https://doi.org/10.31891/2219-9365-2025-82-11
УДК 004.056:004.852:004.75

КОРОЛЬКОВ Олексій
Хмельницький національний університет
https://orcid.org/0009-0004-6843-9498
-mail: adroyal2017@gmail.com
ПОПЛАВСЬКИЙ Сергій
Хмельницький національний університет
https://orcid.org/0009-0006-1949-8656
e-mail: sergey.poplavskii@gmail.com
ГЛУХЕНЬКИЙ Олександр
Хмельницький національний університет
http://orcid.org/0009-0003-1498-3423
e-mail: goldbergoalexander@gmail.com
ПОНОЧОВНА Олена
Полтавський державний аграрний університет
https://orcid.org/0000-0002-4377-0633
e-mail: olena.ponochovna@pdau.edu.ua

МЕТОД КОМПЛЕКСНОЇ ОПТИМІЗАЦІЇ ЕНЕРГОЗБЕРЕЖЕННЯ ТА БЕЗПЕКИ ДЛЯ ТЕХНОЛОГІЙ IoT

У статті представлено новий метод комплексної адаптивної оптимізації енергоспоживання та кібербезпеки в системах Інтернету речей (IoT), розроблений з урахуванням обмежених ресурсів вбудованих пристроїв і необхідності підтримки високого рівня захисту даних у реальному часі. Метод базується на принципах динамічного управління режимами роботи IoT-пристроїв із використанням алгоритмів, які враховують поточний заряд акумулятора, рівень критичності оброблюваних даних, частоту подій та ризики мережевих загроз. Його реалізація дозволяє автоматично змінювати частоту передачі даних і режими енергоспоживання, забезпечуючи збалансовану взаємодію між автономністю пристрою та безпекою інформації.

У межах дослідження було здійснено глибокий аналіз сучасних викликів у сфері IoT, класифіковано існуючі підходи до енергозбереження та розглянуто актуальні криптографічні протоколи, зокрема IPSec, TLS, AES, RSA та ECC. На основі отриманих висновків запропоновано оригінальний алгоритм адаптивного керування енергоспоживанням і захистом передачі даних. Для оцінки його ефективності було розроблено та реалізовано експериментальний прототип IoT-пристрою на базі мікроконтролера ESP32, сенсора DHT22, MQTT-протоколу з TLS-захистом, а також створено програмну візуалізацію на базі Node-RED. Проведені 108-годинні випробування з моделюванням загроз (сканування портів, підміна IP, flood-атаки) показали зменшення енергоспоживання на понад 40% у порівнянні з фіксованим режимом, без втрати точності або стабільності системи. Отримані результати підтверджують високу ефективність розробленого методу та його придатність до впровадження в побутові, інфраструктурні й промислові IoT-системи, де критично важливими є автономність, надійність і безпека даних.

Ключові слова: IoT технології, кібербезпека, енергоспоживання

KOROLKOV Oleksii, POPLAVSKYI Serhii, HLUKHENKYI Oleksandr
Khmelnytskyi National University
PONOCHOVNA Olena
Poltava State Agrarian University

METHOD OF COMPREHENSIVE OPTIMIZATION OF ENERGY CONSERVATION AND SECURITY FOR IoT TECHNOLOGY

The article presents a new method of comprehensive adaptive optimization of energy consumption and cybersecurity in the Internet systems (IOT), developed taking into account the limited resources of built -in devices and the need to maintain a high level of data protection in real time. The method is based on the principles of dynamic control of IOT-gear modes using algorithms that take into account the current battery charge, the level of criticality of the data processed, the frequency of events and the risks of network threats. Its implementation allows you to automatically change the frequency of data transmission and energy consumption modes, ensuring a balanced interaction between the autonomy of the device and the safety of information.

The study made a thorough analysis of current IOT challenges, classified existing approaches to energy saving and considered current cryptographic protocols, including IPSEC, TLS, AES, RSA and ECC. On the basis of the obtained conclusions, the original algorithm of adaptive control of energy consumption and protection of data transmission is proposed. To evaluate its effectiveness, an experimental prototype of the IOT device based on the ESP32 microcontroller, DT22 sensor, MQTT-protocol with TLS defense was developed and implemented, and the Node-Red software visualization was created. 108-hour threat modeling tests (port scanning, IP, Flooda attacks) showed a decrease in energy consumption by more than 40% compared to the fixed mode, without loss of accuracy or stability of the system.

