

Міністерство освіти і науки України  
 Національний технічний університет  
 «Дніпровська політехніка»  
Навчально-науковий Інститут електроенергетики  
 (інститут)  
Факультет інформаційних технологій  
 (факультету)  
Кафедра інформаційних технологій та комп'ютерної інженерії  
 (повна назва)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**  
**кваліфікаційної роботи ступеня бакалавра**

студента Гудакова Сергія Сергійовича

(ПІБ)

академічної групи 123-18-1

(шифр)

спеціальності 123-18-1 Комп'ютерна інженерія

(код і назва спеціальності)

за освітньо-професійною програмою 123-18-1 Комп'ютерна інженерія

(офіційна назва)

на тему: «Кіберфізична система домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі»

(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
Кваліфікаційної роботи	проф. Цвіркун Л.І			
Розділів:				
Розробка апаратної частини комп'ютерної системи	доц. Ткаченко С.М			
Розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				
-----------	--	--	--	--

Нормоконтролер	Проф. Цвіркун Л.І			
----------------	-------------------	--	--	--

Дніпро  
2022

**ЗАТВЕРДЖЕНО:**  
завідувач кафедри  
інформаційних технологій  
та комп'ютерної інженерії  
(повна назва)

\_\_\_\_\_ Гнатушенко В.В.  
(підпис) (прізвище, ініціали)

"\_\_" \_\_\_\_\_ 2022 року.

**ЗАВДАННЯ**  
**на кваліфікаційну роботу**  
**ступеня бакалавр**

студента Гудаков С.С. академічної групи 123-18-1  
(прізвище, ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія  
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія  
(офіційна назва)

на тему Кіберфізична система домашнього Інтернету речей житлового комплексу  
«Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі  
(назва за наказом ректора)

затверджена наказом ректора НТУ «Дніпровська політехніка» від . 2022 № -Л

Розділ	Зміст завдання	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	20.05.2022
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	27.05.2022
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	06.06.2022

**Завдання видано**

(підпис керівника)

\_\_\_\_\_ (прізвище та ініціали)

проф. Цвіркун Л.І.

**Дата видачі**

04.04.2022 р.

**Дата подання до атестаційної комісії**

16.06.2022 р.

**Прийнято до виконання**

\_\_\_\_\_ (підпис студента)

Гудаков С.С.

(прізвище та ініціали)

## РЕФЕРАТ

Пояснювальна записка: \_\_\_\_ с., \_\_\_\_ рис., \_\_\_\_ табл., \_\_\_\_ дод., \_\_\_\_ джерела.

### СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об'єкт розробки: кіберфізична система домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі.

Мета: створення кіберфізичної системи домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі.

Розроблена комп'ютерна система з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову мережі для використання домашнього інтернету речей у житлового комплексу «Бартоломео».

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання функцій з об'єднання підрозділів у мережу; збір обробку, накопичення інформації у базах даних; комунікацію між кінцевими споживачами у різних підрозділах та доступ до загальних ресурсів.

Розробка комп'ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

## ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів	8
Вступ	9
1 Стан питання і постановка завдання	10
1.1 Характеристика підприємства та умов застосування КС	10
1.1.1 Особливості проектування будівництва житлових комплексів	10
1.1.2 Житлові комплекси м. Дніпро	13
1.1.3 ЖК Bartolomeo Resort Town	22
1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства	25
1.3 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань	28
1.4 Розробка схеми організаційної структури підприємства	36
1.5 Постановка завдання	39
2 Розробка апаратної частини комп'ютерної системи підприємства	41
2.1 Технічні вимоги до комп'ютерної системи	41
2.1 Найменування і сфера застосування системи	41
2.2 Вимоги до системи в цілому	42
2.2.1 Показники призначення	42
2.2.2 Вимоги до структури і функціонування системи	42
2.2.3 Склад системи	44
2.2.4 Технічні вимоги до системи	45
2.2.5 Вимоги до структури для підсистеми передачі даних	45
2.2.6 Вимоги до функцій, що виконуються системою	46
2.2.7 Вимоги до безпеки і надійності	46
2.3 Вимоги до обслуговування і експлуатації системи	47

2.3.1 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи	47
2.3.2 Вимоги до упаковки і транспортування	48
2.3.3 Вимоги до чисельності і кваліфікації персоналу, який обслуговує систему і режими її роботи	49
2.4 Вимоги до програмної підсистеми	49
2.4.1 Перелік функцій підсистеми занесення інформації у БД	49
2.4.2 Застосування систем управління базами даних	50
2.4.3 Вимоги до ПО	50
2.4.4 Вимоги до збереження інформації	50
2.4.5 Вимоги до захисту інформації від несанкціонованого доступу	50
3 Розробка корпоративної мережі	52
3.1 Розрахунок схеми адресації корпоративної мережі	52
3.2 Розробка топологічної схеми корпоративної мережі	54
3.3 Розрахунок налаштувань маршрутизації корпоративної мережі	56
3.4 Налаштування та перевірка роботи комп'ютерної системи	56
3.4.1 Базове налаштування конфігурації пристроїв	56
3.4.2 Налаштування маршрутизаторів корпоративної мережі	58
3.4.3 Налаштування роботи Інтернет	60
3.4.4 Перевірка роботи комп'ютерної системи	61
3.5 Захист інформації в комп'ютерній системі від несанкціонованого доступу	63
3.5.1 Розробка методів для захисту інформації в комп'ютерній системі	63
3.5.2 Налаштування маршрутизаторів на підтримку служби AAA	71
3.5.3 Налаштування мережах VLAN та параметрів безпеки комутаторів	74
3.5.4 Налаштування віртуальної приватної мережі VPN	77
4 Кіберфізична система	79
4.1 Загальна інформація	79
4.2 Апаратна частина системи автоматичного управління	80

