

Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА
за спеціальністю 123 «Комп'ютерна інженерія»

Тема наукової роботи: Методи та засоби реалізації технології «розумного будинку» на основі платформи «Arduino»

Виконала	_____	В. В. Просяник
Керівник роботи	_____	Д. І. Кузнєцов
Нормоконтроль	_____	Д. І. Кузнєцов
Завідувач кафедри	_____	А. І. Купін

Кривий Ріг
2022

Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Ступінь вищої освіти
Спеціальність

магістр
123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри, голова циклової комісії

_____ А. І. Купін

“ ____ ” _____ 20__ року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Присяник Валентина Вадимівна

(прізвище, ім'я, по батькові)

1. Тема роботи: Методи та засоби реалізації технології «розумного будинку» на основі платформи «Arduino»

керівник роботи Кузнецов Денис Іванович, канд. т. н., доцент,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “ ____ ” _____ 20__ року № ____

2. Строк подання студентом роботи

3. Вихідні дані до роботи

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень). Презентація PowerPoint

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів роботи	Примітка
1.	Складання та затвердження ТЗ, підбір літератури		
2.	Аналіз системи «Розумний будинок»		
3.	Аналіз протоколів синхронізації та загроз і вразливостей		
4.	Оцінка ризику виділених загроз та вразливостей		
5.	Огляд та вибір засобів управління розумним будинком		
6.	Розробка макету розумного будинку		
7.	Оформлення пояснювальної записки		
8.	Оформлення графічного матеріалу		

Студент _____
(підпис)
(прізвище та ініціали)

Керівник роботи _____
(підпис)
(прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 96 сторінок, 45 рисунків, 25 таблиць, 42 використаних джерела.

Об'єктом дослідження є автоматизована система розумного будинку.

Робота складається з чотирьох розділів.

В першому розділі було виконано огляд особливостей та характеристик різновидів розумних будинків. Особливу увагу приділено різновидам систем розумного дому.

Другий розділ присвячено аналізу протоколів для синхронізації складових частин розумного будинку, а також був проведений аналіз вразливостей системи «*Smart Home*». За допомогою метода ієрархії визначено кращий протокол для синхронізації.

У третьому розділі увага була приділена засобам управління макетом розумного будинку. Було розглянуто мікроконтролери, датчики та модулі за допомогою яких буде здійснюватися управління.

В четвертому розділі подана структурна схема розробленого макету, опис додатку, який створений для керування розумним будинком та опис інтерфейсу I2C.

Ключові слова: ARDUINO, ПРОТОКОЛИ СИНХРОНІЗАЦІЇ, АНАЛІЗ ВРАЗЛИВОСТЕЙ, МЕТОД ІЄРАРХІЇ, РОЗУМНИЙ БУДИНОК, УПРАВЛІННЯ РОЗУМНИМ БУДИНКОМ

					КНУ.РМ.123.22.12.Р			
Змн.	Арк.	№ документа	Підпис	Дата	РЕФЕРАТ	Літера	Аркуш	Аркушів
Розробив	Просяник							
Перевірів	Кузнецов							
Н.контроль	Кузнецов					КІ-21м		
Затвердив	Купін							

Explanatory note: 96 pages, 45 figures, 25 tables, 42 references.

The object of study is an automated system of smart home.

The work consists of four sections.

In the first section, an overview of the features and characteristics of different types of smart homes was made. Particular attention is paid to the types of smart home systems.

The second section is devoted to the analysis of protocols for synchronizing the components of a smart home, as well as an analysis of the vulnerabilities of the Smart Home system. Using the hierarchy method, the best protocol for synchronization was determined.

In the third section, attention was paid to the means of controlling the layout of the smart home. Microcontrollers, sensors and modules that will be used for control were considered.

The fourth section presents a block diagram of the developed layout, a description of the application that is created to control the smart home and a description of the I2C interface.

Keywords: ARDUINO, SYNCHRONIZATION PROTOCOLS, VULNERABILITY ANALYSIS, HIERARCHY METHOD, SMART HOME, SMART HOME MANAGEMENT

ЗМІСТ

Перелік умовних позначень	8
Вступ.....	9
Розділ 1. Поняття розумний будинок.....	11
1.1 Розумне освітлення.....	16
1.2 Розумне водопостачання, опалення, вентиляція і кондиціювання	18
1.3 Системи забезпечення безпеки та комплектації системи розумного будинку.....	19
1.4 Управління та контроль за дітьми і людьми похилого віку	20
1.5. Класифікація систем «Розумний будинок».....	20
1.6 Узагальнення поняття розумний будинок.....	22
1.7. Переваги та недоліки сучасних систем розумного будинку	24
Розділ 2. Аналіз протоколів синхронізації та вразливостей розумного будинку.....	27
2.1. Протоколи для синхронізації складових частин системи розумного будинку.....	27
2.2. Порівняльний аналіз розповсюджених технологій бездротового доступу мережі керування Smart Home	28
2.3. Вибір кращої технології для автоматизації розумного будинку на основі методу аналізу ієрархій	29
2.4. Аналіз уразливостей в системі «розумний дім»	37
2.4.1. Аналіз уразливостей та факторів, що впливають на датчики контролю та захисту в системі «розумний дім».....	43
2.4.2. Аналіз уразливостей та факторів, що впливають на виконавчі пристрої «розумного будинку».....	48
2.4.3. Аналіз уразливостей та факторів, що впливають на безпеку центральних пристроїв «розумного будинку».....	49

					КНУ.РМ.123.22.12.3			
Змн.	Арк.	№ документа	Підпис	Дата				
Розробив	Просяник				ЗМІСТ	Літера	Аркуш	Аркушів
Перевірів	Кузнєцов							
Н.контроль	Кузнєцов					КІ-21м		
Затвердив	Купін							

2.4.4. Аналіз уразливостей та факторів, що впливають на систему зв'язку «розумного будинку».....	52
2.5. Аналіз загроз безпеки «розумного дому».....	58
2.5.1 Загрози конфіденційності, цілісності та доступності інформації ІТ-системи «розумного дому».....	58
2.5.2. Оцінка ризиків інформаційної безпеки «розумного дому».....	60
Розділ 3. Огляд та вибір засобів для управління розумним будинком	65
3.1 Огляд та вибір мікроконтролерів	65
3.1.1 Мікроконтролер <i>Arduino Nano</i>	71
3.1.2 Мікроконтролер <i>Arduino Uno</i>	73
3.2. Огляд та вибір датчиків	75
3.2.1 Ультразвуковий датчик відстані <i>Arduino HC - SR04</i>	75
3.2.2 Інфрачервоний датчик руху <i>HC - SR501</i>	76
3.2.3 Датчик вологості та температури <i>DHT22</i>	78
3.3 Огляд та вибір модулів <i>Arduino</i>	79
3.3.1 Модуль <i>Bluetooth HC-06</i>	79
3.3.2 <i>DS1307</i> - годинник реального часу (<i>RTC</i>).....	80
3.3.3 <i>RFID</i> модуль <i>RC522</i>	81
3.3.4. Звуковий модуль <i>Arduino WTV020-SD-16P</i>	83
Розділ 4 . Розробка макету розумного будинку	85
4.1 Структурна схема макету розумного будинку.....	85
4.2 Інтерфейс <i>I2C</i>	86
4.3 Додаток для управління розумним будинком.....	89
Висновки	92
Список використаних джерел	93

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТКС - інформаційно–телекомунікаційна система;

ОКВ - опалення, кондиціювання та вентиляція;

ПК – персональний комп’ютер;

Сек – секунда;

ШІМ - широтно-імпульсна модуляція;

SCM - структурована кабельна мережа;

SPI - послідовний інтерфейс;

UART (universal asynchronous receiver/transmitter) - універсальний асинхронний приймач/передавач.

					КНУ.РМ.123.22.12.ПС	Арк.
	Арк.	№ документа	Підпис	Дата		

ВСТУП

Сьогодні складно уявити світ без автоматизації і житловий будинок не є виключенням. У звичайному житті в замиському будинку або квартирі виконується величезне число дій, які могли б виконуватися без нашої участі. Можна автоматизувати все, від включення світла до управління мікрокліматом в кімнаті. Ця можливість з'явилася завдяки системі "Розумний будинок".

Система розумного будинку - це система, що дозволяє забезпечити безпеку, комфорт і ресурсозберігання. Ця система розпізнає всілякі ситуації і належним чином реагує на них. У поняття системи розумного будинку, як правило, вкладають автоматизацію побутових, рутинних дій. Наприклад, при займанні в кімнаті зі встановленими спеціальними датчиками система розумного будинку знеструмить усі електроприлади в цьому приміщенні і так далі. Так при пожежі або іншій надзвичайній події, система розумного будинку вмить оповіщає про це господаря. Зранку система відрегулює оптимальну вологість в приміщенні, налаштує роботу кондиціонера на задану температуру і вирішить безліч інших побутових завдань. Уся безліч перемикачів замінює додаток у браузері смартфона або ПК.

Безперечною перевагою системи розумного будинку є можливість управляти всіма датчиками і пристроями у будинку віддалено, з ПК на роботі або із смартфона в пробці. Веб-застосування дозволяє бути в курсі того, що відбувається удома у будь-який час у будь-якому місці. Основною метою цієї роботи є проектування макету системи "Розумний будинок".

Актуальність теми зумовлена стрімким розвитком інформаційно-технологічної (ІТ) інфраструктури, а також її застосуванням для забезпечення комфортного проживання громадян в багатоквартирних та індивідуальних будинках.

На даний час розробка системи розумного будинку є досить актуальною. Я вважаю, що років через 10 така система буде дуже розповсюдженою та доступною для покупців.

Метою і завданням дослідження є:

- Аналіз поняття розумний будинок;
- Дослідження та вибір кращої технології для взаємодії складових частин розумного будинку за допомогою метода аналізу ієрархій;
- Аналіз вразливостей в системі «розумний будинок»;
- Огляд та вибір засобів управління розумним будинком;
- Розробка макету розумного будинку.

					КНУ.РМ.123.22.12.ВС			
Змн.	Арк.	№ документа	Підпис	Дата				
Розробив	Просяник				ВСТУП	Літера	Аркуш	Аркушів
Перевірив	Кузнєцов							
Н.контроль	Кузнєцов					КІ-21м		
Затвердив	Купін							

Об'єктом дослідження є автоматизована система розумного будинку.

Предметом дослідження є реалізація розумного будинку за допомогою *Arduino*.

Методи дослідження: за допомогою метода ієрархії Сааті визначити кращу технологію для взаємодії складових частин розумного будинку, а також методикою оцінки ризиків корпорації "Microsoft" визначити оцінки рівня ризиків системи.

Новизна роботи: на основі використання метода ієрархії Сааті визначено, що кращий варіант технології бездротового доступу мережі управління розумним будинком є технологія ZigBee. Дана технологія дозволяє істотно полегшити процес монтажу і подальшого обслуговування системи розумного будинку, а також ймовірність збою в таких системах практично рівна нулю. Також на основі результатів оцінки ризиків за допомогою методу корпорації "Microsoft" найбільш небезпечними загрозами системи розумного будинку є:

- атаки на центральний сервер;
- впровадження шкідливого коду чи програми;
- перехоплення та підміна переданого сигналу;
- відключення контрольних датчиків.

Практична цінність: Розроблена система та практична реалізація дає змогу використовувати для впровадження в сучасні будинки та робити життя власників безпечнішим та легким в управлінні.

РОЗДІЛ 1. ПОНЯТТЯ РОЗУМНИЙ БУДИНОК

Технології не стоять на місці і вже сьогодні кожному відомо про здібності вчених створювати речі, які раніше могли бути вигадкою фантастів і описувалися тільки в книгах і демонструвалися в рамках кінематографа. Раніше з області фантастики була думка про те, що чайник може закипіти без вашої участі в цьому процесі. А сьогодні це цілком реально і дуже поширено. Все це завдяки технології "розумний будинок".

Що це таке і як працює, знають не всі. Так як не всі жителі планети стежать за розробками Цукерберга, компанії Сяомі та інших. Визначення «розумний будинок»- це запозичений вираз. Як і багато технологій, в принципі. Ця система прийшла до нас із заходу. Перш ніж приступити до опису функцій, нюансів управління, розповідей про те, що вміє розумний будинок, потрібно розібратися з поняттями. «*Smart Home*» в перекладі з англійської означає - «розумний будинок» (рисунок 1.1). Під цією термінологією розуміється таке поняття як автоматизація систем побуту. Створена система для того, щоб спростити життя нам. Завдяки «розумному будинку» рутинні завдання більше не приносять роздратування і не викликають втому у власників будинку.

У нашій країні в це поняття включають все, що може істотно спростувати перебування і проживання в квартирі, будинку і т.д. Ми звикли думати, що «*Smart Home*» - це управління на автоматичному рівні чайниками, кухонними машинами, освітленням, проекторами, телебаченням та іншими мультимедійними пристроями. На заході поділяють на рівні ринку два поняття «*Smart Home*» і «мультирум». Друге - це якраз і є управління телевізором та мультимедійними пристроями.

Але важливо розуміти, що система розумного будинку - це набагато більше, ніж автоматика в активації роботи чайника. «*Smart Home*» включає в себе управління системами опалення, водопостачання, охоронними системами та відеоспостереженням. Організацією працездатності та установки системи розумного будинку зазвичай займається компанія забудовника.

					КНУ.РМ.123.22.12.01.ПРБ			
Змн.	Арк.	№ документа	Підпис	Дата	ПОНЯТТЯ РОЗУМНИЙ БУДИНОК	Літера	Аркуш	Аркушів
Розробив		Просяник						
Перевірів		Кузнєцов						
Н.контроль		Кузнєцов						
Затвердив		Купін				КІ-21м		



Рисунок 1.1 - Схема розумного будинку

Принцип роботи системи розумний будинок заснований на ряді команд (опцій), які можуть бути поставлені як людиною, так і машиною. Активація тієї чи іншої команди також може бути здійснена від запиту спрямованого від людини, або від датчика. Розберемо докладніше ці два варіанти активації системи.

Перший варіант може бути виконаний за допомогою голосового запиту або за допомогою запуску того чи іншого пристрою через додатки. Додаток встановлюється на смартфон і в режимі простих дій запускає той чи інший прилад чи систему. Наприклад, ви можете озвучити запит закип'ятити чайник, зробити тости, відключити опалення, запустити кондиціонер, або ви може дістати багатофункціональний пульт управління чи відкрити програму в вашому смартфоні і клікнути на потрібну команду. Обробивши ваш запит, система розумного будинку відправляє прохання на той прилад, який буде задіяний.

Другий варіант не вимагає вашої присутності безпосередньо в будинку або квартирі. Все тому що при такому варіанті все запрограмовано. Тобто при установці системи задаються певні параметри на той чи інший прилад у будинку. І в певний час він активується. Наприклад, кожен день о 07:30 вмикається чайник, або о 12:00 спрацьовує система опалення. Також в цьому варіанті можливий такий розклад як самостійне прийняття рішень системою. Це означає, що на підставі статистики система сама вирішує, коли запустити або вимкнути опалення чи закип'ятити воду.

Отже виходить, що вся система інтелектуального житлового приміщення складається із 3-х основних елементів. Перший елемент - це датчики. Вони приймають всю інформацію ззовні. Другий елемент -

центрального контролера. Його завдання обробити все те, що надходить до датчиків і після цього прийняти рішення по реалізації запиту. Третій елемент - обладнання. Тобто це все ті прилади і техніка, яка створена для того, щоб полегшити наше життя.

Зв'язок між елементами системи підтримується за допомогою дротового або бездротового зв'язку. Як не дивно, але варіант із дротовим зв'язком менш уразливий до поломок та збоїв системи. Часто можна зустріти виробників на ринку систем розумного будинку, які пропонують дротовий зв'язок. До ряду таких виробників відносять:

- AMX(рисунок 1.2);
- Ctestron;
- Evika;
- Інші.

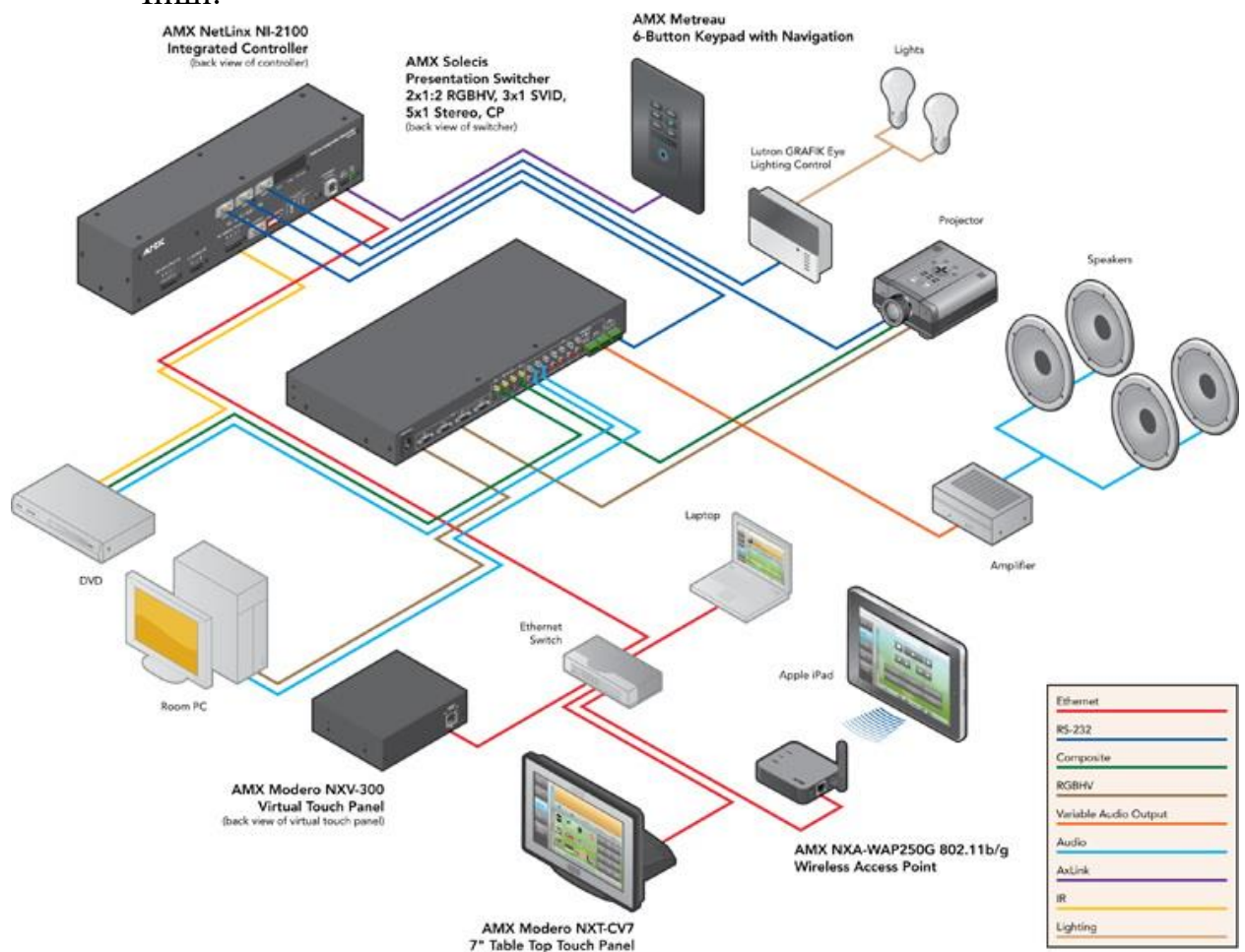


Рисунок 1.2 - Система керування розумним будинком на базі платформи AMX

Бездротові системи зв'язку простіші в плані монтажу та управління. Працює така система на основі *Bluetooth* або *Wi-Fi*. Виробники таких систем:

- Gira;
- Vitrum;
- Z-Wave;
- Jung(рисунок 1.3);

- Zamel;
- Xiaomi(рисунок 1.5);
- Та інші.



Рисунок 1.3 - Модуль система розумного будинку від Jung

Застосування комплексу засобів автоматизації та інформаційних технологій «розумного будинку» дозволяє забезпечити ефективну та безпечну експлуатацію, запобігти ризику нанесення шкоди, що приводить до відмови чи аварії устаткування інженерних комунікацій, вентиляції, опалення, систем енергозабезпечення, газопостачання, охороги, холодного і гарячого водопостачання, водовідведення, систем зв'язку та інших систем будівель і споруд (рисунок 1.4).

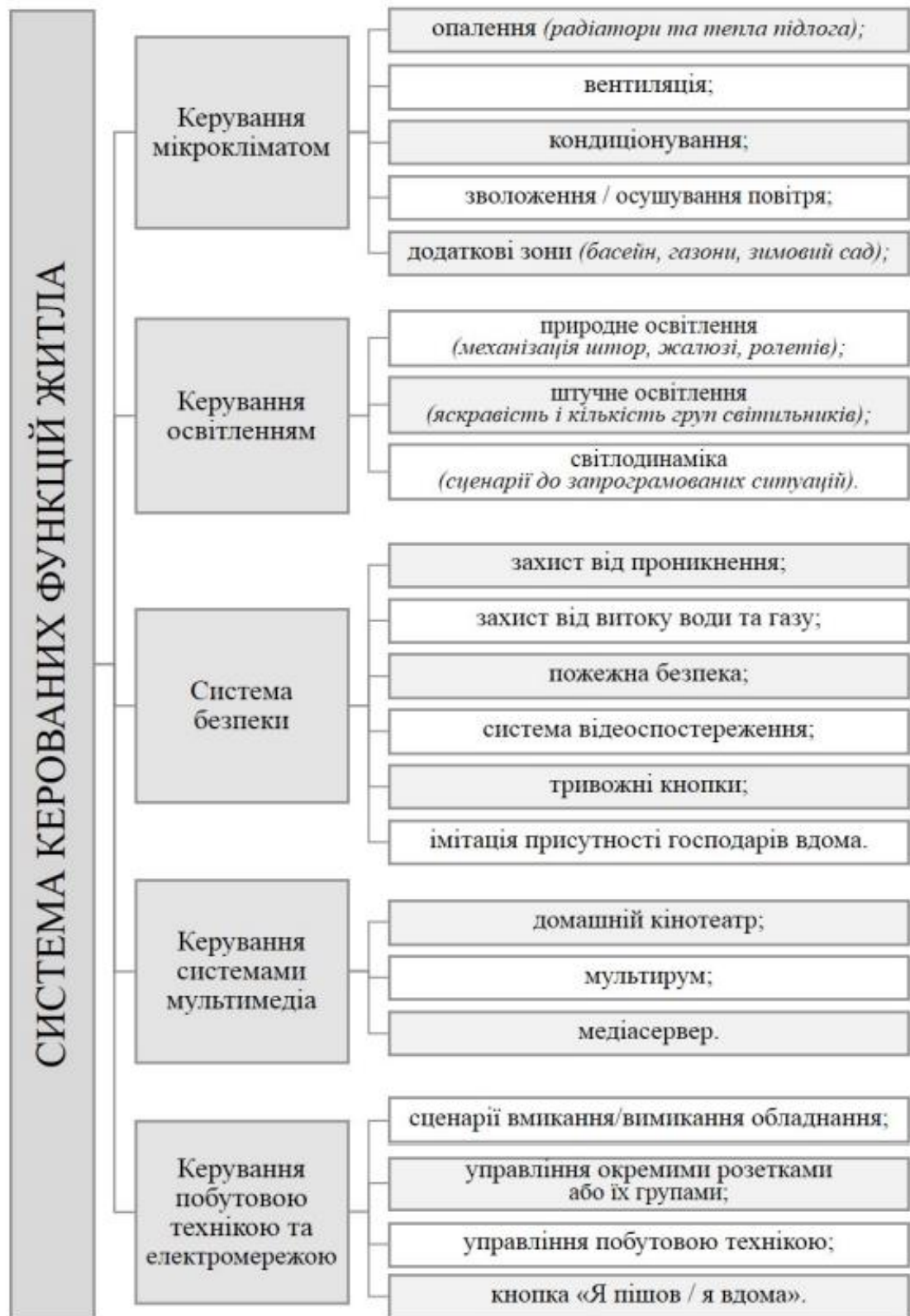


Рисунок 1.4 - Схема основних складових частин системи *Smart Home*

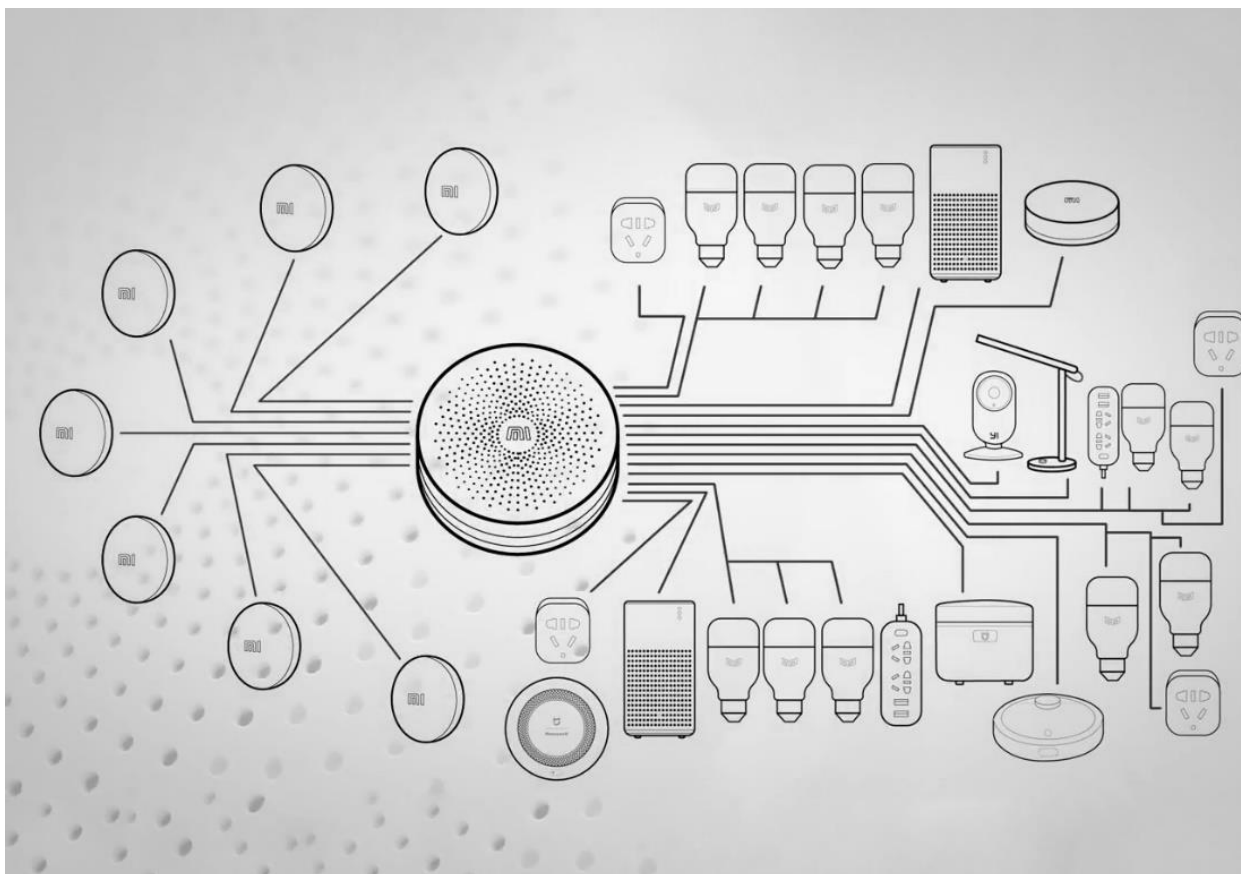


Рисунок 1.5 - Зразок системи розумного будинку від *Xiaomi*

Ще є системи, що працюють на протоколах. У деяких компаній є комплексні рішення. Одночасна робота дротових та бездротових систем забезпечує якісну роботу систему в цілому.