The results confirm the high efficiency of the developed method and its suitability for the introduction into household, infrastructure and industrial IOT systems, where the autonomy, reliability and safety of data are critical.

Keywords: IoT, Cybersecurity, Energy Consumption

Стаття надійшла до редакції / Received 24.04.2025
Прийнята до друку / Accepted 14.05.2025

ISSN 2219-9365

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Концепція «Інтернету речей» передбачає, що до мережі будуть підключені мільйони пристроїв. Серед основних завдань забезпечення оптимального управління і доступність швидко відстежувати збої, конфігурації і продуктивність такої величезної кількості пристроїв за допомогою протоколів управління. Крім цього необхідно забезпечити сумісність в мережі: неоднорідні пристрої та протоколи повинні працювати один з одним з урахуванням збереження конфіденційності та безпеки. У мережі «Інтернету речей» прийнято таку модель: кінцеві пристрої, датчики, сенсори спілкуються один з одним (так зване взаємодія D2D - Device to Device). Дані, зібрані пристроями, відправляються на сервер для подальшого аналізу і обробки (взаємодія D2S - Device to Server).

Кожен вузол мережі Інтернет-речей має свій сервіс, надаючи якусь послугу поставки даних. У той же час вузол такої мережі може приймати команди від будь-якого іншого вузла. Це означає, що всі Інтернет-речі можуть взаємодіяти одна з одною і вирішувати спільні обчислювальні завдання. Інтернет-речі можуть утворювати локальні мережі, об'єднанні певною зоною обслуговування або функцією.

Проблемою при використанні IoT технологій, особливо на підприємствах, є поєднання енергозбереження для продовження тривалого їх функціонування та кібербезпеки, як складових параметрів, що гарантуватимуть їх ефективне використання.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Розглянемо сучасний стан проблеми. ZigBee [1] створений для застосувань, які потребують гарантованої доставки даних при низьких швидкостях передавання (до 250 кбіт/с) та мінімального споживання енергії. Робочий радіус у відкритому просторі може досягати 75 метрів. Основною особливістю ZigBee є підтримка гнучкої топології мережі — зокрема, типів «зірка», «дерево» та «сітка» з можливістю самоорганізації і маршрутизації даних. Пристрої ZigBee можуть більшість часу перебувати в режимі сну, що значно подовжує час автономної роботи. Залежно від функціонального призначення пристрої поділяються на координатори (PAN-координатори), маршрутизатори та кінцеві пристрої (термінали). Координатор ініціює і підтримує структуру мережі, збирає дані та здійснює зв'язок із зовнішніми системами, маршрутизатори передають інформацію далі мережею, а кінцеві пристрої здебільшого виконують функції збору даних. Іншим бездротовим протоколом, орієнтованим на автоматизацію побутових систем, є Z-Wave [2]. Ця технологія, побудована на стандарті ITU G.9959, застосовується у «розумних будинках» для керування освітленням, опаленням, доступом тощо. Вона використовує малопотужні мініатюрні радіомодулі в частотному діапазоні до 1 ГГц, що забезпечує високу стійкість до перешкод, на відміну від перевантаженого діапазону 2,4 ГГц. Z-Wave підтримує топологію сітки з маршрутизацією сигналів через проміжні вузли, що дозволяє покращити покриття. Стандарт визначає три типи вузлів: контролери, маршрутизуючі виконавчі пристрої і звичайні виконавчі пристрої. Максимальна кількість пристроїв у мережі — до 232. Попри простоту та енергоефективність, Z-Wave має обмежену швидкість передавання даних (до 40 кбіт/с), що унеможливлює трансляцію мультимедійних потоків [3].

Шифрування даних [4] — це метод захисту даних шляхом їх кодування таким чином, що їх може розшифрувати або отримати доступ до них тільки особа, яка має правильний ключ шифрування. Коли фізична чи юридична особа отримує доступ до зашифрованих даних без дозволу, вони виглядають зашифрованими або нечитаними. Шифрування даних — це процес перетворення даних з формату, що читається, в зашифрований фрагмент інформації. Це зроблено для того, щоб сторонні не могли прочитати конфіденційні дані у дорозі. Шифрування може застосовуватися до документів, файлів, повідомлень або будь-якої іншої форми мережі. Щоб зберегти цілісність даних, шифрування є життєво важливим інструментом, значення якого неможливо переоцінити. Майже все, що є в Інтернеті, пройшло через певний рівень шифрування. Ручне шифрування використовувалося з римських часів, але цей термін став асоціюватися з маскуванням інформації за допомогою електронних комп'ютерів. Шифрування є базовим процесом криптології. Комп'ютери шифрують дані шляхом застосування алгоритму, тобто набору процедур або інструкцій для виконання певного завдання, до блоку даних. Персональний ключ шифрування або ім'я, відоме лише передавачу повідомлення та його одержувачу, використовується для керування шифруванням даних алгоритмом, таким чином створюючи унікальний зашифрований текст, який можна розшифрувати лише за допомогою ключа. Ключі важливі як формально, так і на практиці, оскільки шифри без змінних ключів можуть бути просто зламані, лише знаючи використовуваний шифр, і тому марні для більшості цілей [5].

