КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.917
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

Парчук Ярослава Ігорівна
магістрант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0002-7349-7364
yaroslava.parchuk.mkbst.2025@lpnu.ua

Терпелюк Максим-Степан Володимирович
магістрант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0001-7015-5855
maksym-stepan.terpeliuk.mkbst.2025@lpnu.ua

СТВОРЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ОБРОБКИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ “ ІНТЕРНЕТ РЕЧЕЙ В “РОЗУМНОМУ МІСТІ”: ЗАГРОЗИ – ТЕХНОЛОГІЇ БЕЗПЕКИ” У ПРОСТОРІ ІНДУСТРІЇ 4.0

Анотація. У просторі завдань Індустрії 4.0 в роботі досліджено питання безпечної інтелектуалізації об’єктів інфраструктури суспільства України на рівні розроблення автоматизованої системи обробки інформації з обмежених доступом (АСОІ з ОД) у сегменті безпеки Інтернету речей (IoT) “розумного міста” (РМ) та алгоритмічно-програмної реалізації засобами мови програмування Python. Проведено аналітичний огляд відомих методологій розроблення безпечних автоматизованих систем обробки інформації та підходів до забезпечення безпеки IoT-систем. Розгорнуто якісний аналіз сегментів “розумного міста” – транспорту, медицини, енергетики, екології методом групування на рівні класифікаційної схеми предметної сфери згідно концепції “об’єкт – загроза – захист”. Створено концептуальну модель предметної сфери “Інтернет речей в “розумному місті”: загрози – технології безпеки” на основі принципів системного аналізу – цілісності, ієрархічності, багатоаспектності. Обгрунтувано критерії вибору реляційної бази даних (РБД), системи управління базою даних (СУБД) SQLite і мови програмування Python та побудовано інформаційну модель РБД для подальшої алгоритмічно-програмної реалізації. Представлено алгоритм безпечного функціонування автоматизованої системи обробки інформації на рівні процедури автентифікації і, на цій основі, розроблено програмну реалізацію АСОІ “Інтернет речей в “розумному місті”: загрози – технології безпеки” засобами Python для сегментів: “розумного транспорту”, “розумної медицини”, “розумної енергетики”, “розумної екології” на рівні веб-застосунку.

Ключові слова: інтелектуалізація об’єктів; безпека; Інтернет речей; “розумне місто”; класифікаційна схема; концептуальна та інформаційна моделі; реляційна база даних; автоматизована система обробки інформації.

ВСТУП

Сьогодні ефективно розвиваються процеси інтелектуалізації об'єктів інфраструктури суспільства, зокрема критичної у просторі Концепції Індустрії 4.0 та Стратегії з кібербезпеки за векторами:

1) інформаційно-комунікаційних технологій (ІКТ), як основного інструментарію підтримки функціонування інтелектуальних об'єктів;

2) підходів та методологій до забезпечення безпеки ІКТ [1, 2, 3].

Одним з актуальних напрямків інтелектуалізації інфраструктури є "розумне місто", що розгортається сегментами – "розумного транспорту", "розумної медицини", "розумної енергетики", "розумної екології". Серед ефективних засобів підтримки безпечного функціонування "розумного міста" є багаторівневі кіберфізичні технології (КФТ) [4]. Безпечне функціонування об'єктів інтелектуалізації вимагає впровадження методологічних підходів до забезпечення безпеки ІКТ, зокрема багаторівневих КФТ, функціонально призначених для:

1) відбору інформації від об'єктів інтелектуалізації предметних сфер засобами Інтернету речей у фізичному просторі КФТ;

2) передавання інформації безпровідними, зокрема сенсорними та провідними технологіями комунікаційного середовища КФТ в кібернетичний простір;

3) обробки, аналізу та прийняття управлінського рішення автоматизованими системами обробки інформації в кібернетичному просторі КФТ.

Відповідно, проблема безпеки Інтернету речей інтелектуальних об'єктів інфраструктури суспільства, як одного з рівнів КФТ є актуальною в контексті розвитку Індустрії 4.0 в Україні, особливо за вектором автоматизації обробки інформації з обмеженим доступом на рівні веб-застосунку.

Постановка проблеми. Безпечна інтелектуалізація об'єктів інфраструктури суспільства передбачає впровадження безпечних КФТ, як одного з ефективних інструментаріїв функціонування "розумних об'єктів". Відповідно розроблення комплексних систем безпеки багаторівневих КФТ, зокрема IoT-систем потребує створення безпечних автоматизованих систем обробки інформації на рівні веб-застосунків для представлення динаміки оновлення: новітніх пристроїв IoT у сегментах РМ, ймовірних загроз, технологій безпеки, міжнародних і державних стандартів у сфері кібербезпеки. Інтернет речей, як один з рівнів КФТ є однією з найважливіших технологій 21-го століття, яка сьогодні динамічно розвивається у просторі "об'єкти інтелектуалізації – пристрої IoT – випадкові і цілеспрямовані загрози – механізми реалізації – методи та засоби захисту". Безпека IoT вимагає розвитку методології створення АСОІ з ОД з врахуванням специфіки індустріального парку інтелектуальних об'єктів сегментів "розумного міста", діапазону IoT-систем відповідно до комплексу ймовірних загроз і технологій безпеки.

Аналіз останніх досліджень і публікацій. Проблемі безпеки процесів інтелектуалізації об'єктів інфраструктури на рівні функціонування безпечних автоматизованих систем обробки інформації та безпечних пристроїв IoT в сегментах "розумного міста" присвячено багато наукових досліджень як на міжнародному рівні, так і в Україні. Дослідження питань безпеки стосуються: підходів, моделей та методологій, апаратного і програмного забезпечення, застосування штучного інтелекту, зокрема у частині технологій машинного навчання, вдосконалення криптографічних алгоритмів шифрування, вдосконалення методів захисту безпровідних мереж і протоколів обміну інформації, розвитку комплексних систем безпеки. Розглянемо деякі

наукові дослідження у просторі безпечної інтелектуалізації об'єктів РМ за цими двома векторами, які проводилися на міжнародному рівні та в Україні.

Розвиток підходів і моделей безпеки автоматизованих систем обробки інформації представлено на таких рівнях. В публікації [5] розглянуто новий підхід до реалізації конфігурації систем автоматизації, орієнтованої на безпеку даних. Аналіз методологій життєвого циклу розроблення програмного забезпечення з використанням методики кібербезпеки NIST проведено в роботі [6]. В праці [7] проаналізовано сучасні методи обробки даних в автоматизованих системах, підкреслено необхідність інтеграції розглянутих підходів для підвищення ефективності та адаптивності систем, обґрунтовано доцільність створення концептуальної моделі управління даними, яка сприятиме розвитку стійкої та безпечної цифрової інфраструктури. Розвинуто концептуальну модель захисту інформації в ACOI, яка інтегрує контроль доступу, виявлення аномалій і шифрування критичних повідомлень, а також передбачає формалізовану оцінку ефективності на основі кількісних метрик [8]. В роботах [9, 10] розгорнуто системну та комплексну моделі безпеки інформаційних технологій, зокрема автоматизованих систем обробки інформації, запропоновано методології безпеки кіберфізичних технологій у просторі Індустрії 4.0.

Вдосконалення методології безпеки IoT-систем "розумного міста" розгорнуто на таких рівнях. У статті [11] досліджено підходи до забезпечення кібербезпеки технологій розумних міст на основі штучного інтелекту з використанням новітніх алгоритмів машинного навчання, систем виявлення аномалій та аналітики прогнозування для виявлення і реагування на кіберзагрози в режимі реального часу. У публікації [12] проаналізовано виклики кіберзагроз для технологій інфраструктури розумних міст, запропоновано багаторівневі стратегії захисту, що поєднують технічні рішення, нормативно-правові акти та впровадження надійних засобів контролю доступу, сегментації мережі на протидію потенційним атакам. Розгортаються тенденції дослідження загроз кібербезпеці технологій функціонування сегментів інфраструктури розумного міста у просторі: вразливостей IoT-пристроїв; ефективних рішень для їх захисту; рекомендацій щодо створення комплексного підходу забезпечення безпеки [13, 14]. Цікавою є тенденція розвитку IoT-систем і кіберфізичних технологій у контексті функціонування розумних міст за період 2013-2023 рр., зокрема дослідження аспектів галузевих стандартів та застосування методів машинного і глибокого навчання [15]. У роботі [16] проаналізовано та досліджено архітектуру Інтернету речей і пов'язані з нею загрози безпеці, класифіковано вразливості на різних рівнях IoT, проведено порівняльний аналіз бездротових технологій та підходів до захисту. Ефективним є аспект інтегральності у просторі безпеки IoT: аналіз факторів забезпечення безпеки технологій розумних міст на основі штучного інтелекту та IoT; розроблення багаторівневих підходів захисту на прикладному, мережевому і фізичному рівнях інфраструктури; формування оцінки ефективності методів машинного навчання (ML) та навчання на базі даних (DL); створення рекомендацій щодо інтеграції рішень з метою підвищення безпеки та стійкості міської інфраструктури в умовах новітніх комунікаційних технологій [17].

В публікації [18] проаналізовано та класифіковано сучасні методи, моделі й програмні засоби реалізації систем IoT, розгорнуто еволюцію та комунікаційні основи Інтернету речей, а також сформовано критерії ефективності, масштабованості й безпеки для оптимізації сучасних IoT-рішень. Актуальними є дослідження на рівні архітектури IoT: аналіз проблеми інформаційної безпеки Інтернету речей у просторі загроз та вразливостей з урахуванням ресурсних обмежень пристроїв; розгортання підходів до

покращення захищеності систем, зокрема шляхом використання локального IoT-шлюзу [19]. В праці [20] досліджено обмеження застосування традиційних мережевих протоколів у середовищі Інтернету речей, розгорнуто елементи стандартизації та захисту комунікаційних технологій, а також класифіковано спеціалізовані протоколи зв'язку за рівнями архітектури IoT. Розвивається апаратна безпека IoT у просторі: дослідження засобів підвищення апаратної безпеки кінцевих пристроїв хмарних обчислень у мережах IoT відповідно до кіберзагроз та апаратних атак; рекомендацій щодо використання стандартних апаратних платформ безпеки з метою зниження вразливості периферійних IoT-систем [21]. В публікації [22] сформовано підхід до проєктування системи інформаційної безпеки мереж Інтернету речей, досліджено особливості IoT-трафіку та сучасних атак, проведено порівняльний аналіз алгоритмів «Дерево рішень» і «K-найближчий сусід» для інтелектуального виявлення вторгнень та рекомендовано їх використання в системах захисту, орієнтованих на роботу в умовах обмежених обчислювальних ресурсів. Авторами публікації [23] представлено методи захисту інформації в технологіях IoT, розроблено ефективні заходи захисту для забезпечення стабільності і безпеки IoT-систем від вразливостей перед атаками, зокрема на основі WiFi jammer. Комплексна модель захисту побутових IoT-пристроїв та уніфікована методологія кількісного оцінювання безпеки, а також аналіз основних загроз й вразливостей IoT-систем та підходи до підвищення кіберстійкості побутових мереж згідно міжнародних стандартів представлені в статті [24]. У дослідженні [25] розглянуто: технології кіберзахисту у системах і пристроях Інтернету речей; розгорнуто підходи до захисту каналів передачі даних; запропоновано комплексні методи підвищення рівня кібербезпеки IoT на основі поєднання відомих технологій, що дозволяє забезпечити надійність, захищеність і перспективи розвитку архітектури обміну даними в мережах Інтернету речей. В контексті розвитку моделей безпеки IoT-систем цікавими є сегменти: ризик-орієнтована модель безпеки IoT-систем, тісно інтегрованих з фізичними процесами керування [26]; аналіз ризиків Shadow IT у публічних хмарних інфраструктурах та підхід до їх ідентифікації та оцінювання у просторі хмаро-інтегрованих моделей безпеки IoT, у яких IoT-платформи покладаються на зовнішні хмарні сервіси для оброблення та керування даними [27]. В праці [28] розглянуто універсальну платформу безпеки КФТ та запропоновано трирівневу модель безпеки Інтернету речей в контексті інтелектуалізації об'єктів інфраструктури. Актуальним завданням інтелектуалізації є безпечне функціонування технологій "розумного міста", зокрема IoT-систем за основними профілями кібербезпеки – конфіденційності, цілісності, доступності. Відповідно одним з ефективних підходів за цим вектором є розвиток методології безпеки IoT сегментів РМ на основі концепції об'єкт – загроза – захист та її реалізація на рівні автоматизованої системи обробки інформації з обмеженим доступом.