1.1 Розумне освітлення

Найпоширеніша функція - управління світлом. Ця функція також є найбюджетнішою. Розумне освітлення може бути автоматизоване таким чином, що воно буде регулюватися не тільки в будинку, але і в під'їзді, на вулиці. Включення світла при русі здійснюється за рахунок димерів і розумних ламп. Не секрет, що така система значно заощадить витрати на електрику.

Якщо говорити про конкретні приклади можливостей та функції інтелектуального освітлення, то варто сказати наступне:

- Є можливість регулювання жалюзей, штор і карнизів. Тим самим відбувається автоматизація і управління природним освітленням.
- Розпізнавання людини в просторі і підлаштування під неї. Тобто автоматичне включення освітлення, як тільки людина входить у кімнату. Такі можливості є у ламп марки Філіпс.
- Регулювання насиченості освітлення і яскравості.

- Загасання джерел світла при включенні телевізора, проектора та інших мультимедійних систем.
- Програмування предметів освітлення під режими неспання, сну, читання, спорту та інших дій.
- Можливість дистанційного керування. Тут можна скористатися різними варіантами: голосовими командами, додатком, багатофункціональним пультом управління.

Всі ці функції використовують різні компанії. Найпоширеніші виробники таких розумних ламп і розумного освітлення «BeON», AMX (рисунок 1.6), *Xiaomi Philips EyeCare 2*, *Philips*, *Nanoleaf Aurora Smarter Kit* і багато інших.

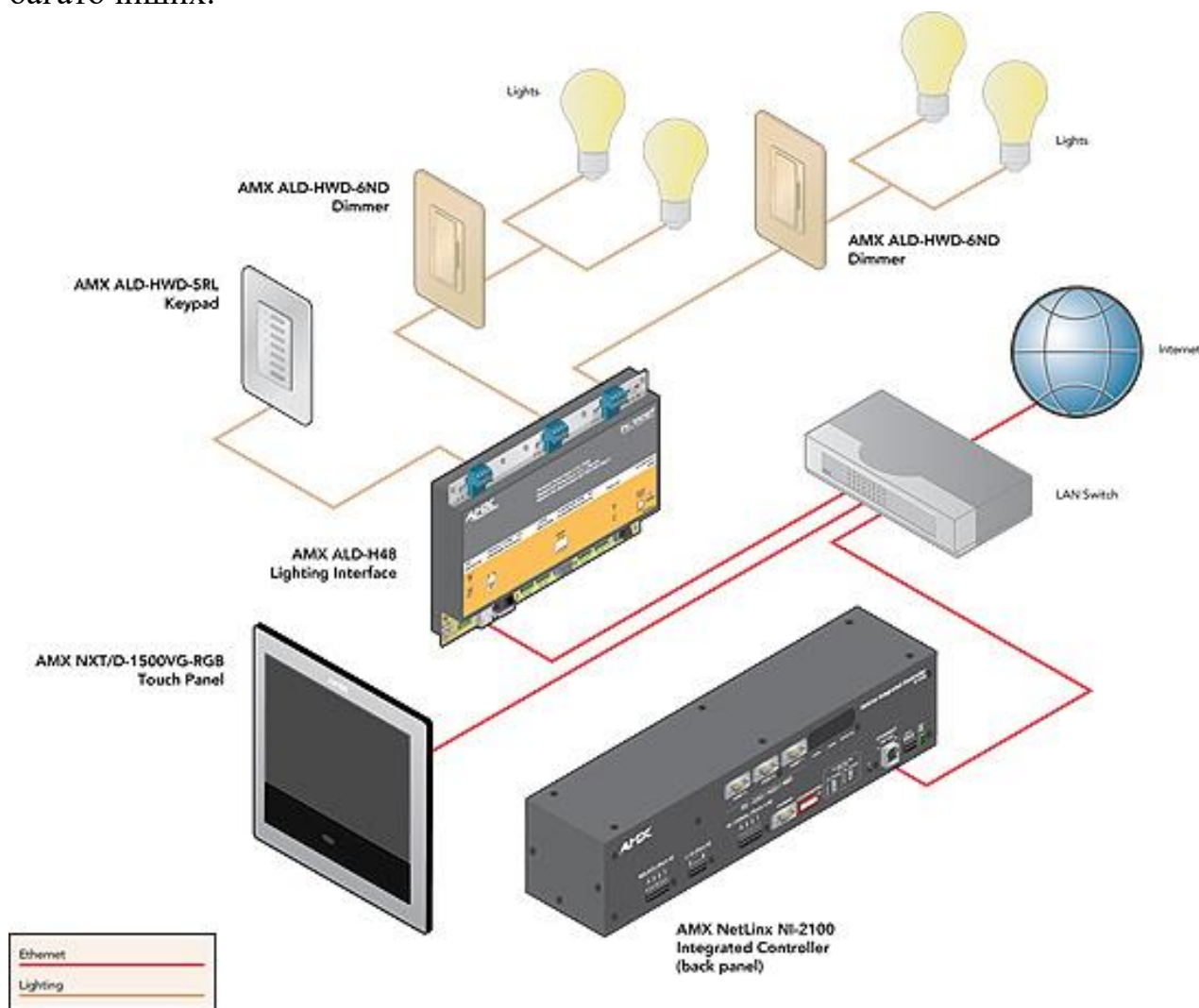


Рисунок 1.6 - Система керування освітленням від AMX

Окремо потрібно зупинитися на лампах від «Aurora», «Elgato Avea Bulb», «Kickstarter LIFX». Вони добре працюють в різних дизайнерських проектах, коли потрібно створити різного роду світлові сценарії. Такі лампи здатні змінювати не тільки режим освітлення (день / ніч), але ще й міняти відтінки світла. Працюють такі розумні лампи від вбудованого акумулятора. Також можна управляти за допомогою смартфона.

1.2 Розумне водопостачання, опалення, вентиляція і кондиціювання

При описі переваг системи розумний будинок потрібно обов'язково зазначити функціонал систем вентиляції, кондиціювання та опалення (рисунок 1.7). За кордоном є таке поняття як «HVAC», яке позначає автоматизацію роботи систем підтримання температурних режимів, вологості повітря, чистоти повітря, економії витрат електроенергії. Створити сукупність таких систем і реалізувати такий проект було вірним рішенням. Відтепер ОКВ (HVAC) - обов'язкова складова будь-якої системи розумного будинку. Вона дозволяє значно полегшити побут і життя в цілому. Від працездатності цих функцій залежить як здоров'я людини, так і безпека. Чим стабільніше і якісніше працює ця частина системи, тим краще якість життя у споживача.

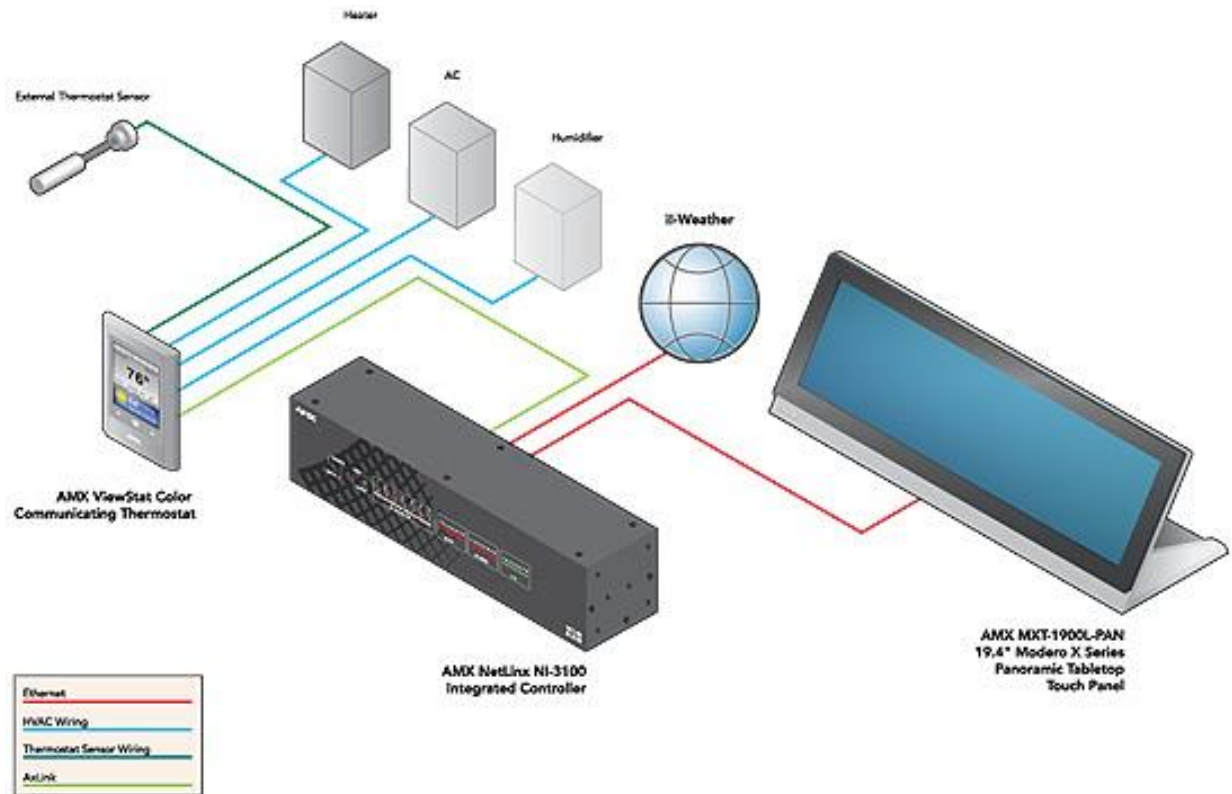


Рисунок 1.7 - Система клімат-контролю від AMX

Як правило, система опалення, вентиляції та кондиціювання працює не залежно від інших функцій «*Smart Home*» [13]. Це дозволяє краще функціонувати системі в цілому. І при виході з ладу будь-якої з частин системи, опалення, кондиціювання і вентиляції система все одно буде підтримувати працездатність, і забезпечувати процеси життєдіяльності. До основних функцій ОКВ відносять:

– Регулювання та підтримання комфортної температури в приміщенні. Автоматизація опалення є у систем «Loxone». За допомогою цієї системи можна регулювати температуру батарей та інших обігрівальних приладів.

– Автоматичне зниження температури і автоматичне її підвищення при присутності людини в приміщенні і при її відсутності. Тим самим відбувається економія витрат.

– Регулювання температурних режимів в залежності від часу доби.

– Зволоження повітря в міру необхідності. Такі функції вже давно впроваджуються на ринок розробки від *Xiaomi*. У них є зволожувач повітря *Smartmi Air Humidifier*, який добре справляється із завданням зволоження, іонізації і осушення.

– Управління і введення в автоматичний режим вентиляторів, кондиціонерів та іншої кліматичної техніки.

– Перекриття води, в разі надходження системі розумного будинку коду «немає людини в будинку». Це дозволяє уникнути потопів і неприємностей з сусідами.

Як і у випадку з розумним освітленням, ОКВ можна регулювати як через мобільний пристрій, так і безпосередньо через основний центр управління.

1.3 Системи забезпечення безпеки та комплектації системи розумного будинку

Систему безпеки все частіше стали встановлювати в свої володіння не тільки заможні громадяни, державні або приватні фірми, але і прості власники майна. Автоматизація систем безпеки зараз є частиною розумного будинку.

Цілісність системи безпеки в розумному будинку забезпечується наявністю відеоспостереження, датчиків виявлення диму і вогню, датчиками сигналізації та іншими охоронними моментами.

У цьому функціоналі потрібно чітко розмежовувати тип наданої безпеки. Є особиста і інженерна безпека від системи розумного будинку. Особиста безпека - це ті самі камери відеоспостереження як зовнішні, так і внутрішні. Сюди ж відносять хмарне зберігання даних, виклик охорони і сигналізація. Цілісність зовнішніх і внутрішніх пропускних систем (дверей зокрема), вікон, перегородок, воріт, іншого. Також розумний будинок має функцію розумного замку. Пропускні системи теж частина системи розумної безпеки.

До функціоналу інженерної безпеки інтелектуального будинку відносять:

- Гасіння пожежі в автоматичному режимі;
- Контроль цілісності проводки;

- Контроль цілісності водопроводу.

Виробники таких систем *NetBotz*, *Elgato Eve Motion*, *Seek Thermal* та інші. Як це прийнято в системі розумного будинку, управління відбувається з центрального апарату. Додатково регулюється виклик охорони.

1.4 Управління та контроль за дітьми і людьми похилого віку

Дивно, але розумний будинок - це не тільки банальні функції по регулюванню світла. Ви будете здивовані абе контроль за домашніми вихованцями теж частина програми інтелектуального будинку. Що ж входить в систему розумний будинок ще? Наприклад, система контролю і спостереження за дітьми, людьми з обмеженими можливостями, і пенсіонерами. Тут може бути зібрано дуже багато функцій, але основні з них, і самі практичні, це:

- Радіоняня;
- Відеоспостереження за дітьми;
- Повідомлення про вчинення якихось дій;
- Перекриття доступу в приміщення;
- Датчики активності і фізичного стану.

Надають такі можливості прилади компанії *Samsung*, *S-max Sella*, *Redmond SkyTracker*, і інші. *Tecnia*, наприклад, може зрозуміти, коли хтось із людей які знаходяться в будинку нервується. На нашому просторі такі прилади рідкість. Але вони активно впроваджуються на наш ринок.

1.5 Класифікація систем «Розумний будинок»

Провівши аналіз принципів реалізації існуючих систем можна визначити наступну класифікацію за принципом зв'язку між окремими модулями системи:

- Централізована система;
- Децентралізована система;
- Змішана система.

Перша група – централізована система, яка складається із головного комп'ютера до якого підключенні виконавче–командні модулі. Вони взаємодіють завдяки центральному комп'ютеру, який подає сигнали керування через канал зв'язку (шина). Всі налаштування зберігаються на сервері, а периферія викону лише отримані від нього команди.

Архітектуру такої системи зображено на рисунку 1.8.

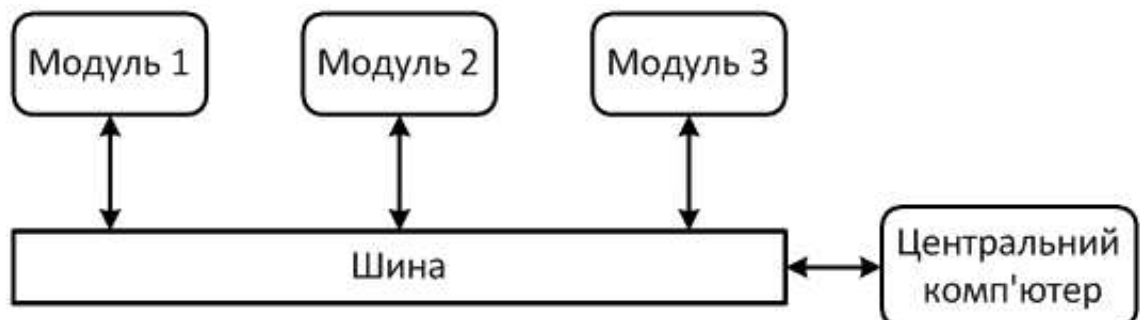


Рисунок 1.8 - Архітектура централізованої системи

Дана концепція дає можливість зібрати автоматизовану систему з єдиним комплексом виконання та приєднати прилади різних виробників, не зважаючи на різні канали зв'язку, які існують на даний час. Також централізована система володіє високою функціональністю та високоякісним графічним інтерфейсом.

Нажаль, існують і негативні сторони даної концепції: висока вартість; значні площі для розміщення технологічного обладнання; відмова центрального контролера призводить до відмови всієї системи; проектування системи вимагає високої кваліфікації і великого досвіду; монтування системи відбувається під час будівництва приміщення чи його капітального ремонту.

Друга група – децентралізованою системою. Як зрозуміло з назви головний керуючий центр в системі відсутній. Система складається із модулів, які виявляють зміни в характеристиках будинку і реагують на ці зміни завдяки контролеру, який вбудований в модуль. Алгоритми взаємодії прописуються з програми контролера безпосередньо в пам'ять кожного пристрою і для їх зміни пристрій буде необхідно перепрограмувати. У зв'язку з відсутністю центрального компонента, зв'язки між приладами встановлюються безпосередньо і є можливість створення автономних груп, замкнених одна на одну.

Архітектуру даної системи наведено на рисунку 1.9.



Рисунок 1.9 - Архітектура децентралізованої системи

Дана концепція не залежить від центрального блоку, тому всі функціональні модулі можуть працювати автономно. Відповідно це підвищує надійність системи в експлуатації. Дана технологія має хороші перспективи для розширення і модернізації апаратури, а також гнучкість при

програмуванні задовольняє потреби замовника. До недоліків такої архітектури можна віднести: порівняно високу ціну; проектування системи вимагає високої кваліфікації і великого досвіду.

Третя група є системою, яка включає в себе децентралізовану та централізовану системи, з метою підвищення гнучкості керування та компенсації недоліків, які є в обох систем.

Архітектуру даної системи зображено на рисунку 1.10.



Рисунок 1.10 - Архітектура змішаної системи

Дана концепція є ефективною з точки зору керування «розумним будинком».

Інтелект для вирішення найскладніших задач знаходиться в ЦК, який відповідає за функціонування всієї системи, особливо дочірніх мікроконтролерів (ДМ). ЦК постійно обмінюється інформацією з ДМ через канали зв'язку, а вони відповідно вже з модулями. Чим цікава ця система, що при відмові ЦК, вона буде працювати, оскільки ДМ мають свою логіку керування, тобто свій алгоритм, який відповідає за виконання різних функцій. ЦК використовується для забезпечення більш складнішого функціонування системи, для більш гнучкішого користування. Без ЦК дочірні контролери не можуть обмінюватися інформацією для більш ефективного керування всієї системи, але надійність під час експлуатації в даній системі є найвища. Звичайно, таку концепцію використовують у важливих воєнних чи наукових центрах для великої надійності захисту даних і забезпечення безпеки будівлі, оскільки дана система є дорогою і потребує багато ресурсів в обслуговуванні, проте це не заважає всім бажаючим мати дану систему керування для своїх «розумних будинків» [14].

1.6 Узагальнення поняття розумний будинок

Кілька десятків років тому складно було уявити, що не потрібно вставати з ліжка, щоб закип'ятити воду для чаю або щоб закрити фіранки. Сьогодні це більш ніж реально. А тепер уявіть, що перебуваючи у себе в

квартирі, ви взагалі не докладаєте зусиль для створення побуту. Все зроблено за вас. Все це можливо завдяки системі розумного будинку і технологій. Наприклад, як у Марка Цукерберга. Тільки уявіть, як плавно переходять світлові прилади при русі, як включається ваша улюблена телепрограма, як приходять оповіщення про те, що ванна набралась, як автоматично відкриваються жалюзі, двері, як шафа сам висуває вам потрібні речі для зустрічі з родичами. Можна все що завгодно, завдяки інтелектуальним програмами.

Організація розумного будинку набирає популярність у політиків, підприємців, великих компаній. Адже на додачу до всіх розумним і неймовірним технологій - це ще й вигідно. Все що робить розумний будинок - це дуже вигідно в плані фінансових витрат. Контроль температурних режимів, наприклад, може заощадити не малу суму. Тим самим ви отримуєте теплий будинок і маленький рахунок в кінці місяця.

Або, наприклад, Ви належите до тих людей, хто забуває перекрити воду або вимкнути праску. Розумний будинок зробить це за вас. Програмування техніки на своєчасне вимикання рятує вас від:

- Величезних рахунків за електропостачання;
- Перевитрати води;
- Перевитрати електроенергії;
- Раптових потопів і раптових ремонтів у сусідів;
- Пожеж.

У будь-якому випадку вибір системи розумного будинку - рішення, до якого потрібно підходити з усією серйозністю. Перш ніж встановити такі опції у себе вдома, вам потрібно визначитися з тим, в яких сферах повсякденних справ ви хочете полегшити собі життя. Часто користувачі вибирають тільки функціонал, пов'язаний з безпекою. Або ж у разі якщо за безпеку є, кому відповідати, то вибір зупиняють на мультимедійному комплексі розумного будинку.

Важливо пам'ятати, що хороша робота будь-якої системи залежить від регулярного технічного обслуговування і своєчасної реакції на будь-які зміни в плані звичайних робочих моментів системи [7].

Основною метою усіх технічних нововведень є спрощення життя людини, щоб зробити його максимально комфортним, особливо у рамках житлового простору. З одного боку, прогресивні технології допомагають зробити будинок теплим, світлим, енергоефективним, а з іншою, підсистем стає настільки багато, що управління усією інженерією стає вкрай складним завданням навіть для обізнаного користувача.

Розумний будинок - це система, що об'єднує усі важливі технічні підсистеми і призначена для того, щоб управління цими підсистемами було простим і зручним [15].

1.7 Переваги та недоліки сучасних систем розумного будинку

Комплекс сучасного високотехнологічного устаткування *Fibaro Starter Kit* містить все, що може зробити побут комфортнішим і безпечнішим. Стартовий набір включає шість базових компонентів, які згодом можуть бути доповнені необхідними пристроями.

Переваги:

- робота по протоколу *Z - wave*;
- можливість підключення 230 датчиків;
- дальність дії 50 м на відкритому просторі і 30 м - в приміщенні;
- використання різних сценаріїв поведінки системи.
- Недоліки:
- не завжди швидка передача *push*- повідомлень;
- висока вартість.

Налаштування і обслуговування комплекту *Fibaro Starter Kit* виконуються через інтерфейс за допомогою комп'ютера, планшета або смартфона [16].

Смарт-система від відомого китайського виробника *Xiaomi Smart Home Suite* відрізняється компактністю, привабливим зовнішнім виглядом, і успішно справляється з сценаріями домашньої сигналізації, дверного замку, нічника, радіо.

Переваги:

- економічність компонентів, що дозволяє працювати до 2 років без заміни батарейок;
- кут охоплення датчика руху - 170 градусів;
- широкі можливості для підключення додаткових пристроїв;
- сумісність з *Android* і *iOS*;
- прийнятна ціна.

Недоліки:

- трьохштиртова вилка контролера(потрібно перехідник);
- немає камери в комплекті.

Незважаючи на відсутність інструкції українською мовою і українізованого застосування, проблем з установкою і налаштуванням системи *Xiaomi Suite*, як правило, не виникає [17].

