

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та систем електронних комунікацій

«Допущено до захисту»
Начальник кафедри інформаційних
технологій та систем електронних
комунікацій

Олександр ПРИДАТКО
“ ___ ” _____ 20__ року

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Розроблення embedded-рішень для сервісу отримання сповіщень
охоронної системи»

Виконав:

здобувач VI курсу, групи КН-61м
спеціальності 122 «Комп'ютерні науки»

(шифр і назва спеціальності)

Орест ФЛЬОРКО

(ім'я та прізвище)

Керівник Юрій БОРЗОВ

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

Львів 2024 рік

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра інформаційних технологій та систем електронних комунікацій

Освітній ступінь магістр

Спеціальність 122 “Комп’ютерні науки”

Освітня програма Комп’ютерні науки

ЗАТВЕРДЖУЮ

Начальник кафедри інформаційних
технологій та систем електронних
комунікацій

Олександр ПРИДАТКО

“ ___ ” _____ 20__ року

ЗАВДАННЯ

на кваліфікаційну роботу магістра

Здобувач Орест ФЛЬОРКО

(ім’я, прізвище)

1. Тема Розроблення embedded-рішень для сервісу отримання сповіщень
охоронної системи

керівник роботи Юрій БОРЗОВ, к.т.н., доцент

(ім’я, прізвище, науковий ступінь, вчене звання)

затверджені наказом ЛДУ БЖД від “ ___ ” _____ 20__ року № _____

2. Термін подання здобувачем роботи _____

3. Початкові дані до роботи

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник, Комп’ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.
2. Erich Schmidt. RFID in Operations and Supply Chain Management / Erich Schmidt - “ESV” - 2017. – 289с.
3. Петрик М.Р. Моделювання програмного забезпечення: науково-методичний посібник / М.Р. Петрик, О.Ю. Петрик – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2015. – 200 с.
4. An Open Source MQTT v3.1/v3.1.1 Broker. Електронний ресурс: <https://mosquitto.org/>
5. Chatbot - Microsoft Bot Framework + Nest.js. Електронний ресурс: <https://medium.com/@mathieupicciolli/lets-make-a-chatbot-microsoft-bot-framework-nest-js-e27b25280934>

4. Зміст кваліфікаційної роботи/проекту (перелік питань, які потрібно розробити)

Вступ

Розділ 1. Аналітичний огляд систем контролю безпеки

Розділ 2. Технології реалізації сервісу отримання сповіщень охоронної системи

Розділ 3. Обґрунтування обраного напрямку проектування

Розділ 4. Проектування сервісу отримання сповіщень охоронної системи

Висновки

Список використаних джерел

Додатки

5. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналітичний огляд систем контролю безпеки		
2	Технології реалізації сервісу отримання сповіщень охоронної системи		
3	Обґрунтування обраного напрямку проектування		
4	Проектування сервісу отримання сповіщень охоронної системи		

Здобувач

(підпис)

Орест ФЛЬОРКО

(ім'я та прізвище)

Керівник роботи

(підпис)

Юрій БОРЗОВ

(ім'я та прізвище)

АНОТАЦІЯ

Орест ФЛЬОРКО. «Розроблення embedded-рішень для сервісу отримання сповіщень охоронної системи». Кваліфікаційна робота за спеціальністю 122 «Компютерні науки» складається з текстової частини, що містить 4 розділи, 68 сторінок і містить 56 ілюстрацій та 15 джерел.

В даній магістерській кваліфікаційній роботі розроблено embedded-рішення для сервісу отримання сповіщень охоронної системи за допомогою клієнт-серверної архітектури об'єднаної з Microsoft Bot Framework. Розроблений сервіс повинен надсилати сповіщення всім користувачам які підписані на конкретний тип сповіщень у відповідні канали. Передача даних від давачів до сервера передається за допомогою протоколу MQTT через безпроводну мережу WiFi.

В роботі обґрунтовано вибір апаратної та програмної платформи.

ABSTRACT

Orest FLYORKO. "Development of embedded solutions for the security system notification service". The qualifying paper for the specialty 122 "Computer Science" consists of a text part containing 4 chapters, 68 pages and contains 56 illustrations and 15 sources.

In this master's qualification work, an embedded solution was developed for the security system notification service using a client-server architecture combined with the Microsoft Bot Framework. The developed service must send notifications to all users who are subscribed to a specific type of notifications in the appropriate channels. Data transmission from the transmitters to the server is carried out using the MQTT protocol over a wireless WiFi network.

The work substantiates the choice of hardware and software platform.

1. АНАЛІТИЧНИЙ ОГЛЯД СИСТЕМ КОНТРОЛЮ БЕЗПЕКИ

Помилка! Закладку не визначено.