Історично склалося так, що шифри часто використовувалися безпосередньо для шифрування або дешифрування без додаткових процедур, таких як автентифікація або перевірка цілісності [6]. Шифрування використовується для аутентифікації джерела інформації та запобігання відмови відправника інформації від того факту, що дані були надіслані саме їм. Для того, щоб прочитати зашифровану інформацію, стороні, що приймає, необхідні ключ і дешифратор (пристрій, що реалізує алгоритм розшифровування). Ідея шифрування полягає в тому, що зловмисник, перехопивши зашифровані дані і не маючи до них ключа, не може ні прочитати, ні змінити інформацію, що передається. Крім того, у сучасних криптосистемах (з відкритим

ключем) для шифрування та розшифрування даних можуть використовуватись різні ключі. Однак з розвитком криптоаналізу з'явилися методики, що дозволяють дешифрувати закритий текст без ключа. Вони ґрунтуються на математичному аналізі переданих даних. Є декілька сучасних алгоритмів шифрування [7], такі як RSA, AES, ECC, які забезпечують шифрування та цілісність даних.

Хакери постійно розробляють складніші методи для порушення безпеки і заподіяння шкоди бізнесу або його клієнтам. Відповідальні власники бізнесу знають, що потрібно захищати свою присутність в Інтернеті за допомогою SSL сертифікатів [8], наданих довіреною сторонньою сертифікацією. Використання SSL-сертифіката дозволяє автентифікувати веб-сервер та передавати конфіденційну інформацію. Алгоритм RSA залишається ефективним варіантом шифрування. Тим не менш, довжина ключів продовжуватиме зростати експоненційно. Інтернет-спільноти відзначили здатність хакерів використовувати потужні комп'ютери для потенційного злому ключів, що наближаються до 1024 біт. Тому NIST рекомендував, щоб до кінця 2013 року сертифікаційні центри не видавали жодних нових сертифікатів SSL/TLS з розмірами відкритого ключа RSA розміром менше 2048 біт. У той же час альтернативні алгоритми шифрування та підписання були прийняті федеральним урядом, який випустив керівні принципи, що базуються на криптографії з еліптичною кривою (ECC) та алгоритмах цифрового підпису (DSA).

Алгоритм шифрування це математична процедура або набір кроків для кодування даних.

1. Впровадження багатофакторної автентифікації для підвищення захисту облікових записів користувачів IoT систем [9]. Рекомендовано використовувати апаратні токени або спеціалізоване програмне забезпечення для управління доступом. Двофакторна автентифікація посилює стандартну схему авторизації, додаючи одноразовий код підтвердження, що надсилатиметься на мобільний телефон або електронну пошту споживача.. Такий код має обмежений термін дії, який запобіігає його повторному використанню. Деякі сучасні системи підтримують ручне введення коду або підтвердження через мобільні застосунки.

2. Мережевий моніторинг і виявлення аномальної активності [10]. Оскільки більшість IoT пристроїв функціонує через бездротові мережі або маршрутизатори, то ефективним інструментом для виявлення потенційних загроз є постійний аналіз мережного трафіку, системи моніторингу дозволяють ідентифікувати нетипову активність, до прикладу, часті запити або спроби несанкціонованого підключення, це допомагає вчасно реагувати на загрози безпеці [9].

3. Резервне копіювання та відновлення даних [11]. Регулярне створення резервних копій критичних систем і даних, є важливим елементом стратегії кіберзахисту. Це дозволяє швидко відновити втрачену інформацію у випадку технічних збоїв, атак програм-вимагачів або пошкодження пристроїв. Рекомендують періодично перевіряти цілісність резервних копій, що б переконатись в можливості повного відновлення функціональності систем.