Система "Безпечний будинок" *Vstarcam C38AR-TZ1V* є повноцінним центром спостереження за приміщенням, здатним забезпечити надійний захист від проникнення у будівлю сторонніх осіб. Камера, яку можна закріпити на стіні або стелі за допомогою спеціальної пластини, оснащена 1-мегапиксельной матрицею і має кут огляду 56 градусів.

Переваги:

- цілодобовий *online*- контроль зі збереженням архіву записів;
- дві антени - для *Wi - Fi* і сигналів датчиків;

- камера з поворотним механізмом на 360 градусів;
- датчик руху з кутом охоплення 110 градусів і робочою відстанню 8м;
- простий і надійний дверний датчик, що спрацьовує на відкриття дверей або вікон;
- зручний пульт управління.

Недоліки:

- не дуже великий радіус дії.

Комплект *Vstarcam C38AR - TZ1V* призначений для використання усередині приміщень. До набору можна додатково підключити "розумну" *Wi-Fi* розетку, яка працює в одному застосуванні з іншими пристроями [18].

Найбільш досвідчені і вимогливі користувачі систем "Розумний будинок" вибирають, як правило, продукцію компаній *Amazon*, *Google* або *Apple*. Розробки цих брендів відрізняються універсальністю, сумісністю з облаштуваннями інших виробників, стильним дизайном.

Google Nest Mini - один з найбільш просунутих комплектів "розумний будинок" нині. Щоб розпочати роботу з системи, досить вимовити вголос "OK, Google" і попросити про яку-небудь послугу, наприклад, включити радіо або встановити будильник.

Переваги:

- висока якість звуку;
- простота використання;
- сучасний дизайн;
- помічник *Google Assistant*.

Недоліки:

- немає *USB*- порту для блоку живлення.

Google Nest Mini - хороший вибір для любителів музики, яким в рівній мірі важливі як технологічність, так і оригінальний зовнішній вигляд пристрою, а також розширений функціонал [19].

Результат розробки фахівцями *Apple* власної версії "розумного будинку" - система *HomeKit*, яка працює через додатки, що управляють домашніми приладами. Взаємодія таких застосувань відбувається у фоновому режимі, тобто управляти усією "розумною" технікою в приміщенні можна прямо з *iOS* пристрою.

Переваги:

- підтримка девайсов інших виробників;
- російськомовний голосовий помічник;
- стильний дизайн;
- можливість створювати сценарії - різні поєднання налаштувань.

Недоліки:

- багато компонент не розраховані на живлення від 220 В;
- для розширення функціональності може знадобитися додатковий ПК з *Linux*.

Щоб віддати команду помічникові *Siri*, необов'язково бути удома. Можна, наприклад, встановити сценарій "Їдемо додому", і *Apple HomeKit* до вашого прибуття настроїть температуру в приміщенні і включить світло.

Центральну роль в управлінні "розумним будинком" *Amazon* грає колонка *Echo Dot* з підтримкою голосового асистента *Alexa*, яка уміє відповідати на питання, програвати музику, передавати команди іншим елементам системи [20].

Переваги:

- сумісність з розробками інших виробників;
- можливість підключити *Innogy SmartHome* для контролю споживання електроенергії;
- підтримка *Nuki* - дверного замку, який повідомляє, хто увійшов до будинку;
- помірна ціна.

Недоліки:

- немає українськомовної підтримки голосового помічника.

За рахунок простого і практичного дизайну усі елементи "розумного будинку" *Amazon*, включаючи інтелектуальну колонку *Echo Dot*, добре підходять для будь-якого інтер'єру - від класики до *hi - tech*.

РОЗДІЛ 2. АНАЛІЗ ПРОТОКОЛІВ СИНХРОНІЗАЦІЇ ТА ВРАЗЛИВОСТЕЙ РОЗУМНОГО БУДИНКУ

2.1. Протоколи для синхронізації складових частин системи розумного будинку

Ми так багато говоримо про переваги системи, але жодного разу не згадали про недоліки. Недоліки все ж таки є. Це відсутність певного базового стандарту. Що це означає? Це означає що немає стандарту, який би працював з усіма пристроями для розумного будинку. Іншими словами ви не можете під одним дахом об'єднати техніку Самсунг і Філіпс на базі розумного будинку. Синхронізувати систему управління розумного будинку з приладами часто просто не вдається.

Але рішення є. Об'єднати і синхронізувати між собою всі складові системи можна за допомогою протоколів. Сьогодні виділяють 2 найвдаліших рішення в плані протоколів. Це *Z-Wave* і *ZigBee*.

Перше що потрібно сказати про ці протоколи, так це те, що вони обидва були розроблені спеціально для домашнього користування системою розумного будинку. Другим моментом, про який потрібно сказати буде мета створення протоколів. Метою протоколів *Z-Wave* і *ZigBee* є забезпечення безпеки та працездатності системи розумного будинку.

Що стосується характеристик *Z-Wave* і *ZigBee*, то це пористі протоколи мереж. Простіше кажучи шляхи рішення того чи іншого питання можуть бути зроблені в кілька способів (кілька варіантів шляху досягнення пункту призначення запиту). Перевага в тому, що ймовірність збою в таких системах знижується до нуля. А якщо один з вузлів зв'язку пошкоджений, потік перенаправляється на інший вузол зв'язку. Кожен з приладів комірчастої мережі пов'язаний з одним або декількома іншими пристроями.

Діапазон роботи *Z-Wave* і *ZigBee* - низькочастотний до 1 ГГц) [2]. Перевага в тому, що при низькочастотному діапазоні менше перешкод. На частоті в 2 ГГц зазвичай працює *Wi-Fi* з'єднання і *Bluetooth*. Яскравим представників використання відкритих протоколів є компанія *Xiaomi*.

Ще однією перевагою *Z-Wave* і *ZigBee* є момент того, що використання протоколу не енергозатратно. Споживання енергії нижче, ніж з використання роутерів. Все більше великих світових компаній стали використовувати пористі мережі з відкритими протоколами.

					КНУ.РМ.123.22.12.02.АПС			
Змн.	Арк.	№ документа	Підпис	Дата				
Розробив	Просяник				АНАЛІЗ ПРОТОКОЛІВ СИНХРОНІЗАЦІЇ ТА ВРАЗЛИВОСТЕЙ РОЗУМНОГО БУДИНКУ	Літера	Аркуш	Аркушів
Перевірив	Кузнецов							
Н.контроль	Кузнецов					КІ-21м		
Затвердив	Купін							

Це істотно полегшує процес монтажу і подальшого обслуговування системи розумного будинку.

2.2. Порівняльний аналіз розповсюджених технологій бездротового доступу мережі керування *Smart Home*

ZigBee — це відкрита технологія бездротового зв'язку для систем збору даних і керування. Технологія ZigBee забезпечує підтримку «сітчастих» топологій мережі, сплячих і мобільних вузлів, а також вузлів, які забезпечують роботу алгоритмів ретрансляції та самовідновлення. В якості робочого діапазону цей стандарт визначає неліцензованому частоти 2,4 ГГц (по всьому світу), 915 МГц (для Америки і Австралії) і 868 МГц (для Європи). Максимальна швидкість передачі даних складає 250 Кбіт / с в діапазоні 2,4 ГГц, 40 Кбіт / с в діапазоні 915 МГц і всього 20 Кбіт / с в діапазоні 868 МГц. Тому практично всі пристрої ZigBee працюють на частоті 2,4 ГГц. ZigBee має високу масштабованість. Здатний підтримувати до 65 000 вузлів, цей стандарт теоретично може забезпечити величезне охоплення, незважаючи на відносно невеликий радіус дії окремих модулів (10-20 м в приміщенні).[2]

Стандарт Wi-Fi є поширеним технічним рішенням організації бездротової TCP / IP мережі призначених для користувача і промислових пристроїв. Wi-Fi є стандартом зв'язку пристроїв в WLAN. Схема мережі Wi-Fi містить не менше однієї точки доступу і не менше одного клієнта. Також можливе підключення двох клієнтів в режимі точка-точка (Ad-hoc), коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережевих адаптерів «безпосередньо». Wi-Fi може легко передавати відео потоки високої чіткості, а межа його пропускну здатності набагато вище, ніж потреби середнього користувача. Деякі старіші версії стандарту 802.11 мають обмеження 11 Мбіт / с або 54 Мбіт / с, але широко використовуваний зараз 802.11n здатний передавати вже десятки і сотні мега біт в секунду, а новіший 802.11ac - ще більше) [21].

Bluetooth - це бездротова взаємодія між двома пристроями, призначена для безперервної передачі даних на дуже невеликі відстані. Технологія «розумного будинку» також починає використовувати переваги цієї технології для забезпечення надійної та ефективної передачі даних. Крім того, Bluetooth має низько енергетичну настройку, відому як Bluetooth Low Energy. Bluetooth Low Energy, як і інші стандарти зв'язку з низьким енергоспоживанням і низькою пропускну здатністю, орієнтований на передачу даних невеликими пакетами і короткий термін його служби на батарейках в активному режимі. Саме в цьому криється його основна відмінність від звичного, класичного Bluetooth, так як пристрої Bluetooth Low Energy з'єднуються один з одним тільки при необхідності відправки або отримання даних [22].

2.3. Вибір кращої технології для автоматизації розумного будинку на основі методу аналізу ієрархій

Метод аналізу ієрархій є систематичною процедурою для ієрархічного уявлення елементів, що визначають суть будь-якої проблеми. Метод полягає в декомпозиції проблеми на більш прості частини і подальшої обробки послідовності суджень особи, яка приймає рішення (ОПР), по парним порівнянням. В результаті може бути виражений відносний ступінь (інтенсивність) взаємодії елементів в ієрархії. Ці судження потім виражаються чисельно. Метод аналізу ієрархії включає процедури синтезу множинних суджень, отримання пріоритетності критеріїв і знаходження альтернативних рішень. Корисно відзначити, що отримані таким чином значення є оцінками в шкалі відносин і відповідають так званим жорстким оцінкам [23].

Метод аналізу ієрархій (MAI), запропонований Т.Л. Сааті, заснований на парних порівняннях альтернативних варіантів за різними критеріями з використанням дев'ятибальної шкали і подальшим ранжуванням набору альтернатив за всіма критеріями і цілям. Взаємини між критеріями враховуються шляхом побудови ієрархії критеріїв і застосування парних порівнянь для виявлення важливості критеріїв і під критеріїв [23].

До основних процедур методу аналізу ієрархій відносяться наступні:

- генерація множини альтернативних варіантів;
- формування множини критеріїв для оцінки альтернативних варіантів і подання його у вигляді ієрархії;
- виявлення переваг експертів на множині альтернатив за різними критеріями;
- встановлення відносної важливості впливу критеріїв на спільну мету і інші критерії;
- отримання ранжируваних наборів альтернатив за всіма критеріями і цілям.

Суть цього методу полягає в декомпозиції проблеми вибору єдиного кращого варіанту проекрованої системи з деякої безлічі варіантів з урахуванням сукупності показників якості. Принцип декомпозиції передбачає структурування проблеми вибору у вигляді ієрархії рівнів з вершини (мета вибору) через проміжний рівень 2 (показники якості системи) до найнижчого рівня 3 (альтернативні варіанти побудови системи). Потім від досвідчених експертів отримують їх суб'єктивні судження у вигляді парних порівнянь відносної важливості різних елементів проблеми вибору. В результаті обробки отриманих чисельних даних складаються матриці парних порівнянь елементів проблеми вибору. Для цих матриць обчислюються їх головні власні вектори, відповідні максимальним власним значенням. Далі згідно з визначеними математичним процедурам отримують вектор

глобальних пріоритетів, компоненти якого визначають пріоритетність вибору кращого варіанту проектованої системи. Єдиному кращому варіанту системи із заданої множини варіантів відповідає максимальне значення компонент вектору глобальних пріоритетів [24].

Принцип порівняльних суджень експертів в МАІ полягає в тому, що елементи проблеми вибору порівнюються експертами попарно за важливістю. Попарно порівнюються відносна важливість різних варіантів систем (на рівні 3) і різних показників якості системи (на рівні 2). Результати парних порівнянь зводяться до матричної форми

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} \\ a_{21} & a_{22} & \dots & a_{2j} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{ij} \end{pmatrix} \quad (2.1)$$

де $a_{ij} = \frac{w_i}{w_j}$ - оцінки парних порівнянь різних елементів w_i, w_j вибору

Діагональ цієї матриці заповнюється значеннями "1", а елементи матриці, що лежать нижче діагоналі, заповнюються відповідними зворотними значеннями.

Оцінки парних порівнянь елементів знаходяться з використанням суб'єктивних суджень експертів, чисельно визначених за шкалою відносної важливості елементів, яка представлена в таблиці 2.1.

Таблиця 2.1 Шкала відносної важливості елементів порівняння

Відносна важливість	Визначення
1	Рівна важливість елементів порівняння
3	Не значна перевага одного елемента над іншим
5	Істотна перевага одного елемента над іншим
7	Значна перевага одного елемента над іншим
9	Дуже сильна перевага одного елемента над іншим
2,4,6,8	Проміжні рішення між двома судженнями

Далі виконується обробка сформованих матриць парних порівнянь, яка з математичної точки зору зводиться до обчислення головного власного вектору, відповідного максимальному власному значенню матриці. Компоненти головного власного вектору матриці парних порівнянь

показників якості обчислюються як середнє геометричне значення в рядку матриці парних порівнянь

$$V_j = \sqrt[n]{\prod_{i=1}^n a_{ij}}, \quad j = \overline{1, n}, \quad (2.2)$$

де n - число показників якості.

Через компоненти головного власного вектору обчислюються відповідні компоненти вектору пріоритетів у вигляді нормованих значень

$$P_j = \frac{V_j}{S}, \quad j = \overline{1, n}, \quad (2.3)$$

$$\text{де } S = \sum_{j=1}^n V_j.$$

Такі процедури виконуються спочатку на рівні 2 для показників якості системи. Аналогічно знаходяться оцінки матриць парних порівнянь варіантів систем на рівні 3 окремо по відношенню до кожного показника якості системи. На основі цих матриць згідно (2) і (3) обчислюються компоненти відповідних головних власних векторів і векторів пріоритетів системи по відношенню до окремими показниками якості системи $\bar{Q}_j, j = \overline{1, n}$ [24].

З використанням отриманих векторів пріоритетів обчислюються значення компонент вектору глобальних пріоритетів $\bar{C}$ згідно

$$C_i = \sum_{j=1}^n P_j Q_{ij}, \quad i = \overline{1, N}, \quad (2.4)$$

де N - число порівнюваних варіантів систем.

За максимальним значенням компонент вектору глобальних пріоритетів (4) вибирається відповідний кращий варіант системи.

Розглянемо особливості застосування методу аналізу ієрархій для вибору єдиного кращого варіанту технологій для розумного будинку з урахуванням сукупності показників якості. Як показники якості обрані основні характеристики технологій, зокрема, час конвергенції, пам'ять, управління. У табл. 2.2 наведені оцінки значень показників якості для різних технологій розумного будинку.

Таблиця 2.2 Показники якості технологій для розумного будинку

Технології	Показники якості технологій				
	Швидкість передачі даних (K1)	Енергоспоживання (K2)	Пропускна здатність (K3)	Дальність зв'язку (K4)	Час безперервної роботи батареї, дні (K5)
Wi-Fi(N1)	300+ Мбіт/с	Високе	До 600 Мбіт/с	Від 20 - до 50 м	0,5 – 5
Bluetooth (N2)	До 3 Мбіт/м	Високе	До 2 Мбіт/с	Від 1- до 100 м	1- 10
ZigBee (N3)	250 Кбіт/с	Низьке	250 Кбіт/с	Від 10 - до 100 м	100 – 1000

У табл. 2.2 наведені співвідношення, які визначають залежності показників якості від основних характеристик технологій. Одразу помітно, що ці показники якості пов'язані між собою і мають конкуруючий характер.

На рисунку 2.1 показано ієрархічне представлення проблеми вибору кращої технології для розумного будинку. На рівні 1 знаходиться мета вибору кращого варіанту технології, на рівні 2 - показники якості технологій, на третьому - альтернативні варіанти технологій.

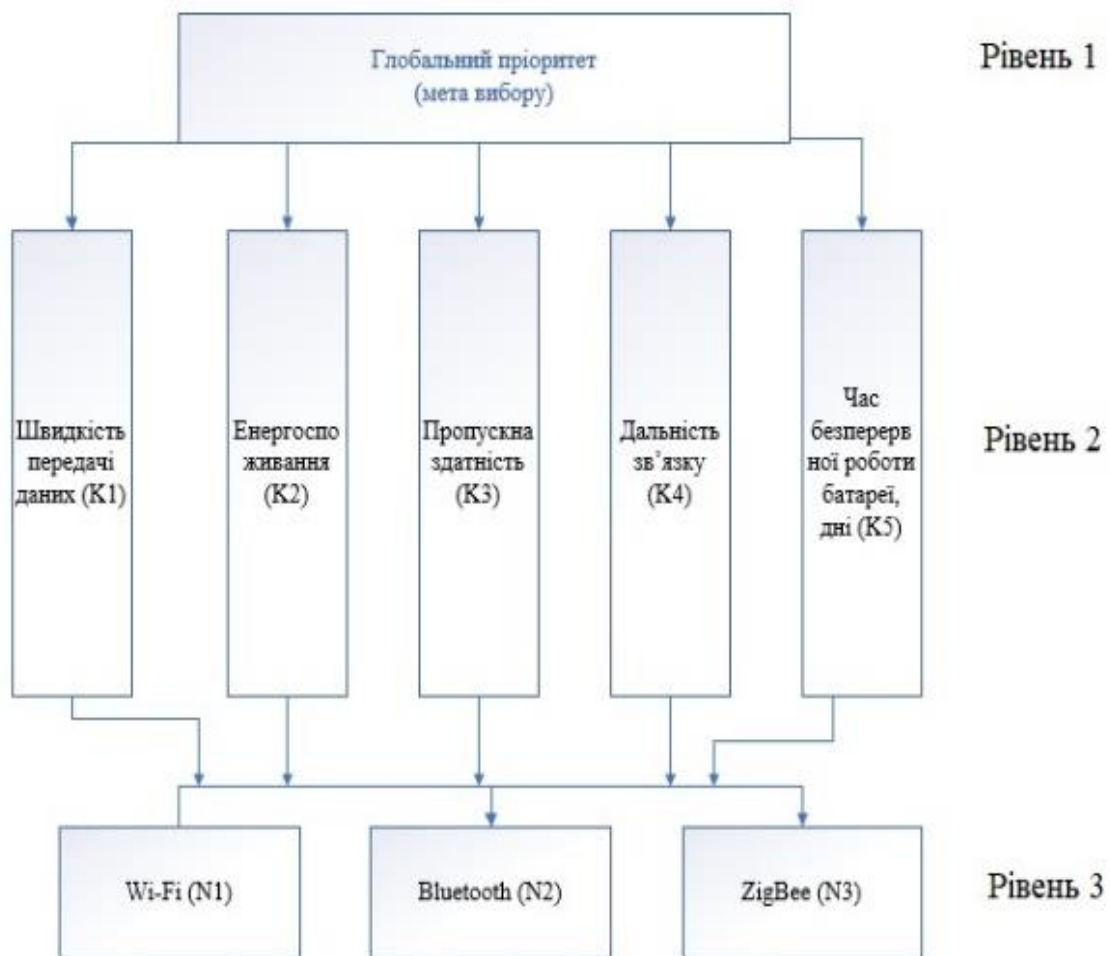


Рисунок 2.1 – Декомпозиція проблеми вибору

Згідно МАІ побудована матриця парних порівнянь для сукупності показників якості (тобто рівні 2) (табл.2.3). Для заповнення цієї таблиці за допомогою досвідченого експерта виконані парні порівняння важливості обраних показників якості, що визначають складність технологій, зокрема, швидкість передачі даних, енергоспоживання, пропускна здатність, дальність зв'язку, час безперервної роботи батареї. Діагональ цієї матриці заповнена значеннями "1", а елементи матриці, що лежать нижче діагоналі, заповнені зворотними значеннями.

Таблиця 2.3 Матриця парних порівнянь показників якості технологій і обчислені оцінки компонент вектора пріоритетів

	K1	K2	K3	K4	K5	Компоненти власного вектора v_j	Компоненти вектора пріоритетів p_j
K1	1	5	4	1/3	1/3	1,168	0,176
K2	1/5	1	1/3	1/4	1/4	0,333	0,05
K3	1/4	3	1	1/5	1/5	0,495	0,075
K4	3	4	5	1	1/3	1,816	0,273
K5	3	4	5	3	1	2,82	0,425

Далі виконані парні порівняння на рівні 3 у вигляді відносної складності альтернативних варіантів технологій по відношенню до кожного показника якості. В результаті обробки отриманих матриць обчислені згідно (2) і (3) власні вектори і вектори пріоритетів, які наведені в табл. 2.4, 2.5, 2.6.

Таблиця 2.4 Матриця парних порівнянь технологій по відношенню до швидкості передачі даних

K1	N1	N2	N3	Компоненти власного вектора v_j	Компоненти вектора пріоритетів Q_{i1}
N1	1	5	6	30	0,96
N2	1/5	1	5	1	0,03
N3	1/6	1/5	1	0,06	0,001

Таблиця 2.5 Матриця парних порівнянь технологій по відношенню до енергоспоживання

K2	N1	N2	N3	Компоненти власного вектора V_j	Компоненти вектора пріоритетів Q_{i2}
N1	1	1/8	1/8	0,015	0,0005
N2	8	1	1/3	2,66	0,099
N3	8	3	1	24	0,899

Таблиця 2.6 Матриця парних порівнянь технологій по відношенню до пропускної здатності

K3	N1	N2	N3	Компоненти власного вектора V_j	Компоненти вектора пріоритетів Q_{i3}
N1	1	3	5	15	0,93
N2	1/3	1	3	1	0,06
N3	1/5	1/3	1	0,06	0,003

Таблиця 2.7 Матриця парних порівнянь технологій по відношенню до дальності зв'язку

K4	N1	N2	N3	Компоненти власного вектора V_j	Компоненти вектора пріоритетів Q_{i4}
N1	1	7	1/7	1	0,0015
N2	1/7	1	1/9	0,015	0,0002
N3	7	9	1	63	0,98

Таблиця 2.8 Матриця парних порівнянь технологій по відношенню до часу безперервної роботи від батареї

K5	N1	N2	N3	Компоненти власного вектора V_j	Компоненти вектора пріоритетів Q_{is}
N1	1	5	1/7	0,14	0,002
N2	1/5	1	1/9	0,02	0,0003
N3	7	9	1	63	0,99

У табл. 2.9 зведені отримані оцінки компонент вектора пріоритетів показників якості, а також векторів пріоритетів технологій, по відношенню до швидкості передачі даних, енергоспоживання, пропускної здатності, дальності зв'язку, часу безперервної роботи батареї. З використанням цих векторів пріоритетів обчислені значення компонент глобального вектора пріоритетів згідно (6), які наведені в останньому стовпчику табл. 2.9.

Таблиця 2.9 Результати обчислення значень компонент глобального вектора пріоритетів

	Q_{i1}	Q_{i2}	Q_{i3}	Q_{i4}	Q_{i5}	C_i
N1	0,96	0,0005	0,93	0,015	0,002	0,24
N2	0,03	0,099	0,06	0,0002	0,0003	0,014
N3	0,001	0,899	0,003	0,98	0,99	0,72
P_j	0,176	0,05	0,075	0,273	0,425	

За максимальним значенням компонент вектора глобальних пріоритетів $\tilde{N}_i$ вибирається кращий варіант технологій бездротового доступу

мережі управління розумним будинком з урахуванням введених показників якості. Такою є технологія ZigBee.

2.4. Аналіз уразливостей в системі «розумний дім»

«Розумний будинок» є автоматизованою будівлею сучасного типу, що організована для зручності людей за допомогою високотехнологічних пристроїв.

«Розумні будинки» - багатофункціональні, і разом з цим складні. У розумному будинку один пристрій може керувати поведінкою інших пристроїв по заздалегідь виробленим алгоритмам. головною особливістю інтелектуальної будівлі є об'єднання окремих пристроїв в єдиний керований комплекс.

Подібними системами обладнуються не тільки житлові будинки, а й державні установи, місця масового скупчення людей, а також стратегічні об'єкти, наприклад, АЕС (Атомні електростанції), аеропорти і т.д. Поєднання різних технологій при побудові однієї автоматизованої системи збільшує кількість можливих недоліків рішення з точки зору безпеки, що, безумовно, привертає увагу зловмисників.

Обслуговування складних об'єктів це комплекс завдань, вирішення яких можливе за допомогою сучасних систем автоматизації життєзабезпечення. Значна частина сучасного обладнання, систем автоматичного керування будівлями різних компаній, можуть бути інтегровані в єдину мережу. Як наслідок, будівлі стають більш функціональними. Однак такі інтеграції мають недоліки. Поєднання різних технологій для створення автоматизованої системи збільшує кількість можливих недоліків безпеки системи. Збільшення кількості пристроїв і технологій, які використовуються в системі, ведуть до зростання вразливості системи. Крім того, процес інтеграції різних рішень не виключає можливість допущення помилки в проектуванні. Це може призвести до появи додаткових слабких місць в системі [25].

