Кондратюк О.В., магістрант,
Нічепорук А.О., к.т.н., доцент кафедри комп'ютерної інженерії та інформаційних систем
Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ТА БЕЗПЕКИ ДЛЯ СИСТЕМИ «РОЗУМНОГО БУДИНКУ»

На сьогоднішній день технології розумного будинку набувають все більшої популярності, оскільки дозволяють автоматизувати повсякденні процеси, підвищувати рівень комфорту мешканців та забезпечувати ефективний контроль безпеки житлових приміщень. З кожним роком зростає кількість розумних пристроїв, що взаємодіють між собою в межах єдиної екосистеми, створюючи складні розподілені системи управління. Одним із ключових завдань сучасних технологій є забезпечення надійного захисту таких систем від зовнішніх і внутрішніх загроз, що включає фізичну охорону, кібербезпеку, контроль доступу та аналіз поведінкових особливостей користувачів.

Безпека в концепції розумного будинку є складною та багатоаспектною задачею, яка включає в себе не тільки захист житла від фізичних проникнень, але й контроль доступу до приміщень, а також оперативне реагування на потенційні загрози, серед яких особливу увагу слід приділити таким, як витоки газу, води або виникнення пожежі [1]. Окремою важливою складовою є забезпечення конфіденційності та захисту персональних даних мешканців [2]. Варто зазначити, що традиційні підходи до забезпечення безпеки, зокрема використання механічних замків, класичних систем відеоспостереження чи ручних методів управління сигналізацією, стають менш ефективними [2]. Це пояснюється необхідністю постійного контролю з боку користувача, що є незручним у сучасних умовах, а також недостатнім рівнем інтеграції цих рішень у єдину екосистему домашньої автоматизації.

З огляду на ці виклики, сучасні тенденції в сфері домашньої безпеки орієнтовані на активне використання можливостей штучного інтелекту, глибокого аналізу великих масивів даних та автоматизації процесів з моніторингу і реагування на загрози у режимі реального часу [1; 4]. Істотний поштовх розвитку цього напряму дало поширення технологій Інтернету речей (IoT), завдяки яким стало можливим створення розподілених сенсорних мереж. Застосування алгоритмів машинного навчання дозволяє значно підвищити точність ідентифікації потенційних загроз та дає системі можливість самостійно адаптуватись до змін у поведінці мешканців чи параметрів навколишнього середовища [4].

Основною метою даного дослідження є розробка комплексного підходу, що дозволяє створити надійну інтелектуальну систему безпеки для розумних будинків. Запропонована в дослідженні концепція передбачає використання аналітичних моделей для аналізу поведінки користувачів, автоматичне керування пристроями та багаторівневу систему захисту інформації. В межах цього дослідження також здійснюється аналіз існуючих рішень, визначаються їхні переваги та обмеження [1; 3].

В основу структури системи покладено три основні функціональні рівні: сенсорний, рівень аналітичної обробки інформації та рівень взаємодії з користувачем. Такий підхід дозволяє реалізувати ефективний процес збирання інформації, оперативного виявлення загроз та ухвалення відповідних рішень у режимі реального часу [1].

На першому, сенсорному рівні, здійснюється безперервний збір інформації про параметри внутрішнього середовища будинку та зовнішні фактори. До складу сенсорного рівня входять різноманітні датчики, зокрема датчики руху, температури, вологості, освітленості, а також сенсори, що реагують на дим, витоки газу та води. Другий рівень — це рівень обробки інформації, що відповідає за аналіз отриманих даних та ухвалення рішень. На цьому рівні реалізуються передові алгоритми машинного навчання, які дозволяють системі передбачати ймовірні загрози, своєчасно розпізнавати незвичні або небезпечні ситуації, а також контролювати доступ до приміщень [4].

Список використаних джерел:

1. Taiwo, O., Ezugwu, A. E., Ikotun, A. M., Oyelade, O. N., Almutairi, M. S. (2021). Internet of Things-Based Intelligent Smart Home Control and Security System. Security and Communication Networks, 2021, 1–17. DOI: 10.1155/2021/9928254.

2. Аніщенко, В. О. (2020). Технології Інтернету речей у сучасних розумних будинках: проблеми безпеки та захисту даних. Інформаційна безпека, 26(4), 345–352. DOI: 10.18372/2410-7840.26.15621.

3. Pacheco, J., & Hariri, S. (2021). IoT security framework for smart homes: An overview and research challenges. Journal of Network and Computer Applications, 174, 102867. DOI: 10.1016/j.jnca.2020.102867.

4. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. IEEE Internet of Things Journal, 8(21), 15833–15854. DOI: 10.1109/JIOT.2021.3079274.