4. Унікальні IP-ідентифікатори та безпечна адресація. У кожному IoT пристрої або групі пристроїв, є унікальна IP-адреса, що спрощує контроль та управління мережею, і також це дозволяє відслідковувати активність пристроїв та налаштовувати індивідуальні правила доступу [12].

5. Використання технологій міжмашинної комунікації. Розвиток IoT став можливим завдяки технологіям M2M, які забезпечують автономну взаємодію пристроїв без участі людини. Ця концепція є базою для створення інтелектуальних систем, де інформація обмінюється в реальному часі між вузлами систем [13].

6. Хмарні та блокчейн платформи. Системи на IoT пристроях активно інтегруються з хмарними технологіями, це забезпечує масштабоване зберігання та обробку великих за обсягом даних. Одночасно впровадження блокчейн рішень відкриває нові можливості для захисту даних завдяки децентралізованій природі таких технологій [14].

7. Орієнтація на фізичне середовище. IoT пристрої безпосередньо взаємодіють з реальним світом, реагуючи на фізичні зміни, такі як рух, температура та тиск. Один лише датчик може генерувати великі обсяги інформації, які потребують ефективної обробки. Наприклад, акустичні сенсори, які використовуються для моніторингу обладнання та створюють великі обсяги даних, що мають бути швидко проаналізовані [15].

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Інтернет речей (IoT) відіграє все більшу роль у цифровій трансформації підприємств, дозволяючи автоматизувати виробничі процеси, знижувати витрати та підвищувати ефективність [16]. Проте впровадження IoT супроводжується низкою серйозних викликів, зокрема в контексті кібербезпеки та енергозабезпечення. Із зростанням кількості підключених пристроїв збільшується вразливість до кібератак, адже багато IoT-рішень мають слабкий захист, використовують стандартні паролі або не передбачають регулярне оновлення програмного забезпечення. Пристрої часто інтегруються в єдину мережу з критичною інфраструктурою, що створює додаткові ризики. Також? викликає занепокоєння безпечність зберігання та передавання чутливих виробничих даних. Водночас стрімке зростання кількості IoT-пристроїв призводить до підвищеного навантаження на системи енергоживлення підприємства. Навіть якщо кожен пристрій споживає небагато, у сукупності вони можуть спричинити серйозні витрати та викликати нестабільність у роботі локальних енергомереж. Особливо це актуально для великих виробничих об’єктів або віддалених регіонів з обмеженими ресурсами. Тому підприємствам необхідно інтегрувати IoT у загальну стратегію кібербезпеки,

запроваджувати шифрування, багатофакторну автентифікацію, енергоменеджмент, а також використовувати локальні джерела живлення та аналітику для прогнозування навантажень. Лише комплексний підхід дозволить повністю розкрити потенціал IoT без шкоди для безпеки та енергостабільності.

Метод комплексної оптимізації енергозбереження та безпеки для технологій Інтернету речей (IoT) передбачає інтегровану стратегію управління енергоспоживанням та кібербезпекою в рамках єдиної цифрової екосистеми підприємства. Цей підхід базується на поєднанні сучасних технологій, таких як хмарні обчислення, штучний інтелект, блокчейн та стандартизовані протоколи безпеки, з метою забезпечення ефективної та безпечної роботи IoT-пристроїв.

На початковому етапі впроваджується детальний аудит усіх IoT-пристроїв, що включає аналіз їх енергоспоживання, функціональних можливостей та рівня захисту. Це дозволяє виявити енергетично неефективні компоненти та потенційно вразливі точки доступу, що можуть бути використані для кібератак. Далі здійснюється класифікація пристроїв за критичністю їх функцій та рівнем ризику, що дозволяє застосувати диференційовані політики управління, включаючи шифрування трафіку, багатофакторну автентифікацію та управління енергоспоживанням.

Центральним елементом методу є впровадження системи динамічного енергоменеджменту, яка в режимі реального часу аналізує активність пристроїв, змінює режими їх роботи на основі алгоритмів машинного навчання та розподіляє навантаження, знижуючи пікове споживання. Це дозволяє не лише зменшити енергоспоживання, але й підвищити стабільність роботи системи. Одночасно з цим застосовуються протоколи безпечного обміну даними та автоматичні засоби виявлення аномалій, що дозволяє знизити ризики втручання без значного навантаження на системи.