Зловмисники можуть отримати несанкціонований доступ до системи «Розумний дім», використати слабкі місця сучасних автоматизованих систем управління життєзабезпеченням, в наслідок чого можуть остаточно блокувати роботу великих об'єктів, наприклад аеропорту, сіяти хаос, і нарешті знищити систему безпеки з середини, що може призвести до серйозних наслідків. При заволодінні контролем над системою у зловмисника відкритий широкий спектр можливостей над використанням системи в своїх цілях.

На жаль, більшість систем автоматизації будівель не мають систему захисту проти кібератак. Більшість рішень для захисту, пов'язані з установкою стандартних програм, які виконують функцію брандмауера. Але у випадку атаки на системи автоматизації будівлі цього недостатньо.

У цілому системи автоматизованого управління будівлею мають кілька типів програмного забезпечення.

Першим типом є програмне забезпечення, яке забезпечує функціонування самої мережі «Розумного будинку». Воно розробляється на мовах програмування нижнього рівня і несе відповідальність за нижні рівні мережевої моделі OSI.

Другий тип програмного забезпечення, програми, які відповідають за взаємодію з користувачем через командну мову. Вони зазвичай використовуються для зовнішнього або віддаленого управління.

Головною частиною будь-якого комплексу ПЗ є сервер. Туди приходять запити від різних клієнтів. Сервер обробляє всі команди, аналізує параметри системи життєзабезпечення і приймає рішення про здійснення дії. Далі сформована команда передається на драйвери для доступу до мережі. Після чого за допомогою вибраного драйвера здійснюється безпосереднє маніпулювання об'єктами. У зворотному напрямку ланцюг також працює.

Користувальницький інтерфейс може бути реалізований різними способами. Є кілька підходів до реалізації цього компонента програмного забезпечення. Кожен із варіантів залежить від протоколу, який використовується для обміну із сервером системи «Розумний будинок». Це може бути і Web-браузер, який спілкується за допомогою протоколу HTTP, і застосування додатків реалізованих на високо-рівневих мовах програмування під ту чи іншу операційну систему. Це може бути навіть мобільний додаток, який встановлюється на мобільному телефоні користувача і призначений для обміну команд та сервісних повідомлень через TCP / IP з'єднання або SMS-повідомлення. Варто відзначити, що більшість протоколів, які використовуються для керування об'єктами є за своєю суттю вразливими, і багато інших, які використовуються для побудови підсистем, часто з неналежною інтеграцією призводять до уразливості. Як уже згадувалося вище, серверне ПЗ встановлюється на вибраному комп'ютері [25].

Машина з'єднує багато допоміжних пристроїв для передачі даних. Це можуть бути GSM-модеми, передавачі Bluetooth і Wi-Fi точки доступу. Крім того, часто на цьому сервері встановлено власне ПЗ.

Розглянемо основні канали розповсюдження вірусів:

- Канал *Bluetooth*. Мережа Bluetooth є надзвичайно ненадійною і легко може прийняти файл з вірусом зловмисника без авторизації ;
- Канал *Wi-Fi*. Мережа Wi-Fi може бути легко скомпрометована зловмисником, і він може минаючи систему авторизації, передати вірус на сервер;
- *HTTP* канал для віддаленого доступу. HTTP обмін з мережею Інтернет може бути одним з каналів зараження системи вірусом;
- *GSM* канал. Через канал GSM також можливий несанкціонований контроль системи. Це можливо, наприклад, за допомогою передачі SMS-повідомлень з фальшивим номером відправника;

– Споріднені канали. Якщо сервер «Розумного будинку» підключений до локальної мережі будівлі, то вірусна програма може потрапити на нього від локальної мережі.

Повноцінних антивірусних систем, що забезпечують комплексний захист від зловмисного ПЗ, не існує. Крім того, код, який властивий вірусам для систем «Розумного будинку», не визнається більшістю сканерів.

Розглянемо вразливості у програмному забезпеченні систем «Розумного будинку» що використовуються зловмисниками :

- відсутність блокування підключення несанкціонованих пристроїв;
- відсутність контролю над трансляцією датаграм в мережі «Розумного будинку»;
- відсутність аутентифікації керуючої програми, яка передає пакети у мережу «Розумного будинку».

На даний момент, є необхідність створювати спеціальні антивірусні засоби, які можуть забезпечити комплексний захист від зловмисного ПЗ.

Антивірусні програми для «Розумних будинків» повинні виконувати наступні функції:

- контролювати появу на сервері «Розумного будинку» будь-яких сторонніх файлів та програм;
- контролювати несанкціоновані підключення пристроїв до мережі;
- контролювати підключення пристроїв до бездротових каналів передачі даних;
- контролювати взаємодію сервера з мережею Інтернет на предмет появи та проникнення вірусів;
- контролювати мережеве обладнання на предмет DoS-атак;
- забезпечити перевірку файлів, які передаються у мережі;
- виконувати пошук наявності на сервері вірусних програм;
- контролювати цілісність системи «Розумний будинок», за допомогою перевірки поточної конфігурації, керуючих процесів і збережених даних.

На даний момент у світі існують лише програмні засоби захисту систем автоматизованого управління будівлями. Переклад частини реалізованих функцій на апаратну основу не тільки знижує вартість і складність розробок, а й істотно підвищує надійність засобів, що забезпечують безпеку систем «Розумного будинку».

Програмні антивірусні продукти не можуть вирішити задачу повного захисту системи через відсутність апаратної складової комплексу. Можна стверджувати, що існуючі програмні антивіруси не дозволяють повністю захистити систему. Таким чином, створення антивірусних засобів, які здатні забезпечити комплексний захист для системи автоматизованого контролю будинком є важливим завданням у найближчі роки.

У міру розвитку технологій можливості отримання, збору, обробки, зберігання, вилучення, відображення та передачі інформації, а також такі

методи та засоби, як знищення, спотворення, пошкодження, несанкціонований доступ до інформації, її блокування також інтенсивно зростають, а також порушення функціонування інформаційно-телекомунікаційних систем (ІТКС).

У цьому контексті зросла роль та значення інформаційної безпеки ІТКС. Тому все більш актуальним стає питання захисту систем «розумний дім», у тому числі елементів ІТКС, від стороннього втручання та ворожого спостереження. Під ворожим моніторингом розуміється непомітне для господарів вторгнення в системи розумного будинку з метою ознайомлення з уразливістю системи охорони, збору інформації про мешканців будинку, про розпорядок дня кожного члена сім'ї, особистих і конфіденційних даних і т.д. для подальшого пограбування, шантажу, вимагання і т.п..

Усі елементи системи «розумний дім», які відповідають за зв'язок, охорону, безпеку та системи життєзабезпечення, мають бути оснащені джерелом безперебійного живлення для збереження працездатності при відключенні електроенергії. Перебої в подачі електроенергії або відключення електроенергії можуть бути викликані сильним вітром, поваленими деревами на лініях електропередач або зловмисниками, які намагаються проникнути у ваш будинок, відключивши ваші системи безпеки та сигналізації. Системи розумного будинку не повинні покладатися на ці фактори. На додаток або замість джерела безперебійного живлення можна використовувати автономний генератор, наприклад, становлений під землею. Він увімкнеться, якщо є проблема з електроживленням.

Міжнародні мережі обміну інформацією, такі як Інтернет, значно розширюють можливості перехоплення та знищення критичної інформації з використанням інформаційної зброї. Інформаційна зброя використовується для крадіжки, викривлення або знищення інформації, обмеження або припинення доступу до інформації законних користувачів, порушення роботи або забезпечення безпеки людського життя.

Існує два найбільш популярні способи побудови системи «розумний дім»: перший спосіб полягає в побудові системи на основ програмованих контролерів, а другий – на основі виділеного комп'ютера, що називається сервером. Але і в тому і в іншому випадку потрібна наявність комп'ютера для зберігання аудіо- та відео архівів з камер спостереження, протоколів подій і звітів про стан системи та іншої інформації. У другому випадку для зберігання архівів можна використовувати сервер. Значить, ці комп'ютери повинні бути захищені від стороннього втручання програмними (установка спеціального програмного забезпечення, що обмежує доступ до інформації, а також забезпечує інформаційну безпеку) і технічними (обладнання розміщується у спеціальному виділеному приміщенні та доступ до цього приміщення обмежений) засобами.

Для можливості відправки системою протоколів подій господареві, що

					КНУ.РМ.123.22.12.02.АПС	Арк.
	Арк.	№ документа	Підпис	Дата		

знаходиться поза домом, Ваш комп'ютер має бути підключений до Інтернету, щоб система могла відправляти протоколи подій хостам на ходу. Тоді вам необхідно використовувати спеціальне програмне забезпечення, здатне захистити ваш комп'ютер від атак та шкідливих програм з глобальних мереж та запобігти витоку інформації. Крім того, бажано, щоб системи, що вже перебувають у стадії запису інформації на комп'ютери, шифрували свої архіви за допомогою стійких до злому методів кодування. І навіть якщо інформацію буде вкрадено, її буде дуже складно чи навіть неможливо розшифрувати.

Захист від програмного впливу здійснюється:

- застосуванням безпечних інформаційних технологій;
- атестацією технічних та програмних засобів та здійснення спеціальних перевірок на наявність закладок;
- запобігання несанкціонованому доступу до інформації, що циркулює в технічних системах;
- застосування програмних методів (засобів) захисту інформації для запобігання виведення з ладу системи розумного будинку зловмисниками;
- прийняти заходи щодо забезпечення безпеки апаратури, яка відповідає за працездатність і безпеку цих систем.
- Для захисту, від виведення зловмисниками з ладу систем розумного будинку бажано передбачити низку заходів:
 - оснастити життєво важливі системи розумного будинку джерелами безперебійного живлення;
 - розміщення апаратури, що забезпечує працездатність і безпеку систем розумного будинку (електричний шафа, монтажний шафа, контролери, сервер і т.д.) здійснити у спеціальному приміщенні поза зоною досяжності сторонніх осіб;
 - обмежити доступ в зазначений вище приміщення;
 - здійснення ремонту, технічної підтримки та заміни елементів систем розумного будинку повинні здійснювати тільки фахівці фірми–інсталятора.

Це дозволить уникнути проникнення в систему закладок та інших шкідливих елементів, які згодом можуть вивести з ладу системи розумного будинку.

З появою нових завдань удосконалюються вимоги до захисту інформації які передбачають:

- захист інформації при передачі її по каналах зв'язку, зберіганні та обробці (конфіденційність інформації);
- забезпечення цілісності та достовірності переданої, що зберігається і оброблюваної інформації ;

- автентифікацію сторін, що встановлюють зв'язок (підтвердження автентичності відправника або одержувача інформації);
- контроль доступу до ресурсів мережі, устаткування і даних абонентів;
- крипто живучість при компрометації частини ключової системи;
- шифрування інформації перед передачею і зберіганням;
- надання користувачу доступу до інформації тільки після аутентифікації та перевірки наявності у нього прав доступу до запитуваної інформації;
- забезпечення взаємодії між різними локальними інформаційними системами при одночасному виключенні можливості «наскрізного» проникнення до найбільш важливих підсистем, в яких циркулює інформація підлягає захисту [25].

Інший спосіб збирання інформації зловмисниками-видалення інформації з неекраниваних кручених пар. Найчастіше він використовується для побудови структурованих кабельних мереж (SCM), з яких пізніше будуються системи розумного будинку. Справа в тому, що при передачі сигналу по неекраниваній крученій парі вона починає випромінювати електромагнітні хвилі і виходить, що інформацію можуть перехопити спеціальні пристрої.

Однак відстань, на якій може бути перехоплено електромагнітне випромінювання кабелі в неекраниваних, не перевищує 0,5 метра. Екранування кручених пари знижує рівень власного випромінювання приблизно на два-три порядки. Це вимагає прямого підключення для отримання інформації. Екранування інформаційних кабелів також є найбільш ефективним рішенням для скорочення відстані між силовою та телекомунікаційною проводкою, забезпечення електромагнітної сумісності активного обладнання. Тому при побудові SCM-структур використання неекраниваних кручених пар і екраниваних кручених пар може поєднуватися, причому останні застосовуються тільки до найбільш вразливих ділянок мережі.

Багато також, щоб система розумного будинку мала ряд вбудованих детекторів, здатних виявити порушення цілісності системи та впровадження в її складові частини, а також вміла вчасно попередити господаря (де б він не знаходився, вдома чи на вулиці) та охоронну організацію про спробу порушення цілісності системи.

2.4.1. Аналіз уразливостей та факторів, що впливають на датчики контролю та захисту в системі «розумний дім»

Ефективна і багатофункціональна система «розумного будинку» включає різноманітні датчики, що реєструють і передають параметри середовища, і іншу важливу інформацію. Датчики автоматизації є конструктивно автономним самостійним пристроєм, що змінює свій сигнал відповідно до відстежуваного параметра.

Ці обов'язкові елементи «розумного будинку» розрізняються за призначенням та принципом дії, умовно їх можна умовно розділити на дві групи: датчики, що відстежують рух та датчики, що реагують на параметри середовища.

Датчики, що відстежують рух, що використовуються в охоронних системах та для побудови інтелектуального освітлення. Такі датчики поділяються на датчики руху та датчики присутності. Датчики присутності відрізняються від датчиків руху тим, що фіксують навіть дуже дрібні рухи, що відбуваються в межах робочої зони датчика, в іншому принцип їхньої роботи однаковий.

В даний час найбільшого поширення набули такі види датчиків руху та присутності:

- 1) інфрачервоні датчики (ІЧ) (рисунок 2.2).



Рисунок 2.2 – Приклад загального виду інфрачервоного датчика

Принцип роботи інфрачервоних датчиків руху полягає у виявленні змін інфрачервоного (теплого) випромінювання навколишніх об'єктів. Кожен об'єкт, що має температуру, випромінює інфрачервоне випромінювання, яке через систему лінз або спеціальних увігнутих сегментованих дзеркал, потрапляє на розташований усередині датчика руху чутливий сенсор, що реєструє це [27] .

Вразливістю даного датчика є т.зв. «сліпа зона», коли він зможе фіксувати об'єкти певної висоти. Крім того, датчик має обмеження діапазону робочих температур, наприклад, тільки в діапазоні від -10 0С до + 40 0С;

2) ультразвукові датчики (рисунок 2.3).



Рисунок 2.3 – Приклад загального виду ультразвукового датчика

Принцип роботи ультразвукового датчика руху полягає у дослідженні навколишнього простору за допомогою звукових хвиль, частотою за межами чутності людським вухом – ультразвуком (залежно від виробника та моделі зазвичай генерується частота звукової хвилі 20-60 кГц). При виявленні зміни частоти відбитого сигналу внаслідок руху об'єктів датчик запускає закладену в неї функцію, це може бути включення освітлення або розрив сигнальної мережі охоронної системи.

Вразливістю даного датчика є обмежений на відстані діапазон чутливості, наприклад, від 200 мм до 8 м. Якщо об'єкт знаходиться на відстані менше 200 мм, відбуваються помилкові спрацювання. Якщо кілька датчиків знаходяться в безпосередній близькості, що може зробити їх вразливими для перехресних перешкод, що запобігає спеціальному контролеру для включення датчиків по одному;

3) мікрохвильові датчики (рисунок 2.4).



Рисунок 2.4 – Приклад загального виду мікрохвильового датчика

Мікрохвильовий датчик руху випромінює високочастотні електромагнітні хвилі (частота хвиль може бути різною залежно від виробника, зазвичай вона становить 5,8 ГГц), які відбиваючись від навколишніх об'єктів, реєструються сенсором і у разі виявлення найменших змін відбитих електромагнітних хвиль, мікропроцесор пристрою приводить в дію закладену у нього функцію.

Вразливістю мікрохвильового датчика є неправильне визначення порогу чутливості.

Поріг - деяке значення, нижче якого сигнали інтерпретуються як шуми. Поріг регулюється під час налаштування датчика. Чим більша чутливість, тим більша ймовірність виявлення. Але зі збільшенням чутливості зростає і частота помилкових тривог, що знижує довіру до системи загалом. Також поява помилкових тривог може бути викликана недоліками конструктивних та схемотехнічних рішень; неправильною установкою та налаштуванням датчика; Недоліками алгоритму обробки сигналів.

Недоліки конструктивних та схемотехнічних рішень можуть призвести до наведень у ланцюгах передачі даних, наприклад, через погане екранування, погану фільтрацію, застосування дешевої неякісної елементної бази. Типовою проблемою є зміна параметрів електронних компонентів при наближенні до меж допустимого температурного діапазону. Для вирішення цієї проблеми доводиться розробляти спеціальні схеми термостабілізації параметрів тощо.

Неправильне налаштування датчика може призвести до виходу зони виявлення датчика за межі зони, що охороняється, особливо в приміщеннях зі складною конфігурацією. Це призведе до того, що такий датчик спрацюватиме, наприклад, при знаходженні людей у сусідніх приміщеннях [28].

Вразливість датчика може бути обумовлена збуреннями середовища, у тому числі електромагнітними наведеннями, паралельною роботою кількох датчиків.

Далі розглянемо т.зв. комбіновані датчики, які мають можливість об'єднувати в системі безпеки функції різних методів реєстрації зміни стану довкілля, розглянуті вище;

4) комбіновані датчики (рисунок 2.5).



Рисунок 2.5 – Загальний вигляд комбінованого датчика

Комбіновані датчики руху поєднують у собі відразу кілька технологій виявлення рухів, наприклад, інфрачервоний датчик та мікрохвильовий. Це найбільш вдале рішення, якщо потрібне точніше визначення переміщень у зоні дії датчика.

Також існують магнітоконтактні датчики, що діють при зміні відстані між магнітом та герконом (змикання та розмикання складових частин) та датчики розбиття скла [28].

За принципом дії датчики пошкодження скла класифікуються:

- електроконтактні датчики – сповіщають про порушення цілісності скляного полотна за допомогою механічної дії, наприклад удару або вирізання отвору;
- п'єзоелектричні датчики, що реєструють механічні коливання, що виникають при ударі скла;
- акустичні датчики, що реагують на звукові коливання, що видаються під час руйнування скла.

Датчики, що реагують на параметри довкілля. Дані пристрої використовуються для регулювання роботи інженерних систем та комунікацій будівель. Існує кілька типів даних датчиків:

- датчики температури;
- датчики рівня освітленості;

- датчики витоку газу;
- датчики протікання води;
- протипожежні датчики (датчики задимлення, датчики температури);
- датчики тиску води, газу;
- датчики дощу та атмосферних опадів;
- датчики – індикатори вогкості/вологості;
- комбіновані.

Всі типи цих датчиків знімають показання навколишнього середовища та передають інформацію про неї в систему «розумного будинку». Перераховані вище датчики можуть передавати цю інформацію по різних каналах зв'язку, як провідним, так і бездротовим, використовуючи різноманітні протоколи передачі інформації.

В цілому для всіх перелічених типів датчиків характерні вразливості, пов'язані з обмеженням конструкції датчиків, які використовуються фізичними принципами, неправильною установкою.

Уразливості проявляється у зв'язку з впливом наступних факторів:

- електромагнітного випромінювання;
- електричні перешкоди;
- акустичні перешкоди;
- перепади освітленості;
- перепади вологості;
- наявність у повітрі хімічних речовин;
- наявність у повітрі пилу та суспензій;
- екранування поля, що випромінюється активними датчиками та об'єктами в зоні виявлення.

Серед перерахованих загроз відсутні у явному вигляді загрози інформаційній безпеці. Проте, захист розглянутих датчиків у зв'язку з виділеними вразливістю необхідна, оскільки загроза імітації хибних спрацьовувань є закономірним наслідком реалізації розглянутих уразливостей і є спосіб впровадження в ІТ-систему «розумного будинку» хибної або зловмисно-спотвореної інформації [29].

Внаслідок цього при розробці та впровадженні прикладного та вбудованого програмного забезпечення в рамках ІТ-систем «розумного дому» слід передбачити програмні процедури перевірки працездатності та режиму функціонування датчиків та реалізувати механізм верифікації оброблюваних показань згідно з вимогами ДСТУ EN 62061:2014 «Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних із безпекою».

Усі параметри ІТ-системи, пов'язані з обробкою показань датчиків, які можуть бути змінені, повинні бути перевірені на захист:

- від помилкових, несумісних чи необґрунтованих значень;
- несанкціонованих змін;
- ушкодження даних.

2.4.2. Аналіз уразливостей та факторів, що впливають на виконавчі пристрої «розумного будинку»

Виконавчі пристрої призначені для перетворення керуючих (командних) сигналів у регулюючі на об'єкт управління. Сигнальна сирена, сервоприводи, що перекривають подачу води або газу, що відкривають вентиляційні вікна, різні силові реле і таймери - відносяться до виконавчих пристроїв. Розглянемо кілька цих пристроїв докладніше у тих аналізу загроз «розумному дому».

Електромагнітні клапани (рисунок 2.6) встановлюються на трубопроводах подачі води та газу для дистанційного керування відкриттям або закриттям потоку робочого середовища, як правило, рідини.



Рисунок 2.6 - Загальний вигляд електромагнітного клапана "Гідролок WINNER"

Варіанти застосування електромагнітних клапанів:

- 1) як аварійний кран у системі подачі води. У цьому випадку керування здійснюється від датчика, вмонтованого в підлогу і спрацьовує від попадання води;
- 2) в системі клімат-контролю електронний (електромагнітний) кран регулюватиме подачу гарячої води, залежно від температури у кімнаті (керівний сигнал подається від датчика температури у приміщенні);
- 3) електромагнітний клапан може використовуватись у системі поливу присадибної ділянки. Подача води здійснюватиметься відповідно до встановленого тимчасового графіка або від сигналу датчика вологості;

4) також є електромагнітні клапани для установки на трубопроводах подачі газу. Такий клапан, підключений до датчика загазованості, перекриє подачу газу при аварійній ситуації [30].

Вразливістю є можливість виведення датчика із ладу шляхом зовнішніх електромагнітних випромінювань.

Електромеханічні приводи відкриття/закриття воріт, хвірток, дверей (рисунок 2.7), вікон, жалюзі та штор тощо.



Рисунок 2.7 Загальний вигляд електромагнітного замку Samsung

Робота приводів може здійснюватися за сценарієм, наприклад, уночі – закриття жалюзі та приглушення світла; при постановці на сигналізацію – закриття всіх вікон та дверей, включення датчиків руху.

Вразливістю приводу є недостатній захист від механічних пошкоджень. Також уразливість таких приводів суттєво зростає при відключенні напруги електроживлення.

2.4.3. Аналіз уразливостей та факторів, що впливають на безпеку центральних пристроїв «розумного будинку»

Центральний пристрій «розумного будинку» координує всі його функції та керує всіма його компонентами. Як обчислювальна платформа центрального пристрою можуть виступати: персональні комп'ютери, ноутбуки, сервери, але найчастіше використовуються контролери різних типів. Завдання контролера полягає у збиранні інформації про функціонування обладнання, перевірку отриманих параметрів, пошук аварійно-функціонуючих пристроїв та виведення обробленої інформації на панель керування. Сьогодні на ринку представлена велика кількість контролерів для «розумного будинку» від різних фірм виробників, нижче

розглядаються типові контролери та їх вразливість.

Контролер виробництва фірми AMX NX-1200 (рисунок 2.8) створений для вирішення завдань управління та автоматизації невеликих систем «розумного будинку», цей контролер обладнаний дев'ятьма портами управління для підключення до чотирьох пристроїв у вигляді, наприклад, інфрачервоних датчиків (ІЧ) та одного послідовного пристрої сторонніх виробників, а також можуть підтримувати шину типу Ethernet [31].



Рисунок 2.8 – Загальний вигляд контролера AMX NX-1200

Вразливість даного контролера була виявлена експериментальним шляхом в ході перевірки процедури аутентифікації: дослідники виявили у внутрішній базі даних користувачів прихований адміністративний обліковий запис, для якого були задані логін і пароль. Отримавши доступ до цього облікового запису можна отримати контроль над пристроєм оскільки цей адміністративний обліковий запис дозволяє отримати доступ до web-консолі управління, а також інтерфейсу командного рядка і здійснювати різні дії, наприклад, перехоплення та заміну трафіку [30].

Інший типовий зразок, контролер фірми X10 MT10 [32] (рисунок 2.9), використовується для керування за часом електропобутовими та освітлювальними приладами в мережі X10 [33], підключається електропроводкою.



Рисунок 2.9 – Загальний вигляд контролера X10 MT10

Можливі наступні режими роботи приладу:

- автоматичний режим – контролер включає та вимикає електроприлади за заздалегідь введеною програмою;
- ручний режим – у будь-який момент можна безпосереднім натисканням кнопок на приладі керувати підключеними електроприладами;
- режим безпеки (імітація присутності господарів у будинку) – автоматичний режим з довільними моментами вмикання та вимкнення електроприладів у межах встановленого інтервалу часу.

Контролер уразливий при електромагнітних перешкодах чи розриві зовнішньої електропроводки, пропаданні електроживлення.

Контролер фірми Honeywell Tuxedo Touch (рисунок 2.10) забезпечує централізоване керування освітленням, термостатом, замками, камерами тощо використовуючи бездротову технологію Z-Wave [34].