Мета статті. Метою роботи є створення методологічного підходу до розроблення автоматизованої системи обробки інформації з обмеженим доступом "Інтернет речей в "розумному місті: загрози – технології безпеки", що розгортається: класифікаційною схемою якісного аналізу предметної сфери безпеки IoT сегментів інфраструктури РМ; концептуальною та інформаційною моделями побудови реляційної бази даних; алгоритмічно-програмною реалізацією безпечного функціонування АСОІ з ОД на рівні веб-застосунку.

Завданням дослідження є:

1. Провести якісний аналіз предметної сфери "Інтернет речей в "розумному місті: загрози – технології безпеки" як фізичного простору КФТ на основі методу

групування і, на цій основі, створення класифікаційної схеми для побудови РБД;
2. Розробити концептуальну модель предметної сфери на основі класифікаційної схеми та побудувати інформаційну модель реляційної бази даних;
3. Обґрунтувати критерії вибору моделі РБД, системи управління базою даних SQLite та мови програмування Python для реалізації АСОІ з ОД;
4. Розробити алгоритмічно-програмну реалізацію безпечного функціонування АСОІ з ОД на рівні веб-застосунку, який має ефективні переваги для користувачів: доступність, простота у використанні, оновлення інформації, інтеграція.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Якісний аналіз даних предметної сфери “Інтернет речей у “розумному місті”: загрози – технології безпеки”.

Структурно-функціональна характеристика Інтернету речей в “розумному місті”. Усі ілюстрації, програмні коди та таблиці мають бути розташовані безпосередньо після тексту, де вони згадані вперше, або на наступній сторінці (не наприкінці статті).

Архітектура IoT-систем сьогодні здебільшого представлена на основі ієрархічної моделі, що включає чотири основні рівні: периферійний рівень (сенсори та актуатори), мережевий рівень (обмін даними безпровідними мережами LPWAN, ZigBee, 4G/5G), рівень граничних обчислень (edge computing для локальної обробки даних) та прикладний рівень (хмарні платформи аналітики та управління). Така структура IoT-систем забезпечує масштабованість, відмовостійкість та ефективну обробку великих обсягів даних, отриманих від фізичних об’єктів інфраструктури “розумного міста” [29]. У сегменті інтелектуалізації об’єктів РМ Інтернет речей стає дедалі актуальнішим як фізичний простір КФТ, що інтегрує фізичні об'єкти інфраструктури з її комунікаційним середовищем і кібернетичним простором, які цілісно призначені для відбору даних від об’єктів, передавання інформації безпровідними технологіями зв’язку, зокрема сенсорними для обробки автоматизованою системою, аналізу даних, прогнозування і прийняття рішення на управління станом об’єкта. Відповідно усі рівні КФТ взаємодіють на основі універсальної платформи технологічного інструментарію функціонування “розумного міста”, що забезпечує інтеграцію окремих сегментів інфраструктури та їх безпеку на основі системного та синергетичного підходів [30]. Одним з актуальних питань процесів інтелектуалізації об’єктів інфраструктури РМ, зокрема критичної є впровадження Інтернету речей у сегменти – розумного транспорту, розумної енергетики, розумної медицини, розумного екологічного моніторингу екосистем довкілля.

Сегмент “розумного транспорту” охоплює широкий діапазон підсистем, зокрема таких: “розумна залізниця” з сенсорами стану рейкового полотна та системами автоматичного керування поїздами; “розумна авіацію” для управління дронами та міською аеромобільністю; “розумні автомобільні дороги” з інтелектуальним покриттям та динамічними інформаційними табло; “розумна логістика” з RFID-мітками та GPS-трекерами для відстеження вантажів; “розумний морський транспорт” з автоматизованими системами швартування; “розумний громадський транспорт” з системами GPS-моніторингу та електронної оплати, а також “розумна міська мобільність”, що інтегрує різні види транспорту через платформи Mobility-as-a-Service (MaaS). Інтелектуальні транспортні системи будь якої з підсистем використовують протоколи: MQTT для обміну даними телеметрії, DSRC для комунікації між

автомобілями та інфраструктурою (V2V/V2I), а також стільникові мережі 4G/5G для передавання відеопотоків [31].

“Розумна медицина” розгорнута “розумними лікарнями”, що включають: мережі медичних сенсорів для моніторингу життєвих показників стану організму пацієнтів; RFID-системи для відстеження персоналу та медичного обладнання; “розумні ліжка” та автоматизовані системи управління ліками; системи телемедицини та дистанційного моніторингу; портативні діагностичні прилади та платформи відеоконсультацій. Інтелектуальні медичні IoT-системи з метою забезпечення основних профілів безпеки конфіденційності, цілісності і доступності використовують протоколи з гарантованою доставкою повідомлень (AMQP) та граничні обчислення для зменшення затримок у критичних сповіщеннях [32]. Інтелектуальна енергетична інфраструктура “розумного міста” включає: розумні електромережі (Smart Grid) з давачами моніторингу стану трансформаторних підстанцій, системами автоматичного виявлення пошкоджень, інтелектуальними вимикачами та інтеграцією розподіленої генерації; системи “розумного обліку” та управління енергоспоживанням через Smart Meters з дистанційним зняттям показів електролічильників; контролери “розумного вуличного освітлення”; системи Home Energy Management та платформи Demand Response. Інтелектуальні енергетичні системи використовують: спеціалізовані протоколи DLMS/COSEM, IEC 61850, технології PLC для передавання даних по лініях електропередач, які використовуються як канали зв’язку та LPWAN-мережі для віддаленого моніторингу стану об’єктів [33].

Екологічний моніторинг параметрів відповідних екосистем довкілля реалізується багаторівневими кіберфізичними технологіями, функціонально призначеними для: відбору даних мережею давачів IoT у фізичному просторі КФТ, передавання інформації безпровідними технологіями зв’язку, зокрема сенсорними з комунікаційного середовища КФТ у кібернетичний простір для автоматизованої обробки, аналізу, прогнозування та прийняття рішення на управління станом відповідної екосистеми. Наприклад, інтелектуальний моніторинг якості екологічних параметрів на рівні відбору інформації від екосистем довкілля реалізується: мобільними давачами Інтернету речей КФТ, які реєструють концентрацію забруднювальних речовин персональними портативними сенсорами та метеостанціями; стаціонарними станціями [34]. Зокрема, інтелектуальний моніторинг водних ресурсів та якості питної води на рівні відбору даних реалізується мережею сенсорів Інтернету речей КФТ, впроваджених у системи: водопостачання, моніторингу стічних вод, контролю якості води у природних водоймах. Для інтелектуальних систем моніторингу екологічних параметрів з великою кількістю територіально розподілених сенсорів, використовують енергоефективні технології LPWAN та протоколи CoAP [35].

Сьогодні одним з актуальних питань екології довкілля є проблема зміни клімату, яка щорічно відстежується в рамках Рамкових конвенцій ООН, зокрема на конференції COP30 (Белен, Бразилія, листопад 2025 р.) Україна представила Довгострокову стратегію низьковуглецевого розвитку. Надзвичайно актуальним питанням наукових досліджень ООН в просторі екологічного моніторингу водних ресурсів є не тільки проблема забруднення води в різних регіонах планети, а й надзвичайна ситуація “глобального водного банкрутства”. Відповідно важливим є ефективне впровадження безпечного інтелектуального екологічного моніторингу параметрів якості води, зокрема питної, особливо безпечних IoT-систем [36].

Загрози безпеці IoT-систем в інфраструктурі “розумного міста”. На IoT-системи “розумного міста” активуються нові вектори кібератак та вразливості, що можуть

призвести до порушення основних профілів безпеки обміну інформацією в інфраструктурі РМ, зокрема в критичній. Масштабність та розподіленість IoT-систем, обмежені обчислювальні ресурси периферійних пристроїв, гетерогенність технологій та протоколів зв'язку і тривалий термін експлуатації IoT-обладнання без оновлень створюють простір для механізмів реалізації атак, який є значно більшим у порівнянні з діапазоном випадкових і цілеспрямованих загроз ІТ-системам [37].

DDoS-атаки на IoT-пристрої залишаються однією з найпоширеніших загроз, коли зловмисники компрометують велику кількість слабозахищених пристроїв та об'єднують їх у ботнети [38]. Несанкціонований доступ до IoT-пристроїв часто стає можливим через елементарні вразливості: слабкі паролі за замовчуванням, відсутність механізмів автентифікації, використання застарілих протоколів без шифрування повідомлень. Це дозволяє зловмисникам отримувати контроль над IoT-пристроями, зокрема сенсорами та актуаторами, використовуючи різні моделі поведінки.

Підміна та маніпуляція даними при перехопленні незашифрованого трафіку між IoT-пристроями та системами управління призводить до прийняття помилкових рішень АСОІ на управління станом об’єктів. Наприклад, маніпуляція сигналами “розумних світлофорів” може створити аварійні ситуації, фальсифікація даних про якість повітря приховує реальні рівні забруднення та створює загрозу здоров'ю населення, а зміна показників медичних сенсорів становить пряму загрозу життю пацієнтів через неправильно встановлений діагноз або призначений курс лікування. Атаки на ланцюг постачання, коли зловмисники впроваджують шкідливий код у прошивку обладнання ще на етапі виробництва, є особливо небезпечними через складність виявлення компрометованих пристроїв після їх масового розгортання в інфраструктурі “розумного міста”.

У просторі кібербезпеки актуальними є загрози об'єктам критичної інфраструктури, функціонування яких підтримується пристроями IoT у фізичному просторі КФТ. Атаки на енергетичні системи, зокрема на “розумні лічильники” та SCADA-системи управління розподільчими мережами, можуть призвести до масштабних блекаутів. У сфері охорони здоров'я компрометація медичних даних порушує конфіденційність інформації про пацієнтів, а ransomware-атаки, які поєднують шкідливий код та механізми криптографії, реалізують недоступність баз даних “розумних лікарень” без спеціального ключа.

Інтелектуальні транспортні системи мають свій діапазон вразливостей до кіберзагроз: компрометація IoT-пристроїв громадського транспорту унеможливлює відстеження поведінки громадян та валідацію платіжних даних, а атаки на системи комунікації між автомобілями (V2V) та інфраструктурою (V2I) можуть спровокувати аварійні маневри, особливо критичні для автономних транспортних засобів. Серед загроз інтелектуальним системам моніторингу екосистем довкілля – модифікація даних про параметри якості води, що призводить до приховування забруднення води токсичними речовинами; атаки на системи раннього виявлення надзвичайних екологічних ситуацій в регіоні, що може призвести до несвоєчасної евакуації населення. Для протоколів передавання даних з IoT-пристроїв, зокрема MQTT та CoAP характерні легковаговість та енергоефективність, але механізми безпеки реалізовані в них як опційні функції, відповідно рівень захищеності є низьким [39].