Інтеграція резервного живлення, наприклад, з використанням локальних джерел, зокрема сонячних панелей чи акумуляторів, додає стійкість до зовнішніх загроз і перебоїв енергопостачання. Крім того, використання хмарних технологій дозволяє забезпечити масштабованість та гнучкість системи, а також спростити управління та моніторинг пристроїв. Блокчейн-технології можуть бути використані для забезпечення прозорості та незмінності даних, що передаються між пристроями, що особливо важливо в умовах підвищених вимог до безпеки та відповідності нормативним вимогам.

Таким чином, метод комплексної оптимізації енергозбереження та безпеки для технологій IoT забезпечує ефективне управління енергоспоживанням та високий рівень кібербезпеки, що є критично важливими факторами для успішного впровадження та експлуатації IoT-рішень на підприємствах. Цей підхід дозволяє не лише знизити витрати та підвищити ефективність, але й забезпечити відповідність сучасним вимогам до безпеки та сталого розвитку.

Розглянемо параметри, які потребують розроблення для забезпечення ефективності.

За допомогою Node-Red була створена підсистема з такими параметрами:

1. Зміна рівня заряду батареї залежно від обраного режиму;
2. Пікові навантаження на систему при виявленні загроз;
3. Час активації захисних механізмів;
4. Порівняння частоти передачі даних в обох системах.

Першим етапом є аналіз вимог і середовища, метою якого є обмеження та вимоги до системи перед її проєктуванням. Основними діями будуть визначення цільових сценаріїв. Це задачі, які має виконувати система, зокрема моніторинг, контроль, передача даних. Наступним буде оцінка критичності даних, визначення рівня конфіденційності та потреби у захисті. Останнім буде аналіз ресурсних обмежень, обмежена потужність акумуляторів, низька обчислювальна здатність, інтервали зв’язку.

Другим етапом буде моделювання системи, метою якої є створення математичної або симуляційної моделі для прогнозування та оцінки ефективності, основними діями якого є створення моделі енергоспоживання, враховуючи режими активності пристроїв, передачі даних та обробки інформації, створення моделі загроз, яка буде визначати потенційні вектори атак, до прикладу, атаки через бездротові інтерфейси, створення топології мережі, таких як, дерево, зірка, mesh, все залежить від потреб користувача.

Третім етапом виступає оптимізація енергоспоживання, метою якого є зменшення споживання енергії без шкоди для функціональності. Основними методами є розгляд режимів енергозбереження використання режимів сну, глибокого сну та пробудження з подією, створення енергоефективних протоколів, таких як, BLE, ZigBee, LoRa. Вони обираються залежно від відстані та обсягу передачі даних. Далі створення адаптивної частоти передачі даних і йде зменшення частоти передачі даних, якщо зміни у даних незначні. І останнім є створення мережевих алгоритмів системи, які оптимізує маршрути з урахуванням енергетичних ресурсів вузлів.

Четвертим етапом є забезпечення безпеки, метою якого є захист пристроїв від атак на всіх рівнях. Основними заходами є аутентифікація пристроїв, яка запобігає підключенню неавторизованих вузлів, створення легких криптографічних алгоритмів, AES-CMM, ECC, спеціально для пристроїв з обмеженими ресурсами, створення безпечного оновлення програмного забезпечення. Це дозволить уникнути впровадження шкідливого коду в систему, і останнім є створення захисту від фізичного втручання в систему, що використовує захищені мікроконтролери.

П’ятим етапом є інтегрована оптимізація, метою якої є досягнення компромісу між енергоспоживанням та безпекою, методами якого є багатокритеріальна оптимізація, алгоритми якої можуть одночасно враховувати кілька критеріїв, до прикладу NSGA-II, допомога штучного інтелекту, де застосовується машинне навчання для адаптації поведінки пристрою до умов навколишнього середовища. І останнім є динамічна політика, зміна режимів якого залежить від ризику, наприклад, при виявленні загрози активується доодаткове шифрування.

Шостим етапом є тестування та валідація, метою якого є переконання в працездатності системи, яка повинна працювати безпечно та енергоефективно, діями якої також є симуляція та емулювання, до прикладу, використання Cooja або NS-3, тестування на витривалість, яка включає в себе перевірку пристроїв при довготривалому навантаженні, і останні є аудит безпеки, коли йде перевірка на відомі вразливості такі як OWASP IoT Top 10.

Останнім, сьомим етапом є розгортання та моніторинг, метою якого є вирішення в реальному середовищі з постійним контролем. Основними завданнями є моніторинг енергоспоживання, виявлення вузлів, що швидко розряджаються, далі виявлення аномалій, який подає сигнали про потенційні атаки чи збої. Останнім є оновлення системи, в якій йде безпечне оновлення прошивки та конфігурацій.

