ІНТЕГРАЦІЯ ІНТЕРНЕТУ РЕЧЕЙ ТА ДОСЛІДЖЕННЯ КІБЕРЗАГРОЗ У РОЗУМНИХ ЖИТЛОВИХ ПРОСТОРАХ. ДИЗАЙН ПЕРСОНАЛІЗОВАНОГО ДОДАТКУ ДЛЯ УПРАВЛІННЯ РОЗУМНИМ ДОМОМ SMARTHOME

Носок Н.С

ДВНЗ «Ужгородський національний університет»,
кафедра твердотільної електроніки та інформаційної безпеки,
Україна.

E-mail: nosoknikoletta@gmail.com

Abstract

The development of Internet of Things (IoT) technologies and integration into smart living spaces opens new opportunities for automation and improving the quality of life, while simultaneously creating new challenges for security. The aim of this work is to study the process of integrating IoT systems into the smart home, specifically through the development of a personalized application for managing various devices and services. The research addresses issues of automation, user interaction, as well as system optimization through the use of data from IoT devices, artificial intelligence. Special attention is given to cybersecurity, system monitoring, and the analysis of potential threats. The proposed solution allows the creation of an integrated platform for efficient smart home management, with maximum attention to user security and the stability of all systems in the context of modern technological challenges.

Інтернет речей (IoT) — це концепція, що охоплює мережу фізичних пристроїв з вбудованими сенсорами та програмним забезпеченням, яка дозволяє автоматизовану взаємодію між реальним світом та комп'ютерними системами. IoT-технології знайшли широке застосування в різних сферах, включаючи промисловість, охорону здоров'я, освіту, транспорт, логістику, розумні міста та розумні будинки. Однак, із розвитком IoT технологій, зокрема в житлових просторах, актуальним стає питання кібербезпеки, оскільки розумні будинки є вразливими до кіберзагроз.

Розглядаючи основні елементи системи розумного будинку, можна виділити три основні типи пристроїв:

1) Контролер (хаб) – це керуючий пристрій, який з'єднує всі елементи системи одним з одним і зв'язує її із зовнішнім світом.

2) Датчики або сенсори - це пристрої, які отримують інформацію про зовнішні умови.

3) Актуатори – пристрої-виконавці. Найчисленіша група в яку входять: розумні вимикачі, розетки, сирени, клімат-контролери і так далі.

Варто зазначати про різницю між розумним будинком та автоматизацією розумного будинку. Автоматизація – це методологія, яка дозволяє вашому розумному дому запускати автоматизовані служби. Вони будуть попередньо запрограмовані користувачем тому для початку у вас повинен бути розумний будинок, щоб мати можливість використовувати домашню автоматизацію. А також важливим критерієм розбіжності є те, що розумні системи потребують Інтернету, тоді як домашня автоматизація працює з електричною системою. Однак деякі розумні домашні пристрої мають певні функції домашньої автоматизації, вбудовані прямо в їхній функціонал.

Чинники, які прискорюють швидкий розвиток Інтернету речей: падіння вартості сенсорів, падіння вартості зберігання даних через хмарні рішення, поширення технологій штучного інтелекту. Штучний інтелект дозволяє нам інтегрувати розумні рішення в наші повсякденні завдання. У май-

бутньому інтеграція ШІ, ймовірно, буде доступна майже на кожному домашньому пристрої. Після взаємодії розумних пристроїв вони можуть відповідати на дистанційні команди голосу користувача або на попередньо програмовану команду.ШІ можуть бути навчені, коли активувати або деактивувати певний пристрій, наприклад обігрівач або вентилятор [1]. Останніми розробками з вбудованим ШІ є розумне дзеркало, розумний дверний дзвінок та бездротова камера безпеки. Все це збільшує ризики кіберзагроз та вразливостей. Пристрої IoT, які часто хвалять за їх можливості підключення та автоматизації, зараз знаходяться в центрі уваги кіберзлочинців. На відміну від традиційних комп'ютерних пристроїв, багатьом продуктам Інтернету речей бракує надійних функцій безпеки, що робить їх легкими мішенями. Наслідками може бути викрадення вашого розумного девайсу для запуску розподіленої атаки на відмову в обслуговуванні (DDoS) до злому вашого розумного замка для отримання фізичного доступу до вашого дому.

