УДК 004.056.53

АРХІТЕКТУРА ПІДСИСТЕМИ МОНІТОРИНГУ ТА СПОВІЩЕННЯ ПРО НЕСАНКЦІОНОВАНИЙ ДОСТУП ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ КОМП'ЮТЕРНОГО ЗОРУ

Норик А.О.

Харківський національний автомобільно-дорожній університет, Харків

В умовах глобальної цифровізації суспільства, інтенсивного розвитку інформаційних технологій та суттєвого зростання рівня загроз у сфері кібернетичної й фізичної безпеки актуалізується потреба у впровадженні високоефективних автоматизованих систем захисту об'єктів. Особливої значущості набувають інтелектуальні системи, здатні в режимі реального часу здійснювати безперервний моніторинг контрольованого середовища, оперативно виявляти потенційні загрози, здійснювати їх аналіз та приймати обґрунтовані рішення щодо реагування. Одним з найбільш перспективних напрямів у цій галузі є використання методів комп'ютерного зору для автоматизованого виявлення несанкціонованого доступу до об'єктів інфраструктури.

У процесі розроблення системи, що ґрунтується на інтеграції апаратних та програмних засобів, було сформовано цілісну та структурно впорядковану архітектуру системи моніторингу й сповіщення про факти несанкціонованого проникнення із застосуванням технологій комп'ютерного зору та комплексу сенсорних засобів, подану на рисунку 1.

Запропонована архітектура забезпечує узгоджену взаємодію всіх функціональних модулів і дозволяє реалізувати адаптивний підхід до аналізу подій безпеки.

Ключовим елементом побудованої архітектури є блок обробки даних, який виконує роль центрального логічного ядра системи [1]. Саме на нього покладено функції збору, фільтрації, обробки та багаторівневого аналізу інформації, що надходить від усіх периферійних компонентів, зокрема

сенсорів руху, вібрації, інфрачервоних датчиків, відеокамер та модулів керування доступом. Даний блок реалізує алгоритми прийняття рішень, координує роботу виконавчих пристроїв та забезпечує обмін даними між підсистемами.

