Секція 2

ФУНКЦІОНАЛЬНА БЕЗПЕКА РОЗУМНИХ БУДИНКІВ

Кіріченко Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

Актуальність. Розвиток Інтернету речей (IoT) та штучного інтелекту зробив розумні будинки звичним явищем, що забезпечує комфорт, ефективність та автоматизацію [1, 2]. Проте інтеграція інтелектуальних систем підвищує ризик збоїв і зловмисного втручання, що може призвести до матеріальних збитків і порушення конфіденційності. Тому функціональна безпека розумного будинку є ключовою для захисту користувачів і стабільної роботи систем [2, 3].

Метою роботи є аналіз основних загроз для функціональної безпеки та розробка рекомендацій для підвищення надійності та захисту функцій автоматизованих систем.

Основні положення. Розумний будинок – це комплекс систем і пристроїв, об'єднаних в єдину мережу для забезпечення автоматизації, зручності та енергоефективності. Основними компонентами є системи управління освітленням, клімат-контролю, системи безпеки, медіасистеми та побутова техніка. Всі елементи взаємодіють між собою за допомогою дротових або бездротових каналів зв'язку та центрального контролера [3, 4]. В роботі розглянуто основні загрози функціональної безпеки [4, 5]. Кібератаки: злом мереж через вразливості Wi-Fi і Bluetooth, перехоплення даних через незашифровані канали, та використання пристроїв зі слабкими паролями у DDoS-атаках. Програмні вразливості: недостатні оновлення прошивки і незахищені API створюють ризики несанкціонованого доступу. Фізичні загрози: відключення живлення без резерву та зношеність обладнання можуть порушити роботу систем безпеки. Стандартні паролі: прості паролі полегшують доступ зловмисникам. Соціальна інженерія: використання фішингу для отримання доступу від недосвідчених користувачів. В роботі також розглянуто засоби підвищення функціональної безпеки: сегментація мережі для ізоляції критично важливих систем від загальнодоступного інтернету; системи виявлення вторгнень для моніторингу аномальних дій і запобігання несанкціонованому доступу; регулярне оновлення програмного забезпечення для усунення вразливостей безпеки; використання багатофакторної автентифікації для контролю доступу до систем

управління; резервне копіювання даних для збереження налаштувань і забезпечення безперебійної роботи в разі збою [4, 5].

Висновки. Функціональна безпека розумних будинків є необхідною умовою для їх повноцінної роботи та захисту мешканців. Впровадження заходів з підвищення функціональної безпеки мінімізує ризики, пов'язані з кібератаками і технічними збоями, а також забезпечує стабільну, безпечну і комфортну роботу розумного будинку.

Список літератури

1. Mantas G., Lymberopoulos D., Komninos N. Security in smart home environment. *Wireless technologies for ambient assisted living and healthcare*. Page 170–191. DOI: https://doi.org/10.4018/978-1-61520-805-0.ch010.

2. Systematic analysis of safety and security risks in smart homes / H. Ullah Khan et al. *Computers, materials & continua*. 2021. Volume 68(1). Page 1409-1428. DOI: https://doi.org/10.32604/cmc.2021.016058.

3. Dewsbury G., Linskell J. Smart home technology for safety and functional independence: The UK experience. *NeuroRehabilitation*. 2011. Volume 28(3). Page 249–260. DOI: https://doi.org/10.3233/nre-2011-0653.

4. Al-Wahah M., Al-Hossenat A. Safety assurance in IoT-based smart homes. *Edge computing - architecture and applications for smart cities [working title]*. 2024. DOI: https://doi.org/10.5772/intechopen.1005492.

5. Smart Home Automation Safety and Security. *Advantage Insuarance Solutions*. URL – https://www.teamais.net/blog/keeping-your-child-and-home-safe-with-smart-technology (дата звернення: 03.11.2024).

Відомості про авторів

Кіріченко Данило Володимирович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.kirichenko@student.csn.khai.ed

Землянко Георгій Андрійович, ст. викладач кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@csn.khai.edu