Однією з ключових проблем безпеки IoT є різноманітність і кількість пристроїв. Кожен пристрій, від розумного годинника до підключеного автомобіля, має свої унікальні вразливості. Ця неоднорідність робить стандартизацію протоколів безпеки складним завданням. Крім того, багато користувачів не знають про потенційні ризики, часто нехтуючи основними методами безпеки, такими як зміна паролів за умовчанням або оновлення мікропрограми. [2]

За останніми дослідженнями 56% респондентів здебільшого стурбовані використанням і захистом своїх пристроїв підключених до Інтернету речей, коли мова йде про саме такі як камери спостереження за немовлятами чи домашніми тваринами, які використовуються для шпигування за ними або їх зламують через Wi-Fi. 56% власників гаджетів розумного будинку вважають, що вони відповідальні за їх захист. Наразі 61% мають вдома будь-які девайси «Розумний дім» або «Інтернет речей», причому найпоширенішими є переносні варіанти (26%), розумні колонки (24%) або камери з підтримкою Wi-Fi (20%). Проте це не змінює людського фактора та нехтування безпекою або прийняття потрібних заходів безпеки занадто пізно [3].

Найпоширенішими атаками, що впливають на безпеку розумних будинків та IoT-систем, є фішинг і крадіжка даних, ботнети, атаки методом підбору пароля (brute-force), відмова в обслуговуванні (DoS, DDoS), атаки типу Man-in-the-Middle, а також зловмисне програмне забезпечення (malware), програмне забезпечення для вимагання викупу (ransomware) та експлуатація вразливостей у стандартних протоколах IoT. Підвищується і рівень загроз для хмарної безпеки даних, яка є важливою в контексті розумного житлового простору, адже використання локального зберігання інформації, даних користувачів вважається застарілим та рідше використовується. Зберігання даних у хмарі може бути пов'язане з юридичними ризиками, якщо дані переміщуються між різними юрисдикціями, де закони щодо конфіденційності та безпеки можуть відрізнятися. Крім того, безпека хмарних технологій вимагає застосування додаткових методів захисту, щоб зменшити ризики витоку даних або несанкціонованого доступу. Важливо також враховувати, що належна хмарна безпека потребує постійного моніторингу і застосування новітніх технологій захисту, оскільки хмарні платформи можуть бути привабливими цілями для кіберзлочинців. [5]

У зв'язку з постійним розвитком кіберзагроз для IoT-систем та хмарних технологій, необхідно впроваджувати найновіші методи захисту. Це включає дворівневу автентифікацію, шифрування даних, використання сучасних стандартів безпеки, таких як ETSI TS 103 645, а також регулярне переглядання безпекових політик і стандартів для запобігання несанкціонованому доступу та зловмисним атакам.

Одним з важливих аспектів, що дозволяє підвищити безпеку, є розробка персоналізованого додатку для управління IoT-пристроями розумного дому. Додаток Smart Home є інтегрованою платформою для управління всіма розумними пристроями в будинку, що дозволяє користувачам контролювати їх з одного інтерфейсу. Важливою особливістю цієї системи є адаптація до індивідуальних налаштувань і сценаріїв, що дає можливість максимально оптимізувати роботу пристроїв і забезпечити високий рівень комфорту.

Для захисту від кіберзагроз у додатку реалізовано багаторівневий захист, включаючи шифрування даних, багатофакторну аутентифікацію, а також постійний моніторинг через систему без-пеки Cyber Guardian (окремий сервіс), що гарантує високий рівень кіберзахисту. Завдяки інтеграції з іншими платформами, користувач може створювати єдину екосистему для управління різними пристроями, що підтримують різні технології.

