УДК 004.738.5: 640.4

Шевцова Д.С.[1], Бабаєва О.В.[2]

[1]студ. гр. ДГР-24мг, Харківський національний університет імені В. Н. Каразіна, м. Харків

[2]канд. геогр. наук, доцент, Харківський національний університет імені В. Н. Каразіна, м. Харків

СТРАТЕГІЇ ВПРОВАДЖЕННЯ ІНТЕРНЕТУ РЕЧЕЙ В ОРГАНІЗАЦІЮ РОБОТИ СЛУЖБИ НОМЕРНОГО ФОНДУ ГОТЕЛЮ

Сьогодні у готельному бізнесі активно впроваджуються технології інтернету речей (Internet of Things – IoT) з метою вдосконалення якості обслуговування та підвищення ефективності операцій. Це підтверджується прогнозами: ринок IoT у сфері туризму та готельного бізнесу, за даними Research and Markets, до 2027 року досягне 28 мільярдів доларів [1]. Особливо актуальними ці процеси стають для роботи служби номерного фонду готелю.

Впровадження IoT в роботу служби номерного фонду готелю має безліч переваг, які трансформують як гостьовий досвід, так і операційні процеси.

Вдосконалення гостьового досвіду – персоналізація налаштувань номерів (наприклад, автоматичне управління температурою, освітленням і завісами), безконтактна реєстрація та виїзд, пристрої на основі голосового управління.

Підвищення операційної ефективності – автоматизація процесів, таких як обслуговування та облік активів. Превентивне обслуговування інфраструктури номерного фонду запобігає поломкам і знижує витрати на ремонт.

Зниження витрат – оптимізація енергоспоживання за допомогою датчиків, які автоматично вимикають світло та опалення в приміщеннях номерів, що не використовуються.

Аналіз даних – збір даних щодо вподобань гостей та їх поведінки для вдосконалення послуг і маркетингових стратегій [2].

Незважаючи на переваги, впровадження IoT стикається з серйозними проблемами:

1. Проблеми сумісності IoT-пристроїв.

Залежність від постачальників – використання рішень від одного постачальника може обмежити гнучкість і збільшити витрати, створюючи так звану «залежність від одного постачальника (vendor lock-in).

Інтеграція систем – складнощі при інтеграції пристроїв від різних виробників можуть призвести до технічних проблем і необхідності управління декількома інтерфейсами для персоналу.

Відмінності в протоколах – відмінності між протоколами, такими як Bluetooth Low Energy (BLE) і Wi-Fi, впливають на енергоефективність і швидкість передачі даних. Наприклад, BLE споживає менше енергії, але має меншу пропускну здатність (1 Мбіт/с), тоді як Wi-Fi швидший (до 1,3 Гбіт/с), але споживає більше енергії.

2. Ризики кібербезпеки.

Вразливі пристрої – багато пристроїв IoT мають недостатньо надійну систему безпеки, що робить їх легкою мішенню для кібератак.

Витік даних – компрометація конфіденційної інформації гостей може призвести до фінансових втрат і шкоди репутації.

Загроза загальній мережі готелю – недостатньо захищені пристрої IoT можуть стати точкою входу для атак на загальну мережу готелю. Так, наприклад, дослідження показують, що 89% готелів у Великій Британії не мають достатнього захисту кінцевих точок [3].

З метою подолання перерахованих вище проблем доцільно використовувати наступні стратегії.

1. Стратегії вирішення проблем сумісності:

Індивідуальні рішення – розробка індивідуальних IoT-рішень, які можуть масштабуватися та інтегруватися з майбутніми доповненнями, уникаючи залежності від одного постачальника. Такі рішення забезпечують гнучкість і довгострокову сумісність.

Стандартизація протоколів – прийняття галузевих стандартів, таких як LoRaWAN для внутрішніх операцій і Wi-Fi для гостьових додатків, щоб забезпечити сумісність пристроїв. LoRaWAN, наприклад, забезпечує безпечну передачу даних на великі відстані.

Використання посередників – застосування проміжних платформ для інтеграції різних систем, що дозволяє створити єдиний інтерфейс для персоналу, спрощуючи управління і знижуючи технічні складнощі.

2. Стратегії вирішення проблем недостатньої кібербезпеки:

Більш надійна аутентифікація – впровадження багатофакторної аутентифікації (MFA) для доступу до пристроїв і мереж IoT, що знижує ризик несанкціонованого доступу.

Шифрування даних – забезпечення шифрування даних як у стані спокою, так і під час передачі для захисту конфіденційної інформації.

Регулярні аудити та оновлення – проведення частих аудитів безпеки та своєчасне оновлення всіх пристроїв до останніх версій прошивки для усунення вразливості до кібератак.

Навчання персоналу – проведення регулярного навчання співробітників з розпізнавання фішингових атак, безпечної обробки даних та інших практик кібербезпеки.

Плани реагування на інциденти – розробка та тестування планів реагування на кібератаки для швидкого усунення наслідків та мінімізації збитків.

Партнерство з експертами – співпраця з компаніями, що спеціалізуються на кіберзахисті, для забезпечення просунутого моніторингу загроз і швидкого реагування.

Доцільно навести приклади великих готельних мереж, які демонструють успішне впровадження IoT у роботу служби номерного фонду, поєднуючи інновації з заходами безпеки: Marriott International – створила інноваційну лабораторію для розробки та тестування IoT-технологій, зосередившись на створенні безшовного та безпечного гостьового досвіду.

IHG Hotels & Resorts – у партнерстві з Josh.ai реалізувала голосове управління номерами, підвищивши зручність для гостей при збереженні безпеки.

AccorHotels – впровадили IoT-системи для управління номерами, що збільшило операційну ефективність і задоволеність гостей.

Крім того, IoT активно використовується готелями для:

Моніторингу енергоспоживання – датчики відстежують енергоспоживання, скорочуючи витрати на електроенергію, які становлять 60-70% комунальних витрат [2].

Виявлення витоків води – вчасне виявлення протікань запобігає вартісним ремонтам і порушенням роботи.

Безпеки персоналу – пристрої для екстрених викликів з точним визначенням місцезнаходження.

Таким чином, впровадження інтернету речей в організацію роботи служби номерного фонду готелю надає значні переваги, але вимагає ретельного планування для подолання проблем сумісності та кібербезпеки. Використання індивідуальних рішень, стандартизація протоколів і реалізація заходів кібербезпеки дозволяють готелям безпечно використовувати IoT для вдосконаленнння операцій і гостьового досвіду. Приклади успішних впроваджень, таких як Marriott і IHG, демонструють, що з правильним підходом IoT може стати потужним інструментом у сфері готельного бізнесу.

Список використаних джерел:

1. Cost of a Data Breach Report 2025. IBM. URL : https://www.ibm.com/reports/data-breach (дата звернення 20.10.2025).

2. Використання IoT для автоматизації процесів у готельному бізнесі: інновації та переваги. SalesBox. URL : https://salesbox.ua/blog/vykorystannia-iot-u-hotelnomu-biznesi-yak-avtomatizatsiia-pidvyshchuie-komfort-i-znyzhuie-vytraty/ (дата звернення 20.10.2025).

3. Hospitality Industry: Sectors, Markets, and Trends. Altexsoft. URL : https://w.altexsoft.com/blog/hospitality-industry/ (дата звернення 20.10.2025).