1.1. Огляд існуючих рішень.....	Помилка! Закладку не визначено.
1.1.1. Взаємодія з використанням електронних ключів..	Помилка! Закладку не визначено.
1.1.2. Взаємодія за допомогою текстових команд.....	Помилка! Закладку не визначено.
1.1.3. Домофонні системи	13
1.2. Системи контролю доступу	17
1.3. Доступ за допомогою карт та зчитувачів	18
1.4. Керування системою безпеки за допомогою текстових повідомлень.....	21
1.5. Постановка завдання	23

2. ТЕХНОЛОГІЇ РЕАЛІЗАЦІЇ СЕРВІСУ ОТРИМАННЯ СПОВІЩЕНЬ ОХОРОННОЇ СИСТЕМИ

Помилка! Закладку не визначено.

2.1. Вибір середовища розробки	Помилка! Закладку не визначено.
2.2. Вибір мови програмування.....	Помилка! Закладку не визначено.
2.3. Nest Framework	26
2.4. Протокол MQTT.....	31
2.5. Висновки до розділу 2.....	38

3. ОБГРУНТУВАННЯ ОБРАНОГО НАПРЯМКУ ПРОЕКТУВАННЯ

Помилка! Закладку не визначено.

3.1. Структура та загальний алгоритм роботи сервісу отримання сповіщень.....	Помилка! Закладку не визначено.
3.2. Опис апаратних засобів реалізації	Помилка! Закладку не визначено.
3.2.1. Сенсор руху.....	42
3.2.2. Мікроконтролер ESP8266	43
3.2.3. Модуль RFID RC522	Помилка! Закладку не визначено.
3.2.4. Модуль GSM SIM800L.....	47
3.4. Висновки до розділу 3	48

4. ПРОЕКТУВАННЯ СЕРВІСУ ОТРИМАННЯ СПОВІЩЕНЬ ОХОРОННОЇ СИСТЕМИ 49

4.1. Проектування архітектури сервісу.....	49
4.2. Опис кореневого модуля AppModule	50
4.3. Опис модуля UsersModule	51
4.4. Опис модуля BotModule.....	54
4.5. Реалізація взаємодії з базою даних	59
4.6. Налаштування MQTT.....	62
4.7. Висновки до розділу 4.....	65

ВИСНОВКИ 66

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 67

ВСТУП

Статистично, в наш час, кількість проблем з несанкціонованим доступом до приміщень не знижується, особливо гостро це питання стоїть для офісних та складських приміщень, де об'єм завданої фінансової шкоди може нести серйозний негативний вплив на компанію та в деяких випадках може зруйнувати її як таку. Стає зрозумілим те, що питання безпеки повинно бути розглянуто достатню уважно, а саме засоби забезпечення належного рівня безпеки. На жаль, часто саме людський фактор є вузьким місцем в системі охорони, тож зміщення основних завдань охорони з працівників на технічні засоби є цілком прийнятним рішенням з точки зору ефективності та якості роботи системи безпеки в цілому.

Основним завдання системи безпеки стає обмеження доступу до приміщень, а відповідно і до майна та інформації що знаходиться там, та надання його лише тим особам, які мають таке право. Сам захист можна реалізувати по-різному, але основними підходами є саме ідентифікація персоналу та надання конкретних прав різним рівням працівників в залежності від їх обов'язків.

Готові рішення часто мають багато зайвого функціоналу, є дорогими в обслузі та складними в користуванні. Часто саме надлишковий функціонал може мати негативний вплив і погіршувати роботу система, а у особливих випадках може стати причиною зламу системи через банальну відсутність конфігурацій, які мали б попередньо бути встановленими.

Вирішення цієї проблеми можливе за рахунок використання сучасної бази елементів з використанням мікропроцесорних модулів, безпроводного з'єднання та можливості заміни одних частин системи іншими для покращення надійності. Також, це дозволить зробити конфігурування всієї системи

гнучкішим та простішим у використанні, а модулі, які вийшли з ладу простими в заміні та монтуванні.

Зазвичай першим модулем безпеки, з яким може зіткнутись зловмисник є будь який тип замка, наприклад механічний, електронний чи електронно-механічний дверний замок. Проте, навіть такі екземпляри часто піддаються зламу, незважаючи на те, що над ними постійно ведеться робота з покращення якості та безпеки, а самі модулі удосконалюються. Власне, електронним замком можна вважати різні види замків, наприклад: кодові, біометричні, електромагнітні, замки з електроблокуванням та інші. Такі рішення мають ряд переваг в порівнянні з простими механічними замками, а саме: підвищена надійність та секретність, змога віддаленого керування, ідентифікація особи що скористалась замком та можливість збереження цієї інформації в базу даних.

Проте, з точки зору зламу за допомогою фізичної сили електронні замки можуть мати таку ж, або і меншу стійкість ніж механічні аналоги. Комбінованим рішенням може бути електро-механічний замок, що має подвійний рівень захисту та може вимагати не тільки електронну ідентифікацію, а і використання звичайних ключів. Вибір конкретного виду замка напряму залежить від цілей для яких встановлюється замок. Наприклад, використання такого замка є доцільним на головних входних дверях в об'єкт і він може бути найбільш вразливим. Для замикання приміщень всередині об'єкту допускається використання лише електронних замків, це доцільно з економічної точки зору.