Рисунок 2.10 – Контролер Honeywell Tuxedo Touch

У контролера є ряд уразливостей, які суттєво впливають на безпеку використання, у тому числі обхід автентифікації користувача та заміна міжсайтових запитів.

Як видно з наведених вище прикладів, центральні контролери «розумного будинку» схильні до різних видів уразливостей, реалізація яких може призвести до виведення з ладу фрагмента або всієї системи в цілому.

2.4.4. Аналіз уразливостей та факторів, що впливають на систему зв'язку «розумного будинку»

В даний час з усіх представлених на ринку технологій побудови ІТ-систем «розумний дім» можна виділити кілька готових до застосування комплексних систем, які є типовими представниками у своєму класі:

- централізовані, наприклад, системи фірми Creston;
- децентралізовані системи, наприклад, ЕІВ.

Також системи можна класифікувати на:

- провідні, наприклад, X10;
- бездротові, наприклад, Z-Wave.

На прикладі цих комплексних систем розглянемо основні фактори, що впливають на безпеку інформації «розумного будинку», що захищається, побудованого на основі готових систем.

Відповідно до [28], зазначені фактори поділяються на:

- 1) за ознакою ставлення до природи виникнення:
 - об'єктивні;
 - суб'єктивні.
- 2) стосовно об'єкта інформації:
 - внутрішні;
 - зовнішні.

Система управління будинком фірми Crestron – це централізована система керування. Як правило, вона будується на основі застосування широкого спектру керуючих центральних контролерів та безлічі виконавчо-командних блоків. Керуючі контролери Crestron мають великий набір вбудованих можливостей, сумісні з безліччю поширених протоколів передачі.

Для даної системи фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 2.10 та табл. 2.11.

Таблиця 2.10 Об'єктивні фактори, що впливають на безпеку інформації, що захищається централізованої системи управління «розумним будинком»

Внутрішні фактори	Зовнішні чинники
Випромінювання акустичних сигналів супутні вимовної технічним засобом (МС) мови	Збої, відмови та аварії систем забезпечення об'єкта інформації (ОІ)
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Термічні фактори (пожежі тощо)
Дефекти, збої та відмови, аварії ТЗ та систем обробки інформації	Кліматичні фактори (повені тощо)

Таблиця 2.11 Суб'єктивні фактори, що впливають на безпеку інформації, що захищається централізованої системи управління будинком

Внутрішні фактори	Зовнішні чинники
Розголошення інформації, що захищається особами, які мають до неї право доступу через передачу інформації по відкритих лініях зв'язку	Доступ до інформації, що захищається, із застосуванням ТЗ знімання інформації
Несанкціонований доступ до інформації шляхом підключення до технічних засобів та систем ОІ	Несанкціонований доступ до інформації, що захищається шляхом використання закладних засобів
Використання програмного забезпечення (ПЗ) технічних засобів ОІ через внесення програмних закладок	Блокування доступу до інформації, що захищається шляхом перевантаження ТЗ обробки інформації хибними заявками на її обробку

Система управління будинком EIB (European Installation Bus) – це децентралізована відкрита мережева технологія, підтримана десятками провідних компаній виробників електротехнічної продукції – членів європейської неурядової організації EIBA (European Installation Bus Association) (рисуюнок 2.11).

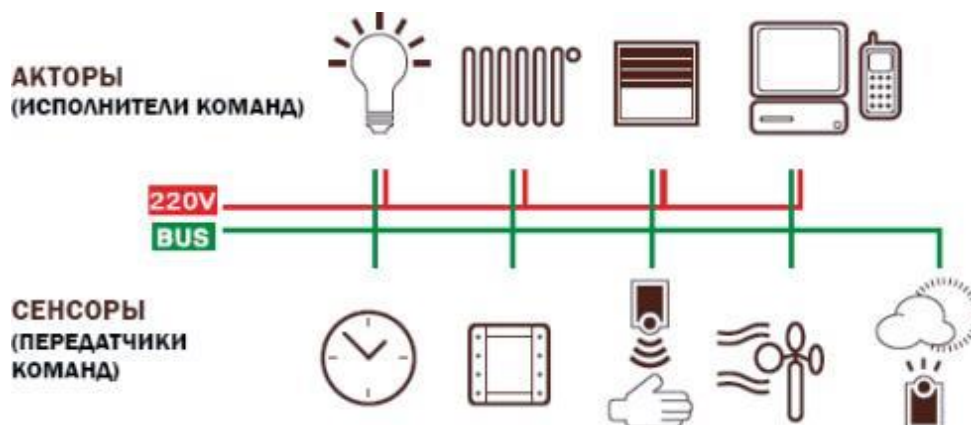


Рисунок 2.11 – Загальна схема підключення ЕІВ

Пристрої (передавачі або приймачі) в ЕІВ зв'язуються один з одним безпосередньо без ієрархії або центрального контролюючого приладу. Компоненти здійснюють передачу послідовно, асинхронно, конфлікти під час передачі повідомлень вирішуються розстановкою пріоритетів повідомлень. Призначена для передачі інформація збирається в пакети-телеграми і через шину передається приймачеві або групі приймачів. Повідомлення отримують усі абоненти, але реагують нею лише ті, кому воно адресовано. Сьогодні ЕІВ-протокол підтримує обмін по кручений парі, безпосередньо по силовій лінії, по радіо та по ІЧ-каналі. До децентралізованих систем відносяться такі готові системи, як Gira, Berker, Vticino, Vimar та ін [35].

Для систем з децентралізованим управлінням фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 2.12 та табл. 2.13.

Таблиця 2.12 Об'єктивні фактори, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком»

Внутрішні фактори	Зовнішні чинники
Дефекти, збої та відмови ПЗ	Збій, відмови та аварії систем забезпечення ОІ
Наведення в лініях зв'язку, викликані побічними електромагнітними випромінюваннями, що несуть інформацію	Термічні фактори (пожежі тощо)
Наявність акустоелектричних перетворювачів в елементах ТС ОІ	Кліматичні фактори (повені тощо)

Таблиця 2.13 Суб'єктивні фактори, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком»

Внутрішні фактори	Зовнішні чинники
Неправомірні дії з боку осіб, які мають право доступу до інформації, що захищається, шляхом несанкціонованої зміни інформації	Доступ до інформації, що захищається із застосуванням ТЗ технічної комп'ютерної розвідки
Недоліки організаційного забезпечення захисту інформації під час завдання вимог щодо захисту інформації	Спотворення, знищення або блокування інформації шляхом розкрадання носія інформації
Несанкціонований доступ до інформації шляхом внесення програмних закладок	Спотворення, знищення або блокування інформації шляхом використання програмних або програмно-апаратних засобів при здійсненні мережевої атаки

Система управління домом X-10 – міжнародний відкритий промисловий стандарт, який застосовується для зв'язку електронних пристроїв у системах домашньої автоматизації. Стандарт X10 визначає методи та протокол передачі сигналів керування електронними модулями, до яких підключені побутові прилади, з використанням звичайної електропроводки або бездротових каналів.

Мережа X10 включає такі основні компоненти: передавачі, приймачі, трансивери, пульти ДУ і лінійні компоненти [36]. Системам використовують провідні технології побудови системи «розумний дім» (зокрема стандарт X10) властиві фактори, що впливають на безпеку інформації, що захищається представлені в табл. 2.14 та табл. 2.15.

Таблиця 2.14 Об'єктивні фактори, що впливають на безпеку інформації проводової системи управління «розумним будинком», що захищається

Внутрішні фактори	Зовнішні чинники
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Ненавмисні електромагнітні опромінення ОІ
Наведення в електричних ланцюгах ТС викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Електромагнітні фактори (грозові розряди тощо)
Наведення в ланцюгах заземлення викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Кліматичні фактори (повені тощо)

Таблиця 2.15 Суб'єктивні фактори, що впливають на безпеку інформації проводової системи управління «розумним будинком», що захищається

Внутрішні фактори	Зовнішні чинники
Розголошення інформації, що захищається особами, які мають до неї право доступу через осіб, які не мають права доступу до інформації, що захищається	Доступ до інформації, що захищається із застосуванням ТЗ радіоелектронної розвідки
Несанкціонований доступ до інформації шляхом порушення функціонування ТЗ обробки інформації	Спотворення, знищення або блокування інформації шляхом навмисного електромагнітного впливу по мережі електроживлення
Помилки користувачів або обслуговуючого персоналу під час експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом навмисного силового впливу фізичної природи

Система управління будинком Z-Wave є запатентованим бездротовим протоколом зв'язку, розробленим для домашньої автоматизації, зокрема контролю та управління в житлових і комерційних об'єктах. Технологія використовує малопотужні та мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку та різні пристрої, такі як освітлювальні прилади, опалювальні прилади, пристрої контролю доступу, розважальні системи та побутову техніку. Більшість систем використовують бездротові канали зв'язку схильні до факторів, що впливають на безпеку інформації, що захищається, перерахованих у табл. 2.16 та табл. 2.17.

Таблиця 2.16 Об'єктивні фактори, що впливають на безпеку інформації бездротової системи управління «розумним будинком», що захищається

Внутрішні фактори	Зовнішні чинники
Електромагнітні випромінювання та поля в радіодіапазоні	Ненавмисні електромагнітні опромінення ОІ
Побічні електромагнітні випромінювання на частотах роботи височастотних генераторів пристроїв, що входять до складу ТЗ ОПІ	Радіаційні опромінення ОІ
Побічні електромагнітні випромінювання на частотах самозбудження підсилювачів пристроїв, що входять до складу ТЗ ОПІ	Природні явища, стихійні лиха

Таблиця 2.17 Суб'єктивні фактори, що впливають на безпеку інформації бездротової системи управління «розумним будинком», що захищається

Внутрішні фактори	Зовнішні чинники
Несанкціонований доступ до інформації шляхом підключення до ТЗ та систем ОІ	Доступ до інформації, що захищається із застосуванням ТЗ радіоелектронної розвідки
Розголошення інформації, що захищається особам, які не мають до неї право доступу	Доступ до інформації, що захищається шляхом використання шкідливого ПЗ
Помилки обслуговуючого персоналу під час експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом здійснення мережевої атаки

Таким чином розроблено систему суб'єктивних та об'єктивних факторів, що впливають на систему «розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного дому».

2.5. Аналіз загроз безпеки «розумного дому»

2.5.1 Загрози конфіденційності, цілісності та доступності інформації ІТ-системи «розумного дому»

Під загрозою безпеки інформації розумітимемо сукупність умов та факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. Під уразливістю розуміється властивість інформаційної системи, що зумовлює можливість реалізації загроз безпеці оброблюваної у ній інформації.

Базовими загрозами інформаційної безпеки «розумного дому» є:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності інформації.

У контексті аналізу «розумного будинку» під конфіденційністю мається на увазі такий стан ІТ-системи управління «розумним будинком», за якого відсутня можливість витоку інформації через підсистеми. Приклад реалізації небезпеки - витік персональної інформації або витік інформації про конфігурацію ІТ-систем «розумного будинку».

Цілісність інформації – це достовірність та повнота інформації, що отримується системою від різних датчиків і пристроїв, встановлених у системі, наприклад, при отриманні невірної інформації системою про наявність у приміщенні людини може призвести до помилкового спрацювання системи контролю доступу [37].

Доступність інформації стосовно «розумного будинку» – це стан інформації або ресурсів ІТ-системи, при якому суб'єкти або сама система, які мають права доступу, можуть реалізувати різні дії відповідно до сценарію роботи (вимикати/вмикати датчики, відкривати замки тощо). Приклад реалізації цієї небезпеки – виведення з ладу комунікаційного устаткування системи.

Відповідно до загрози інформаційної безпеки за природою виникнення можна розділити на 2 групи: загрози, зумовлені людським фактором та загрози середовища (природні).

Зокрема, загрози першої групи розрізняються за способом здійснення: цілеспрямовані (навмисні) та випадкові (ненавмисні). Деякі приклади таких загроз наведено у табл. 2.18, слід зазначити, що загрози другої групи (загрози середовища) не піддаються прогнозуванню і, як правило, під ними мають на

увазі природні катаклізми.

Таблиця 2.18 Класифікація загроз безпеки інформації ІТ-системи «розумного дому»

Загрози, зумовлені людським фактором		Загрози середовища
Цілеспрямовані	Випадкові	
Модифікація інформації	Помилки ПЗ	Пожежа
Перехоплення інформації	Помилки користувача	Затоплення
Викрадення обладнання	Помилки під час обслуговування	Блискавка
Хакерська атака	Апаратні відмови	Землетрус
Шкідливе програмне забезпечення (ПЗ)	Помилки маршрутизації	Екстремальні величини температури та вологості

Іншим істотним фактором для визначення загроз інформаційній безпеці є ідентифікація можливих джерел загроз залежно від їхнього розташування: внутрішні та зовнішні. До внутрішніх загроз відносяться загрози, розташовані всередині контрольованої зони, до зовнішніх – зовні (табл. 2.19). Більш повний список загроз можна знайти на сайті бази даних загроз безпеки інформації.

Таблиця 2.19 Приклади внутрішніх та зовнішніх загроз інформації ІТ-системи «розумного будинку»

Внутрішні загрози	Зовнішні загрози
Загроза впровадження коду чи даних	Загроза відключення (екранування) контрольних датчиків
Загроза використання механізмів розробника	Загроза спотворення інформації, що вводиться і виводиться на периферійні пристрої інформації
Загроза заміни програмного забезпечення	Загроза несанкціонованого віддаленого позасмугового доступу до апаратних засобів
Загроза доступу/перехоплення/зміни HTTP-cookies	Загроза подолання фізичного захисту
Загроза доступу до локальних файлів сервера за допомогою URL	Загроза міжсайтової підробки запиту

2.5.2. Оцінка ризиків інформаційної безпеки «розумного дому»

Загрози інформаційної безпеки ІТ-системи «розумний дім» в першу чергу залежать від обраних способів та технологій побудови даної системи, оскільки визначення можливих загроз впливає склад устаткування. Для оцінки ризиків інформаційної безпеки «розумного дому» розглянемо найімовірніші загрози, реалізація яких може призвести до порушення інформаційної безпеки «розумного дому», побудованого за централізованою технологією [38].

Далі виявлені загрози порівнюються з уразливістю, і визначається, які властивості активу (конфіденційність – К, цілісність – Ц, доступність – Д) можуть порушувати ті чи інші загрози (табл. 2.20).

Таблиця 2.20 Загрози та вразливості безпеки «розумного дому»

№	Загроза	Вразливість	Властивості, які загроза може порушити		
			К	Ц	Д
1	Атаки на центральний сервер	Підключення мережі «розумного дому» до Інтернету. Недостатня ефективність захисту мережі «розумного дому»	+	+	+
2	Впровадження шкідливого коду чи програми	Підключення мережі «розумного дому» до Інтернету. Відсутність (недостатня ефективність) механізмів захисту трафіку	+	+	+
3	Перехоплення та підміна переданого сигналу	Можливість доступу зловмисника до мереж передачі. Відсутність (недостатня ефективність) механізмів захисту трафіку	+	+	
4	Доступ до мережі нелегітимних користувачів	Відсутність (недостатня ефективність) механізмів автентифікації та ідентифікації	+		
5	Використання механізмів розробника	Відсутність (недостатня ефективність) механізмів автентифікації та ідентифікації	+	+	

Продовження таблиці 2.20

6	Тривале утримання обчислювальних ресурсів користувачами	Слабкі механізми балансування навантаження та розподілу обчислювальних ресурсів			+
7	Доступ до файлів, що захищаються з використанням обхідного шляху	Слабкості механізму розмежування доступу	+	+	
8	Вимкнення контрольних датчиків	Відсутність (недостатня ефективність) системи контролю доступу			+
9	Подолання фізичного захисту об'єкту	Уразливості у системі контролю фізичного доступу	+	+	+
10	Крадіжка апаратури або носіїв інформації	Незахищене зберігання	+	+	+
11	Знищення апаратури чи носіїв інформації	Відсутність (недостатня ефективність) системи фізичної охорони об'єкта		+	+
12	Несправності у системі електропостачання	Відсутність системи автономного живлення. Чутливість до перепадів напруги			+
13	Помилки користувача	Відсутність механізмів моніторингу. Складний інтерфейс користувача		+	+
14	Помилки ПЗ	Використання неліцензійного програмного забезпечення.			+
15	Стихійні лиха	Відсутність (недостатня ефективність) системи фізичної охорони об'єкта		+	+

Для оцінки ризиків скористаємося методикою оцінки ризиків корпорації "Microsoft". Для цього складемо зведену таблицю, в якій оцінимо (таблиця 2.21):

– ймовірність реалізації загрози виходячи з частоти її реалізації за певний період, де висока – ймовірність реалізації однієї чи кількох загроз у межах року, середня – виникнення загрози в межах 2-3 років, та низька – поява загрози протягом 3 років малоімовірна;

– рівень схильності до впливу, за наступною шкалою: високий – значний або повний збиток для активу, середній – середній або обмежений збиток, низький – незначний збиток (відсутність);

Таблиця 2.21 Визначення рівня впливу

Клас активу	Високий вплив (ВВ)	Середній	Високий	Високий
	Середній вплив (СВ)	Низький	Середній	Високий
	Низький вплив (НВ)	Низький	Низький	Середній
		Низький	Середній	Високий
		Рівень схильності до впливу		

Підсумковий рівень ризику визначається відповідно до табл. 2.22.

Таблиця 2.22 Визначення підсумкового ризику

Вплив (див. табл. 2.21)	Високий	Середній	Високий	Високий
	Середній	Низький	Середній	Високий
	Низький	Низький	Низький	Середній
		Низький	Середній	Високий
		Рівень ймовірності реалізації загрози		

– клас активу відповідно до табл. 2.20 де високий вплив – вплив на КІД інформації завдає значних або фатальних збитків для організації (власникам), середні – середні або обмежені збитки, низькі – незначні збитки або його відсутність.

В результаті отримаємо таблицю для якісної оцінки рівня ризиків системи розумний будинок (табл. 2.23).

Таблиця 2.23 Рівень ризику для загроз «розумного дому»

№	Загроза	Ймовірність реалізації	Рівень схильності до впливу	Клас активу	Рівень ризику
1	Атаки на центральну північ	Висока	Високий	Високий	Високий
2	Впровадження шкідливого коду чи програми	Висока	Високий	Високий	Високий
3	Перехоплення та підміна переданого сигналу	Висока	Середній	Середній	Високий
4	Доступ до мережі нелегітимних користувачів	Висока	Середній	Середній	Середній
5	Використання механізмів розробника	Висока	Високий	Середній	Високий
6	Тривале утримання обчислювальних ресурсів користувачами	Висока	Середній	Низький	Середній
7	Доступ до файлів, що захищаються з використанням обхідного шляху	Середня	Середній	Середній	Середній
8	Вимкнення контрольних датчиків	Висока	Середній	Середній	Високий
9	Подолання фізичного захисту об'єкту	Середня	Високий	Високий	Високий
10	Крадіжка апаратури або носіїв інформації	Низька	Високий	Високий	Середній
11	Знищення апаратури чи носіїв інформації	Низька	Високий	Високий	Середній
12	Несправності у системі електропостачання	Середня	Середній	Середній	Середній
13	Помилки користувача	Середня	Середній	Середній	Середній
14	Помилки ПЗ	Середня	Середній	Середній	Середній
15	Стихійні лиха	Низька	Високий	Високий	Середній

На основі результатів оцінки ризиків найбільш небезпечними загрозами є:

- атаки на центральний сервер;
- впровадження шкідливого коду чи програми;
- перехоплення та підміна переданого сигналу;
- використання механізмів розробника;
- відключення контрольних датчиків;
- подолання фізичного захисту об'єкта

Також небезпечними є ризики, пов'язані з несправностями у роботі систем електроживлення та помилками користувача та/або програмного забезпечення.

У зв'язку з цим необхідне застосування таких захисних заходів для зниження ризиків, пов'язаних з реалізацією даних загроз:

- 1) застосування механізмів ідентифікації та аутентифікації користувачів;
- 2) застосування механізмів шифрування та контролю цілісності переданих даних;
- 3) використання антивірусного ПЗ;
- 4) організація системи контролю керування доступом;
- 5) використання механізмів розподілу навантажень;
- 6) періодична перевірка працездатності всіх елементів;
- 7) використання резервного джерела живлення.

РОЗДІЛ 3. ОГЛЯД ТА ВИБІР ЗАСОБІВ ДЛЯ УПРАВЛІННЯ РОЗУМНИМ БУДИНКОМ

3.1 Огляд та вибір мікроконтролерів

Комп'ютери вже давно стали частиною нашого життя. Але не всі люди здогадуються про існування ще інших пристроїв, що схожі за функціоналом на звичні нам комп'ютери і вони мають назву мікроконтролери.

Мікроконтролерні системи зараз майже всюди, починаючи від побутових приладів до автомобілів і т.д.. ще мікроконтролери використовуються у різних інноваційних пристроях, наприклад в квадрокоптерах чи таких системах, як «*Smart Home*», або ж навіть у роботизованих системах.

Arduino – це мала плата з процесором, що по потужності може зрівнятися з комп'ютерами кінця 90-х років. Ця плата має певний набір контактів в залежність від модифікації, до яких можна підключати будь-які пристрої: сервомотори, лампи (світлодіоди), сенсори, роутери, динаміки та інші модулі. Щоб керувати даною платою, слід просто запрограмувати її через спеціальну програму і потім завантажити її на плату через *USB*.

Платформа користується величезною популярністю в усьому світі завдяки зручності і простоті мови програмування, а також відкритій архітектурі і програмного коду.

Пристрої на базі *Arduino* можуть отримувати інформацію про навколишнє середовище за допомогою різних датчиків, а також можуть управляти різними виконавчими пристроями, що досить актуально в наш час.

Для реалізації дистанційного керування освітленням необхідні апаратно-програмні засоби, які будуть обробляти сигнал, що надходить з датчиків або камери, а потім подавати сигнал на виконавчі пристрої. Як такі апаратно-програмні засоби розглянемо продукти розробників *Arduino Software* і *Raspberry Pi Foundation*.

Плати *Arduino* стали одними з найпопулярніших мікроконтролерів на ринку з величезною різноманітністю плат. Деякі плати *Arduino* найкраще підходять для певних застосувань. Порівняємо деякі з найпопулярніших плат, створених *Arduino*. Uno, Micro та Mega 2560, рисунок 3.1 та 3.2.

					КНУ.РМ.123.22.12.03.ОВЗ			
Змн.	Арк.	№ документа	Підпис	Дата				
Розробив	Просяник				ОГЛЯД ТА ВИБІР ЗАСОБІВ ДЛЯ УПРАВЛІННЯ РОЗУМНИМ БУДИНКОМ		Літера	Аркуш
Перевірів	Кузнецов							
Н.контроль	Кузнецов						КІ-21м	
Затвердив	Купін							



Рисунок 3.1 – Плата Arduino Mega 2560

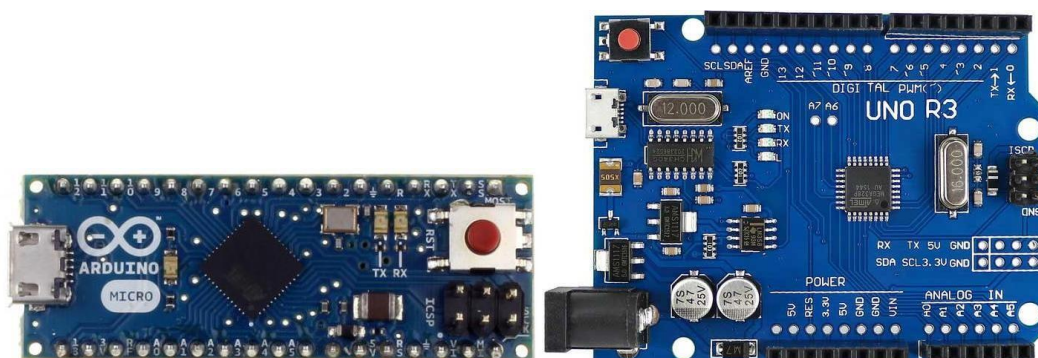


Рисунок 3.2 – Плати Arduino Micro та Arduino Uno R3

Розмір Arduino Micro входить до його переваг 1.8 x 4.8 см, що робить його однією з найменших плат мікроконтролерів. На протилежному боці спектру Mega 2560 становить близько 10 x 5 см. Десь посередині Uno, що мають розміри 5 x 2.5 см. Ціна для Micro зазвичай становить близько 19-25 доларів, а Uno - близько 20-23 доларів, а Mega 2560 - 36 доларів.

Для підключення до комп'ютера та початку написання коду, Uno та Mega 2560 можуть бути легко підключені за допомогою стандартного кабелю USB A/B, у той час як Micro знадобиться кабель Micro-USB.

Кожен із цих Arduino має різну кількість контактів вводу/виводу. Плата з найбільшою кількістю контактів - Mega 2560, яка поставляється з колосальними 54 цифровими контактами вводу/виводу (з них 15 мають PWM) і має 16 вхідних аналогових контактів. Дивно, але Micro друга плата серед трьох за кількістю контактів має 20 цифрових входів/виходів (з 7 з них з PWM) і 12 вхідних аналогових контактів. Uno має 14 цифрових входів/виходів (з 6 з них з PWM) та 6 вхідних аналогових контактів.