Технології забезпечення безпеки IoT-систем інфраструктури “розумного міста”. Розглянемо деякі актуальні технології безпеки IoT-систем. Шифрування безпровідних каналів зв'язку є фундаментальним методом захисту інформації за профілями конфіденційності та цілісності, що передаються між IoT-пристроями та системами

управління. Для IoT-систем застосовуються легковагові криптографічні алгоритми, такі як AES-128, ChaCha20 або еліптична криптографія (ECC), що забезпечують прийнятний рівень захисту при мінімальних обчислювальних витратах. Протоколи TLS/DTLS (Transport Layer Security / Datagram TLS) використовуються для захисту каналів зв'язку на транспортному рівні, хоча для ресурсообмежених IoT-пристроїв часто застосовуються спрощені версії цих протоколів. Важливим аспектом є управління криптографічними ключами в розподілених IoT-системах, що реалізується через інфраструктуру відкритих ключів (PKI) або децентралізовані механізми на основі блокчейн-технологій для забезпечення безпечного розповсюдження та ротації ключів [40].

Автентифікація пристроїв та користувачів є критично важливою для запобігання несанкціонованому доступу до IoT-систем інфраструктури "розумного міста". Двофакторна або багатофакторна автентифікація стає стандартом для доступу користувача до систем управління критичною інфраструктурою, поєднуючи пароль, токен, смарт-карту та біометричні дані. Для автентифікації IoT-пристроїв широко використовуються цифрові сертифікати X.509, що дозволяють однозначно ідентифікувати кожен пристрій в мережі та перевіряти його автентичність. Перспективним напрямком є використання технологій Physical Unclonable Functions (PUF), що створюють унікальний ідентифікатор на основі фізичних характеристик мікросхем, практично неможливий для клонування або підробки.

Сегментація мережі є ефективним методом обмеження поширення атак та мінімізації їх наслідків. IoT-системи інфраструктури РМ повинні бути розділені на ізольовані сегменти відповідно до рівня критичності систем та чутливості даних, які підлягають обробці [41]. Віртуальні локальні мережі (VLAN), програмно-конфігуровані мережі (SDN – Software-Defined Networking) та мікросегментація дозволяють створювати динамічні периметри безпеки та забезпечувати принцип найменших привілеїв для взаємодії між різними компонентами системи. Особливо важливою є ізоляція критичних систем управління (наприклад, SCADA-систем енергетичних мереж) від менш захищених компонентів та зовнішніх мереж.

Системи виявлення та запобігання вторгненням (IDS/IPS) адаптуються до специфіки IoT-трафіку, що характеризується регулярністю, передбачуваністю моделей поведінки та специфічними протоколами [42]. Сучасні системи використовують методи машинного навчання та штучного інтелекту для виявлення аномалій поведінки IoT-пристроїв, що можуть свідчити про їх компрометацію, наприклад несподівані зміни в обсягах або частоті передавання даних, спроби встановлення з'єднань з нетиповими адресами, зміни в структурі споживання ресурсів.

Апаратні засоби безпеки відіграють ключову роль у створенні довіреного середовища виконання для IoT-пристроїв. Криптографічні співпроцесори та апаратні модулі безпеки (HSM – Hardware Security Module) забезпечують захищене зберігання криптографічних ключів та виконання криптографічних операцій, значно підвищуючи швидкість шифрування та знижуючи навантаження на основний процесор. Використовуються захищені елементи (Secure Elements) – спеціалізовані мікросхеми з підвищеним рівнем захисту від фізичного втручання, що вбудовуються в IoT-пристрої для зберігання конфіденційних даних та виконання критичних операцій безпеки. Технологія Trusted Platform Module (TPM) забезпечує апаратну основу довіри для перевірки цілісності прошивки та операційної системи IoT-пристроїв при завантаженні, запобігаючи виконанню зловмисного коду.

Програмні засоби безпеки IoT включають платформи управління ідентифікацією та доступом (IAM – Identity and Access Management), що централізовано керують правами доступу мережі IoT-пристроїв та користувачів до ресурсів системи. Спеціалізовані IoT-брандмауери здатні інспектувати трафік специфічних IoT-протоколів (MQTT, CoAP, Modbus) та застосовувати політики безпеки на рівні протоколів прикладного рівня. Платформи безпеки IoT (IoT Security Platforms) надають комплексні можливості для моніторингу стану безпеки розподіленої інфраструктури IoT-систем, управління вразливостями, автоматизованого застосування заходів безпеки та координацію реагування на інциденти. Системи Security Information and Event Management (SIEM), адаптовані для IoT, агрегують та аналізують величезні обсяги подій безпеки з великої множини IoT-пристроїв з метою виявлення складних багатоетапних атак. Безпека на рівні веб-застосунків передбачає впровадження практик безпечного розроблення (Secure Development Lifecycle), що включають моделювання загроз, статичний та динамічний аналіз коду, тестування на проникнення. Для IoT-систем критично важливим є механізм безпечного оновлення прошивки Over-The-Air (OTA), який дозволяє оперативно усувати виявлені вразливості без необхідності фізичного доступу до пристроїв. Цифрові підписи оновлень прошивки забезпечують автентичність та цілісність програмного забезпечення, запобігаючи встановленню зловмисних модифікацій.

Розглянемо деякі аспекти нормативного забезпечення безпеки IoT-систем на міжнародному рівні через низку стандартів та рекомендацій. Стандарт ДСТУ ISO/IEC 27001:2023 визначає вимоги до систем управління інформаційною безпекою і є базовим для організацій, що розгортають впровадження IoT-систем в інфраструктуру “розумного міста”. Стандарт ДСТУ EN IEC 62443-4-1:2019 регламентує безпеку систем промислової автоматизації та керування, зокрема у частині вимог до життєвого циклу розроблення безпечної продукції, що використовується в критичній інфраструктурі, включаючи енергетику і транспорт. Стандарт NIST Cybersecurity Framework (CSF) 2.0 (2024) надає структурований підхід до управління кіберризиками та включає специфічні рекомендації для IoT-систем. Стандарт ETSI EN 303 645 V3.1.3 (2024-09) визначає базові вимоги кібербезпеки для споживчих IoT-пристроїв, включаючи заборону паролів за замовчуванням та вимоги до безпечного оновлення прошивки. Міжнародна організація IEEE, яка визначає напрямки розвитку технологій розробляє стандарти, що використовуються в промисловості, науці, IT, телекомунікаціях, зокрема у частині безпечних IoT-протоколів, наприклад стандарт IEEE 802.1X-2020 надає рекомендації щодо процедури аутентифікації в мережах.

Концепція Security by Design наголошує на необхідності інтеграції механізмів безпеки на всіх етапах розроблення IoT-систем, починаючи з архітектурного проектування. Принцип найменших привілеїв, глибокорівневий захист (defense in depth), відмовобезпечність (fail-safe) та відмовостійкість повинні бути закладені в архітектуру IoT-систем “розумного міста” Аудит безпеки, тестування на проникнення, управління вразливостями та життєвим циклом IoT-пристроїв, включаючи безпечну утилізацію, є невід'ємними компонентами комплексної стратегії забезпечення безпеки IoT-систем інфраструктури розумного міста, що дозволяє створити стійку до кіберзагроз платформу безпечного “розумного міста”.

Класифікаційна схема предметної сфери на основі методу групування даних. Метод групування є одним із базових інструментів якісного аналізу даних і полягає у поділі досліджуваної сукупності об’єктів предметної сфери або явищ на однорідні групи за суттєвими якісними ознаками. Класифікаційна схема предметної сфери “Інтернет

речей в “розумному місті”: загрози – технології безпеки” створена для сегментів інфраструктури “розумний транспорт”, “розумна медицина”, “розумна енергетика”, “розумна екологія”, але в роботі розгорнута тільки “розумна екологія” на рівні моніторингу водних ресурсів та якості води (див. табл. 1, табл. 2).

Таблиця 1

Класифікаційна схема “Інтернет речей в “розумному місті”: загрози”

Сфера (a)	
Екологія	
Компонента сфери (b)	2. Моніторинг водних ресурсів та якості води
Структурно-функціональний опис	
Архітектура (c)	Розподілена архітектура: – Вимірювання (буї, підводні станції, зонди, давачі); – Мережа (супутниковий зв’язок, LoRaWAN, 4G); – Edge-обробка (локальні контролери); – Централізний рівень (моніторинг, прогнозування); – Прикладний рівень (попередження, портали, метеоінтеграція).
Призначення та використання (d)	– Безперервний моніторинг якості води в річках, озерах та водосховищах; – Контроль параметрів питної води в системах водопостачання; – Виявлення джерел забруднення з вимірами в реальному часі; – Моніторинг рівня води для попередження паводків; – Контроль стічних вод підприємств перед випуском у водойми; – Оцінка стану водних екосистем та біорізноманіття; – Управління водними ресурсами та оптимізація водорозподілу; – Раннє попередження населення про непридатність води для використання; – Наукові дослідження гідрологічних та гідрохімічних процесів.
Пристрої IoT (e)	– Багатопараметричні зонди (pH, розчинений кисень, каламутність, температура); – Давачі електропровідності та солоності води; – Нітратні та фосфатні аналізатори для виявлення евтрофікації; – Давачі рівня води ультразвукові та радарні; – Флуоресцентні давачі для виявлення водоростей та нафтопродуктів; – Давачі важких металів з вольтамперометрією; – Автоматичні пробовідбірники для лабораторного аналізу; – Гідрофони для моніторингу підводного шуму; – GPS-буї для моніторингу течій та переміщення водних мас; – Підводні камери для візуального моніторингу; – Метеостанції на буях для комплексного моніторингу.
Загрози (f)	
Випадкові	– Біообростання давачів, що спотворює випромінювання; – Пошкодження обладнання через шторми, паводки, зсуви; – Збій калібрування давачів рівня води під час тривалого занурення; – Втрата супутникового зв’язку буїв через погодні умови; – Механічне пошкодження кабелів стаціонарних станцій рибальськими снастями; – Розрядження батарей через холодну воду з підвищеною теплопровідністю.
Цілеспрямовані	– Фізичне пошкодження або крадіжка давачів та буїв; – Кібератаки на системи моніторингу з метою приховування скидів забруднень; – Підміна даних про якість води підприємствами-забруднювачами; – Злом систем оповіщення для створення паніки серед населення; – DDoS-атаки на портали гідрологічної інформації; – Маніпуляції з даними про водокористування для незаконного відбору води; – Саботаж систем раннього попередження про паводки.