Також, важливою частиною безпеки є система сповіщень, що спрацьовує у випадку поміченого несанкціонованого доступу до приміщення, то що. Такий функціонал можливо реалізувати тільки за наявності централізованої системи керування. На жаль, більшість пропозицій на ринку мають дуже обмежений набір можливостей для інтеграції в різні системи сповіщень, велика їх частина зазвичай використовує СМС-сповіщення як єдиний вид зворотнього зв'язку, що не завжди є надійним та якісним підходом до вирішення цього питання, а GSM сигнали часто можуть подавлювати для запобігання спрацювання сповіщень.

Також це не дуже зручно з точки зору користувача, адже в наш час, на жаль, кількість СМС повідомлень отриманих протягом одного дня може бути досить великою через агресивну маркетингову модель різноманітних магазинів.

Оновлення до сучасних модулів дозволить зробити цей процес набагато гнучкішим, а канали для надсилання сповіщень зможуть бути вибрані з широкого списку. Можливе також збільшення надійності за рахунок додавання декількох каналів зв'язку, наприклад при виявленні відсутності доступу до мережі через основні канали – використання мережі GSM чи аварійної лінії інтернет, передбаченої саме для таких випадків.

ВИСНОВКИ

В магістерській роботі була розроблено embedded-рішення для сервісу отримання сповіщень охоронної системи. В ході роботи були вирішені наступні завдання:

1. Проведено аналіз методів керування системою за допомогою текстових повідомлень.
2. Обрані технології реалізації сервісу отримання сповіщень охоронної системи.
3. Розроблено структуру та алгоритм роботи сервісу отримання сповіщень та обрано апаратні засоби реалізації.
4. Виконано проектування сервісу отримання сповіщень охоронної системи.
5. Проведене тестування функціоналу MQTT брокера.

В результаті було реалізовано сервіс отримання сповіщень охоронної системи на базі бот-інтерфейсу Microsoft Bot Framework, давачів руху, RFID карт та за допомогою клієнт-серверної архітектури на основі фреймворку Nest.

Розроблено деревоподібну архітектуру що базується на модулях, контролерах та сервісах. Також серверну частину поєднано з бот-інтерфейсом Microsoft Bot Framework. Доступ до бот-інтерфейсу наданий через два канали: Slack та Telegram з можливістю підключення додаткових каналів за потреби.

Описано та обгрунтовано програмні засоби реалізації сервісу які надаються інструментами використаними для розробки. Використано протокол MQTT для передачі повідомлень від давачів руху та карт доступу через безпроводну мережу WiFi, що працює на основі протоколу HTTP.

Розроблено діаграми класів та алгоритм роботи сервісу, також описаний основний набір доступних для користувача команд через бот-інтерфейс. Розроблена структура бази даних MongoDB та схема опису її колекцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник, Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.
2. Рамський Ю.С., Олексюк В.П., Балик А.В. Р21 Адміністрування комп'ютерних мереж і систем: Навч. пос. —Тернопіль: Навчальна книга – Богдан, 2010. - 196 с.
3. Андрушко О. А. Аналіз процесів використання Docker для побудови мікросервісів / О. А. Андрушко, Ю. О. Борзов, І. О. Малець, О. В. Придатко // Науковий вісник НЛТУ України: Зб. нак.праць. Львів: НЛТУ, 2017. - №9(27) – С.95-98.
4. Петрик М.Р. Моделювання програмного забезпечення: науково-методичний посібник / М.Р. Петрик, О.Ю. Петрик – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2015. – 200 с.
5. Telegram Bot Platform. Електронний ресурс: <https://telegram.org/blog/bot-revolution>
6. Datasheet_SIM800L. URL: <https://arduino.ua>.
7. Erich Schmidt. RFID in Operations and Supply Chain Management / Erich Schmidt - “ESV” - 2017. – 289с.
8. Daymon Manning WPF In Action with Visual Studio 2010 by Arlen Feldman and Maxx/ Daymon Manning - 2011
9. Azure Bot Service. Електронний ресурс: <https://docs.microsoft.com/en-us/azure/bot-service/?view=azure-bot-service-3.0>
10. Chatbot - Microsoft Bot Framework + Nest.js. Електронний ресурс: <https://medium.com/@mathieupicciolli/lets-make-a-chatbot-microsoft-bot-framework-nest-js-e27b25280934>
11. An Open Source MQTT v3.1/v3.1.1 Broker. Електронний ресурс: <https://mosquitto.org/>

12. Software-Defined Networking : The New Norm for Networks. White Paper, Open Networking Foundation, April 2012 - 105 с.
13. Prydatko O. Informational System of Project Management in the Areas of Regional Security Systems' Development / Prydatko O., Solotvynskyi I., Smotr O., Borzov Y., Didyk O.– Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018. Lviv, 2018 (№ статті 8478543). P. 187–192.
14. TypeScript Підручник [Електронний ресурс]; Режим доступу до ресурсу: <https://w3schoolsua.github.io/typescript/index.html>
15. ESP8266 Wi-Fi SoC | Espressif Systems. URL: <https://www.espressif.com/en/products/socs/esp8266>