Ці етапи дозволяють створити стійкі, ефективні IoT-рішення для різних сфер, починаючи від системи «Розумний дім». Проведемо аналіз енергоспоживання, паралельно розраховуючи середнє значення енергоспоживання за останній період активності. Це значення враховує час у активному та пасивному режимах. Для включення енергоспоживання до загальної моделі прийняття рішень проводимо нормалізацію даних.

Кожне рішення, яке приймає система, фіксується в лог файлі, потім ця інформація надсилається через MQTT-брокер до Node-RED, де формується інтерактивна оглядова панель: графіки заряду акумулятора, індикатор ризику, активний режим. Це дозволяє формувати повну історію дій системи, яка може бути використана для навчання алгоритму та корекції коефіцієнтів у моделі.

Усі результати роботи пристрою фіксуються у форматі JSON і передаються на віддалений сервер. Також впроваджено систему журналювання подій для реєстрації кожного прийнятого рішення та зміни стану пристрою. Метод адаптивної енергетичної та безпекової оптимізації, реалізований на базі контролера ESP32, запроваджувався поетапно з урахуванням взаємодії програмного забезпечення і апаратних елементів, які забезпечують адаптивне управління залежно від поточних умов.

Перший крок — це детальний моніторинг ключових характеристик функціонування пристрою. Для цього здійснюється зчитування рівня заряду акумулятора через вбудований аналогово-цифровий перетворювач (АЦП), що забезпечує точне вимірювання напруги. Отримані значення нормалізуються до інтервалу. Паралельно відстежується мережева активність, зокрема, кількість відправлених і прийнятих пакетів, затримка з’єднання (ping), а також спроби повторного підключення до мережі. Окремо виконується аналіз середовища за допомогою сенсорів температури, освітлення або вологості, що дозволяє ідентифікувати контекст (наприклад, день чи ніч), і відповідно адаптувати поведінку системи. Основними параметрами для оцінки є кількість запитів за останню хвилину, незвичні IP-адреси, а також розбіжності з історичними шаблонами поведінки пристрою. У результаті формується ризиковий індекс R (від 0 до 1), де 1 відповідає найвищому рівню загрози.

ЕКСПЕРИМЕНТ

Для перевірки ефективності запропонованого методу комплексної адаптивної оптимізації енергозбереження та безпеки в системах Інтернету речей (IoT) було проведено експеримент тривалістю 108 годин у реальному офісному середовищі з використанням двох однотипних мікроконтролерів ESP32 (табл. 1). Один з пристроїв був налаштований на функціонування в умовах класичного фіксованого режиму, при якому дані передавались строго з інтервалом у 60 секунд незалежно від змін у навколишньому середовищі. Другий пристрій працював на основі адаптивного алгоритму, що реалізовував динамічне керування інтервалами передачі даних та режимами енергоспоживання залежно від рівня активності мережі, загроз або зміни навколишніх умов. Обидва пристрої живились від однакових акумуляторних батарей ємністю 3000 мА·г, а з’єднання здійснювалося через Wi-Fi мережу з передачею даних по протоколу MQTT. Під час експерименту проводилось моделювання різних типів мережевих загроз, зокрема сканування портів, підміна IP-адрес, flood-атаки, створення підозрілої активності, що могло вплинути на стабільність або безпеку IoT-платформи.

Окрему увагу було приділено спостереженню за реакцією пристроїв у ситуаціях підвищеної загрози. Пристрій з фіксованим режимом не демонстрував жодної зміни поведінки, продовжуючи працювати у встановленому циклі, що у випадку реального використання означає відсутність гнучкості та підвищене споживання енергії навіть у спокійні періоди. У той же час пристрій з адаптивним керуванням не лише зменшував частоту обміну даними під час нормальної роботи, а й переходив у режим підвищеної чутливості у відповідь на виявлення аномальної активності. Для фіксації та візуалізації результатів була побудована інтерактивна оглядова панель на базі Node-RED, що містила серію графіків: рівень заряду батареї обох

пристроїв у динаміці, навантаження на систему під час виявлення потенційних атак, час реакції на загрозу, а також частоту передачі повідомлень у двох режимах роботи. За результатами аналізу було виявлено, що адаптивний пристрій забезпечив значно довший час автономної роботи (приблизно на 27% більше), більш точну реакцію на загрози з меншим навантаженням на мережу, а також демонстрував стабільні показники в умовах підвищеної небезпеки без втрати функціональності.

