

## **КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ СИСТЕМ ОХОРОНИ РОЗУМНОГО БУДИНКУ**

Комп'ютерно-інтегровані технології систем охорони для розумного будинку – це сукупність рішень і технологій, що використовують сучасні інформаційні та комунікаційні засоби для забезпечення безпеки житла. Вони включають в себе апаратну, програмну частини та інтелектуальні алгоритми, що працюють разом для автоматизації захисту будинку.

Комп'ютерно-інтегровані технології систем охорони для розумного будинку набувають все більшої актуальності з кількох причин.

По-перше, зростання рівня життя та вимог до безпеки, адже сучасні люди прагнуть забезпечити максимальний рівень комфорту та безпеки у своїх домівках. Системи «розумного будинку» дозволяють автоматизувати багато процесів, включаючи охорону, що значно полегшує життя та підвищує рівень захищеності. Розвиток технологій, а саме швидкий розвиток електроніки, програмного забезпечення та інтернету речей сприяє створенню більш досконалих та доступних систем безпеки. З'являються нові датчики, пристрої та алгоритми, що дозволяють розширити функціональність систем охорони.

Також збільшення кількості кіберзагроз, а саме зростання кількості кіберзагроз вимагає вдосконалення систем безпеки. Сучасні системи охорони для розумного будинку можуть бути інтегровані з іншими системами безпеки, що дозволяє створити більш надійний захист від різних типів загроз.

Зі сторони використання користувачів зазначимо, що сучасні системи охорони для розумного будинку дуже прості у використанні. Завдяки мобільним додаткам та інтуїтивно зрозумілим інтерфейсам користувач може легко керувати системою з будь-якого місця, де є інтернет-з'єднання.

Варто не забути і про енергоефективність, що в наш час відіграє не останню роль. Системи «розумного будинку» дозволяють оптимізувати споживання енергії, що сприяє зниженню витрат на комунальні послуги. Основні компоненти системи «розумного будинку»:

1. Системи відеоспостереження: камери з функцією розпізнавання облич, IP-камери з доступом через інтернет, зберігання відеозаписів у хмарних сервісах.

2. Системи сигналізації: датчики руху, вібрації, відкриття дверей/вікон, звукові та світлові сирени, інтеграція з мобільними пристроями для отримання сповіщень.

3. Контроль доступу, електронні замки, біометричні пристрої (відбитки пальців, сканування обличчя), системи розпізнавання номерів автомобілів.

4. Мережеві технології: Wi-Fi або ZigBee для бездротового з'єднання компонентів, інтеграція з інтернетом речей (IoT), VPN для захисту від хакерських атак.

5. Програмне забезпечення: інтерфейси для управління через мобільні додатки чи веб-браузер, аналітика для виявлення підозрілої активності, інтеграція з голосовими асистентами (Google Assistant, Alexa).

Незважаючи на значний прогрес, системи охорони для «розумного будинку» мають потенціал для подальшого розвитку: розширення функціоналу (додавання нових функцій, таких як розпізнавання облич, голосове управління, аналіз поведінки мешканців для проактивного запобігання небезпечним ситуаціям), підвищення рівня безпеки (впровадження більш надійних алгоритмів шифрування даних, використання багатофакторної автентифікації, захист від DDoS-атак та інших кіберзагроз), збільшення автономності (розвиток автономних систем, які можуть працювати без постійного підключення до мережі Інтернет), спрощення установки та налаштування (розробка простих у використанні інтерфейсів, автоматизація процесу встановлення та налаштування системи), інтеграція з різними платформами (забезпечення сумісності з різними платформами та протоколами для забезпечення максимальної гнучкості) та розвиток штучного інтелекту (використання штучного інтелекту для аналізу даних, прийняття рішень та адаптації системи до змінних умов).

### **Список використаних джерел**

1. Розумний будинок – новий стандарт комфорту. URL: <https://cemsc.vntu.edu.ua/?p=501> (дата звернення: 16.11.2024).

2. Vakula A. Temperature dependent microwave properties of Fe<sub>3</sub>O<sub>4</sub> nanoparticles synthesized by various techniques. Telecommunications and Radio Engineering. 2016. Vol. 75, No 3. P. 229–234.

3. Дистанційний курс «Тестування та діагностика комп'ютерних систем та мереж» / упоряд. Шкіль О. С. Харків, 2010. URL: <http://openarchive.nure.ua/handle/123456789/2810> (дата звернення: 16.11.2024).