Таблиця 2

Класифікаційна схема “Інтернет речей в “розумному місті”: технології безпеки”

Сфера (a)	
Екологія	
Компонента сфери (b)	2. Моніторинг водних ресурсів та якості води
Технології безпеки	
Методи захисту (g)	– Регулярна очистка давачів від біообростання автоматичними механічними або ультразвуковими системами; – Шифрування гідрологічних даних при передачі від станцій до центрів; – Фізичний захист дорогого обладнання якірними системами та GPS-моніторингом; – Резервування каналів зв’язку (супутник + сотові мережі); – Контроль цілісності даних з використанням цифрових підписів; – Багаторівнева автентифікація операторів систем моніторингу; – Моніторинг аномалій для виявлення підробки гідрохімічних даних; – Географічно розподілене зберігання критичних даних про водні ресурси; – Перехресна валідація даних між сусідніми станціями моніторингу.
Апаратні засоби захисту (h)	– Антивандальні буї з корпусами високої міцності та яскравим маркуванням; – Криптомодулі в підводних станціях для захисту телеметрії; – GPS-трекери на обладнанні з оповіщенням про переміщення; – Автоматичні системи очищення давачів (механічні щітки, UV-опромінення); – Захищені кабельні вводи IP68 для підводних з’єднань; – Резервні акумулятори великої ємності з сонячними панелями на буях; – Апаратні HSM для зберігання ключів шифрування гідрологічних даних; – Захищені шлюзи з вбудованими міжмережевими екранами; – Давачі розкриття корпусів з оповіщенням про втручання.
Програмні засоби захисту (i)	– Платформа гідромоніторингу з вбудованим шифруванням та контролем доступу; – Алгоритми машинного навчання для виявлення аномальних вимірювань; – Системи автоматичної калібровки давачів з компенсацією дрейфу; – Blockchain для незмінного зберігання даних про якість води; – Системи валідації даних з гідрологічними моделями; – SIEM для моніторингу кіберзагроз в мережі водних давачів; – Захищені API для інтеграції з системами водоканалів; – Системи управління інцидентами для швидкого реагування на забруднення; – Автоматичні системи резервного копіювання гідрологічних баз даних.
Стандарти (j)	
Міжнародні	– ISO/IEC 30179:2023; – ISO/IEC 27400:2022; – ISO 24512:2024; – NIST CSF 2.0:2024; – NIST SP 800-213:2021; – EN ISO 10523:2012; – IEEE 802.15.4:2020.
Національні стандарти України	– ДСТУ EN ISO 5667-1:2025; – ДСТУ EN ISO 5667-6:2025; – ДСТУ EN ISO 5814:2025; – ДСТУ EN ISO 7887:2025; – ДСТУ EN ISO 4373:2022; – ДСТУ ISO/IEC 30141:2019; – ДСТУ ISO 15839:2022.

Концептуальна модель предметної сфери та інформаційна модель реляційної бази даних.

Концептуальна модель предметної сфери: принципи цілісності. ієрархічності, багатоаспектності. Основою створення концептуальної моделі предметної сфери “Інтернет речей в “розумному місті”: загрози – технології безпеки” є класифікаційна схема та принципи системного аналізу – цілісності, ієрархічності, багатоаспектності, які системно дозволяють структурувати компоненти IoT сегментів інфраструктури “розумного міста”, систематизувати випадкові і цілеспрямовані загрози і обґрунтовувати відповідність технологій безпеки. Концептуальна модель предметної сфери “Інтернет речей в “розумному місті”: загрози – технології безпеки” (див. рис. 1) побудована для сегментів інфраструктури: “розумний транспорт” (a1), “розумна медицина” (a2). “розумна енергетика” (a3), “розумна екологія” (a4) і є основою для створення інформаційної моделі бази даних та розроблення алгоритмічно-програмної реалізації АСОІ з обмеженим доступом у просторі безпечного функціонування життєвого циклу інформації на рівні веб-застосунку.

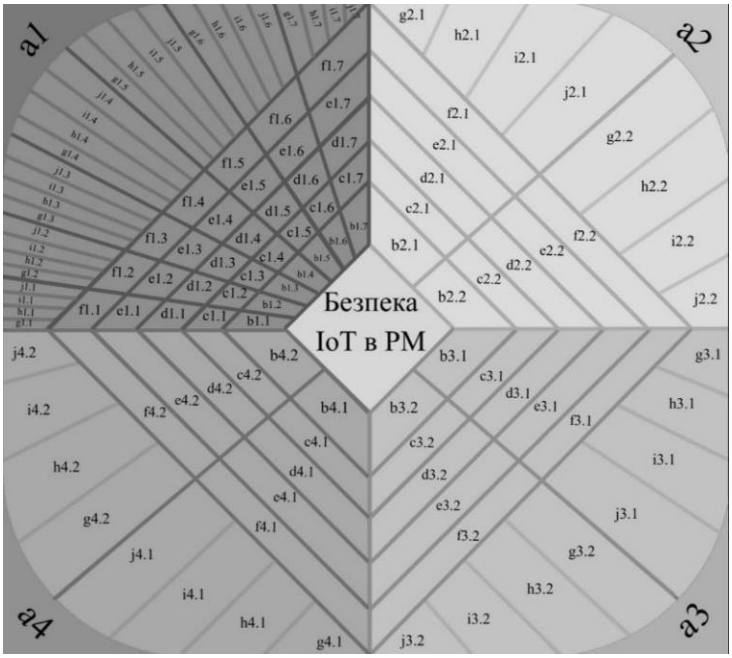

Рис. 1. Концептуальна модель предметної сфери “Інтернет речей в “розумному місті: загрози – технології безпеки”

Концептуальна модель відображає розгортання сегментів інфраструктури компонентами: “розумного транспорту”: розумна залізниця; розумна авіація; розумні автомобільні дороги; розумна логістика; розумний морський транспорт; розумний громадський транспорт; розумна міська мобільність (b1.1 - b1.7); “розумної медицини”: розумні лікарні; телемедицина та дистанційний моніторинг (b2.1 - b2.2); “розумної енергетики”: розумні електромережі; розумний облік та управління енергоспоживанням (b3.1 - b3.2); “розумної екології”: моніторинг якості повітря; моніторинг водних ресурсів та якості води (b4.1 - b4.2).

Інформаційна модель бази даних: обґрунтування вибору реляційної бази даних, системи управління базою даних, мови програмування. Для розроблення АСОІ з ОД “Інтернет речей в “розумному місті”: загрози – технології безпеки” за типом зв'язку між даними обгрунтовано реляційну базу даних (РБД). У такій моделі об’єкти та зв’язки між ними представлені у вигляді двовимірних таблиць, при цьому зв’язки між відношеннями

розглядаються також як об’єкти. Модель РБД обґрунтована за критеріями: структурованості даних, ідентифікації запису, ефективності використання. В якості СУБД для програмної реалізації обрано SQLite. Це реляційна система управління базами даних використовує структуровану мову запитів SQL (Structured Query Language). Основні критерії вибору SQLite: сумісність та простота; підтримка стандартів; портативність.

Інформаційна модель реляційної бази даних (див. рис. 2) у поєднанні з СУБД SQLite є ефективним інструментарієм функціонування життєвого циклу інформації в підсистемах предметної сфери “Інтернету речей розумного міста: загрози – технології безпеки”.

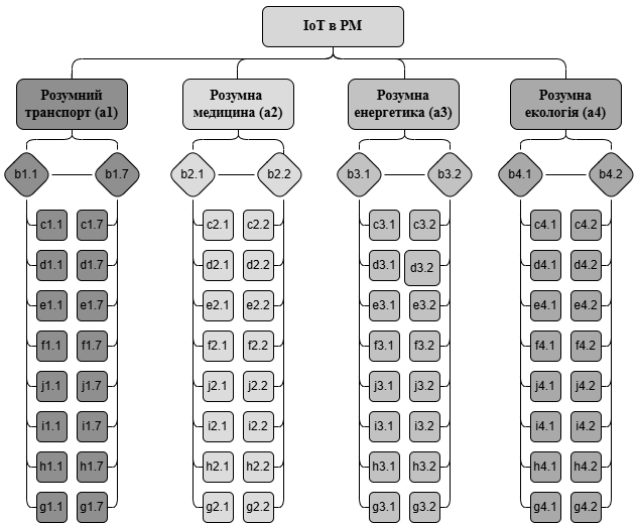

Рис. 2. Інформаційна модель реляційної бази даних “Інтернет речей в “розумному місті”: загрози – технології безпеки”

Алгоритмічно-програмна реалізація безпечного функціонування АСОІ з ОД “Інтернет речей в “розумному місті”: загрози – технології безпеки”

Алгоритм безпечного функціонування автоматизованої системи обробки інформації з обмеженим доступом. Розглянемо етапи розроблення АСОІ “Інтернет речей в “розумному місті”: загрози – технології безпеки” з обмеженим доступом. Автоматизована система призначена для введення, зберігання, обробки та відображення інформації сегментів критичної інфраструктури РМ: “розумного транспорту”, “розумної медицини”, “розумної енергетики”, “розумної екології”. Особливістю розробленої АСОІ з ОД є алгоритмічно-програмна реалізація механізму санкціонованого доступу на основі процедури автентифікації. Технічно система реалізована як веб-застосунок на рівні таких компонентів:

1. Серверної частини (Backend): написана мовою Python з використанням фреймворку Flask;
2. Клієнтської частини (Frontend): HTML-сторінки, що відображають дані;
3. Бази даних: СУБД SQLite для зберігання облікових записів та інформації про сегменти критичної інфраструктури РМ.

Функціонування АСОІ ґрунтується на основі клієнт-серверної архітектури. Взаємодія користувача з АСОІ відбувається за алгоритмом, який забезпечує безпеку даних:

1. Початок роботи (Вхід): При спробі зайти на будь-яку сторінку ACOI, сервер перевіряє, чи є користувач авторизованим. Якщо ж ні – відбувається автоматичне перенаправлення на сторінку входу. Користувач вводить свій email та пароль, які підлягають звіренню системою із записами в базі даних;
2. Реєстрація нових користувачів: Для отримання доступу новий користувач повинен пройти процедуру реєстрації. При цьому система виконує перевірку на унікальність електронної пошти. Пароль користувача під час реєстрації проходить процедуру криптографічного перетворення (хешування) перед записом у базу даних, що гарантує його захист від крадіжки;
3. Робота з інформацією (Навігація): Після входу користувач потрапляє на головну панель, де дані структуровані за категоріями («Транспорт», «Медицина» тощо). Вибір категорії ініціює запит до бази даних, яка повертає список лише відповідних пристроїв чи систем;
4. Політика безпеки (Зміна пароля): В ACOI реалізовано функціонал зміни пароля, який має обмеження – користувачу надається лімітована кількість спроб доступу (у даній реалізації – 3 спроби). Це зроблено для запобігання частих та безконтрольних змін облікових даних, що є частиною політики безпеки;
5. Завершення роботи: Користувач може безпечно вийти з ACOI, активувавши “Вихід”. Це знищує поточну сесію і закриває доступ до даних до наступного введення пароля.

З метою безпечного функціонування ACOI розроблено структуру бази даних SQLite, яка складається з двох основних таблиць, що дозволяє розділити дані користувачів та дані самої системи:

Таблиця 1. users (Користувачі). Таблиця відповідає за безпеку та авторизацію і містить:

- id: Унікальний номер користувача,
- email: Логін для входу в систему,
- password: Хешований пароль (незворотне перетворення символів),
- changes_left: Лічильник, який контролює, скільки разів користувач ще може змінити свій пароль.

Таблиця 2. iot_systems (Об'єкти захисту). Таблиця є основним інформаційним ресурсом ACOI і містить уніфікований набір атрибутів, що дозволяє описати будь-яку підсистему “Інтернету речей “розумного міста”: загрози – технології безпеки” незалежно від її галузевої приналежності. Атрибути таблиці логічно поділяються на три функціональні групи:

А. Група ідентифікації та архітектури:

- id (Ідентифікатор запису): Унікальний первинний ключ запису в системі,
- category (Галузева категорія): Ідентифікатор галузевої приналежності, що дозволяє класифікувати підсистеми за сферами застосування (критична інфраструктура, комунальне господарство, соціальна сфера тощо),
- name (Найменування системи): Назва КФТ у фізичному просторі IoT як інструментарій функціонування інфраструктури “розумного міста”,
- architecture (Архітектура системи): Тип та структура архітектури,
- purpose (Призначення та використання): Цільове призначення та основні функції системи у інфраструктурі розумного міста,

- devices (Апаратні засоби): Сукупність IoT-пристроїв, включаючи сенсори, контролери, виконавчі механізми та засоби зв'язку, що забезпечують функціонування КФТ у фізичному просторі IoT.