Всі три плати Arduino мають власний рівень обчислювальної потужності, тому розглянь докладніше їхню частоту/тактову частоту. Частота/тактова частота цих платах просто означає, наскільки швидко може

виконувати команди. Приємно дивує, що вони мають однакову тактову частоту на частоті 16 МГц, таблиця 3/1.

Флеш-пам'ять на Uno та Micro однакова – 32 КБ, а Mega 2560 має 256 КБ, що дає їй у 8 разів більший простір пам'яті. Флеш-пам'ять просто означає, наскільки великий скетч/код можна завантажити в Arduino, тому якщо код має великий розмір, тоді вибір за Mega 2560.

Плати Arduino використовують статичний оперативний пристрій (SRAM (Static Random-Access Memory)). Mega 2560 має найбільший простір СОЗУ 8 КБ, що у 4 рази більше, ніж у Uno, та у 3,2 рази більше, ніж у Micro. З великою кількістю простору СОЗУ Arduino більше простору для створення і управління змінними при запуску.

У таблиці нижче показано порівняння специфікацій Arduino Uno, Mega 2560 та Micro.

Таблиця 3.1 - Порівняння мікроконтролерів Arduino Uno, Micro та Mega 2560

Назва	Uno	Micro	Mega 2560
Процесор	ATmega328P	ATmega32U4	ATmega2560
Робоча/Вхідна напруга	5 V / 7-12 V	5 V / 7-12 V	5 V / 7-12 V
Тактова частота	16 MHz	16 MHz	16 MHz
Аналогові In/Out	6/0	12/0	16/0
Цифрові IO/PWM	2	43301	54/15
EEPROM [КБ]	1	1	4
SRAM [КБ]	2	43222	8
Flash [КБ]	32	32	256
USB	Regular	Micro	Regular
УАБП	1	1	4
WIFI	Hi (Shield)	Hi	Hi (Shield)
Bluetooth LE			
Ethernet			

Звідси можна зробити висновок, що у разі необхідності компактності проекту, у відсутності необхідності великої кількості контактів введення-виведення, наявності бюджету на мікроконтролер цінової категорії вище середньої, та відсутності цілей додавання будь-яких розширювальних плат, вибір за Arduino Micro.

Якщо є великий обсяг коду, потрібно багато контактів введення-виведення для проекту і необхідно, щоб у нього була встановлена розширювальна плата, тоді вибір Arduino Mega 2560.

Якщо потрібно розробляти невеликий проект, є цілі додавання розширювальної плати, маленький бюджет, то вибір за Arduino Uno.

Для керування реле освітлення кількох ламп в умовах обмеженості бюджету вибір падає на Arduino Uno

Тепер необхідно визначити вибір порівняння продуктів розробників Arduino Software та Raspberry Pi Foundation.

Arduino Uno і Raspberry Pi 3 є популярним вибором, коли йдеться про DIY, IoT або просто цікаві інженерні проекти. Вони можуть використовуватися для прототипування та реальних інженерних рішень. Розглянемо кожну плату.

Обидві плати виглядають однаково, але кожна має свою власну категорію. Raspberry Pi 3 це одноплатний комп'ютер (SBC). Це означає, що плата є повністю функціональним комп'ютером з власним виділеним процесором, пам'яттю і може запускати операційну систему (працює на Linux). Raspberry Pi 3 включає власні USB-порти, аудіовихід і графічний драйвер для виходу HDMI, що показує, як він може запускати кілька програм. Ви можете навіть встановити інші операційні системи, включаючи Android, Windows 10 або Firefox.

Arduino Uno Rev 3 це мікроконтролер. Мікроконтролери не такі сильні, як SBC, але вони можуть бути хороші для швидкого встановлення. Мікроконтролери чудові при керуванні невеликими пристроями (такими як світлодіоди, двигуни, кілька різних типів датчиків), але не можуть працювати з повною операційною системою. Arduino Uno запускає одну програму за один раз.

Raspberry Pi 3 може підключатися до пристроїв Bluetooth та інтернету прямо з коробки за допомогою Ethernet або через підключення до Wi-Fi. Arduino Uno не може зробити це без плати розширення (Shield), яка додає з'єднання з Інтернетом або Bluetooth. Плати розширення (HAT (Hardware Attached on Top)) та Shields допомагають у цьому.

HAT і Shields мають по суті одну й ту саму мету, додаючи додаткову або спрощуючу функціональність. HAT можна використовувати на Raspberry Pi 3 де деякі HAT включають Pi для управління матрицею RGB, додаючи сенсорний екран.

Shields, які можуть використовуватися на Arduino Uno, включають релейну плату, плату сенсорного екрана або Bluetooth-плату. Існують сотні Shields та HAT, які забезпечать функціональність, яку ви регулярно використовуєте.

Raspberry Pi 3 також має порт HDMI, аудіо порт, 4 порти USB, порт камери та порт LCD, що робить його ідеальним для мультимедійних програм. Arduino Uno не має жодного з цих портів на платі (хоча деякі з них можуть бути додані через Shields).

Для початку розглянемо сильні сторони Raspberry Pi 3. Оскільки це міні-комп'ютер, він може працювати в багатозадачному режимі з кількома програмами з однокристальною системою Broadcom BCM2837, а це означає, що створення складного проекту, для якого необхідно кілька дій в один час, можливо обробити без високого навантаження процесор.

Raspberry Pi 3 також набагато швидше, ніж Arduino (1,2 ГГц порівняно з 16 МГц), що дає можливість виконувати щоденні завдання, які роблять комп'ютери - відтворення відео, перегляд в інтернеті, прослуховування музики і т.д. Це робить Raspberry Pi 3 простим вибором, якщо необхідно використовувати його для медіа центрів.

Більш спрощений підхід Arduino Uno може бути привабливішим, коли йдеться про створення проекту. Arduino Uno спрощує взаємодію з аналоговими датчиками, двигуном або іншими компонентами, тоді як Raspberry Pi 3 складніший шлях для отримання показань датчика (наприклад, встановлення бібліотек, програмного забезпечення та підключення до монітора/клавіатури/миші).

Arduino також можна просто підключити, і він одразу почне виконувати свій код, тому немає необхідності в установці. Це робить Arduino Uno відмінним вибором, якщо необхідно почати розробку досліду зразу і потрібно прочитати набір даних і зробити одну дію на основі цих даних. Нижче наведено таблицю 3.2 порівняння характеристик сімейства одноплатних комп'ютерів Raspberry Pi.

Таблиця 3.2 - Порівняння характеристик сімейства Raspberry Pi

Найменування	Модель A	Модель A+	Модель B+	RPi2	RPi3
Пам'ять/для	MicroSD	MicroSD	MicroSD	MicroSD	MicroSD
ОС					
ОЗУ	256 MB SDRAM / 400 MHz	256 MB SDRAM / 400 MHz	512 MB SDRAM / 400 MHz	1GB SDRAM / 400 MHz	1GBSDRAM / 400 MHz
Найменування	Модель A	Модель A+	Модель B+	RPi2	RPi3

Продовження таблиці 3.2

Процесор	Broadcom BCM2835 32bit ARMv6 SoC full HD, одне ядро.	Broadcom BCM2835 32bit ARMv6 SoC full HD, одне ядро.	Broadcom BCM2835 32bit ARMv6 SoC full HD, одне ядро.	Broadcom BCM2836 32bit ARMv7, чотири ядра.	Broadcom BCM2837 64bit ARMv8, чотири ядра.
Швидкість процесора	700 МГц	700 МГц	700 МГц	900 МГц	1.25 ГГц
живлення	1.2 A/5 V	1.8 A/5 V	1.8 A/5 V	1.8 A/5 V	2.5 A/5 V
USB 2.0	1 x USB Port	1 x USB Port	4 x USB Ports	4 x USB Ports	4xUSB Ports
GPU	Videocore IV	Videocore IV	Videocore IV	Videocore IV	Videocore IV
GPIO	26 pin	40 pin	40 pin	40 pin	40 pin
WIFI	Hi	Hi	Hi	Hi	Вбудований
Найменування	Модель А	Модель А+	Модель В+	RPi2	RPi3
Bluetooth LE	Hi	Hi	Hi	Hi	Вбудований
Ethernet	Hi	Hi	Так	Так	Так

Якщо проект, що включає кілька функціональних можливостей одночасно, потрібен легкий доступ до Інтернету і потрібні можливості для доступу до мультимедіа, то вибір за Raspberry Pi 3.

Якщо проект вимагає легкого зчитування з датчиків, який повинен виконувати лише кілька вихідних сигналів на основі даних датчика, легко обмінюватися даними з іншими частинами машини і швидко запускатися практично без будь-якої іншої попередньої установки, тоді вибір за Arduino Uno.

3.1.1 Мікроконтролер *Arduino Nano*

Arduino Nano - цей повнофункціональний мініатюрний пристрій на базі мікроконтролера *ATmega328* (*Arduino Nano 3.0*) або *ATmega168* (*Arduino Nano 2.x*) (рисунок 3.3), адаптований для використання з макетними платами.

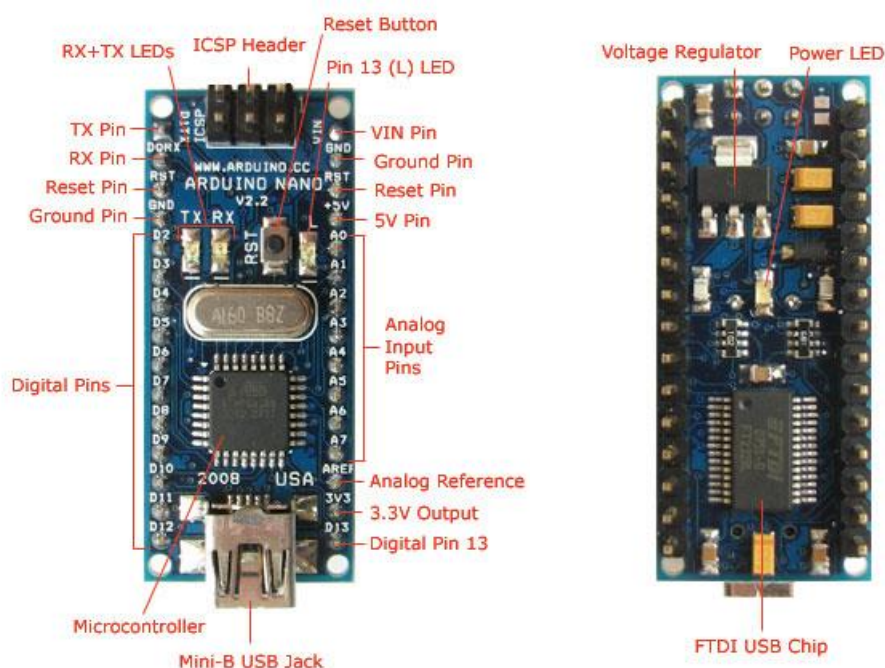
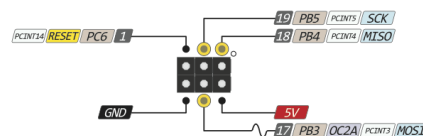


Рисунок 3.3 - Зовнішній вигляд мікроконтролера *Arduino Nano*



Напруга на мікросхемі *FTDI FT232RL* подається тільки у разі живлення *Arduino Nano* через *USB*. Тому при живленні пристрою від інших зовнішніх джерел (не *USB*), вихід 3.3В (сформований мікросхемою *FTDI*) буде неактивний, внаслідок чого світлодіоди *RX* і *TX* можуть мерехтати за наявності високого рівня сигналу на виходах 0 і 1.

Об'єм пам'яті програм мікроконтроллера *ATmega168* складає 16 КБ (з них 2 КБ використовуються завантажувачем); у *ATmega328* - цей об'єм складає 32 КБ (з яких 2 КБ також відведені під завантажувач). Окрім цього, *ATmega168* має 1 КБ оперативної пам'яті *SRAM* і 512 байт *EEPROM* (для взаємодії з якою служить бібліотека *EEPROM*); а мікроконтроллер *ATmega328* - 2 КБ *SRAM* і 1 КБ *EEPROM*.

З використанням функцій *pinMode ()*, *digitalWrite ()* і *digitalRead ()* кожний з 14 цифрових виходів *Arduino Nano* може працювати входом або виходом. Робоча напруга виходів - 5В. Максимальний струм, який може віддавати або споживати одне виведення, складає 40 мА. Усі виходи зв'язані з внутрішніми підтягуючими резисторами номіналом 20-50 кОм. Окрім основних, деякі виходи *Arduino* можуть виконувати додаткові функції(рисунок 3.4).

Послідовний інтерфейс: вихід 0 (RX) і 1 (TX). Вони використовуються для отримання (RX) і передачі (TX) даних через послідовний інтерфейс. Ці виходи підключені до відповідних виходів мікросхеми перетворювача USB-UART FTDI.

ШІМ: виходи 3, 5, 6, 9, 10 і 11. Використовуючи функцію *analogWrite ()*, 8-битні аналогічні значення можуть бути відображені як ШІМ-сигнал.

Інтерфейс *SPI* : вихід 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). Дані виводи здійснюють зв'язок за допомогою інтерфейсу *SPI*. У пристрої реалізована апаратна підтримка *SPI*.

I2C: виходи 4 (SDA) і 5 (SCL). З використанням бібліотеки *Wire* ці виходи можуть здійснювати прийом та передачу інформації по інтерфейсу *I2C (TWI)* [3].

3.1.2 Мікроконтролер *Arduino Uno*

Arduino Uno - цей пристрій на основі мікроконтроллера *ATmega328* (Рисунок 3.5). До його складу входять всі необхідні для зручної роботи з мікроконтроллером: 14 цифрових входів/виходів (з них 6 можуть використовуватися як ШІМ-виходи), 6 аналогових входів, кварцевий резонатор на 16 МГц, роз'єм *USB*, роз'єм живлення, роз'єм для внутрішньосхемного програмування (*ICSP*) і кнопка скидання(рисунок 3.6).

Відмінність *Arduino Uno* від інших плат є те, в якості перетворювача інтерфейсів *USB - UART* використовується мікроконтроллер *ATmega16U2* (*ATmega8U2* до версії R2) замість мікросхеми *FTDI*.

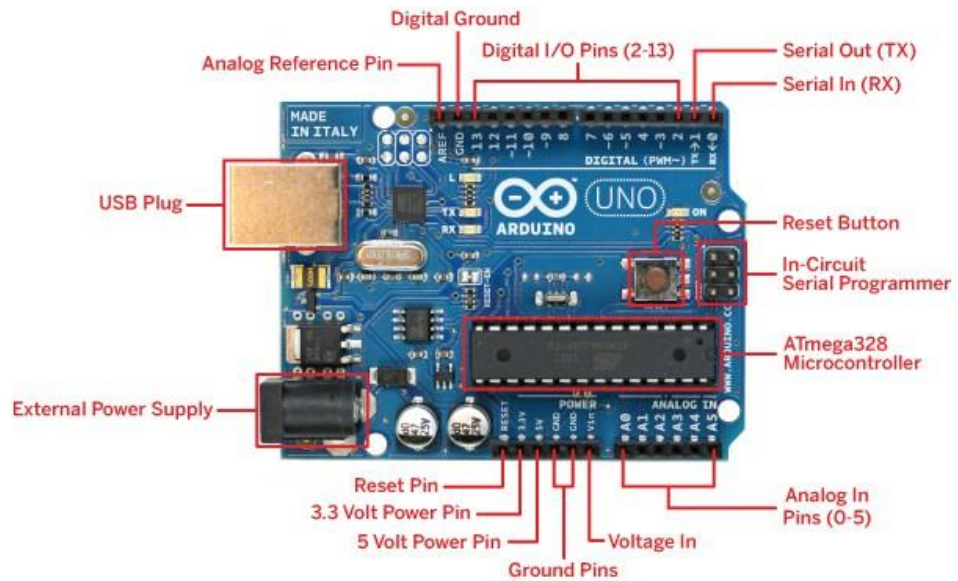


Рисунок 3.5 - Зовнішній вигляд мікроконтролера *Arduino Uno*

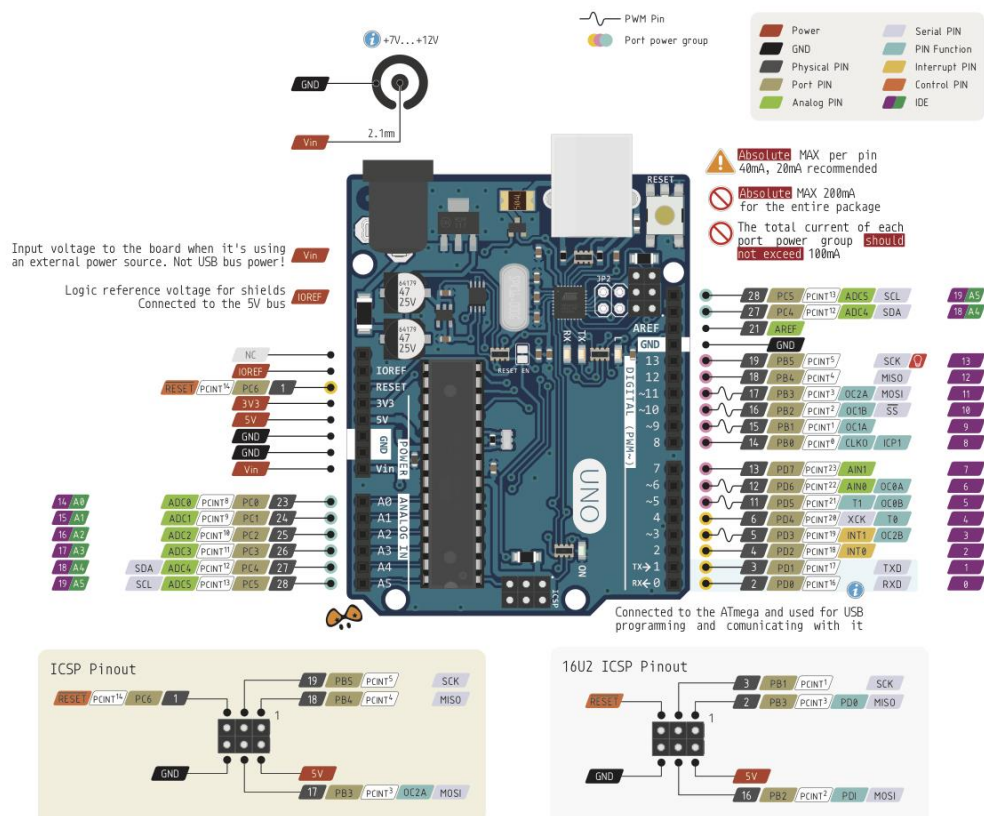


Рисунок 3.6 - Входи/виходи мікроконтролера *Arduino Uno*

Характеристики мікроконтролера *Arduino Uno*:

- Мікроконтроллер - *ATmega328*;
- Робоча напруга - 5В;
- Напруга живлення (рекомендована) - 7-12В;
- Напруга живлення (гранична) - 6-20В;

- Цифрові входи/виходи - 14 (з них 6 можуть використовуватися як ШИМ-виходи) ;
- Аналогові входи - 6;
- *Flash*- пам'ять 32 КБ (*ATmega328*) з яких 0.5 КБ використовуються завантажувачем;
- *SRAM* 2 КБ (*ATmega328*) ;
- *EEPROM* 1 КБ (*ATmega328*) ;
- Тактова частота 16 МГц.

Arduino Uno може працювати від *USB* або від зовнішнього джерела, наприклад, від блоку живлення. Живлення - тип джерела вибирається автоматично.

Напруга зовнішнього джерела живлення може бути в межах від 6 до 20 В. Проте, зменшення напруги живлення нижче 7 В призводить до зменшення напруги на виведенні 5v, що може стати причиною роботи з перебоями. Напруга більше ніж 12В може призвести до перегрівання стабілізатора напруги і виходу плати з ладу. З урахуванням цього, рекомендується використати джерело зовнішнього живлення з напругою в діапазоні від 7 до 12В.

У *Arduino Uno* є 6 аналогових входів (A0 - A5), кожен з яких може представити аналогову напругу у вигляді 10-бітового числа (1024 різні значення). Стандартно, вимірювання напруги на платі здійснюється відносно діапазону від 0 до 5 В. Проте, верхню межу цього діапазону можна змінити, використовуючи виведення *AREF* і функцію *analogReference ()*. Окрім цього, деякі з аналогових входів мають додаткові функції, зокрема *TWI* (*I2C*): виведення A4 або *SDA* і виведення A5 або *SCL*. З використанням бібліотеки *Wire* ці виведення можуть здійснювати зв'язок по інтерфейсу *TWI*.

Окрім перерахованих на платі існує ще декілька виведень:

1. *AREF*. Опорна напруга для аналогових входів. Може задіюватися функцією *analogReference ()*.
2. *Reset*. Формування низького рівня (*LOW*) на цьому виведенні приведе до перезавантаження мікроконтролера. Зазвичай це виведення служить для функціонування кнопки скидання на платах розширення [2].

3.2. Огляд та вибір датчиків

3.2.1 Ультразвуковий датчик відстані *Arduino HC - SR04*

Ультразвукові датчики відстані *Arduino* дуже популярні в робототехнічних проектах через свою відносну простоту, досить непогану точність і доступність. Вони можуть бути використані як прилади, що допомагають об'їжджати перешкоди, отримувати розміри предметів, моделювати карту приміщення і сигналізувати про наближення або видалення об'єктів. Одним з поширених варіантів такого пристрою є датчик

відстані, в конструкцію якого входить ультразвуковий далекомір *HC SR04* (рисунок 3.7).

Здатність ультразвукового датчика визначати відстань до об'єкту ґрунтується на принципі сонара - посилаючи пучок ультразвуку, і отримуючи його відображення із затримкою, пристрій визначає наявність об'єктів і відстань до них. Ультразвуковий сигнал, що генерується приймачем, відбивається від перешкоди і повертається до перешкоди через певний час. Саме цей часовий інтервал стає тією характеристикою, яка допомагає визначити відстань до об'єкта.

Датчик відстані *Arduino* є приладом безконтактного типу, і забезпечує високоточний вимір і стабільність. Діапазон дальності його виміру складає від 2 до 400 см. Електромагнітне випромінювання та сонячна енергія суттєво не впливають на його роботу [39].

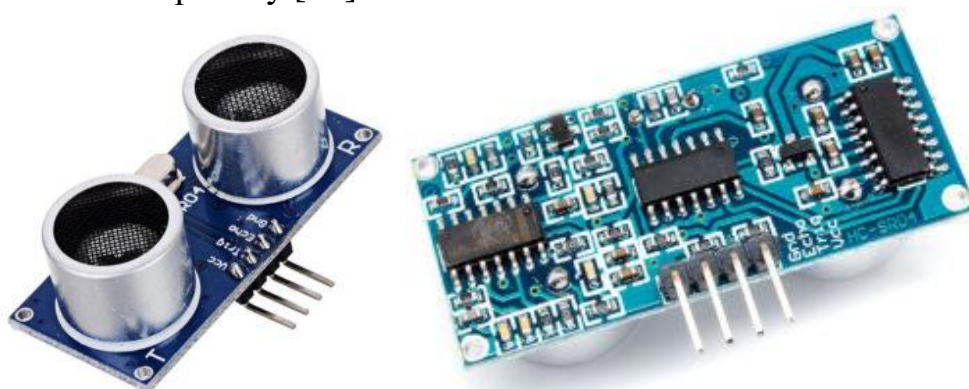


Рисунок 3.7 - Зовнішній вигляд *Arduino HC - SR04*

Ультразвуковий далекомір *HC SR04* має такі технічні параметри:

- Живляча напруга 5В;
- Робочий параметр сили т ока - 15 мА;
- Сила струму в пасивному стані < 2 мА;
- Оглядовий кут - 15°;
- Сенсорний дозвіл - 0,3 см;
- Вимірювальний кут - 30°;
- Ширина імпульсу - 10-6 с.
- Датчик оснащений чотирма виведеннями (стандарт 2, 54 мм) :
- Контакт живлення позитивного типу - 5В;
- *Trig* (T) - вихід сигналу входу;
- *Echo* (R) - виведення сигналу виходу;
- *GND* - виведення "Земля".

3.2.2 Інфрачервоний датчик руху *HC - SR501*

Модуль датчика руху (чи присутності) *HC-SR501* (рисунок 3.9) на основі піроелектричного ефекту складається із *PIR*- датчика з додатковою електричною розв'язкою на мікросхемі *BISS0001* і лінзи Френеля (рисунок

3.8), яка використовується для збільшення радіусу огляду і посилення інфрачервоного сигналу. Модуль використовується для виявлення руху об'єктів, випромінюючих інфрачервоне випромінювання. Чутливий елемент модуля - *PIR*- датчик 500bp. Принцип його роботи ґрунтований на піроелектриці. Це явище виникнення електричного поля в кристалах при зміні їх температури.