4.2.1 Розробка структурної схеми системи управління	83
4.2.2 Вибирання технічних засобів і елементної бази	85
4.2.2.1 Датчики	85
4.2.2.1.1 Контактні датчики	85
4.2.2.1.2 Інфрачервоні датчики руху	88
4.2.2.1.3 Датчик вологості	89
4.2.2.1.4 Акустичні датчики	90
4.2.2.1.5 Вібраційні датчики	92
4.2.2.1.6 Датчики газу	93
4.2.2.1.7 Теплові і пожежні датчики	94
4.2.2.1.8 Датчик витоку води	96
4.3.2.2 Виконавчі пристрої	97
4.2.2.2.1 Звукова сирена	97
4.2.2.2.2 Магнітний пускач	99
4.2.2.3 Додаткові пристрої	100
4.2.2.3.1 Акумулятори	100
4.2.2.4 Мікроконтролер	100
4.2.2.5 Безпроводні засоби передачі інформації	102
4.2.2.5.1 GSM– модуль SIM300DZ, SIM300C	102
4.2.2.5.2 Радіо–облаштування приймача даних TRC101	105
4.3 Розробка схеми автоматизації	107
4.3.1 Функціональна схема контролера	108
Висновки	114
Перелік посилань	115
Додаток А – Текст програми	119
Додаток Б – Таблиці маршрутизації	126
Відгуки консультантів кваліфікаційної роботи	133
Відгук	<b>Помилка! Закладку не визначено.</b>



**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,  
СКОРОЧЕНЬ І ТЕРМІНІВ**

EOM	– Електронна обчислювальна машина
КС	– Комп’ютерна система;
ПК	– Персональний комп’ютер;
Ethernet	– Технологія передачі даних по мережі;
Wi-Fi	– технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;
GSM	– (Global System for Mobile Communications) глобальний стандарт цифрового мобільного стільникового зв’язку з розділенням каналів за часом та частотою



## ВСТУП

Містобудування народилося в глибинах архітектури, але з часом міста стали настільки великими і складними, що для їх планування і обслуговування були потрібні нові знання – про гігієну, соціальне благополуччя, економіку, екологію, транспорт і багато іншого. Зокрема, розвивається екологічна економіка, тобто економіка, яка підвищує добробут людей, забезпечує соціальну справедливість і в той же час значно знижує ризики для навколишнього середовища і здоров'я громадян [10]. Багато галузей, галузей і діяльності на рівні держави, бізнесу і суспільства трансформуються. Швеція, Данія, Фінляндія, Німеччина, Франція та Велика Британія, в останні роки Китай, Бразилія та Індія були тим, як економіки впроваджують інновації.

Україна активно переймає досвід розвинених країн, але стикається з низкою проблем, таких як недосконалість законодавства, відсутність економічних стимулів, труднощі у усуненні екологічної шкоди, незахищеність умов для підприємництва, нерозуміння важливості інновацій як ефективного інструменту підвищення конкурентоспроможності регіону та країни тощо [11].

Сучасні міста повинні прагнути бути зеленими, екологічними, комфортними, привабливими для своїх мешканців, мати особливу атмосферу, пропонувати якісно нове середовище проживання, відповідно, інноваційна діяльність повинна вестися в рамках міських університетів і бути переважно екологічно орієнтованою [12]. Існує потреба в грамотному, економічно та соціально ефективному використанні міських територій, заснованих на принципах сталого розвитку та «зеленої» економіки [13].

Сучасні інновації інкапсують концентрацію гуманістичних, природозберігаючих і законодавчих ідей (право людини на чисте навколишнє середовище).

## **1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ**

### **1.1 Характеристика підприємства та умов застосування КС**

#### **1.1.1 Особливості проектування будівництва житлових комплексів**

Процес проектування житлового комплексу зазвичай ускладнюється в першу чергу з точки зору архітектурної концепції зовнішнього вигляду фасадів і вибору планувальних рішень для кожного житлового багатоквартирного будинку в складі житлового комплексу.

У сучасних умовах недостатньо спроектувати і побудувати комплекс – його ще потрібно продати. А в боротьбі за покупця на перше місце виходить розташування житлового комплексу, вартість і зручність планування квартир. При проектуванні планувальних рішень для квартир в житловому будинку необхідно спроектувати таке планування, щоб воно було затребуване більшістю потенційних покупців і вигідно порівнювалося з плануванням конкурентів.

З одного боку, покупець хоче максимальну кількість кімнат і квадратних метрів, з іншого боку, він обмежений бюджетом покупки. Тому при проектуванні житлового будинку архітектори і забудовники намагаються виходити з «портрета» середнього покупця на ринку.

Сучасні планування житлових комплексів в дизайні зазвичай включають в себе однокімнатні квартири, розраховані на покупців з невеликим бюджетом – самотніх молодих людей або молодих пар, яким не потрібно багато кімнат, двокімнатних, розрахованих на сім'ї з одним–двома дітьми і помірною площею, і вартість і трикімнатні, розраховані на сім'ї, але пропонують велику площу щодо двокімнатних квартир.

Останнім часом в гонитві за вартістю квартири забудовники все частіше вказують в дизайні житлових комплексів в технічних умовах на планування однокімнатної квартири. Як правило, чотирикімнатні квартири рідше

зустрічаються на ринку (вважається масовий сегмент житлових комплексів) – це пов'язано з високою вартістю квартири і труднощами з її реалізацією [17].