Б. Група моделювання дестабілізуючих факторів:

- threats_accidental (Випадкові загрози): Фактори природного або техногенного ймовірного впливу на профілі безпеки IoT-системи (технічні збої, вплив навколишнього середовища, помилки персоналу),
- threts_targeted (Цілеспрямовані загрози): Перелік актуальних векторів кібератак, спрямованих на порушення основних профілів безпеки – конфіденційності, цілісності, доступності інформації, характерних для даного типу архітектури IoT-системи.

В. Група комплексної системи захисту сегменту РМ "Інтернет речей в "розумному місті": загрози – технології захисту":

- methods (Методи захисту): Загальні організаційні та технічні стратегії, що застосовуються для мінімізації ризиків;
- protection_hard (Апаратні засоби захисту): Відомості про фізичні та апаратні засоби безпеки, інтегровані в обладнання IoT-системи для протидії втручанню та несанкціонованому доступу;
- protection_soft (Програмні засоби захисту): Програмні механізми та криптографічні протоколи, що забезпечують захист даних в життєвому циклі інформації в АСОІ,
- purpose standards (Нормативна відповідність): Інформація про відповідність технологій безпеки стандартам з інформаційної та кібербезпеки (міжнародним, державним та галузевим).

Безпечне функціонування АСОІ з ОД реалізовано трьома методами (див. рис. 3):

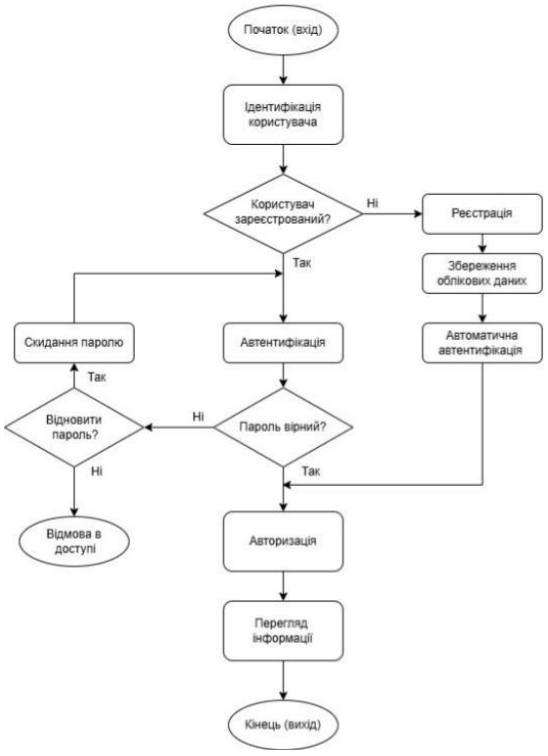

Рис. 3. Блок-схема алгоритму функціонування автоматизованої системи обробки інформації з обмеженим доступом

1. Сесійна автентифікація: Використовується механізм сесій (session). Це своєрідний “цифровий пропуск”, який сервер видає браузеру після введення правильного пароля. При кожному наступному запиті сервер перевіряє цей пропуск і якщо його немає, то доступ блокується;
2. Захист паролів: У базі даних паролі не зберігаються у відкритому вигляді (як звичайний текст). Замість цього використовується хешування. Навіть якщо зловмисник отримає доступ до файлу бази даних, він побачить лише набір незрозумілих символів, з яких неможливо відновити реальний пароль;
3. Контроль дій користувача: Введення ліміту на зміну пароля (поле changes_left) є елементом керування політикою безпеки, що дисциплінує користувачів та захищає систему від зловживань функціоналом.

Програмна реалізація автоматизованої системи обробки інформації з обмеженим доступом. Архітектура розробленої АСОІ на рівні веб-застосунку грунтується на взаємодії клієнтської частини з серверною логікою, реалізованою засобами мікрофреймворку Flask. Ключовими етапами програмної реалізації АСОІ є забезпечення захисту облікових даних користувачів та організація динамічного доступу до реляційної бази даних. З метою забезпечення безпеки АСОІ за профілями конфіденційності, цілісності та доступності в модулі реєстрації користувачів імплементовано механізм криптографічного перетворення паролів. Замість зберігання паролів у відкритому вигляді, система використовує алгоритм хешування з додаванням «солі» (salting), що реалізовано за допомогою бібліотеки werkzeug.security. На першому фрагменті програмного коду наведено процедуру реєстрації нового користувача, яка включає генерацію хешу пароля та автоматичну ініціалізацію сесії після успішного запису даних в СУБД.

```
from werkzeug.security import generate_password_hash, check_password_hash

@app.route('/register', methods=['POST'])
def register():
    email = request.form['email']
    password = request.form['password']
        hashed_pw = generate_password_hash(password)

    try:
        conn = get_db_connection()
        cursor = conn.execute(
            'INSERT INTO users (email, password) VALUES (?, ?)',
            (email, hashed_pw)
        )
            user_id = cursor.lastrowid
            conn.commit()
            conn.close()

            session['user_id'] = user_id
            session['email'] = email
            return redirect(url_for('index'))
        except sqlite3.IntegrityError:
            flash('This email is already registered.', 'error')
    return render_template('register.html')
```

ISSN 2663 – 4023

Другим важливим компонентом АСОІ є модуль візуалізації даних, який відповідає за обробку HTTP-запитів та формування веб-сторінок на основі інформації, що зберігається в базі даних SQLite. Архітектурна модель Flask дозволяє чітко розділити логіку маршрутизації та представлення даних. На другому фрагменті програмного коду представлено реалізацію контролера для відображення певної категорії класифікації. Алгоритм передбачає перевірку прав доступу (наявність активної сесії), виконання параметризованого SQL-запиту для вибірки відповідних систем та передавання отриманих об’єктів у шаблон інтерфейсу.

```
@app.route('/category/<category_id>')
def show_category(category_id):
    if 'user_id' not in session: return redirect(url_for('login'))

    conn = get_db_connection()
    systems = conn.execute(
        'SELECT id, name FROM iot_systems WHERE category = ? ORDER BY
id',
        (category_id,)
    ).fetchall()
    conn.close()

    return render_template('category_list.html', systems=systems)
```

Скріншоти безпечного функціонування АСОІ з ОД “Інтернет речей в “розумному місті”: загрози – технології безпеки” на рівні веб-застосунку представлені на Рис. 4-15.

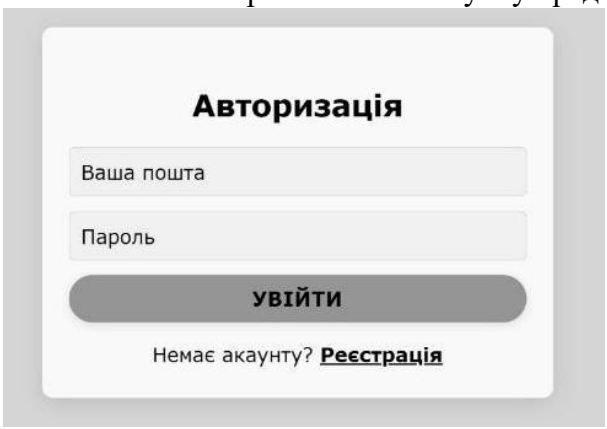

Рис. 4. Сторінка авторизації користувача

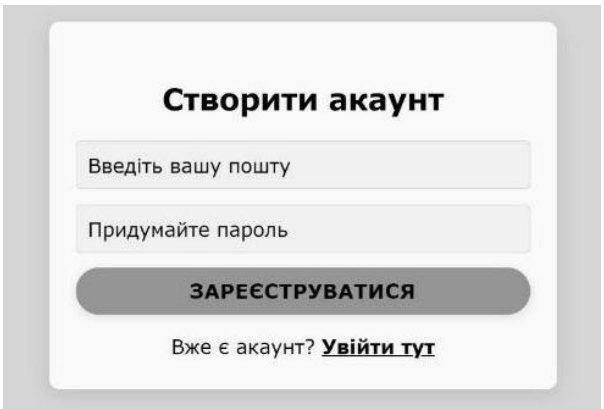

Рис. 5. Сторінка реєстрації користувача

ISSN 2663 – 4023

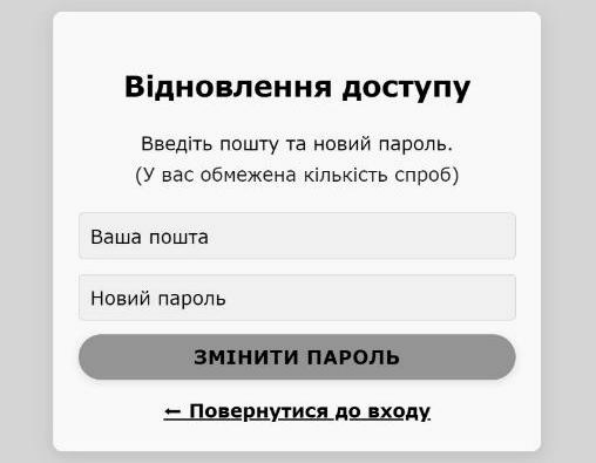

Рис. 6. Сторінка зміни паролю

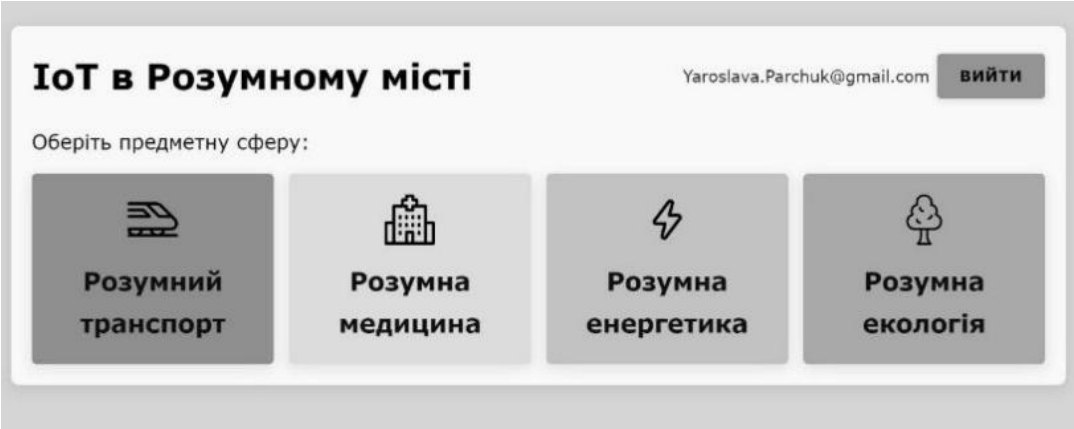

Рис. 7. Головна сторінка АСОІ з ОД

Рис. 8. Сторінка підсистеми "Розумного транспорту"

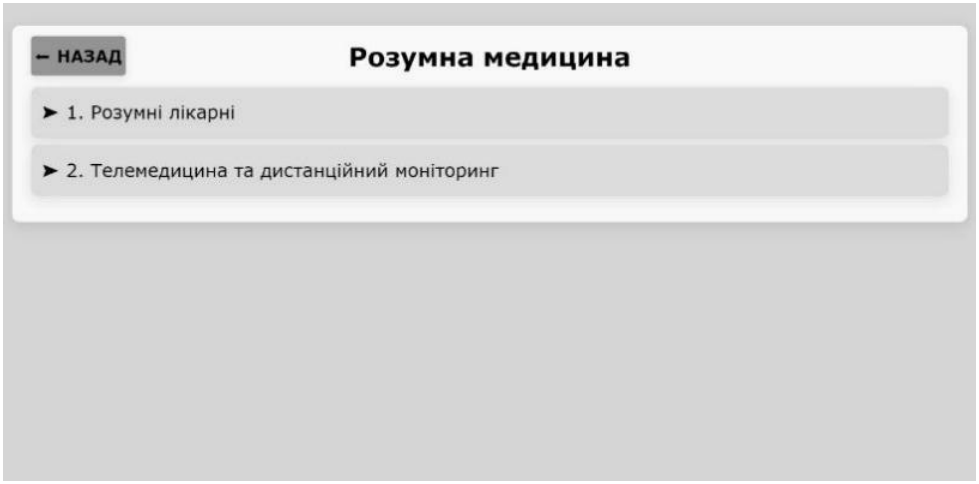

Рис. 9. Сторінка підсистеми "Розумної медицини"