Управління роботою датчика здійснює мікросхема *BISS0001*. На платі розташовані два потенціометри, за допомогою першого налаштовується дистанція виявлення об'єктів (від 3 до 7 м), за допомогою другого - затримка після першого спрацювання датчика (5 - 300 сек). Модуль має два режими - *L* і *H*. Режим роботи встановлюється за допомогою перемички. Режим *L* - режим одиничного спрацювання, при виявленні об'єкту, що рухається, на виході *OUT* встановлюється високий рівень сигналу на час затримки, встановлений другим потенціометром. Цей режим можна використати в системах охорони для подання сигналу тривоги на сирену. У режимі *H* датчик спрацює кожного разу при виявленні руху. Цей режим можна використовувати для включення освітлення. При включенні модуля відбувається його калібрування, тривалість калібрування приблизно одна хвилина, після чого модуль готовий до роботи. Встановлювати датчик бажано далеко від відкритих джерел світла [40].



Рисунок 3.8 - Лінза Френеля

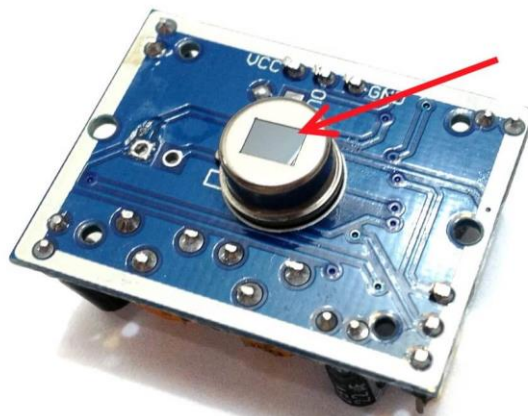


Рисунок 3.9 - Інфрачервоний датчик руху *HC* - *SR501*

Технічні характеристики *HC* - *SR501*:

- Напруга живлення : 4.5-20 В;
- Струм споживання : 50 мА;

- Напруга на виході *OUT* : *HIGH* - 3,3 В, *LOW* - 0 В;
- Інтервал виявлення : 3-7 м;
- Тривалість затримки після спрацьовування: 5 - 300 сек;
- Режим роботи : *L* - поодинокі спрацьовування, *H* - спрацьовування при кожній події;

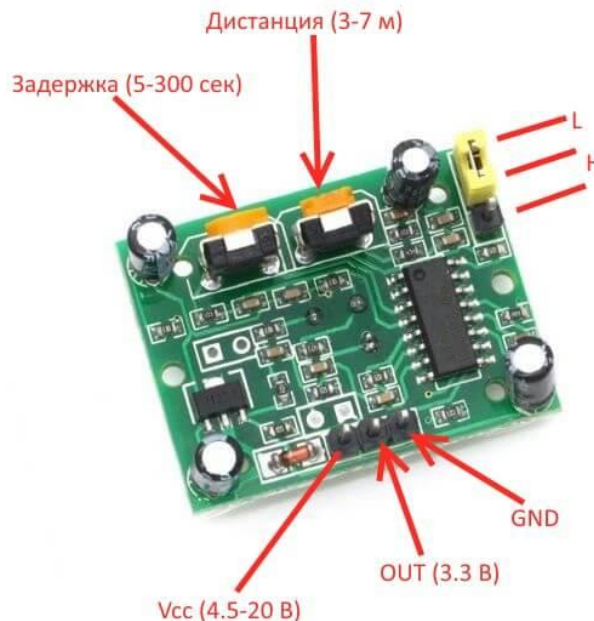


Рисунок 3.10 - Входи/виходи датчика руху *HC - SR501*

Модуль має 3 виходи (рисунок 3.10) :

- *VCC* - живлення 5-20 В;
- *GND* - земля;
- *OUT* - цифровий вихід (0-3.3В).

3.2.3 Датчик вологості та температури *DHT22*

Датчик складається з двох частин: ємнісного датчика температури та гігрометра (рисунок 3.11). Перший використовується для виміру температури, другий, - для вологості повітря. Мікросхема в середині може виконувати аналого-цифрове перетворення та виводити цифровий сигнал, який зчитується мікроконтролером.



Рисунок 3.11 - Датчик температури та вологості *DHT22*

Характеристики датчика температури та вологості *DHT22*:

- Живлення - від 3 до 5 Вольт;
- Максимальний струм при перетворенні - 2,5 мА;
- Здатний вимірювати вологість в інтервалі від 0 до 100%
- Точність вимірів коливається від 2 до 5%
- Минимальная вимірювана температура - мінус 40, максимальна - 125 градусів за Цельсієм (точність вимірів - 0,5);
- Пристрій здатний здійснювати один вимір 2 секунд. Частота - до 0,5 Гц;

Датчик температури і вологості *DHT22*, як і його аналог, має один цифровий вихід, відповідно знімати свідчення можна не частіше, ніж один раз в 1-2 секунди [41].

3.3 Огляд та вибір модулів *Arduino*

3.3.1 Модуль *Bluetooth HC-06*

Нерідко в проектах виникає необхідність дистанційного керування або передачі даних з телефону або іншого пристрою. Одним з найпопулярніших і зручніших способів є обмін даних через *Bluetooth*. Для зв'язку плати *Arduino* і комп'ютера використовується інтерфейс *UART (Serial)*. Оскільки будь-яка плата *Arduino* має хоч би 1 послідовний порт *UART*, для підключення *Bluetooth* модуля не потрібно спеціалізовані бібліотеки і схеми [4].

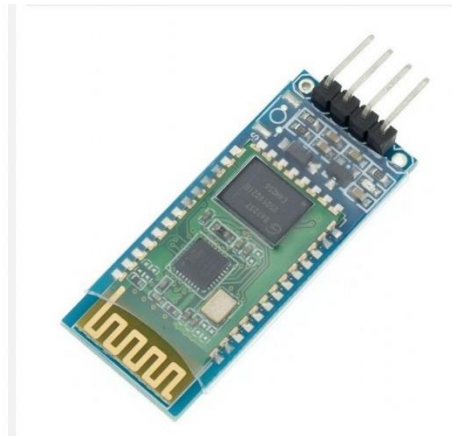


Рисунок 3.12 - Модуль *Bluetooth HC-06*

Всі існуючі типи модулів *Bluetooth* мають свої особливості, але схожі за функціями та роботою. Одним з видів модулів є *Bluetooth HC 06* (рисунок 3.12). *Arduino* модуль виглядає як звичайний послідовний інтерфейс, тому можна відразу налагодити взаємодію з пристроєм на комп'ютері.

Основні характеристики модуля :

- Живлення 3,3В - 6 В;
- Максимальна вхідна напруга 5 В;
- Максимальний струм 45 мА;
- Швидкість передачі даних 1200-1382400 бод;
- Робочі частоти 2,40 ГГц - 2,48ГГц;
- Підтримка специфікації *bluetooth* версії 2.1;
- Мале споживання енергії;
- Високий рівень захисту даних;
- Дальність зв'язку 30 м;

Для підключення до смартфона використовуються наступні дані - пароль "1234", швидкість передачі даних 9600, ім'я модуля *HC - 06*.

3.3.2 *DS1307* - годинник реального часу (*RTC*)

DS1307 це невеликий модуль, призначений для підрахунку часу (рисунок 3.13). Зібраний на базі мікросхеми *DS1307ZN* з реалізацією живлення від літєвої батарейки (*LIR2032*), що дозволяє працювати автономно впродовж тривалого часу. Також на модулі, встановлена енергонезалежна пам'ять *EEPROM* об'ємом 32 Кбайт(*AT24C32*). Мікросхема *AT24C32* і *DS1307ZN* пов'язані загальною шиною інтерфейсом *I2C*.



Рисунок 3.13 - Модуль годинника реального часу *DS1307*

Технічні характеристики

- Напруга живлення: 5В;
- Робоча температура: - 40 °С ... + 85 °С;
- Пам'ять: 56 байт (незалежна) ;
- Батарейка: *LIR2032* (автоматичне визначення джерела живлення) ;
- Інтерфейсу: *I2C*;

Завдяки своїй пам'яті і автономності, можна реєструвати події, (при автономному живленні) наприклад зміна температури і так далі, дані зберігаються в пам'яті їх можна дістати з пам'яті модуля. Отже, модуль *DS1307* часто використовують, коли контролерам *Arduino* необхідно знати точний час, для запуску якого то події і так далі [5].

3.3.3 *RFID* модуль *RC522*

Радіочастотна ідентифікація (*RFID*) - це технологія безконтактної ідентифікації об'єктів за допомогою радіочастотного каналу зв'язку. Ідентифікація об'єктів робиться по унікальному ідентифікатору, який має кожна електронна мітка.

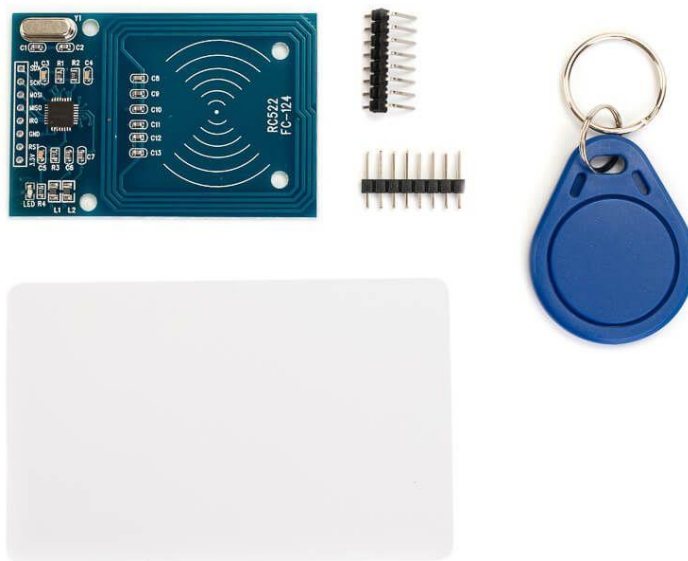


Рисунок 3.14 - *RFID* модуль *RC522*

Зчитувач випромінює електромагнітні хвилі певної частоти. Мітки відправляють у відповідь інформацію - ідентифікаційний номер, дані пам'яті і ін.

Переваги технології *RFID* :

- Безконтактна;
- можливість прихованої установки міток;
- висока швидкість прочитування даних;
- можливість установки в шкідливих середовищах;
- неможливість підробки.

Існує велика різноманітність *RFID*- міток. Мітки бувають активні і пасивні (без вбудованого джерела енергії, живляться від струму, що індукується в антені сигналом від рідера). Мітки працюють на різній частоті: *LF* (125 - 134 кГц), *HF* (13.56 МГц), *UHF* (860 - 960 МГц). Пристрій, який зчитує інформацію з мітки та записує дані, називається зчитувачем. У проектах *Arduino* в якості зчитувача дуже часто використовують модуль *RFID* - *RC522* (рисунок 3.14). Модуль виконаний на мікросхемі *MFRC522* фірми *NXP*, яка забезпечує роботу з мітками *HF* (на частоті 13,56 МГц). У комплекті з модулем *RFID* - *RC522* йдуть дві мітки, одна у вигляді карти, інша у виді брелока.

Характеристики *RFID* модуля *RC522*:

- Напруга живлення : 3.3v;
- Споживаний струм : 13-26ma;
- Робоча частота: 13.56mhz;
- Дальність прочитування : 0 - 60 мм;
- Інтерфейс: *SPI*;

– Швидкість передачі : максимальна 10МБит/з.

Мікросхема *MFRC522* підтримує інтерфейси *SPI*, *UART* і *I2C*. Вибір інтерфейсу здійснюється установкою логічних рівнів на певних виведеннях мікросхеми. На цьому модулі вибраний інтерфейс *SPI*.

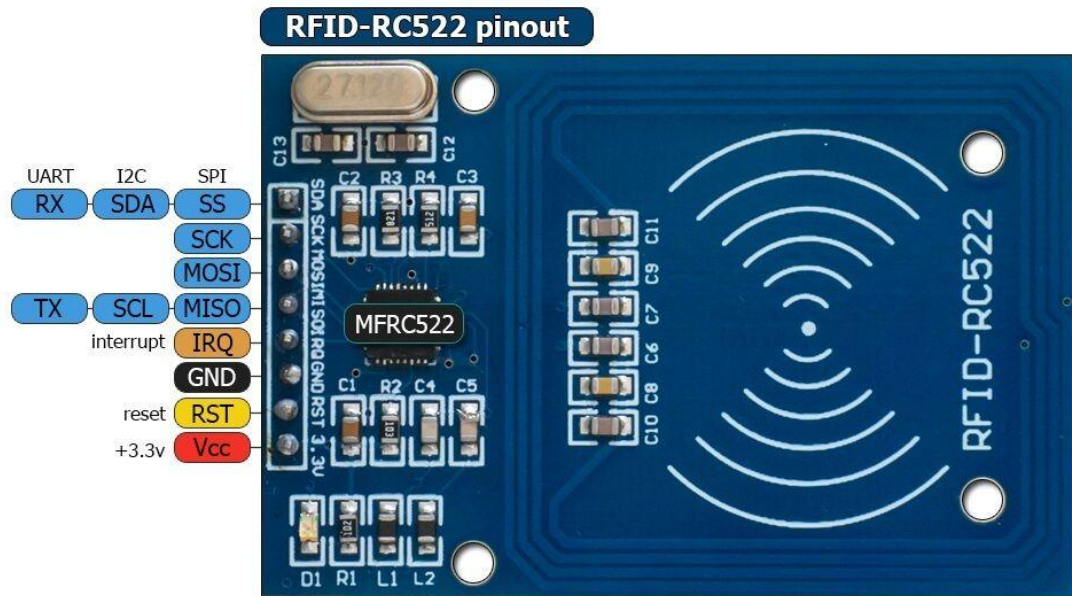


Рисунок 3.15 - Входи/Виходи *RFID* модуля *RC522*

Призначення виходів інтерфейсу *SPI* (рисунок 3.15):

- *SDA* - вибір веденого;
- *SCK* -сигнал синхронізації;
- *MOSI* - передача від *master* до *slave*;
- *MISO* - передача від *slave* до *master*;
- *RST* - виведення для скидання;
- *IRQ* - виведення переривання;
- *GND* - земля;
- *Vcc* -живлення 3.3 В.

Сигнал скидання *RST* - це сигнал, що поступає від цифрового виходу контроллера. При надходженні сигналу *LOW* відбувається перезавантаження зчитувача. Також рідер установкою на *RST* низького рівня повідомляє, що знаходиться в режимі сну, для виведення модуля з режиму сну необхідно подати на цей вихід сигнал *HIGH* [6].

3.3.4.Звуковий модуль *Arduino WTV020-SD-16P*

Модулі та мікросхеми серії *WTV020-SD* (рисунок 3.16) призначені для додатків, яким потрібне просте та не дороге рішення для зберігання та відтворення тривалих аудіо- та музичних повідомлень з високою якістю звуку. Для збереження голосових повідомлень використовується стандартна флеш-карта *SD* або *microSD*. Аудіоінформацію можна змінити, просто замінивши або перезаписавши флеш-карту.



Рисунок 3.16 - Звуковий модуль *Arduino WTV020-SD-16P*

Основні переваги модулів та мікросхем *WTV020-SD*:

- мінімальні розміри (модуль *WTV020-SD (micro)*: всього 22 x 19 мм);
- дозволяє зберігати та відтворювати великий обсяг аудіо інформації: до 512 файлів загальною тривалістю до 46 годин;
- вбудований високошвидкісний аудіо процесор, забезпечує якісне і чисте звучання;
- проста схема включення: всього одна мікросхема;
- швидка та зручна зміна звукових повідомлень: простою заміною *flash* карти або перезаписом її на будь-якому картрідері;
- підтримується формат файлів *AD4* (аналог *mp3*) ;
- ШІМ (*PWM*) вихід для прямого підключення динаміка з вихідною потужністю 0.25 / 0.5Вт;
- максимальний об'єм підтримуваної карти 1Гб;
- напруга живлення 3-3.3В [42].

РОЗДІЛ 4 . РОЗРОБКА МАКЕТУ РОЗУМНОГО БУДИНКУ

4.1 Структурна схема макету розумного будинку

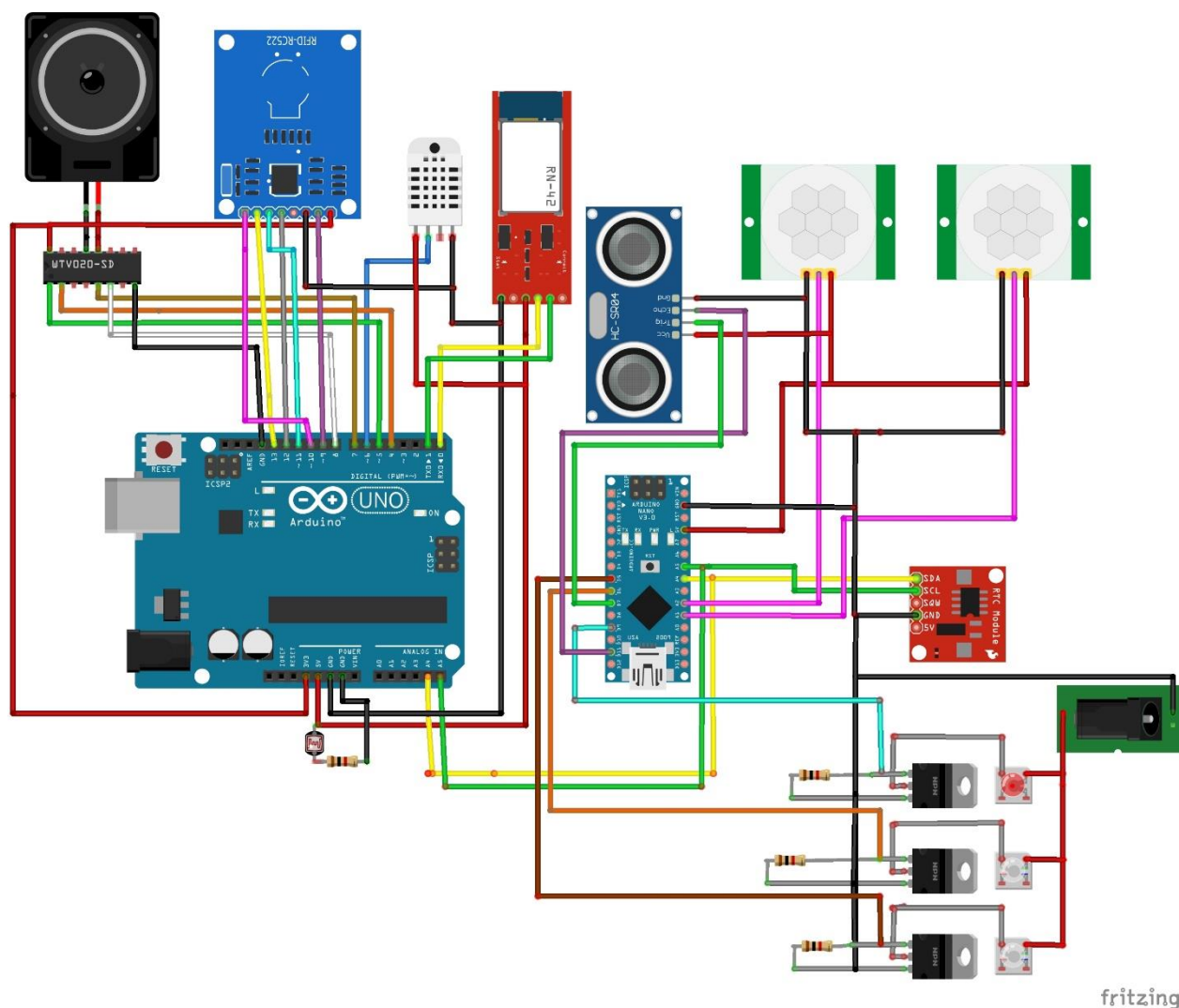


Рисунок 4.1 - Структурна схема макету розумного будинку

До складу схеми (рисунок 4.1) входять:

- Мікроконтролер *Arduino Uno*;
- Мікроконтролер *Arduino Nano*;
- Ультразвуковий датчик відстані *Arduino HC-SR04*;
- Інфрачервоний датчик руху *Arduino HC-SR501*;
- Датчик вологості на температури *Arduino DHT22*;
- Модуль *Bluetooth HC-06*;

					КНУ.РМ.123.22.12.04.РМРБ			
Змн.	Арк.	№ документа	Підпис	Дата	РОЗРОБКА МАКЕТУ РОЗУМНОГО БУДИНКУ	Літера	Аркуш	Аркушів
Розробив	Просяник							
Перевірив	узнєцов							
Н.контроль	Кузнєцов					KI-21м		
Затвердив	Купін							

- Модуль реального часу *Arduino DS1307*;
- *RFID* модуль *RC522*;
- Звуковий модуль *Arduino WTV020-SD-16P*;
- Фоторезистор.

Мікроконтролери *Arduino Uno* та *Arduino Nano* спілкуються через шину I2C за допомогою бібліотеки *Wire*.

Схема живиться від двох блоків живлення розрахованих на 12В. Один блок живлення живить мікроконтролер *Arduino Uno*, а отже і майже всю схему, окрім світлодіодної стрічки. Стрічка живиться від окремого джерела живлення розрахованого на 12 В.

4.2 Інтерфейс I2C

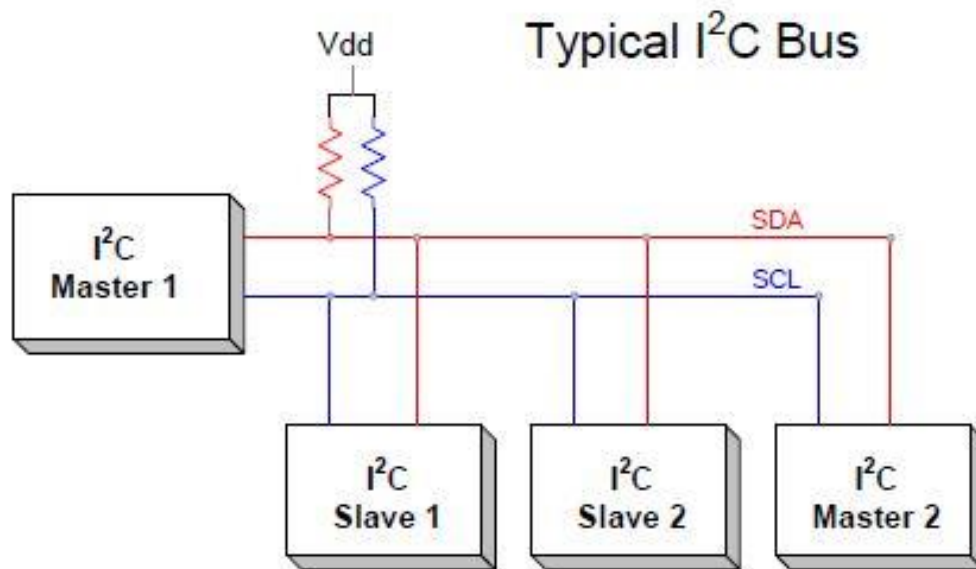
Як розширити функціональність розроблюваної системи на основі мікроконтролера? Так, це питання цікавить багатьох схемотехніки, що працюють над прототипами електронних пристроїв. Дивно, але додати до системи нові блоки, не змінюючи схеми, дозволить шина, розроблена інженерами *Philips* більше 30 років тому.

Мабуть, другий за популярністю інтерфейс в *Arduino* середовищі після *UART*, де найчастіше використовується для обміну даними між контроллером, датчиками і виконавчими пристроями. Відрізняється від *UART* більш високою швидкістю стабільної передачі даних і стабільнішою передачею даних на високій швидкості (рисунок 4.2).

Завдяки інтерфейсу *I2C* можна перетворити мікроконтролер в простий конструктор, до якого можна підключити декілька десятків мікросхем.

Схема внутрішнього зв'язку - так можна розшифрувати назву шини, яку сьогодні можна зустріти практично в кожному електронному пристрої. Варто відзначити, що в *Philips* запатентували настільки вдале в практичному плані рішення і інші виробники дублювали *I2C* під іншими назвами.

Саме ця шина встановлюється для зв'язку із зовнішнім світом дисплеїв, камер, стільникових телефонів. Кількість периферичних пристроїв, що підключаються до пристроїв за допомогою *I2C*, взагалі не піддається обліку.



Р

исунок 4.2 - Інтерфейс I2C

Шина являє собою два провідники, а для управління інтерфейсом досить одного мікроконтролера. Дивно, але подібна простота дозволяє проводити відключення мікросхем в процесі роботи. Спеціальний вбудований фільтр здатний справлятися зі сплесками, гарантуючи збереження оброблюваної інформації.

Серед недоліків *I2C*, крім обмеженої місткості, складність програмування і труднощі з визначенням несправності в ситуації зі станом низького рівня.

Спочатку швидкість шини була всього 100 кбіт, а підключити до неї було можна всього 120 пристроїв. У 90-х роках стандарти змінилися і швидкість передачі даних збільшилася в 4 рази і з'явилася можливість підключення до 1000 мікросхем. Однак більшість виробників інтерфейсу зациклилися на 400 кбіт з підключенням 120 пристроїв.

