

Перспективи впровадження доступних охоронних систем на основі сучасних технологій і відкритих платформ

Вінницький національний технічний університет

Анотація. Теза присвячена дослідженню проблеми забезпечення доступної охорони приміщень шляхом використання сучасних технологій та відкритих платформ. Проаналізовано переваги та недоліки традиційних охоронних систем, а також досліджено можливості застосування відкритих апаратно-програмних рішень для створення доступних альтернатив. Розглянуто перспективу розробки доступної охоронної системи з функціями віддаленого керування та оповіщення через чат-бот для оперативного реагування на загрози. Проведено порівняльний аналіз комерційних охоронних систем та потенціалу відкритих альтернатив.

Ключові слова: охоронна сигналізація, доступність, відкриті платформи, безпека, віддалене керування, чат-бот.

Abstract. The thesis is dedicated to exploring the issue of ensuring affordable security for premises through the use of modern technologies and open platforms. The advantages and disadvantages of traditional security systems are analyzed, along with an examination of the potential for implementing open hardware and software solutions to create cost-effective alternatives. The study considers the development of an accessible security system with remote control and notification functions via a chat-bot for rapid threat response. A comparative analysis of commercial security systems and the potential of open alternatives has been conducted.

Keywords: security alarm, affordability, open platforms, security, remote control, chat-bot.

Вступ

У сучасному світі забезпечення належного рівня безпеки приміщень є ключовим аспектом захисту фізичних даних та інформації. Надійні охоронні системи необхідні для запобігання несанкціонованому доступу, саботажу з боку працівників або інших подібних загроз. Традиційні охоронні системи, такі як камери спостереження, датчики руху та сигналізації, здатні ефективно забезпечувати фізичний захист об'єктів. Однак вони мають суттєві недоліки, серед яких висока вартість, складність встановлення та обслуговування, а також ліцензійні обмеження на вдосконалення або модифікацію.

Результати дослідження

Забезпечення безпеки приміщень малого бізнесу та приватних осіб стає дедалі важливішим у світлі зростання злочинності та нових загроз. Традиційні охоронні системи, такі як Ajax та Hikvision, пропонують високий рівень безпеки, але вони мають суттєві недоліки: високу вартість, складність монтажу та обслуговування, а також обмеження в можливостях кастомізації та інтеграції з іншими системами.

Сучасна система Ajax - це універсальні пристрої, що дозволяють встановлювати їх в житлових будинках, квартирах і офісних приміщеннях. Основа даної охоронної системи сигналізації - це датчики, в основному бездротові, що функціонують на вбудованих акумуляторах. Компанія «Аїах» виготовляє охоронні пристрої, сирени, центральні блоки керування для встановлення їх у житлових, офісних та інших приміщеннях. Компактність, ергономіка, сучасний мінімалістичний дизайн і висока якість є особливою рисою даних пристроїв [1].

Однак серед недоліків варто відзначити високу вартість обладнання, обмежену можливість розширення системи за рахунок зовнішніх датчиків або інтеграції з іншими технологіями, такими як IoT або штучний інтелект. Крім того, система потребує стабільного інтернет-з'єднання для нормальної роботи і хмарне функціонування системи [2].

Hikvision є ще однією популярною системою для охорони приміщень, яка пропонує як відеоспостереження, так і датчики руху для моніторингу. Ця система здатна інтегруватися з іншими охоронними пристроями та забезпечувати високий рівень безпеки. Завдяки використанню IP-камер та аналітики відео, система здатна не лише сповіщати про порушення, а й автоматично класифікувати події за допомогою алгоритмів комп'ютерного зору.

Основною перевагою Hikvision є можливість використання складних технологій відеоспостереження і аналізу даних, що дозволяє контролювати не тільки ситуацію в реальному часі, але й історію подій. Однак ця система має високу вартість, складність у налаштуванні та потребує спеціалізованого обладнання для зберігання відеоархіву. Крім того, великі витрати на обслуговування

і постійну оновленість програмного забезпечення можуть бути важким навантаженням в фінансовому плані. Також не варто забувати про консервативність країни виробника, що може загрожувати конфіденційності користувача[3].

