Попович Андрій Олегович, студент магістратури

Науковий керівник – к. т. н., доцент. Яковлєва І.Д..

Чернівецький Національний університет, Чернівці

0009-0000-7275-087X

**Актуальність розробки IoT-системи для моніторингу та управління безпекою на основі Arduino**

Сьогодні у світі зростає популярність IoT систем для моніторингу безпеки екологічно чистих, ефективних та легко інтегрованих з різними пристроями та платформами, які дозволяють віддалено керувати та моніторити стан об’єктів у реальному часі. Понад 50% виробників у різних країнах світу віддають перевагу використанню IoT для систем безпеки. Для обробки даних використовуються різні технології: датчики руху, диму, температури та інші IoT пристрої. Дослідження від компанії MarketsandMarkets показують, що ринок IoT пристроїв для безпеки зростатиме з 11,42 млрд доларів до 42,11 млрд доларів до 2026 року, що становить приріст у 13,9% річно. Як зазначається у дослідженні [1] великою перевагою технологій на базі В контексті стрімкого розвитку технологій Інтернету речей (IoT) та зростаючої потреби в забезпеченні безпеки, створення інтегрованої системи моніторингу на базі IoT є актуальним завданням. Ця система повинна ефективно виявляти, обробляти та реагувати на різноманітні загрози у реальному часі. Розробка системи, що включає в себе інноваційні IoT компоненти, як Arduino та ESP для управління даними з датчиків газу, вологості, температури тощо, дозволяє не тільки оптимізувати процес моніторингу за допомогою автоматизованого збору та аналізу даних, а й підвищити ефективність реагування на екстрені ситуації. Таким чином, актуальність розробки інтегрованої IoT системи моніторингу безпеки є безсумнівною, враховуючи потребу в підвищенні рівня безпеки житлових та промислових об'єктів в умовах зростаючих загроз та необхідності їх оперативного усунення. Після розробки та успішного тестування системи, наступним кроком є її впровадження та промоція. Це включає демонстрацію функціональності системи потенційним користувачам, організацію тренінгів для операторів та адміністраторів, а також розробку маркетингових матеріалів, щоб підкреслити переваги та унікальні можливості системи. Моніторинг та підтримка: Завершальним етапом є постійний моніторинг роботи системи та надання технічної підтримки користувачам. Це гарантує стабільність роботи системи та своєчасне виявлення та усунення будь-яких проблем або вразливостей. Також цей етап передбачає регулярні оновлення програмного забезпечення та апаратної частини для підтримання високого рівня безпеки та адаптації до змін у технологічному середовищі. Постійний розвиток та оптимізація: Для забезпечення довгострокової ефективності, система повинна регулярно оновлюватися та оптимізуватися на основі зворотного зв'язку від користувачів та аналізу роботи. Оновлення можуть включати покращення алгоритмів обробки даних, вдосконалення інтерфейсу користувача, а також розширення функціональності системи з введенням нових датчиків та інтеграцією додаткових сервісів. Завдяки цим заходам, система IoT для моніторингу безпеки стане не лише технологічним рішенням, а й надійним інструментом для забезпечення безпеки, який можна адаптувати до різних умов та потреб користувачів, забезпечуючи при цьому високий рівень захисту та оперативного реагування на загрози.

**Розробка архітектури системи**: Створити структурну схему системи, що включатиме основні модулі: збір даних, обробку даних, реагування на події та користувацький інтерфейс. Інтеграція апаратного забезпечення: Вибір та налаштування мікроконтролерів та датчиків (датчик газу, датчик вологості, датчик температури Arduino Nano), а також засобів для комунікації (модуль ESP для WiFi). Розробка програмного забезпечення: Як зазначається у дослідженні [2] написання програмного коду є обовязковим для зчитування даних з датчиків, обробки отриманих даних, управління актуаторами та комунікації з користувачем через мобільний додаток або веб-інтерфейс. Тестування та налагодження системи: Верифікація коректності роботи всіх модулів системи, аналіз даних для оптимізації реакції системи на потенційні загрози. Забезпечення безпеки системи: Реалізація заходів кібербезпеки для захисту системи від зовнішніх та внутрішніх загроз. Завершення цих задач дозволить створити надійну та ефективну систему моніторингу безпеки, яка зможе адаптуватися до різних оперативних умов і забезпечити високий рівень захисту обраного об'єкта. Запровадження та масштабування системи: Після завершення первинного тестування та оптимізації системи, наступним етапом є її запровадження в реальні умови експлуатації. Цей процес включає встановлення обладнання на об'єктах моніторингу, налаштування зв'язку з центральною системою управління, та інтеграцію з існуючими системами безпеки та автоматизації. Для масштабування системи на більшу кількість об'єктів розробляється модульний підхід, який дозволяє легко додавати нові елементи без потреби зміни основної архітектури системи. Підтримка та оновлення: Регулярна підтримка та оновлення системи є критичними для забезпечення її стабільності та відповідності до змінних умов та загроз. Планується розробка програмних патчів, оновлення безпеки та функціональних можливостей відповідно до останніх тенденцій в області IoT та кібербезпеки. Залучення зацікавлених сторін та розширення мережі партнерів: Кінцевою метою є створення високоефективної, надійної та легко адаптованої системи моніторингу безпеки на базі IoT, яка не тільки забезпечує нагляд і контроль за безпекою на об'єктах, але й вносить вклад у розумне управління ресурсами та енергоефективність, відкриваючи нові можливості для інновацій і розвитку.

**СПИСОК ЛІТЕРАТУРИ**

1. Дослідження ринку IoT у системах безпеки: перспективи та виклики. Київ: ТОВ "Аналітика Технологій", 2022. – 192 с.
2. Ковальчук С. О., Петренко А. В. Інтеграція Інтернету речей у сучасні системи моніторингу: навчальний посібник. Одеса: ОНУ ім. І.І. Мечникова, 2023.