Що стосується будівництва житлових комплексів, то сьогодні для цього використовується безліч сучасних матеріалів, спеціального обладнання та будівельної техніки. Особливу увагу забудовники приділяють тепло- і звукоізоляційним властивостям будинків, а також їх якості і рівню сейсмічної стійкості. Житлові будинки, як правило, будуються з цегли і панелей, а гіпсокартон, сендвіч-панелі та інші матеріали найчастіше використовуються для створення несучих стін і перегородок.

Житлові комплекси складаються не тільки з багатоповерхових будівель, але і з інфраструктури, яка представлена ресторанами, магазинами, навчальними закладами, аптеками та іншими громадськими місцями. Крім усього іншого, навколо кожного будинку повинна бути площа, на якій розташовані лавки, дитячі майданчики і багато іншого. Сьогодні на території житлових комплексів є важливі для сучасного суспільства паркінги, санаторії, басейни, спортзали та інші важливі для сучасного суспільства будівлі.

Квартири в новобудовах можна здати в експлуатацію з готовим ремонтом, а також оснастити новими системами зв'язку, пластиковими вікнами і встановленими міжкімнатними дверима. Ще однією перевагою житлових комплексів сучасного типу є близьке розташування транспортних маршрутів. При будівництві будинків все більше число забудовників використовують залізобетонні конструкції, які використовуються для армування стін і перегородок. Такі конструкції підвищують надійність і міцність будівлі, але при цьому надають навантаження на землю, тому в процесі будівництва необхідно приділяти особливу увагу створенню високоміцного фундаменту [18].

Сучасні технології безпеки, такі як відеоспостереження, в даний час проникають в будь-яку галузь і сферу людської діяльності. Будівництво житлових об'єктів в цьому плані не є винятком. Тому нещодавно побудовані житлові

комплекси (ЖК) – це новий тип житла, який включає в себе нововведення не тільки у використанні сучасних матеріалів, але і кардинально нові принципи облаштування прибудинкової території.

Ідентифікаційні особливості сучасних комплексів для житла відображені в наступних особливостях нового типу житлового комплексу:

- комплекс складається з декількох багатоповерхових будинків, які відрізняються кількістю поверхів, рівнем квартир;
- є парковка, як біля будинку (якщо дозволяє вільний простір), так і в самій будівлі (підземний або надземний паркінг, що займає кілька поверхів);
- наявність розвиненої інфраструктури, в тому числі розважальних, освітніх і комерційних установ;
- планування квартир вибирається на розсуд майбутнього власника і може бути виконане за індивідуальним замовленням на етапі будівництва будинку;
- тип матеріалів, що використовуються в будівництві, відповідає стандартам пожежної безпеки, є високоенергетичним, функціональним, а також спрямований на економію енергоресурсів;
- безпека таких об'єктів;
- безпека житлових комплексів.

Також ключовою особливістю нових житлових комплексів є безпека. Таке житло гарантує високий рівень захисту його мешканців. При цьому не останню роль в цьому питанні відіграє установка відеоспостереження. Разом з професійними охоронцями і огорожею території від небажаних відвідувачів досягається високий ступінь захисту.

Питання безпеки зараз відіграють важливу роль у будь-якому об'єкті. Тому при покупці житла майбутній власник приділяє вивченню цього аспекту не менше часу і уваги, ніж сам житловий простір, де він і члени його сім'ї будуть жити.

Вартість житла в сучасних житлових комплексах, до стандартного набору факторів (площа, ремонт, підлога і т. д.) При цьому не завжди житло одного рівня, розташоване ближче до центру міста, обійдеться дорожче, ніж квартири в житловому комплексі, який знаходиться досить далеко від центру.

Згідно з останніми тенденціями, квартири в тихих місцях з красивою природою поблизу (парк, ліс, ставок) користуються великим попитом [16].

### 1.1.2 Житлові комплекси м. Дніпро

Основна частина елітних будинків будується за сучасною технологією монолітного каркасного будівництва, що збільшує термін служби будівлі і робить її стійкою до зовнішніх і внутрішніх впливів. З цегли виготовляються ті ж житлові комплекси, що і Жукофський, Амстердам, Каскад, Дуєт. Більшість будівель утеплені мінеральною ватою. Стіни зводяться і армуються газом або залізобетоном, цеглою, порцеляновим кам'яним посудом. Внутрішнє оздоблення виготовляється з сучасних матеріалів, опалення здійснюється автономна або індивідуально. Стелі квартир мають висоту 2,7... ,3 м.



Будинок має 92 квартири, площею від 87 м<sup>2</sup>, вартість від 22 770 грн/м<sup>2</sup>. Розташований в історичній частині міста, панорамний вид на Дніпро, суцільні вітражі. Будівля відзначена як кращий будинок України в 2008 році.

Рисунок 1.1 – ЖК Славія, пр. Дмитра Яворницького, 1а



19–24 поверхи, 850 квартир, площа від 46 м<sup>2</sup>, вартість від 20 240 грн/м<sup>2</sup>. Прекрасний вид з вікон квартир на місто і річку.

Рисунок 1.2 – ЖК Панорама, вул. Сімферопольська, 2 к



17 поверхів, 128 квартир, площа від 45 м<sup>2</sup>, вартість – від 18 200 грн/м<sup>2</sup>. Місце в престижному районі з розвиненою інфраструктурою, прекрасним видом з вікон і близькістю до популярних розважальних закладів, відомих шкіл.

Рисунок 1.3 – ЖК Панорама – вул. Івана Акініфієва, 30



16–18 поверхів, площа від 85 м<sup>2</sup>, вартість – від 25 200 грн/м<sup>2</sup>.