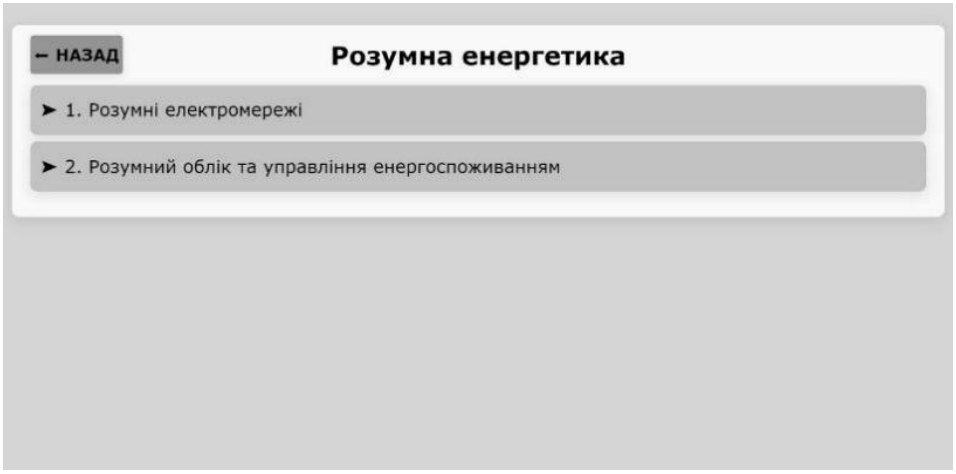

Рис. 10. Сторінка підсистеми "Розумної енергетики"

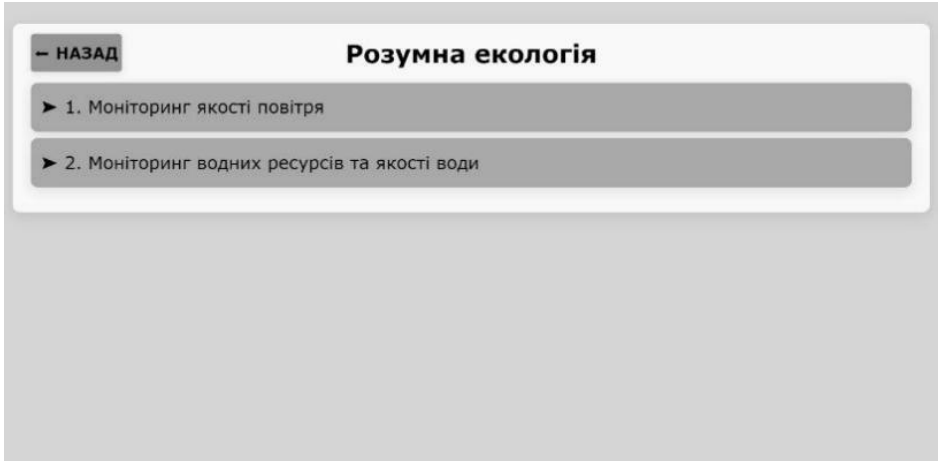

Рис. 11. Сторінка підсистеми "Розумної екології"

← НАЗАД

1. Розумна залізниця

АРХІТЕКТУРА	ПРИЗНАЧЕННЯ	ПРИСТРОЇ IOT	ВИПАДКОВІ ЗАГРОЗИ	ЦІЛЕСПРЯМОВАНІ ЗАГРОЗИ	МЕТОДИ ЗАХИСТУ	АПАРАТНІ ЗАСОБИ	ПРОГРАМНІ ЗАСОБИ	СТАНДАРТИ
Розподілена ієрархічна архітектура. • Давачі на рейках і поїздах передають дані через промислові шлюзи до центральної системи диспетчерського управління. • Edge-обробка для критичних сигналів безпеки.	• Моніторинг стану рейок поїздів; • Автоматизація керування рухом; • Попередження аварій; • Оптимізація розкладів; • Контроль завантаження вагонів.	• Вібро- акустичні давачі на рейках; • GPS/ GLONASS; • Трекери локомотивів; • Давачі температури підшипників; • Системи технічного зору на переїздах; • Інтелектуальні семафори з V2I.	• Відмова давачів через екстремальні погодні умови (сильні морози, спека); • Пошкодження обладнання внаслідок вібрації та механічного зносу; • Збої в системах зв'язку через електромагнітні перешкоди.	• Кібератаки на систему диспетчерського управління для порушення розкладу руху; • Фізичне пошкодження сенсорів та комунікаційного обладнання зловмисниками; • Підміна сигналів семафорів через злом мережі; • DDoS-атаки	• Резервування критичних систем; • Фізичний захист обладнання; • Криптографічний захист каналів зв'язку; • Сегментація мережі; • Контроль доступу до систем управління.	• Захищені промислові контролери з підвищеною стійкістю до вібрацій; • Апаратні криптомодулі для шифрування GSM-R зв'язку; • Резервні канали зв'язку (оптоволокно + радіо); • Захищені корпуси для давачів з антивандальним	• Системи виявлення вторгнень (IDS/IPS) для промислових мереж; • Програмне шифрування даних телеметрії; • Системи контролю цілісності файлів; • Багаторівнева аутентифікація диспетчерів; • Антивірусне	• IEC 62443; • ДСТУ ISO/IEC 27001:2023; • ДСТУ EN 50159:2015; • ДСТУ EN 50126-2:2022.

Рис. 12. Сторінка підсистеми "Розумна залізниця"

← НАЗАД

1. Розумні лікарні

АРХІТЕКТУРА	ПРИЗНАЧЕННЯ	ПРИСТРОЇ IOT	ВИПАДКОВІ ЗАГРОЗИ	ЦІЛЕСПРЯМОВАНІ ЗАГРОЗИ	МЕТОДИ ЗАХИСТУ	АПАРАТНІ ЗАСОБИ	ПРОГРАМНІ ЗАСОБИ	СТАНДАРТИ
Чотирирівнева архітектура. • Давачі. • Мережа (внутрішня мережа, бездротові точки). • Обробка даних (медична інформаційна система, інтеграційна шина). • Прикладний рівень (електронні картки, під-	• Безперервний моніторинг життєвих показників пацієнтів; • Автоматизація процесів лікарні; • Відстеження медичного обладнання та ліків; • Контроль параметрів навколишнього середовища в операційних та реаніма-	• Носимі монітори ЕКГ та пульсоксиметри; • Розумні ліжка з давачами тиску та положення; • RFID-мітки для відстеження обладнання та пацієнтів; • Давачі температури та вологості в палатах; • Розумні інфузійні помпи	• Відмова бездротових давачів через радіоперешкоди від медичного обладнання; • Розрядка батарей носимих пристроїв в критичний момент; • Збої в роботі систем через перевантаження мережі; • Помилки в алгоритмах	• Ransomware атаки на медичні інформаційні системи з блокуванням доступу до даних пацієнтів; • Крадіжка конфіденційних медичних записів через злом мережі; • Маніпуляції з показниками медичних пристроїв через вразливості	• Сегментація медичної мережі від загальної; • Шифрування медичних даних при передачі та зберіганні; • Сувора автентифікація медичного персоналу; • Резервування критичних систем моніторингу; • Контроль цілісності да-	• Медичні ізольовані мережеві сегменти з апаратними міжмережевими екранами; • Криптопроцесори в медичних пристроях для захисту даних; • Захищені RFID-мітки з шифруванням; • Резервні джерела жив-	• Рішення для захисту медичних даних згідно HIPAA; • Медична інформаційна система (HIS/EMR) з вбудованим шифруванням; • Системи виявлення аномалій в роботі медичних пристроїв; • Багаторівнева автентифікація пер-	• IEC 80001-1:2021; • IEC 81001-2-2:2025; • IEC 81001-5-1:2022; • ISO 27799:2025; • ISO/IEC 27400:2022); • ISO/IEC 30141:2024; • NIST FIPS 140-2; • IEEE 11073; • ДСТУ 3396.0-96; • НД ТЗІ 1.1-002-99;

Рис. 13. Сторінка підсистеми "Розумні лікарні"

← НАЗАД

1. Розумні електромережі

АРХІТЕКТУРА	ПРИЗНАЧЕННЯ	ПРИСТРОЇ IOT	ВИПАДКОВІ ЗАГРОЗИ	ЦІЛЕСПРЯМОВАНІ ЗАГРОЗИ	МЕТОДИ ЗАХИСТУ	АПАРАТНІ ЗАСОБИ	ПРОГРАМНІ ЗАСОБИ	СТАНДАРТИ
Ієрархічна архітектура. • Польові пристрої (лічильники, давачі, PMU), підстанції (концентратори, RTU, автоматика). • Передача (оптоволокно, PLC, бездротові мережі). • Диспетчерське управління (SCADA, EMS/DMS). • Інтеграція	• Двосторонній обмін даними між споживачами та постачальниками; • Автоматичне управління навантаженням мережі; • Швидке виявлення та ізоляція аварій; • Інтеграція розподіленої генерації та відновлюва-	• Розумні електролічильники з AMI-функціоналом; • PMU-пристрої синхровимірювання; • Давачі струму та напруги на ЛЕП; • Реклозери з дистанційним керуванням; • Давачі температури трансформа-	• Відмова обладнання через перенапруги від блискавок; • Збої в передачі даних через електромагнітні перешкоди на підстанціях; • Пошкодження лічильників внаслідок стихійних лих; • Помилки в алгоритмах прогнозува-	• Кібератаки на SCADA-системи для відключення енергопостачання регіонів; • Злом розумних лічильників для крадіжки електроенергії; • DDoS-атаки на диспетчерські центри; • Маніпуляції даними PMU для дестабілізації мережі;	• Сегментація мереж за рівнями Purdue; • Глибокоешелонований захист SCADA-систем; • Шифрування каналів зв'язку між підстанціями; • Сувора автентифікація диспетчерського персоналу; • Безперервний моніто-	• Апаратні міжмережеві екрани промислового класу; • Криптомодулі для захисту протоколів IEC 61850 та DNP3; • Захищені RTU з функціями виявлення вторгнень; • Однонаправлені data diode	• Системи виявлення вторгнень для промислових протоколів (SCADA IDS); • SIEM-платформи для енергетичних об'єктів; • Системи whitelist для SCADA-систем; • Програмне шифрування телеметрії з лічильників; • Системи	• IEC 62351; • ISO/IEC 27019:2024; • NIST IR 7628:2014; • ДСТУ IEC 62351; • ДСТУ IEC/ISO 27001:2023; • НД ТЗІ 2.5-004-99.