На відміну від *UART*, *I2C* є протоколом синхронного зв'язку, це означає, що обмін даними відбувається по загальному для усіх пов'язаних пристроїв сигналу синхронізації. Генерацією сигналу займається тільки єдиний головний пристрій, він же є ведучим, по іншому майстром. Пристрій "говорить" і "дає слово" іншим, які називаються веденими, по-англійськи *Slave*. Усі ведені пристрої мають унікальний номер, навіть якщо такий пристрій на усю мережу один. Майстер номера не має, його і так усі знають. Ведені мовчать, слухають, що говорить майстер і відкликаються тільки тоді, коли ведучий їх про це просить, називаючи їх по імені (номеру), тому в мережі завжди панує зразковий порядок.

Наступним етапом роботи є передача адреси того пристрою, до якого потрібно звернутися. Звернення майстра розпочинається з падіння рівня на шині даних *SDA*, що є стартовим сигналом для ведених. Підвищення рівня *SDA* при високому тактовому сигналі являється для них стоп-командою. Все, що відбувається між цими подіями, називається "повідомлення", тобто передача даних.

При цьому потрібно пам'ятати, що зчитування даних здійснюється при $SCL = 1$, а передача йде вперед старшим бітом. Перші 7 біт - адреса пристрою, 8 - команда записати (0) або читати (1). Слейв отримає всі вісім сигналів, притисне лінію *SDA* на дев'ятому такті *SCL* якщо йому все зрозуміло. Якщо немає - то формується сигнал стоп і передача даних здійснюється знову. При завершенні роботи відпускається лінія *SDA*, при цьому *SCL* не чіпають.



Рисунок 3.3 - Структура повідомлення



Рисунок 4.3 - Структура повідомлення побітово

Що таке "старт" і "стоп" зрозуміло. Адреса 7-10 біт, залежно від різновиду протоколу, той самий ідентифікатор конкретного веденого пристрою, до якого звертається майстер (рисунок 4.3). Далі біт читання або запису, що пояснює що ми хочемо, - передати дані або отримати їх. *ACK/NACK* – біти підтвердження або непідтвердження прийому інформації кожного кадру. Так, *ACK* єдиний біт, який генерується в лінії *SCL* веденим пристроєм. На жаль, без додаткових заходів ми не можемо скористатися цією інформацією про доставку, вона лише скорочує час передачі, обриваючи її, коли приймаючий пристрій перестає відповідати.

Інтерфейси *i2c*, як правило, розроблені для досить швидкої та надійної передачі на короткі відстані в межах одного пристрою. Насправді довжина дроту обмежена кількома метрами. Він займає своєрідне проміжне положення між *UART* та *SPI* з точки зору швидкості, надійності, відстані та використання ресурсів.

4.3 Додаток для управління розумним будинком

Управління розумним будинком здійснюється через додаток(рисунок 4.4) для операційної системи *Windows*. Додаток був розроблений в середовищі *Visual Studio 2013* на базі платформи *WPF(Windows Presentation Foundation)*.

Платформа розробки *WPF* підтримує широкий набір компонентів для розробки додатків. *WPF* використовує розширювану мову розмітки для додатків(*XAML*), щоб надати декларативну модель для програмування додатків.

За допомогою додатку можна керувати освітленням в автоматичному або ручному режимі. Також в додатку можна задати температуру в приміщенні, отримати інформацію з датчика температури та вологості.

Окреме значення в управлінні розумним будинком займає охоронний режим(рисунок 4.5- 4.7), який також представлений в додатку.

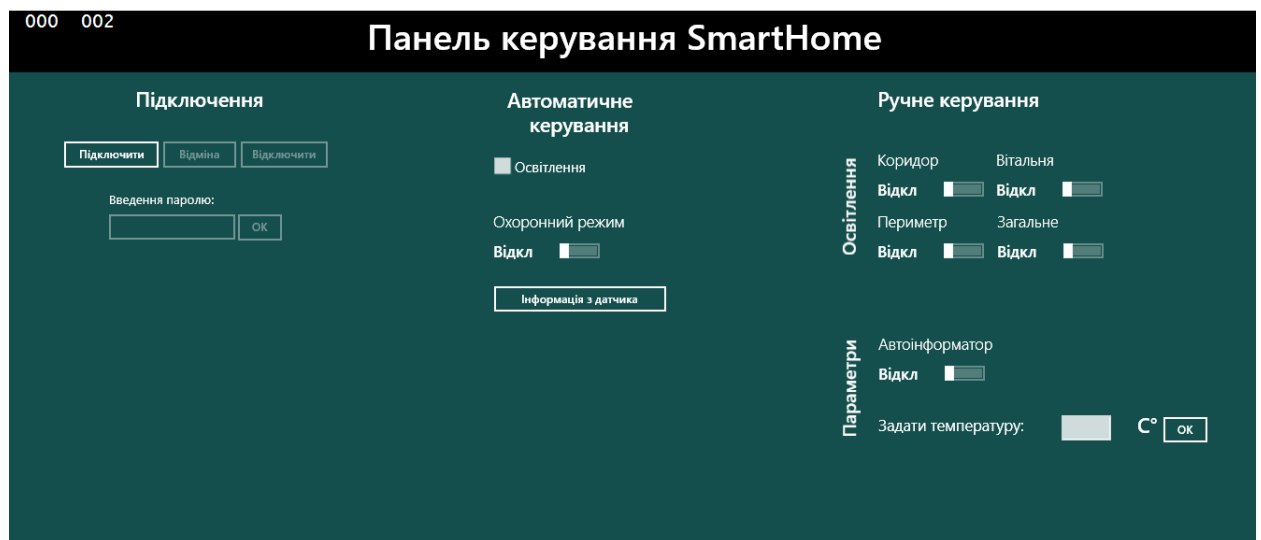


Рисунок 4.4 – Інтерфейс програми

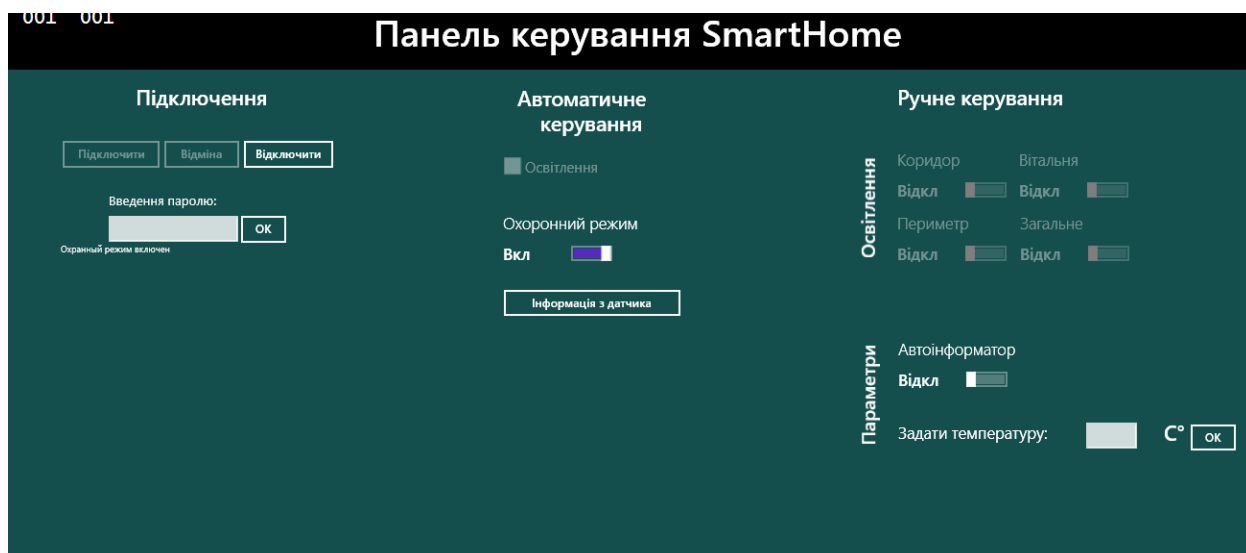


Рисунок 4.5 - Ввімкнення охоронного режиму

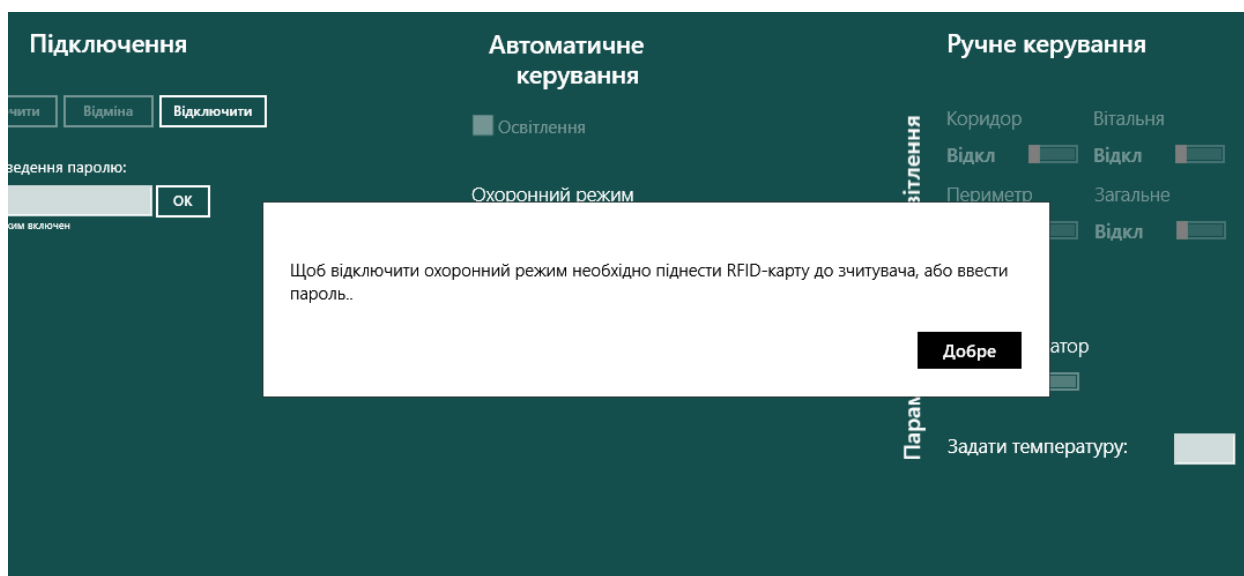


Рисунок 4.6 - Повідомлення про те, як потрібно відключати охоронний режим

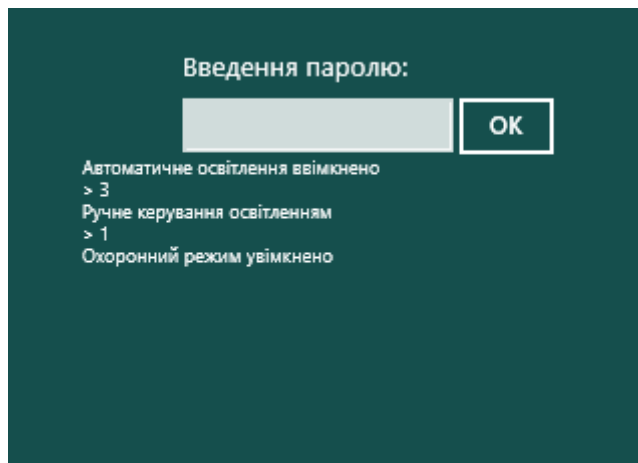


Рисунок 4.7 - Блок повідомлень додатку

Додаток починає працювати лише в тому випадку, якщо користувач підключився до модулю *Bluetooth* (рисунок 4.8). Але, для того, щоб модуль можна було підключити до додатку, перш за все його потрібно синхронізувати з самим комп'ютером.

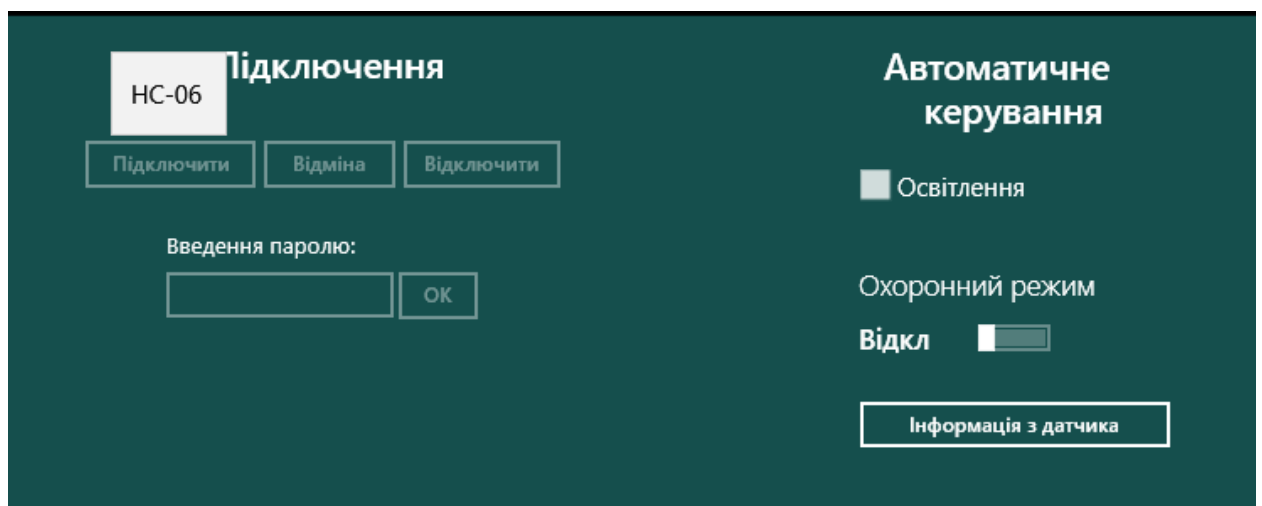


Рисунок 4.8 - Підключення до модулю *Bluetooth*

ВИСНОВКИ

В даній роботі досліджувалися питання побудови системи розумного будинку, вибору засобів управління, технологій, обладнання та інші актуальні питання організації та роботи розумного будинку. Робота присвячена розробці макету розумного будинку з використанням *Arduino*.

В першому розділі було виконано огляд особливостей та характеристик різновидів розумних будинків. Особливу увагу приділено різновидам систем розумного дому.

Другий розділ присвячено аналізу протоколів для синхронізації складових частин розумного будинку, а також був проведений аналіз вразливостей системи «*Smart Home*».

У третьому розділі увага була приділена засобам управління макетом розумного будинку. Було розглянуто мікроконтролери, датчики та модулі за допомогою яких буде здійснюватися управління макетом розумного будинку.

В четвертому розділі подана структурна схема макету, опис додатку, який створений для керування розумним будинком та опис інтерфейсу *I2C*.

В кінці роботи отримано макет розумного будинку та додаток для здійснення керування. На основі використання метода ієрархії Сааті визначено, що кращий варіант технології бездротового доступу мережі управління розумним будинком є технологія *ZigBee*. Дана технологія дозволяє істотно полегшити процес монтажу і подальшого обслуговування системи розумного будинку, а також ймовірність збою в таких системах практично рівна нулю.

Також на основі результатів оцінки ризиків за допомогою методу корпорації "Microsoft" найбільш небезпечними загрозами системи розумного будинку є:

- атаки на центральний сервер;
- впровадження шкідливого коду чи програми;
- перехоплення та підміна переданого сигналу;
- відключення контрольних датчиків.

Таким чином всі пункти технічного завдання виконано повністю.

					КНУ.РМ.123.22.12.В			
Змн.	Арк.	№ документа	Підпис	Дата	ВИСНОВКИ			
Розробив	Просяник							
Перевірив	Кузнєцов							
Н.контроль	Кузнєцов							
Затвердив	Купін				КІ-21м			

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Береговський В.В. Математичне та програмне забезпечення автоматизованого проектування систем “інтелектуального будинку”. Дисертація на здобуття наукового ступеня кандидата технічних наук. – Львів. – 2017 [Електронний ресурс] Режим доступу: URL: https://otherreferats.allbest.ru/management/00006537_0.html (дата звернення: 20.11.2022).
2. Arduino Uno [Електронний ресурс] Режим доступу: URL: <http://arduino.ru/Hardware/ArduinoBoardUno> (дата звернення: 20.11.2022).
3. Arduino Nano [Електронний ресурс] Режим доступу: URL: <http://arduino.ru/Hardware/ArduinoBoardNano> (дата звернення: 20.11.2022).
4. Підключення Arduino Bluetooth HC-06 [Електронний ресурс] Режим доступу: URL: <https://arduinomaster.ru/datchiki-arduino/arduino-bluetooth-hc05-hc06/> (дата звернення: 20.11.2022).
5. Real Time Clock Модуль з батареєю (DS1307) [Електронний ресурс] Режим доступу: URL: <https://arduino.ua/prod22-Real Time Clock Modyl DS1307> (дата звернення: 20.11.2022).
6. RFID модуль RC522 [Електронний ресурс] Режим доступу: URL: <https://3d-diy.ru/wiki/arduino-moduli/rfid-modul-rc522/> (дата звернення: 20.11.2022).
7. Що таке розумний будинок [Електронний ресурс] Режим доступу: URL: https://tech.24tv.ua/smart-kvartira-abo-rozumniy-budinok-shho-tse-take-poradi-oblashtuvannya_n1454850 (дата звернення: 20.11.2022).
8. AMX [Електронний ресурс] Режим доступу: URL: <https://www.hi-fi.lviv.ua/ua/product/23/32> (дата звернення: 20.11.2022).
9. Система автоматизованого управління домом. Система умный дом [Електронний ресурс] Режим доступу: URL: <https://works.doklad.ru/view/7RPctZTlr6I.html> (дата звернення: 20.11.2022).
10. Вашкулат К. С. Магістерська дисертація на тему: «Методи впровадження відеоспостереження за об'єктами в системі «розумного будинку». – Київ. – 2020 [Електронний ресурс] Режим доступу: URL: https://ela.kpi.ua/bitstream/123456789/38535/1/VashkulatKS_magistr.pdf (дата звернення: 20.11.2022).
11. Умный дом – оборудование и автоматика для дома [Електронний ресурс] Режим доступу: URL: <https://smarton.com.ua/novosti-umnogo-doma/tpost/ktu5fma9m1-umnii-dom-oborudovanie-i-avtomatika-dlya> (дата звернення: 20.11.2022).

					КНУ.РМ.123.22.12.СВД			
Змн.	Арк.	№ документа	Підпис	Дата	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ			
Розробив	Просяник							
Перевірив	узнєцов							
Н.контроль	Кузнєцов							
Затвердив	Купін							
						Літера	Аркуш	Аркушів
						КІ-21м		

12. ТОП 5: Рейтинг лучших систем «Умный дом» по производителям 2021 года [Электронный ресурс] Режим доступа: URL: <https://vencon.ua/articles/rejting-sistem-umnyy-dom-po-proizvoditelyam> (дата звернення: 20.11.2022).
13. Управління вентиляцією [Електронний ресурс] Режим доступу: URL: https://www.smarthouse.ua/ua/upravlenie_ventiljaciej.html (дата звернення: 20.11.2022).
14. Чеботар Д. О. Дипломна робота на тему: «Інтерфейс системи «Розумний дім»». – Київ. – 2016 [Електронний ресурс] Режим доступу: URL: http://kivra.kpi.ua/wpcontent/uploads/file/work/2016/Chebotar/Chebotar_PZ.pdf (дата звернення: 20.11.2022).
15. Що таке розумний будинок та які можливості він надає. Переваги і недоліки [Електронний ресурс] Режим доступу: URL: <https://zakarpattyia.net.ua/News/216485-Shcho-take-rozumnyi-budynok-ta-iaki-mozhlyvosti-vin-nadaie-Perevahy-i-nedoliky> (дата звернення: 20.11.2022).
16. Комплект для розумного будинку FIBARO STARTER KIT [Електронний ресурс] Режим доступу: URL: <https://secur.ua/komplekt-dlja-umnogo-doma-fibaro-starter-kit.html> (дата звернення: 20.11.2022).
17. Xiaomi Smart Home Suite [Електронний ресурс] Режим доступу: URL: https://iots.com.ua/index.php?route=product/product&path=59_61&product_id=71 (дата звернення: 20.11.2022).
18. Комплект Vstarcam C38AR - TZ1V [Електронний ресурс] Режим доступу: URL: <https://vstarcam.ua/reviews/vstarcam-c38ar-tz1v/> (дата звернення: 20.11.2022).
19. Google Nest Mini [Електронний ресурс] Режим доступу: URL: <https://z-wave.com.ua/p1137240071-umnaya-kolonka-google.html> (дата звернення: 20.11.2022).
20. Apple HomeKit [Електронний ресурс] Режим доступу: URL: <https://ilounge.ua/catalog/apple-homekit> (дата звернення: 20.11.2022).
21. Стандарт Wi-Fi [Електронний ресурс] Режим доступу: URL: https://my.volia.com/kyiv/ru/faq/article/standarti-roboti-wi-fi-bgn?partner=organic_search&utm_source=google&utm_medium=organic (дата звернення: 20.11.2022).
22. Перспективи Bluetooth Mesh для розумного будинку [Електронний ресурс] Режим доступу: URL: <https://oxorona.com/bluetooth-mesh/> (дата звернення: 20.11.2022).
23. Сааті Т., Кернс К. Аналітичне планування Організація систем: Пер. з англ. - - М.: Радіо і зв'язок, 1991. – 224с.
24. Безрук В.М., Чеботарьова Д.В., Скорик Ю.В. Многокритериальный анализ и выбор средств телекоммуникаций: Монография. – Харьков: ФОП Коряк С.Ф., 2017. - 268с.
25. Угрозы конфиденциальной информации [Електронний ресурс]. – Режим доступу: URL: <https://studfile.net/preview/5178442/page:3/> (дата звернення: 20.11.2022).

26. Страхи и проблемы будущего умных домов. [Электронный ресурс]. – Режим доступа: URL: <https://habr.com/ru/company/iridiummobile/blog/385311/> (дата звернення: 20.11.2022).

27. Bangali J., Shaligram A. Design and Implementation of Security Systems for Smart Home Based on GSM Technology: International Journal of Smart Home.2018 Vol.7, No.6. P.201-208.

28. Chitnis S., Deshpande N., Shaligram A. An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. Wireless Sensor Network. 2020. Vol. 68, No 7. doi: 10.4236/wsn.2020.84006.

29. Choudhary V., Parab A., Bhapkar S., Jha N., Kulkarni Ms. Medha. Design and Implementation of Wi-Fi based Smart Home System, International Journal Of Engineering And Computer Science. 2016. Vol.5, No 6. PP.15852-15855.

30. Kumar A., Tiwari N. "Energy Efficient Smart Home Automation System", International Journal of Scientific Engineering and Research (IJSER). 2021. Vol. 3, No 1. PP. 2347-3878.

31. Shirisha Tadoju., J. Mahesh. "Bluetooth Remote Home Automation System using Android Application", International Journal Of Advanced Technology and Innovative Research. 2019. Vol.07, No 10. PP.1815-1818.

32. Table Of Contents -X10 MT10 Owner's Manual. [Электронный ресурс]. – Режим доступа: URL: <https://www.manualslib.com/manual/720184/X10-Mt10.html?page=2#manual>. (дата звернення: 21.12.2021).

33. Протокол X10 [Электронный ресурс]. – Режим доступа: URL: <http://www.iq-home.ru/tech/x10.html>. (дата звернення: 3.02.2022).

34. Honeywell Ademco TUXWIFIW Tuxedo .URL: https://www.jmac.com/Honeywell_Ademco_TUXWIFIW_p/honeywell-ademcotuxwifiw.htm. (дата звернення: 21.12.2021).

35. H. Jiang, B. Liu and C. W. Chen, "Performance analysis for ZigBee under WiFi interference in smart home,"2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6.

36. Adams C. E. Home area network technologies. BT Technology Journal.20.02.2020.N12. P.53–72.

37. F. Liu and H. Zhao, "The Design of WIFI-Based Smart Home Communication Hardware Adapter," 2015 Fifth International Conference on 53 Instrumentation and 55 Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, 2015, pp. 1193-1197.

38. Протоколи «Інтернету речей»: основні відомості // Засоби і системи автоматизації. URL: <https://www.rtsoft.ru> (дата звернення 19.11.2022).

39. Ультразвуковий датчик відстані Arduino HC - SR04 [Електронний ресурс] Режим доступа: URL: <https://www.robostore.com.ua/moduli-i-datchiki/datchiki-zvuka/ultrazvukovoj-datchik-rasstoyaniya-hc-sr04/> (дата звернення 19.11.2022).

40. Інфрачервоний датчик руху *HC - SR501* [Електронний ресурс]
Режим доступу: URL: <https://www.robostore.com.ua/moduli-i-datchiki/sensory-datchiki-i-moduli/infrakrasnyj-datchik-dvizheniya-hc-sr501/> (дата звернення 19.11.2022).

41. Датчик вологості та температури *DHT22* [Електронний ресурс]
Режим доступу: URL: <https://arduino.ua/prod2618-modyl-datchika-temperatyri-i-vlajnosti-dht22> (дата звернення 19.11.2022).

42. Звуковий модуль *Arduino WTV020-SD-16P* [Електронний ресурс]
Режим доступу: URL: <https://arduino.ua/prod2170-zvykovoi-modyl-wtv020-sd-16p-arduino> (дата звернення 19.11.2022).