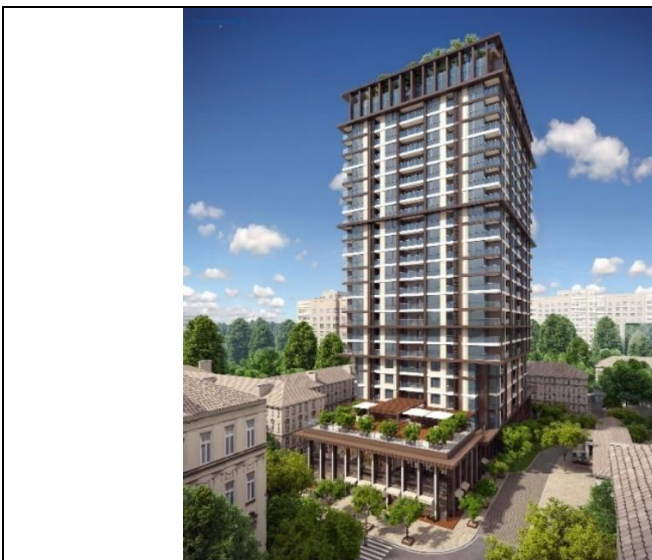
Будинок побудований з урахуванням безпеки, комфорту мешканців.

Рисунок 1.4 – ЖК Duet – вул. Крутогорна, 28



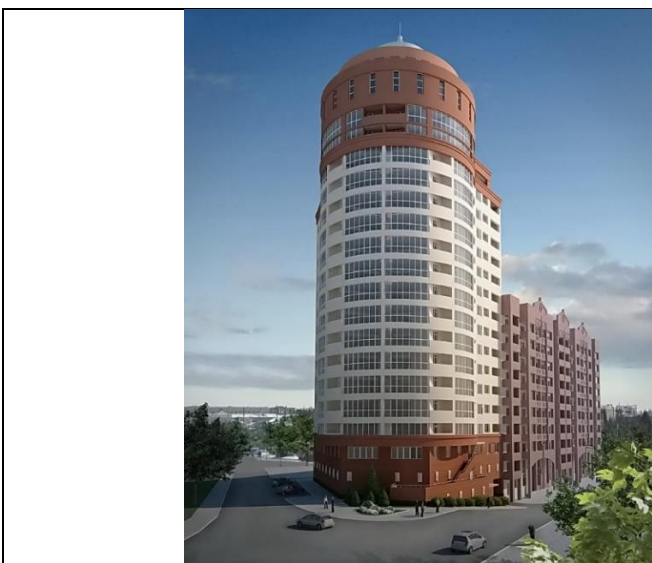
10 поверхів, 180 квартир, площа від 38 м<sup>2</sup>, вартість – від 17 210 грн/м<sup>2</sup>. Сучасна висотка з обладнаною закритою територією в будинку, зручне розташування.

Рисунок 1.5 – ЖК Жуковський – вул. Жуковського, 16...24



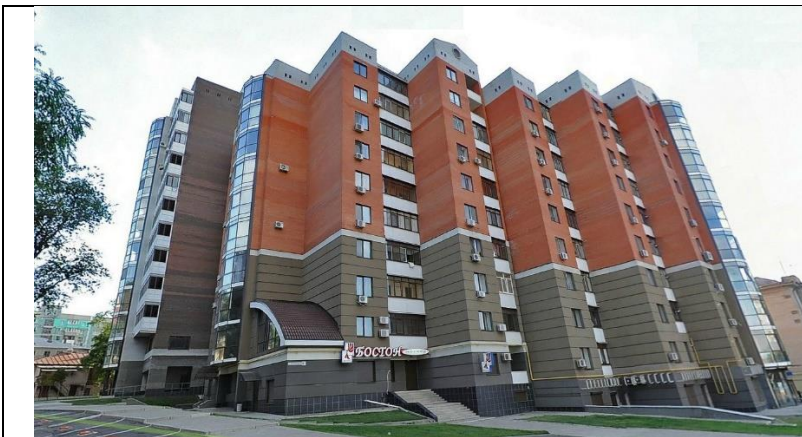
24 поверхи, площа від 46 м<sup>2</sup>, вартість – від 22 860 грн/м<sup>2</sup>. Престижна гірська частина Дніпропетровська, біля парку Шевченка, заклади та установи для комфортного життя.

Рисунок 1.6 – ЖК Новодворянський – вул. Володимира Вернадського, 33



14 поверхів, 104 квартири, площа від 65 м<sup>2</sup>, вартість від 15 000 грн за м<sup>2</sup>. Просторі апартаменти вільного планування, в під'їзді є консьєрж, 3-поверховий паркінг під землею. Гарне розташування в розвиненій частині міста.

Рисунок 1.7 – ЖК Чкалівський – вул. Святослав Хоробрий



12 поверхів, 85 квартир, площа від 70 м<sup>2</sup>, вартість – від 23 940 грн/м<sup>2</sup>. У будинку розташовані офіси і магазини, що не заважає затишному проживанню, але робить його більш комфортним.

Рисунок 1.8 – ЖК Каскад– вул. Херсонська, 9 а



23 поверхи, 258 квартир, площа від 60 м<sup>2</sup>, вартість – від 20 160 грн/м<sup>2</sup>. Розташований в престижному центральному районі міста.

Рисунок 1.9 – ЖК Кіровський – пр. Олександра Поля, 16



7 поверхів, 56 квартир, площа від 160 м<sup>2</sup>, вартість – від 55 640 грн/м<sup>2</sup>. Завдяки формі амфітеатру він має розкішний вид, тераси відкритого типу. Тут є спортивно-фітнес-центр і SPA-салон для мешканців.