Крім того, додаток інтегрує штучний інтелект для адаптації до звичок користувачів. З часом він може навчатися на поведінці користувача, автоматично налаштовуючи систему під його потреби — наприклад, автоматичне регулювання температури або освітлення в будинку в залежності від часу

доби чи наявності користувача вдома. Це дозволяє не лише забезпечити комфорт, але й знизити енергоспоживання. Створення цієї інтегрованої системи дозволяє ефективно долати виклики, що виникають під час розробки екосистеми для розумного дому, а саме проблеми з електромагнітною сумісністю мереж і безпекою даних. Застосовані рішення дозволяють створити стабільне і безпечне середовище, де користувач може з комфортом і безпекою управляти своїм будинком, а також постійно удосконалювати свою взаємодію з пристроями через персоналізовані сценарії.Хоча розробка додатку на етапі дизайну розв'язання таких проблем передбачені завчасно.

Додаток Smart Home є не просто інструментом для керування пристроями в розумному будинку, а й передовою платформою, яка враховує всі аспекти ефективності, стабільності, безпеки та персоналізації. Завдяки використанню інтелектуальних технологій, система дозволяє автоматично налаштовувати пристрої на оптимальні параметри для забезпечення стабільної роботи, навіть в умовах змінюваних середовищ чи навантажень. Це дає можливість користувачам максимально персоналізувати свої налаштування, адаптуючи будинок до своїх звичок і вподобань, при цьому гарантуючи високу ефективність роботи кожного пристрою. Безпека в той час залишається основним пріоритетом.

Звертаючись до українського досвіду в сфері розумних будинків, особливо в умовах воєнного часу, можна зазначити, що технології IoT та автоматизації стають важливими не лише в цивільному житті. Інтеграція систем моніторингу та управління дозволяє контролювати енергопостачання, забезпечуючи автоматичне включення генераторів або освітлення під час перебоїв з електрикою, що має критичне значення в умовах блекауту або частих атак на енергетичні мережі. Системи безпеки в таких будинках можуть автоматично реагувати на загрози в реальному часі, активуючи сигналізації, перевіряючи доступ до важливих зон або повідомляючи про проникнення через камери та датчики. Вони також можуть бути інтегровані в централізовані платформи для моніторингу інфраструктури, що дозволяє оперативно реагувати на загрози та знижувати ризики.

Завдяки аналізу даних з IoT-пристроїв можна виявляти порушення, пов'язані з воєнними злочинами, що може бути використано для подальших розслідувань та забезпечення відповідальності, як цифрові докази. В умовах війни, де кожна помилка або втрата даних може мати катастрофічні наслідки, цифрова криміналістика забезпечує важливі інструменти для моніторингу та оперативного реагування на загрози, що виникають у результаті агресії або внутрішніх загроз.

Таким чином додаток Smart Home створює нову еру в управлінні розумним будинком, де кожен аспект — від комфорту до захисту — стає інтегрованим і бездоганно адаптованим до потреб користувача, гарантуючи безперервний розвиток та надійність в умовах постійно змінюваного технологічного середовища.

Інтернет речей і розумні будинки є невід'ємною частиною технологічного прогресу, що забепечує автоматизацію та підвищує комфорт користувачів. Однак розвиток IoT також створює нові виклики в сфері безпеки, оскільки пристрої часто мають обмежені можливості для захисту, що робить їх вразливими до кіберзагроз.

Надійні механізми безпеки, є критично важливими для захисту систем IoT. Персоналізовані додатки для управління пристроями розумного будинку можуть забезпечити ефективну інтеграцію цих технологій і дозволяють не лише підвищити рівень комфорту, але й гарантувати високий рівень надійності. Перспективи розвитку включають вдосконалення протоколів безпеки, підвищення обізнаності користувачів щодо потенційних загроз, а також удосконалення технологій захисту хмарних даних, що є критично важливою частиною екосистеми розумного дому.

*Л*ітература

1. Goyal, V., & Kumar, A. (2023). *Artificial Intelligence for IoT*. Springer Nature.
2. Cisco. (n.d.). *Звіт Cisko з кібербезпеки*. Retrieved from https://www.cisco.com/c/uk_ua/products/security/securityreports.html#~download-th
3. Kaspersky. (2023). *IoT Survey Report 2023*. Retrieved from https://www.kaspersky.com/blog/iot-survey-report-2023/
4. Piasecki, S., Urquhart, L., & McAuley, D. (2021). *Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards*. *ScienceDirect*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364921000157
5. Bertino, E., Sandhu, R., & Paci, F. (2020). Security and Privacy Issues in Smart Homes: An Overview. Springer.