Рис. 14. Сторінка підсистеми "Розумні електромережі"

– НАЗАД

2. Моніторинг водних ресурсів та якості води

АРХІТЕКТУРА	ПРИЗНАЧЕННЯ	ПРИСТРОЇ IOT	ВИПАДКОВІ ЗАГРОЗИ	ЦІЛЕСПРЯМОВАНІ ЗАГРОЗИ	МЕТОДИ ЗАХИСТУ	АПАРАТНІ ЗАСОБИ	ПРОГРАМНІ ЗАСОБИ	СТАНДАРТИ
Розподілена архітектура. • Вимірювання (буї, підводні станції, зонди, давачі). • Мережа (супутниковий зв'язок, LoRaWAN, 4G). • Edge-обробка (локальні контролери). • Центральний рівень (моніторинг,	• Безперервний моніторинг якості води в річках, озерах та водосховищах; • Контроль параметрів питної води в системах водопостачання; • Виявлення джерел забруднення водойм в реальному часі; • Моніторинг рівня води	• Багатопараметричні зонди (pH, розчинений кисень, каламутність, температура); • Давачі електропровідності та солоності води; • Нітратні та фосфатні аналізатори для контролю евтрофікації; • Давачі рівня води ультразвукові та ра-	• Біообростання давачів водоростями що спотворює вимірювання; • Пошкодження обладнання через шторми, льодохід, повені; • Калібрувальний дрейф сенсорів через тривале занурення у воду; • Втрата супутникового зв'язку буїв	• Фізичне пошкодження або крадіжка дорогих давачів та буїв; • Кібератаки на системи моніторингу для приховування скидів забруднень; • Підміна даних про якість води підприємствами-забруднювачами; • Злом систем оповіщення	• Регулярна очистка давачів від біообростання автоматичними механічними або ультразвуковими системами; • Шифрування гідрологічних даних при передачі від станцій до центрів; • Фізичний захист дорогого обладнання якірними	• Антивандальні буї з корпусами високої міцності та яскравим маркуванням; • Криптомодулі в підводних станціях для захисту телеметрії; • GPS-трекери на обладнанні з оповіщенням про переміщення; • Автоматичні системи очи-	• Платформа гідромоніторингу з вбудованим шифруванням та контролем доступу; • Алгоритми машинного навчання для виявлення аномальних вимірювань; • Системи автоматичної калібровки давачів з компенсацією дрейфу;	• ISO/IEC 27400:2022; • ISO 24512:2024; • NIST CSF 2.0:2024; • NIST SP 800-213:2021; • EN ISO 10523:2012; • IEEE 802.15.4:2020. • ДСТУ EN ISO 5667-6:2025; • ДСТУ EN ISO

Рис. 15. Сторінка підсистеми "Моніторинг водних ресурсів та якості води"

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розглянуто якісний аналіз предметної сфери безпеки Інтернету речей в сегментах "розумного міста" і, на цій основі, побудовано класифікаційну схему методом групування та створено концептуальну модель "IoT в "розумному місті: загрози – технології безпеки". Розроблено алгоритмічно-програмну реалізацію безпечного функціонування автоматизованої системи обробки інформації "Інтернет речей в "розумному місті": загрози – технології безпеки" із застосуванням методів сесійної аутентифікації, захисту паролів та контролю дій користувача на основі інформаційної моделі реляційної бази даних, системи управління базою даних SQLite засобами мови програмування Python. Запропонований методологічний підхід до розроблення ACOI з ОД "Інтернет речей в "розумному місті: загрози – технології безпеки" може ефективно використовуватись для вирішення прикладних завдань безпечної інтелектуалізації об'єктів інфраструктури суспільства з урахуванням сучасних тенденцій кібервикликів в епоху Індустрії 5.0, яка передбачає інтеграцію фізичних, цифрових та біологічних систем у просторі забезпечення безпечних технологій протидії кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Association of Industrial Automation Enterprises of Ukraine. (2018). *Industry 4.0 development strategy*. https://mautic.appau.org.ua/asset/42:strategia-rozvitku-4-0-v3.pdf
2. European Union Agency for Cybersecurity. (2021). *International strategy of the EU Agency for Cybersecurity*. https://www.enisa.europa.eu/sites/default/files/all_files/2022-02%20B16%20ENISA%20International%20Strategy.pdf
3. National Security and Defense Council of Ukraine. (2021). *Cybersecurity Strategy of Ukraine for 2021–2025*. https://www.rnbo.gov.ua/les/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf
4. Dudykevych, V. B., Mykytyn, H. V., & Rebets, A. I. (2018). Quintessence of cyber-physical system information security. *Bulletin of the National University "Lviv Polytechnic". Series: Information Systems and Networks*, (887), 58–68. http://nbuv.gov.ua/UJRN/VNULPICM_2018_887_10
5. Asatiani, A., Hakkarainen, T., Paaso, K., & Penttinen, E. (2024). Security by envelopment: A novel approach to data-security-oriented configuration of lightweight automation systems. *European Journal of Information Systems*, *33*(5), 631–653. https://doi.org/10.1080/0960085X.2023.2217362

6. Balocon, O. H. (2024). Prioritizing information security: Analysis of software development life cycle methodologies using the NIST cybersecurity framework. *Ignatian International Journal for Multidisciplinary Research*, *2*(4), 1495–1508.
7. Smyk, D., & Burak, N. (2025). Methods and means of data processing in modern automated systems. *Bulletin of Lviv State University of Life Safety*, *31*, 41–49. https://doi.org/10.32447/20784643.31.2025.05
8. Panovyk, U. (2025). Information protection in automated systems based on a conceptual model with formalized efficiency evaluation. *Cybersecurity: Education, Science, Technique, 4*(28), 307–320. https://doi.org/10.28925/2663-4023.2025.28.798
9. Bobalo, Y. Y., Dudykevych, V. B., & Mykytyn, H. V. (2020). *Strategic security of the "object – information technology" system*. Lviv: Lviv Polytechnic Publishing House.
10. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., & Balagura, D. (2024). Development of the sociocyberphysical systems multi-contour security methodology. *Eastern-European Journal of Enterprise Technologies*, *127*(9). https://doi.org/10.15587/1729-4061.2024.298844
11. Chirra, D. R. (2024). *AI-enabled cybersecurity solutions for protecting smart cities against emerging threats*.
12. Oliha, J. S., Biu, P. W., & Obi, O. C. (2024). Securing the smart city: A review of cybersecurity challenges and strategies. *Engineering Science & Technology Journal, 5*(2), 496–506. https://doi.org/10.53022/oarjms.2024.7.1.0013
13. Mohammed, A. (2024). Cybersecurity in smart cities: As cities become smarter, new vulnerabilities arise. *Pioneer Research Journal of Computing Science, 1*(1), 75–82. https://prjcs.com/index.php/prjcs/article/view/19
14. Mohammed, A. (2022). Cybersecurity in smart cities: Securing IoT and smart infrastructure. *Journal of Innovative Technologies, 5*(1). https://acadexpinnara.com/index.php/JIT/article/view/334
15. Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of Internet of Things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions. *Information*, *14*(7), 388. https://doi.org/10.3390/info14070388
16. Sharma, R., & Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of the art. *Transactions on Emerging Telecommunications Technologies*, *34*(11), e4571. https://doi.org/10.1002/ett.4571
17. Ali, J., Singh, S. K., Jiang, W., Alenezi, A. M., Islam, M., Daradkeh, Y. I., & Mehmood, A. (2025). A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks. *Computer Communications*, *229*, 108000. https://doi.org/10.1016/j.comcom.2024.108000
18. Khomenko, Y. (2024). Modern methods, models and software tools for implementation and optimization of IoT systems. *Information Technologies in Education*, *55*, 72–84. https://doi.org/10.14308/ite000782
19. Kovalenko, A., Yaroshevich, R., & Balenko, O. (2021). Internet of Things: Problems of information security and methods of improvement. *Control, Navigation and Communication Systems, 2*(64), 78–80. https://doi.org/10.26906/SUNZ.2021.2.078
20. Klimushin, P. S., & Petro, S. K. (2025). Communication technologies and specialized communication protocols for ensuring cybersecurity of the Internet of Things. *LAW, 52*. https://doi.org/10.32631/pb.2025.2.05
21. Zhurylo, O., Lyashenko, O., & Avetisova, K. (2023). Hardware security overview of fog computing end devices in the Internet of Things. *Innovative Technologies and Scientific Solutions for Industries*, *1*(23), 57–71. https://doi.org/10.30837/ITSSI.2023.23.057
22. Andrushchak, I., & Kosheliuk, V. (2025). Specific aspects of designing an information security system to protect IoT networks from attacks. *International Science Journal of Engineering & Agriculture*, *4*(5), 27–39. https://doi.org/10.46299/j.isjea.20250405.03
23. Oliinyk, Y., Platonenko, A., Cherevyk, V., Vorokhob, M., & Shevchuk, Y. (2025). Methods of information security in IoT technologies. *Cybersecurity: Education, Science, Technique, 3*(27), 100–108. https://doi.org/10.28925/2663-4023.2025.27.705
24. Yashchuk, V., Panovyk, U., Cherkas, S., Ivanusa, A., & Tkachuk, R. (2025). Comprehensive protection model of IoT devices in the home environment: Threats, vulnerabilities and neutralization methods. *Bulletin of Lviv State University of Life Safety*, *32*, 125–140. https://doi.org/10.32447/20784643.32.2025.10
25. Malinovsky, V. I., Kuperstein, L. M., Lukichov, V. V., & Dudatev, A. V. (2024). Issues and approaches to improving security in data transmission channels of IoT systems and devices. *Bulletin of Vinnytsia Polytechnic Institute*, *4*, 105–115. https://doi.org/10.31649/1997-9266-2024-175-4-104-114
26. Yuzevych, V., Obshta, A., Opirskyy, I., & Harasymchuk, O. (2024). Algorithm for assessing the degree of information security risk of a cyber-physical system for controlling underground metal constructions. *CEUR Workshop Proceedings*, *3702*, 400–412.
27. Martseniuk, Y., Partyka, A., Harasymchuk, O., Nyemkova, E., & Karpiński, M. (2024). Shadow IT risk analysis in public cloud infrastructure. *CEUR Workshop Proceedings*, *3800*, 22–31.

28. Dudykevych, V., Mykytyn, G., Stosyk, T., & Skladannyi, P. (2024). Platform for the security of cyber-physical systems and IoT in the intellectualization of society. *Cybersecurity Providing in Information and Telecommunication Systems*, 449–457.
29. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017, 9324035. https://doi.org/10.1155/2017/9324035
30. Dudykevych, V. B., Mykytyn, G. V., & Galunets, M. O. (2020). System model of information security for a smart city. *Information Processing Systems*, *2*(161), 93–98. https://doi.org/10.30748/soi.2020.161.11
31. Arena, F., & Pau, G. (2019). An overview of vehicular communications. *Future Internet*, *11*(2), 27. https://doi.org/10.3390/fi11020027
32. Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A., Bairagi, A. K., Khan, M. A. M., & Kee, S. H. (2022). IoT-based healthcare monitoring system towards improving quality of life: A review. *Healthcare*, *10*(10). https://doi.org/10.3390/healthcare10101993
33. Orlando, M., Estebsari, A., Pons, E., Pau, M., Quer, S., Poncino, M., & Patti, E. (2021). A smart meter infrastructure for smart grid IoT applications. *IEEE Internet of Things Journal*, *9*(14), 12529–12541. https://doi.org/10.1109/JIOT.2021.3137596
34. Dudykevych, V. B., Mykytyn, G. V., Bordulyak, S. M., & Fur, Y. M. (2025). Comprehensive security system for an intelligent cyber-physical emergency monitoring system. *Modern Information Protection*, *1*, 249–258. https://doi.org/10.31673/2409-7292.2025.014428
35. Khatide, N. N., Laka, K. V., & Khauoe, T. N. (2025). Applications and challenges of network technologies in IoT-based biological water monitoring systems. https://doi.org/10.21203/rs.3.rs-7337247/v1
36. Madani, K. (2026). Water bankruptcy: The formal definition. *Water Resources Management*, *40*, 78. https://doi.org/10.1007/s11269-025-04484-0
37. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
38. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201
39. Ouakasse, F., & Rakrak, S. (2022). CoAP and MQTT: Characteristics and security. *International Conference on Networking, Intelligent Systems and Security*, 157–167. https://doi.org/10.1007/978-3-031-15191-0_15
40. Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(13), 3625. https://doi.org/10.3390/s20133625
41. Bredesen, R., & Mujeye, S. (2025). Network segmentation security with the implementation of threats. *Proceedings of the 8th International Conference on Software Engineering and Information Management*, 137–141. https://doi.org/10.1145/3725899.3725920
42. Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. *Digital Communications and Networks*, *8*(4), 540–551. https://doi.org/10.1016/j.dcan.2022.05.027