Рисунок 1.10 – ЖК Кіровський – вул. Володимира Вернадського, 35 т





5–16 поверхів, 216 квартир, площа від 60 м<sup>2</sup>, вартість – від 35 000 грн/м<sup>2</sup>. Всі житлові квартири розташовані з двох сторін. На верхньому поверсі розташовані дворівневі пентхауси. Цілодобова система безпеки та відеоспостереження.

Рисунок 1.11 – ЖК Фестивальний – Січеславська Набережна, 45, 47, 49, 49, 49 а



21 поверх, 34 квартири, площа від 141,7 м<sup>2</sup> вартість – від 55 640 грн/м<sup>2</sup>. Вид на Дніпро, два швидкісних ліфта, власний парк, енергозберігаючі вітражі.

Рисунок 1.12 – ЖК Летуаль – вул. Володимира Вернадського



10 поверхів, 117 квартир, площа від 50 м<sup>2</sup>, вартість від 63 270 грн/м<sup>2</sup>. У будинку знаходиться торговий центр і магазини, дитячий світ, SPA-центр, ресторани.

Рисунок 1.13 – ЖК Cascade Plaza – Катеринославський бульвар, 1

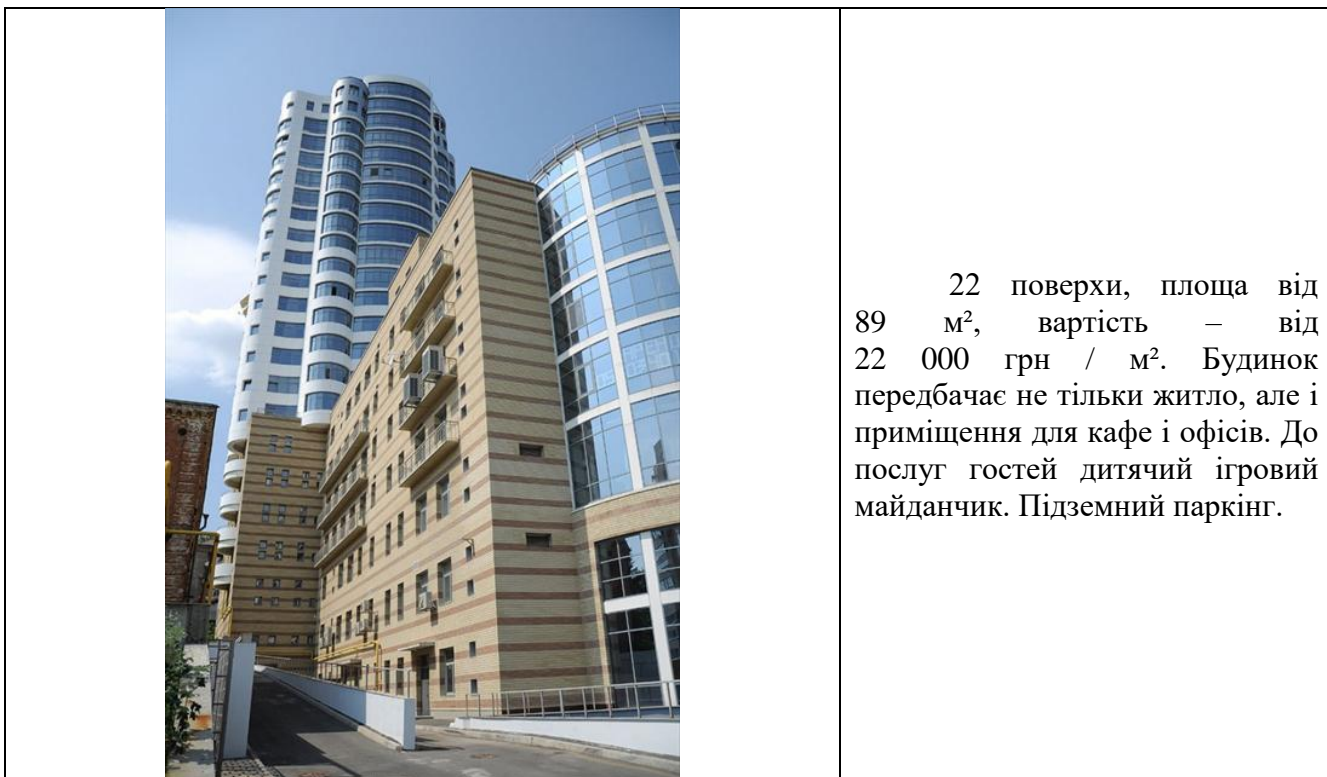


Рисунок 1.14 – ЖК Магнат – пр. Дмитра Яворницького, 5

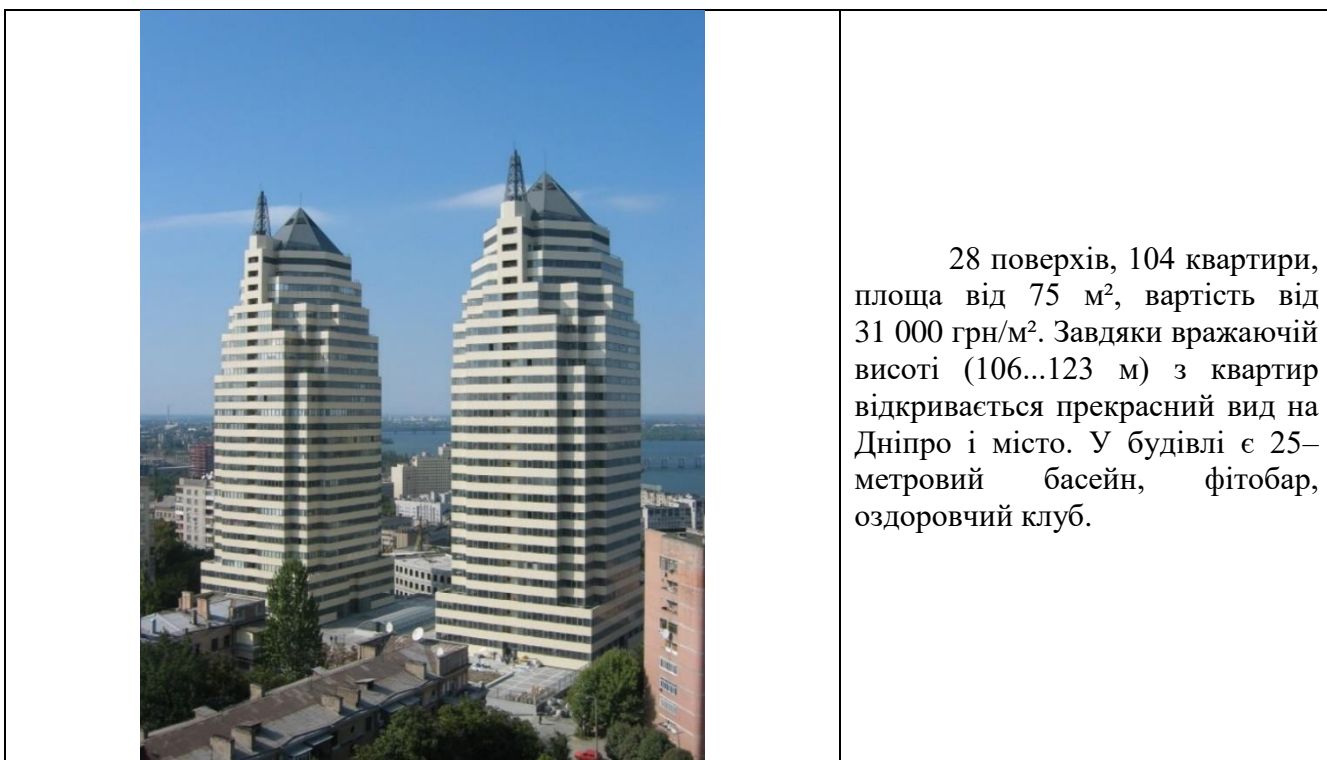


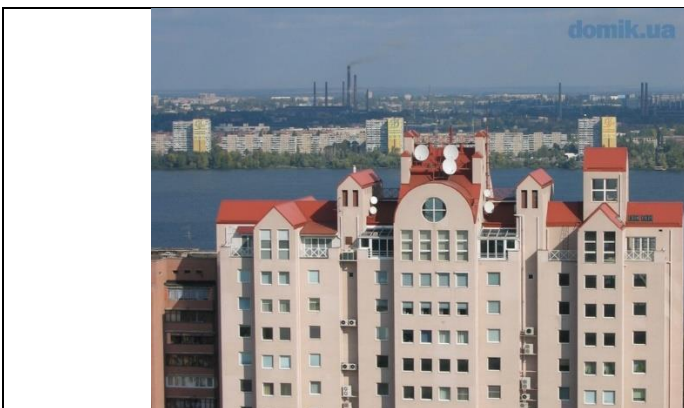
Рисунок 1.15 – ЖК Вежі – вулиця Володимира Вернадського, 35 Б



10 поверхів, площа від 150 м<sup>2</sup>, вартість – від 30 000 грн/м<sup>2</sup>. Один з найрозкішніших елітних комплексів. До послуг гостей фітнес-зал, басейн, прекрасний вид на Комсомольський острів, Набережну і Річку Дніпро.

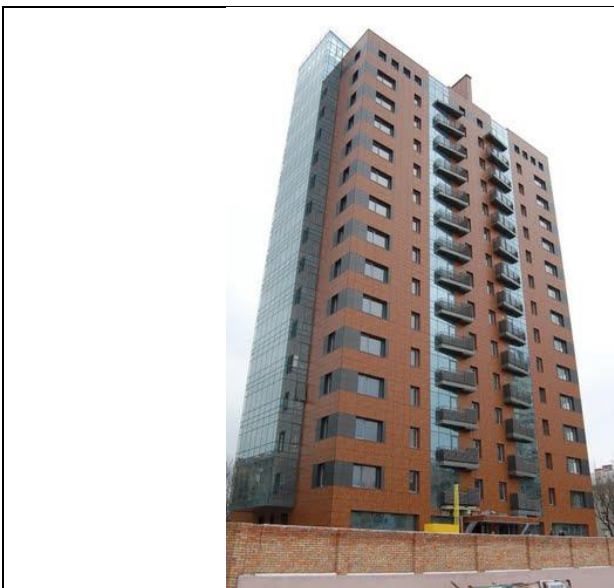
Рисунок 1.16 – ЖК Амстердам – вул. Шагумяна, 15

ЖК Бельведер (р-н парку Шевченко) (рис. 1.17).