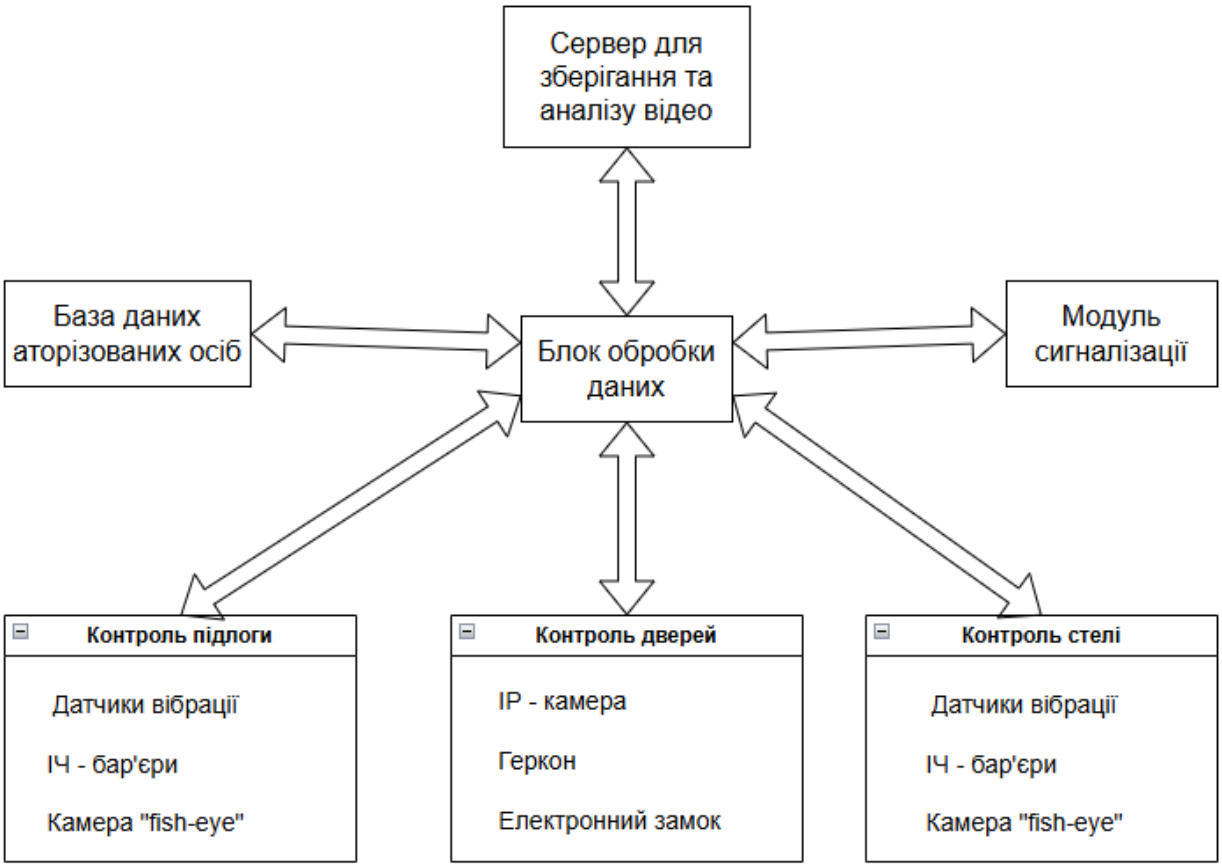

Рисунок 1. - Архітектура підсистеми моніторингу й сповіщення

Контроль доступу до об’єкта організовано за трьома основними напрямами: через двері, стелю та підлогу, що дозволяє забезпечити комплексне покриття потенційних шляхів проникнення. У зоні дверей використовується IP-камера для відеоспостереження[2], герконовий датчик[3] для фіксації факту відчинення та електронний замок [4], який функціонує у взаємодії з базою даних авторизованих осіб. Така комбінація засобів забезпечує як фізичний контроль доступу, так і візуальну ідентифікацію користувачів.

Контроль верхньої зони (стелі) реалізовано із застосуванням вібраційних сенсорів, інфрачервоних бар'єрів та ширококутної камери типу «fish-eye» [5], яка здійснює панорамний огляд простору згори. Подібні технічні рішення, а саме вібраційні датчики та ІЧ-сенсори, використовуються і для контролю підлогової зони, що дозволяє фіксувати навіть мінімальні механічні впливи або переміщення об'єктів у контрольованому середовищі.

Уся зібрана з різних сенсорних каналів інформація передається до блока обробки даних, де в режимі реального часу відбувається комплексний аналіз поточної активності. У разі виявлення об'єкта система автоматично запускає процедуру його розпізнавання на основі алгоритмів комп'ютерного зору. Якщо ідентифікована особа наявна у базі даних авторизованих користувачів, фіксується факт легітимного входу, здійснюється керування електронним замком та продовжується подальший моніторинг ситуації.

У випадку відсутності підтвердження авторизації або реєстрації нештатних подій (перетин інфрачервоного бар'єра, виникнення вібрацій, спроби несанкціонованого відкривання тощо) активується модуль сигналізації, який передає відповідні повідомлення службі безпеки або системному адміністратору.

Паралельно з основними процесами контролю відеопотік у режимі безперервної передачі надходить на сервер зберігання й аналітичної обробки. Це забезпечує формування архіву відеоданих та можливість подальшого використання накопиченої інформації для детального аналізу інцидентів, статистичної обробки та навчання моделей комп'ютерного зору з метою підвищення точності розпізнавання.

У цілому система функціонує як складний багаторівневий кіберфізичний комплекс, у якому кожен окремий компонент виконує чітко визначену функцію, а їхня взаємодія реалізується через центральний блок обробки даних. Такий підхід забезпечує високий рівень надійності, адаптивності та масштабованості системи безпеки.

Література:

1. Блок обробки даних Raspberry Pi 4 Model B. [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.com/products/raspberry-pi-4- model-b/ – 17.11.25
2. IP-камера Raspberry Pi Camera Module 2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.com/products/camera-module-v2/ – 15.11.25.
3. Геркон Y213 [Електронний ресурс] – Режим доступу до ресурсу: https://www.mini-tech.com.ua/gerkon – 16.11.25
4. Електрозамок Yli Electronics YE-304NO [Електронний ресурс] – Режим доступу до ресурсу: https://www.bezpeka-shop.com/ua/product/elektrozamok-ye- 304no-power-open-dlya-sistemy-kontrolya-dostupa/?srsltid=AfmBOoojxPIc79KKP3HnuZsNP1155b3v4YXAFEBqyTFWvY3kf wKld8j9 – 16.11.25
5. Камера Raspberry Pi High Quality Camera [Електронний ресурс] – Режим доступу до ресурсу: https://evo.net.ua/kamera-raspberry-pi-high-quality- camera/?srsltid=AfmBOoqUcv9JS3oUEOGB1xQMGQOsMMpi5 - nTYW1Yk8KVM2Qt8ilfPA6q – 15.11.25