Перспективи впровадження доступних охоронних систем на основі відкритих платформ, таких як наприклад Arduino або ESP, є дуже багатообіцяючими. Використання відкритих технологій дозволяє створювати охоронні рішення, адаптовані до конкретних потреб користувачів, що знижує витрати порівняно з дорогими комерційними системами, де найбільшу частку вартості складають саме датчики. Ці системи легко масштабуються та налаштовуються під індивідуальні вимоги, що робить їх ідеальним вибором для різних сфер застосування, а відкритість коду забезпечує гнучке налаштування[4].

А відкритість коду дасть змогу більш вибірково налаштовувати такі системи.

Крім того, інтеграція таких систем з технологіями IoT дозволяє створювати не лише гнучкі та адаптивні рішення, але й забезпечувати віддалений моніторинг і управління через популярні мобільні додатки та чат-боти. Такий підхід забезпечує високий рівень безпеки завдяки миттєвим сповіщенням про загрози та можливості оперативного реагування. Однією з ключових переваг є можливість інтеграції з іншими смарт-пристроями, такими як розумні замки або камера відеоспостереження, що розширює функціональність системи.

Використання Arduino, ESP або їх аналогів значно знижує вартість охоронних систем, роблячи їх доступними для широкого кола користувачів, навіть з обмеженим бюджетом, та дозволяє впроваджувати ефективні й економічно вигідні рішення для безпеки. Така технологія дозволяє впроваджувати ефективні, але економічно вигідні рішення для безпеки.

У майбутньому такі системи можуть стати основою для більш складних рішень, включаючи штучний інтелект для автоматичного виявлення загроз, а також інтеграцію з хмарними сервісами для зберігання даних. Подібні інновації можуть змінити підхід до безпеки, зменшуючи залежність від дорогих апаратних рішень і забезпечуючи максимальну адаптацію під потреби користувачів.

Висновки

У дослідженні було проведено аналіз сучасних комерційних охоронних систем Ajax та Hikvision, виявлено їхні переваги, такі як висока надійність, та суттєві недоліки, зокрема висока вартість, складність налаштування та обмеженість інтеграції. Як альтернативу розглянуто використання відкритих апаратних та програмних платформ, що надає можливість створення гнучких та кастомізованих охоронних систем, адаптованих до індивідуальних потреб користувачів та інтегрованих з іншими пристроями IoT. Перспективи розвитку таких систем є значними, особливо у поєднанні з технологіями штучного інтелекту для інтелектуального виявлення загроз та хмарними сервісами для зберігання та аналізу даних, що відкриває шлях до створення більш доступних, надійних та ефективних охоронних рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Офіційний сайт компанії AJAX [Електронний ресурс]. Режим доступу: <https://ajax.systems/ua/> (дата звернення: 18.03.2025).
2. Плюси та мінуси безпроводної сигналізації Ajax [Електронний ресурс]. Режим доступу: <https://protocol.ua/ua/plyusi-ta-minusi-bezprovodnoyi-signalizaciyi-ajax/> (дата звернення: 18.03.2025).
3. Hikvision - International sponsor of war [Електронний ресурс]. Режим доступу: <https://web.archive.org/web/20230707193702/https://sanctions.nazk.gov.ua/en/boycott/31/>. (дата звернення: 18.03.2025).
4. Taking an Open-Source Approach to Hardware [Електронний ресурс]. Режим доступу: <https://web.archive.org/web/20141220162858/http://www.wsj.com/articles/SB10001424052748703499404574559960271468066> (дата звернення: 18.03.2025).

Ніколайчук Олександр Вікторович – студент групи 2КІДС-216, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: oleksandernikol@gmail.com

Науковий керівник: **Зоря Ірина Сергіївна** – ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: iryna.zoria03@gmail.com

Nikolaychuk Oleksandr Viktorovych – student of group 2KIDS-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksandernikol@gmail.com

Supervisor: **Zoria Iryna Serhiivna** – assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: iryna.zoria03@gmail.com