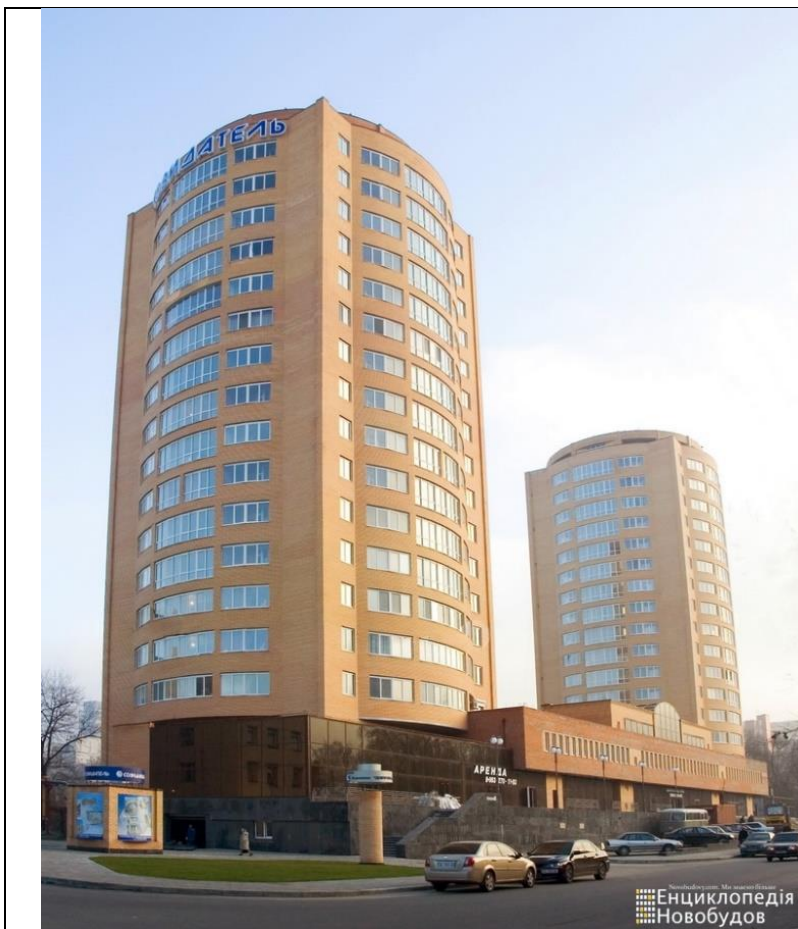
13 поверхів, 32 квартири, площа від 128 м<sup>2</sup>, вартість від 30 000 грн/м<sup>2</sup>. Унікальна архітектура, оригінальна не тільки фасад, але і планування квартир, пентхаусів на верхніх поверхах.

Рисунок 1.17 – ЖК Бельведер – вул. Шаумяна, 10



15 поверхів, 42 квартири, площа від 74,5 м<sup>2</sup>, вартість від 25 000 грн/м<sup>2</sup>. Фітнес-зал і салон на 1-му поверсі, зимовий сад – на 15-му. Хороший варіант для тих, хто віддає перевагу тиші і комфорту.

Рисунок 1.18 – ЖК Ворошилов вул. Ворошилова, 21 к



17 поверхів, площа від 65 м<sup>2</sup>, вартість від 25 000 грн/м<sup>2</sup>. На другому поверсі — тренажерний зал, кафетерій. Поруч з будівлею розташовані торгові центри, розважальні заклади і супермаркети.

Рисунок 1.19 – ЖК Дніпровський – вул. Баумана, 10



9–15 поверхів, площа від 80 м<sup>2</sup>, вартість – від 18 000 грн/м<sup>2</sup>. З апартаментів і пентхаусів можна побачити Монастирський острів, Новий міст через Дніпро. Три пентхауси з цікавим плануванням мають вихід на відкриту терасу.

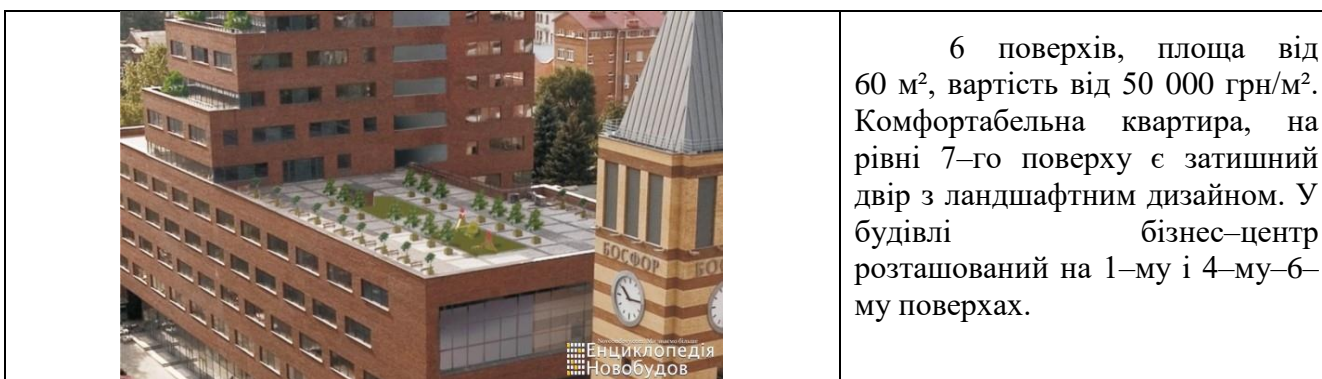
Рисунок 1.16 – Будинок Крейніна – вул. Крутогорна 33



18 поверхів, площа від 75 м<sup>2</sup>, вартість – від 18 500 грн/м<sup>2</sup>. Квартири просторі, планування передбачає консолідацію квартир або перепланування для мешканця. У будівлі є ресторан і торговий центр, офіси.

Рисунок 1.21 – ЖК Класичний – проспект Гагаріна, 23

ЖК Enigma – (рис. 1.22).



6 поверхів, площа від 60 м<sup>2</sup>, вартість від 50 000 грн/м<sup>2</sup>. Комфортабельна квартира, на рівні 7-го поверху є затишний двір з ландшафтним дизайном. У будівлі бізнес-центр розташований на 1-му і 4-му–6-му поверхах.

Рисунок 1.22 – ЖК Enigma – вул. Шевченка, 53



16 поверхів, 63 квартири, площею від 85 м<sup>2</sup>, вартість від 20 000 грн за м<sup>2</sup>. Перші два поверхи призначені для комерційної нерухомості. Поруч розташовані школи, дитячі садки для дітей, торгові центри і магазини. Панорамний вид на Дніпро.