Ключовим досягненням розробленого методу є здатність гнучко балансувати між безпекою, ефективністю обробки подій і енергоспоживанням без залучення потужних обчислювальних ресурсів, що критично важливо для IoT-пристроїв з обмеженими можливостями. Крім того, до системи було інтегровано базові стандарти безпеки, включаючи шифрування даних, автентифікацію через TLS, обмеження доступу до MQTT-брокера, а також попередньо розроблений механізм фільтрації аномальної активності. Для подальшого вдосконалення системи передбачено можливість впровадження блокчейн-механізмів зберігання логів, використання криптографічних протоколів ACE (Authentication and Authorization for Constrained Environments), інтеграцію апаратних модулів довіреного середовища TPM (Trusted Platform Module), що дозволяє реалізувати не лише динамічне, а й структурно захищене IoT-середовище. Загалом експеримент підтвердив ефективність запропонованого методу як життєздатної моделі для впровадження в промислові, офісні та інші критичні середовища, де ресурси обмежені, а вимоги до надійності систем високі.

Таблиця 1

Ефективність гібридного підходу

Показник	Стандартний режим	З алгоритмом оптимізації	Покращення в %
t-автономної роботи	38	34	+45%
Середнє споживання струму	81.6	68	-33.5%
Час реакції на загрозу, сек	5.4	2.1	-61%
Кількість успішних атак	3	1	-100%
Кількість переданих повідомлень	4320	2850	-34%
Завантаження процесора при навантаженнях,%	43	31	-25%

Результати проведеного 108-годинного експерименту підтверджують ефективність методу комплексної адаптивної оптимізації енергозбереження та безпеки для IoT-платформ. Адаптивний алгоритм, реалізований на пристрої ESP32, продемонстрував значні переваги над традиційним фіксованим режимом роботи: зниження енергоспоживання, продовження часу автономної роботи, зменшення навантаження на мережу, а також підвищену здатність до виявлення та обробки загроз у режимі реального часу. Застосування гнучкого підходу до частоти передачі даних та переходу між режимами енергоспоживання дозволяє більш ефективно керувати обмеженими ресурсами пристроїв без втрати функціональності.

Інтеграція стандартів безпеки IoT, зокрема шифрування, автентифікації, а також потенційне використання технологій блокчейн, ACE та TPM, відкриває нові горизонти для підвищення довіри до розумних пристроїв у критичних середовищах. Побудована на базі Node-RED аналітична панель підтвердила, що адаптивна система здатна забезпечити не лише стабільність, а й прозору оцінку ефективності в умовах динамічного ризику.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У результаті проведеного дослідження розроблено, реалізовано та експериментально апробовано метод комплексної оптимізації енергоспоживання та кібербезпеки для систем Інтернету речей (IoT). Основною метою було створення ефективного алгоритмічного підходу, який дозволяє зменшити енергоспоживання IoT-пристроїв без втрати функціональності та із забезпеченням високого рівня захисту даних. Під час дослідження здійснено аналіз сучасного стану IoT-систем, виокремлено основні виклики, пов’язані з енергетичними обмеженнями та вразливістю до кіберзагроз, класифіковано методи енергозбереження та проаналізовано актуальні протоколи безпеки (IPSec, TLS, AES, RSA, ECC), адаптовані до IoT-середовища.

На основі отриманих даних було запропоновано алгоритм адаптивного управління енергоспоживанням на базі мікроконтролера ESP32 з урахуванням рівня критичності даних, поточного заряду акумулятора та оцінки ризиків. Розроблено фізичний прототип IoT-пристрою з використанням сенсора DHT22, протоколу MQTT і TLS-захисту, що дозволило провести натурне тестування алгоритму в умовах реального офісного середовища. Результати експериментальних випробувань продемонстрували зменшення енергоспоживання на понад 40% у порівнянні з традиційною моделлю, зберігаючи при цьому високу точність передачі та стабільність роботи системи. Отримані результати засвідчують ефективність та доцільність впровадження запропонованого методу в побутових і промислових IoT-системах, де важливими є автономність, стабільність та захищеність переданих даних.

