0003-4275-8285
halyna.v.mykytyn@lpnu.ua

Andrii Mozol
Master's Student at the Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID:0009-0004-0728-5552
andrii.mozol.kb.2022@lpnu.ua

METHODOLOGICAL PRINCIPLES FOR BUILDING A SECURE OPERATING PLATFORM FOR THE INTERNET OF MEDICAL THINGS

Abstract. Processes aimed at the secure digitalisation of Ukraine's social infrastructure are ongoing. Medical infrastructure is a key area within the context of Industry 4.0 and Ukraine's Cybersecurity Strategy. One of the key modern tools for the digitalisation of medicine is secure cyber-physical technology, particularly in relation to the secure Internet of Medical Things (IoMT). Effective mechanisms for implementing intelligent diagnosis of a person's health status include secure processes such as: the collection of biophysical parameters relating to the functioning of a patient's organs and systems; transmission of medical information via wireless communication channels; processing and analysis of data on the body's condition; and the making of clinical decisions regarding diagnosis and, on this basis, the prescription of treatment, which form the basis of the functional architecture of the Internet of Medical Things. This paper proposes a methodology for constructing a secure IoT architecture platform based on the 'sensors – sensor networks – cloud infrastructure – user – privacy and security' model, which implements the functional algorithm 'collection – exchange – processing – analysis – decision-making' in accordance with the 'object – threat – protection' concept and potential external accidental and targeted threats. Security systems for IoT components-sensors, sensor networks and cloud infrastructure components are presented in accordance with the STRIDE threat model and the OSI model. The practical implementation of secure medical data exchange in a Bluetooth sensor network is examined, specifically with regard to the cryptographic protection of information at the level of algorithmic and software-based message encryption using AES-256-GCM and Python.

Keywords: intellectualisation, methodology, Internet of Medical Things, sensors, sensor networks, cloud infrastructure, users, external accidental and targeted threats, security systems, message encryption.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Association of Industrial Automation Enterprises of Ukraine. (2018). Industry 4.0 development strategy [In Ukrainian].
2. National Security and Defense Council of Ukraine. (2021). Cybersecurity strategy of Ukraine for 2021–2025 [In Ukrainian].
3. Vasylyshyn, S., Opirskyy, I., Susukailo, V., Mykhaylova, O., Harasymchuk, O., Sovyn, Y., Tyshyk, I., Dudykevych, V., Mykytyn, H., Bobalo, Y., & Stosyk, T. (2025). Advancements in cybersecurity next-generation systems and applications: Collective monograph. CRC Press.
4. Mathkor, D. M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., & Haque, S. (2024). Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare

systems: An overview of current and future innovative trends. Journal of Infection and Public Health, 17(4), 559–572. https://doi.org/10.1016/j.jiph.2024.01.013