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

Yaroslava Parchuk
Master's Student at the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0002-7349-7364
yaroslava.parchuk.mkbst.2025@lpnu.ua

Maksym-Stepan Terpeliuk
Master's Student at the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0001-7015-5855
maksym-stepan.terpeliuk.mkbst.2025@lpnu.ua

CREATION OF AN AUTOMATED INFORMATION PROCESSING SYSTEM WITH RESTRICTED ACCESS “INTERNET OF THINGS IN A ‘SMART CITY’: THREATS – SECURITY TECHNOLOGIES” IN THE INDUSTRY 4.0 SPACE

Abstract. Within the scope of Industry 4.0 tasks, this paper examines the issue of secure intellectualization of Ukraine's social infrastructure at the level of developing an automated restricted-access information processing system (AIPS with RA) in the Internet of Things (IoT) security segment of a “smart city” (SC) and algorithmic and software implementation using the Python programming language. An analytical review of known methodologies for developing secure automated information processing systems and approaches to ensuring the security of IoT systems was conducted. A qualitative analysis of the segments of a “smart city” – transport, health, energy, ecology – was carried out by grouping them at the level of the classification scheme of the subject area according to the “object – threat – protection” concept. A conceptual model of the subject area “Internet of Things in a ‘smart city’: threats – security technologies” was created based on the principles of system analysis – integrity, hierarchy, and multifacetedness. The criteria for selecting a relational database (RDB), SQLite database management system (DBMS), and Python programming language were justified, and an RDB information model was constructed for further algorithmic and software implementation. An algorithm for the secure operation of an automated information processing system at the authentication procedure level has been presented and, on this basis, a software implementation of the AIPS “Internet of Things in a Smart City: threats – security technologies” using Python for the segments: “smart transport”, “smart health”, “smart energy”, “smart ecology” at the web application level.

Keywords: intellectualization of objects; security; Internet of Things; “smart city”; classification scheme; conceptual and information models; relational database; automated information processing system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Association of Industrial Automation Enterprises of Ukraine. (2018). *Industry 4.0 development strategy*.
2. European Union Agency for Cybersecurity. (2021). *International strategy of the EU Agency for Cybersecurity*.

3. National Security and Defense Council of Ukraine. (2021). *Cybersecurity Strategy of Ukraine for 2021–2025*.
4. Dudykevych, V. B., Mykytyn, H. V., & Rebets, A. I. (2018). Quintessence of cyber-physical system information security. *Bulletin of the National University "Lviv Polytechnic". Series: Information Systems and Networks*, (887), 58–68. http://nbuv.gov.ua/UJRN/VNULPICM_2018_887_10
5. Asatiani, A., Hakkarainen, T., Paaso, K., & Penttinen, E. (2024). Security by envelopment: A novel approach to data-security-oriented configuration of lightweight automation systems. *European Journal of Information Systems*, *33*(5), 631–653. https://doi.org/10.1080/0960085X.2023.2217362
6. Balocon, O. H. (2024). Prioritizing information security: Analysis of software development life cycle methodologies using the NIST cybersecurity framework. *Ignatian International Journal for Multidisciplinary Research*, *2*(4), 1495–1508.
7. Smyk, D., & Burak, N. (2025). Methods and means of data processing in modern automated systems. *Bulletin of Lviv State University of Life Safety*, *31*, 41–49. https://doi.org/10.32447/20784643.31.2025.05
8. Panovyk, U. (2025). Information protection in automated systems based on a conceptual model with formalized efficiency evaluation. *Cybersecurity: Education, Science, Technique*, *4*(28), 307–320. https://doi.org/10.28925/2663-4023.2025.28.798
9. Bobalo, Y. Y., Dudykevych, V. B., & Mykytyn, H. V. (2020). *Strategic security of the "object – information technology" system*. Lviv: Lviv Polytechnic Publishing House.
10. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., & Balagura, D. (2024). Development of the sociocyberphysical systems multi-contour security methodology. *Eastern-European Journal of Enterprise Technologies*, *127*(9). https://doi.org/10.15587/1729-4061.2024.298844
11. Chirra, D. R. (2024). *AI-enabled cybersecurity solutions for protecting smart cities against emerging threats*.
12. Oliha, J. S., Biu, P. W., & Obi, O. C. (2024). Securing the smart city: A review of cybersecurity challenges and strategies. *Engineering Science & Technology Journal*, *5*(2), 496–506. https://doi.org/10.53022/oarjms.2024.7.1.0013
13. Mohammed, A. (2024). Cybersecurity in smart cities: As cities become smarter, new vulnerabilities arise. *Pioneer Research Journal of Computing Science*, *1*(1), 75–82. https://prjcs.com/index.php/prjcs/article/view/19
14. Mohammed, A. (2022). Cybersecurity in smart cities: Securing IoT and smart infrastructure. *Journal of Innovative Technologies*, *5*(1). https://acadexpinnara.com/index.php/JIT/article/view/334
15. Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of Internet of Things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions. *Information*, *14*(7), 388. https://doi.org/10.3390/info14070388
16. Sharma, R., & Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of the art. *Transactions on Emerging Telecommunications Technologies*, *34*(11), e4571. https://doi.org/10.1002/ett.4571
17. Ali, J., Singh, S. K., Jiang, W., Alenezi, A. M., Islam, M., Daradkeh, Y. I., & Mehmood, A. (2025). A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks. *Computer Communications*, *229*, 108000. https://doi.org/10.1016/j.comcom.2024.108000
18. Khomenko, Y. (2024). Modern methods, models and software tools for implementation and optimization of IoT systems. *Information Technologies in Education*, *55*, 72–84. https://doi.org/10.14308/ite000782
19. Kovalenko, A., Yaroshevich, R., & Balenko, O. (2021). Internet of Things: Problems of information security and methods of improvement. *Control, Navigation and Communication Systems*, *2*(64), 78–80. https://doi.org/10.26906/SUNZ.2021.2.078
20. Klimushin, P. S., & Petro, S. K. (2025). Communication technologies and specialized communication protocols for ensuring cybersecurity of the Internet of Things. *LAW*, *52*. https://doi.org/10.32631/pb.2025.2.05
21. Zhurylo, O., Lyashenko, O., & Avetisova, K. (2023). Hardware security overview of fog computing end devices in the Internet of Things. *Innovative Technologies and Scientific Solutions for Industries*, *1*(23), 57–71. https://doi.org/10.30837/ITSSI.2023.23.057
22. Andrushchak, I., & Kosheliuk, V. (2025). Specific aspects of designing an information security system to protect IoT networks from attacks. *International Science Journal of Engineering & Agriculture*, *4*(5), 27–39. https://doi.org/10.46299/j.isjea.20250405.03
23. Oliinyk, Y., Platonenko, A., Cherevyk, V., Vorokhob, M., & Shevchuk, Y. (2025). Methods of information security in IoT technologies. *Cybersecurity: Education, Science, Technique*, *3*(27), 100–108. https://doi.org/10.28925/2663-4023.2025.27.705

24. Yashchuk, V., Panovyk, U., Cherkas, S., Ivanusa, A., & Tkachuk, R. (2025). Comprehensive protection model of IoT devices in the home environment: Threats, vulnerabilities and neutralization methods. *Bulletin of Lviv State University of Life Safety, 32*, 125–140. https://doi.org/10.32447/20784643.32.2025.10
25. Malinovsky, V. I., Kuperstein, L. M., Lukichov, V. V., & Dudatev, A. V. (2024). Issues and approaches to improving security in data transmission channels of IoT systems and devices. *Bulletin of Vinnytsia Polytechnic Institute, 4*, 105–115. https://doi.org/10.31649/1997-9266-2024-175-4-104-114
26. Yuzevych, V., Obshta, A., Opirskyy, I., & Harasymchuk, O. (2024). Algorithm for assessing the degree of information security risk of a cyber-physical system for controlling underground metal constructions. *CEUR Workshop Proceedings, 3702*, 400–412.
27. Martseniuk, Y., Partyka, A., Harasymchuk, O., Nyemkova, E., & Karpiński, M. (2024). Shadow IT risk analysis in public cloud infrastructure. *CEUR Workshop Proceedings, 3800*, 22–31.
28. Dudykevych, V., Mykytyn, G., Stosyk, T., & Skladannyi, P. (2024). Platform for the security of cyber-physical systems and IoT in the intellectualization of society. *Cybersecurity Providing in Information and Telecommunication Systems*, 449–457.
29. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 2017, 9324035. https://doi.org/10.1155/2017/9324035
30. Dudykevych, V. B., Mykytyn, G. V., & Galunets, M. O. (2020). System model of information security for a smart city. *Information Processing Systems, 2*(161), 93–98. https://doi.org/10.30748/soi.2020.161.11
31. Arena, F., & Pau, G. (2019). An overview of vehicular communications. *Future Internet, 11*(2), 27. https://doi.org/10.3390/fi11020027
32. Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A., Bairagi, A. K., Khan, M. A. M., & Kee, S. H. (2022). IoT-based healthcare monitoring system towards improving quality of life: A review. *Healthcare, 10*(10). https://doi.org/10.3390/healthcare10101993
33. Orlando, M., Estebsari, A., Pons, E., Pau, M., Quer, S., Poncino, M., & Patti, E. (2021). A smart meter infrastructure for smart grid IoT applications. *IEEE Internet of Things Journal, 9*(14), 12529–12541. https://doi.org/10.1109/JIOT.2021.3137596
34. Dudykevych, V. B., Mykytyn, G. V., Bordulyak, S. M., & Fur, Y. M. (2025). Comprehensive security system for an intelligent cyber-physical emergency monitoring system. *Modern Information Protection, 1*, 249–258. https://doi.org/10.31673/2409-7292.2025.014428
35. Khatide, N. N., Laka, K. V., & Khauoe, T. N. (2025). Applications and challenges of network technologies in IoT-based biological water monitoring systems. https://doi.org/10.21203/rs.3.rs-7337247/v1
36. Madani, K. (2026). Water bankruptcy: The formal definition. *Water Resources Management, 40*, 78. https://doi.org/10.1007/s11269-025-04484-0
37. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
38. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84. https://doi.org/10.1109/MC.2017.201
39. Ouakasse, F., & Rakrak, S. (2022). CoAP and MQTT: Characteristics and security. *International Conference on Networking, Intelligent Systems and Security*, 157–167. https://doi.org/10.1007/978-3-031-15191-0_15
40. Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors, 20*(13), 3625. https://doi.org/10.3390/s20133625
41. Bredesen, R., & Mujeye, S. (2025). Network segmentation security with the implementation of threats. *Proceedings of the 8th International Conference on Software Engineering and Information Management*, 137–141. https://doi.org/10.1145/3725899.3725920
42. Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. *Digital Communications and Networks, 8*(4), 540–551. https://doi.org/10.1016/j.dcan.2022.05.027

Отримано редакцією журналу / Received: 05.01.26
Прорецензовано / Revised: 20.02.26
Схвалено до друку / Accepted: 26.03.26