Література

1. Rezaei, M. DeepSOCIAL: Social Distancing Monitoring and Infection Risk Assessment in COVID-19 Pandemic. Applied Sciences, 2020, Vol. 10, No. 21, p. 144.
2. Shorten, C., Khoshgoftaar, T. M., Furht, B. Deep Learning Applications for COVID-19. Journal of Big Data, 2021, Vol. 8, Article 18, p. 145.
3. Sivakumar, S. A. T. J., John, G. T., Selvi, B., Madhu, C. U., Shankar, K. P., Arjun. IoT-based Intelligent Attendance Monitoring with Face Recognition Scheme. In: 5th International Conference on Computing
4. Belongie, S., Wilber, M., Viet, A. Residual Networks Behave Like Ensembles of Relatively Shallow Networks, 2016, pp. 107–113.
5. Benchmark Analysis of Representative Deep Neural Network Architectures. URL: https://arxiv.org/pdf/1810.00736.pdf (Accessed: 15.04.2021).
6. Hartley, R., Zisserman, A. Multiple View Geometry in Computer Vision. Cambridge University Press, 2003, p. 674.
7. Solem, E. Programming Computer Vision with Python: Tools and Algorithms for Analyzing Images. O'Reilly Media, 2012, p. 408.
8. Murphy, K. P. Machine Learning: A Probabilistic Perspective. MIT Press, 2012, p. 1067.
9. Géron, A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly Media, 2019, p. 745.
10. Ciobanu, G., Rudeanu, S. Final and Sequential Behaviours of M-Automata. Acta Informatica, 2009, Vol. 46, pp. 361–374.
11. Face Recognition. URL: https://viso.ai/application/face-recognition/ (Accessed: 22.04.2023).
12. Facial Emotion Analysis, 2021. URL: https://viso.ai/application/emotion-analysis/ (Accessed: 22.04.2023).
13. Gibson, J. J. The Perception of the Visual World. Boston: Houghton Mifflin, 2020.
14. Google Ngram Viewer, Stanford University, 2021. URL: https://books.google.com/ngrams/graph?content=computer+vision%2C+machine+vision.
15. Grape, G. R. Model Based (Intermediate-Level) Computer Vision: PhD Dissertation / Gunnar Rutger Grape, 2010. URL: https://apps.dtic.mil/sti/pdfs/AD0763673.pdf
16. Intrusion Detection. URL: https://viso.ai/application/intrusion-detection/

References

1. Rezaei, M. DeepSOCIAL: Social Distancing Monitoring and Infection Risk Assessment in COVID-19 Pandemic. Applied Sciences, 2020, Vol. 10, No. 21, p. 144.
2. Shorten, C., Khoshgoftaar, T. M., Furht, B. Deep Learning Applications for COVID-19. Journal of Big Data, 2021, Vol. 8, Article 18, p. 145.
3. Sivakumar, S. A. T. J., John, G. T., Selvi, B., Madhu, C. U., Shankar, K. P., Arjun. IoT-based Intelligent Attendance Monitoring with Face Recognition Scheme. In: 5th International Conference on Computing
4. Belongie, S., Wilber, M., Viet, A. Residual Networks Behave Like Ensembles of Relatively Shallow Networks, 2016, pp. 107–113.
5. Benchmark Analysis of Representative Deep Neural Network Architectures. URL: https://arxiv.org/pdf/1810.00736.pdf (Accessed: 15.04.2021).
6. Hartley, R., Zisserman, A. Multiple View Geometry in Computer Vision. Cambridge University Press, 2003, p. 674.
7. Solem, E. Programming Computer Vision with Python: Tools and Algorithms for Analyzing Images. O'Reilly Media, 2012, p. 408.
8. Murphy, K. P. Machine Learning: A Probabilistic Perspective. MIT Press, 2012, p. 1067.
9. Géron, A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly Media, 2019, p. 745.
10. Ciobanu, G., Rudeanu, S. Final and Sequential Behaviours of M-Automata. Acta Informatica, 2009, Vol. 46, pp. 361–374.
11. Face Recognition. URL: https://viso.ai/application/face-recognition/ (Accessed: 22.04.2023).
12. Facial Emotion Analysis, 2021. URL: https://viso.ai/application/emotion-analysis/ (Accessed: 22.04.2023).
13. Gibson, J. J. The Perception of the Visual World. Boston: Houghton Mifflin, 2020.
14. Google Ngram Viewer, Stanford University, 2021.
15. Grape, G. R. Model Based (Intermediate-Level) Computer Vision: PhD Dissertation / Gunnar Rutger Grape, 2010. URL: https://apps.dtic.mil/sti/pdfs/AD0763673.pdf
16. Intrusion Detection. URL: https://viso.ai/application/intrusion-detection/