5. Nadhir, A. M., Mounir, B., Abdelkader, L., & Hammoudeh, M. (2025). Enhancing cybersecurity in healthcare IoT systems using reinforcement learning. Transportation Research Procedia, 84, 113–120. https://doi.org/10.1016/j.trpro.2025.03.053
6. Maksymovych, V., Nyemkova, E., Justice, C., Shabatura, M., Harasymchuk, O., Lakh, Y., & Rusynko, M. (2022). Simulation of authentication in information-processing electronic devices based on Poisson pulse sequence generators. Electronics, 11(13), Article 2039. https://doi.org/10.3390/electronics11132039
7. Shevchuk, D., Harasymchuk, O., Partyka, A., & Korshun, N. (2023). Designing secured services for authentication, authorization, and accounting of users. CEUR Workshop Proceedings, 207–225.
8. Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a secure and sustainable internet of medical things (IoMT): Requirements, design challenges, security techniques, and future trends. Sustainability, 15(7), Article 6177. https://doi.org/10.3390/su15076177
9. Harasymchuk, O., Opirskyy, I., et al. (2025). Modern methods of ensuring information protection in cybersecurity systems using artificial intelligence and blockchain technology: Collective monograph. Technology Center PC. https://doi.org/10.15587/978-617-8360-12-2
10. Mintser, O. P., Romanov, V. O., Haleliuka, I. B., & Voronenko, O. V. (2020). Artificial intelligence technologies in medical practice [In Ukrainian]. Medical Informatics and Engineering, (2), 17–27. https://doi.org/10.11603/mie.1996-1960.2020.2.11171
11. Hupalo, & Melnyk, A. (2021). Acquisition and processing of data in CPS for remote monitoring of the human functional state. Advances in Cyber-Physical Systems, 6(1), 14–20. https://doi.org/10.23939/acps2021.01.014
12. Jabeen, T., Jabeen, I., Ashraf, H., Ullah, A., Jhanjhi, N. Z., Ghoniem, R. M., & Ray, S. K. (2023). Smart wireless sensor technology for healthcare monitoring system using cognitive radio networks. Sensors, 23(13), Article 6104. https://doi.org/10.3390/s23136104
13. Bobalo, Yu. Ya., Dudykevych, V. B., & Mykytyn, H. V. (2020). Strategic security of the "object–information technology" system: Monograph [In Ukrainian]. Lviv Polytechnic Publishing House.
14. Ameen, A. H., Mohammed, M. A., & Rashid, A. N. (2024). Enhancing security in IoMT: A blockchain-based cybersecurity framework for machine learning-driven ECG signal classification. Fusion: Practice & Applications, 14(1), 221–251. https://doi.org/10.54216/FPA.140117
15. Harasymchuk, O., Opirskyy, I., Banakh, R., et al. (2025). Intelligent cyber defence systems: Detection of ransomware and protection of wireless networks based on artificial intelligence technologies: Collective monograph. Technology Center PC. https://doi.org/10.15587/978-617-8360-22-1
16. Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., Hammoudeh, M., & Qadir, J. (2022). Secure Bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. Sensors, 22(21), Article 8280. https://doi.org/10.3390/s22218280
17. Soni, M., & Singh, D. K. (2022). LAKA: Lightweight authentication and key agreement protocol for internet of things based wireless body area network. Wireless Personal Communications, 127, 1067–1084. https://doi.org/10.1007/s11277-021-08565-2
18. Rezk, N. G., Alshathri, S., Sayed, A., Hemdan, E. E. D., & El-Behery, H. (2025). Secure hybrid deep learning for MRI-based brain tumor detection in smart medical IoT systems. Diagnostics, 15(5), Article 639. https://doi.org/10.3390/diagnostics15050639
19. Tokar, P. Yu. (2025). Methods for protecting the confidentiality of patient data in medical information systems: An analytical review [In Ukrainian]. Scientific Works of Vinnytsia National Technical University, (3), 133–137. https://doi.org/10.31649/2307-5376-2025-3-133-137
20. Baryshev, Yu. V., & Lanova, V. S. (2023). A method for secure storage of medical data based on a relational database and blockchain [In Ukrainian]. Scientific Works of Vinnytsia National Technical University, (3), 9–17. https://doi.org/10.31649/2307-5376-2023-3-9-17
21. Havrysh, B. M., Tymchenko, O. V., & Kustra, N. O. (2023). Methods for anonymizing medical databases [In Ukrainian]. Scientific Papers, 1(66), 68–79. https://doi.org/10.32403/1998-6912-2023-1-66-68-79
22. Petriv, P., Opirskyy, I., & Mazur, N. (2024). Modern technologies of decentralized databases, authentication, and authorization methods. In Proceedings of the Workshop "Cybersecurity Providing in Information and Telecommunication Systems II" (Vol. 3826, pp. 60–71). CEUR-WS.
23. Opirskyy, I., Lys, S., & Shakh, V. (2026). Analysis and testing of systems countering phishing and social engineering attacks at the corporate level. International Journal of Information Security, 25(2), Article 69.
24. Drozdova, Ye., & Kozel, V. (2025). Modern methods of database protection under cyber threats and wartime conditions [In Ukrainian]. Bulletin of Kherson National Technical University, 2(3), 177–185. https://doi.org/10.35546/kntu2078-4481.2025.3.2.22

25. Dzamesi, L., & Elsayed, N. (2025). A review on the security vulnerabilities of the IoMT against malware attacks and DDoS. In Proceedings of the 2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI) (pp. 1–8). IEEE. https://doi.org/10.48550/arXiv.2501.07703
26. Gosálvez-White, I., Rodríguez-Martín, N., Barajas-García, N., Mena-Gallardo, C., & García-Teodoro, P. (2025). MEDIotWALL: Securing smart healthcare environments through IoT firewalls. Sensors, 25(19), Article 6235. https://doi.org/10.3390/s25196235
27. Dudykevych, V. B., Mykytyn, H. V., Nasylevskyi, V. P., & Fihurniak, V. R. (2023). On the issue of secure authentication in web applications [In Ukrainian]. Information Protection, 25(2), 76–82.
28. Boskin, O. O., Kornilovska, N. V., Polishchuk, V. M., & Sarafannikova, N. V. (2023). Web application security and hacker attacks [In Ukrainian]. Bulletin of Kherson National Technical University, 3(86), 83–92. https://doi.org/10.35546/kntu2078-4481.2023.3.11

Отримано редакцією журналу / Received: 30.01.26
Прорецензовано / Revised: 09.02.26
Схвалено до друку / Accepted: 24.09.26