Рисунок 1.23 – ЖК Аркадіївська вежа – вулиця Гоголя, 20 Б

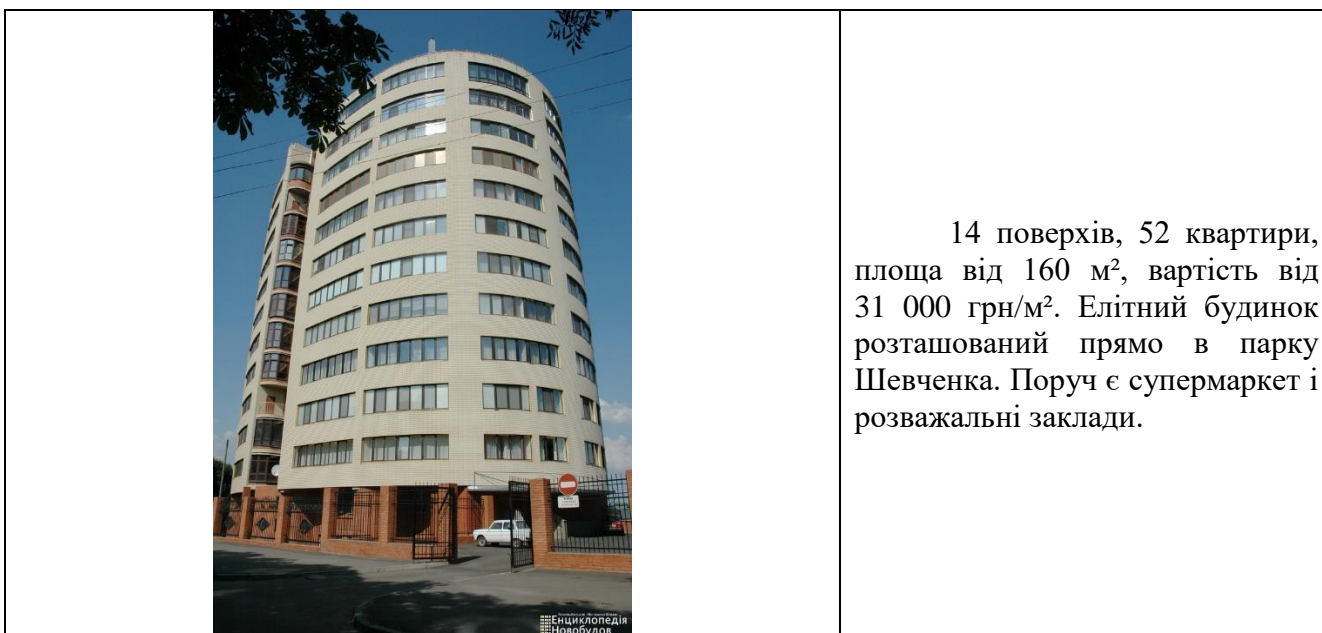


Рисунок 1.24 – ЖК Олександрійський – вул. Шевченка, 4

У багатьох житлових комплексах на перших поверхах є можливість розмістити комерційну нерухомість [19].

### 1.1.3 ЖК Bartolomeo Resort Town

Адрес: Дніпро, район Соборний, вул. Набережна Перемоги, 9б

Геолокація ЖК Bartolomeo Resort Town показана на рисунку 1.25.

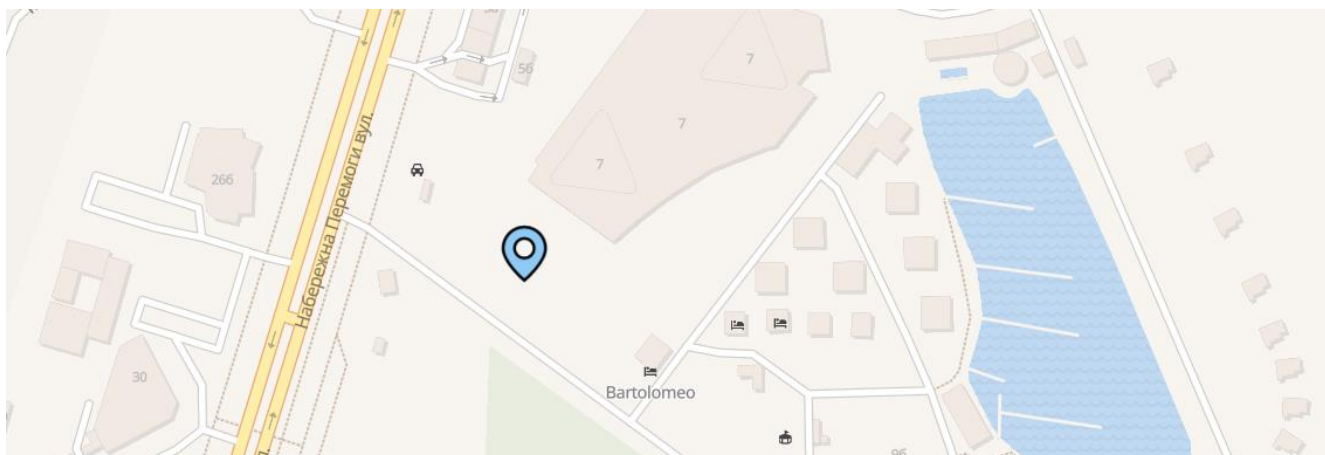


Рисунок 1.25 – Геолокація розташування ЖК Bartolomeo Resort Town

З фото рисунку 1.26 видно, що дизайн, атмосфера, кожен елемент цієї будівлі надихає, дає простір і сили для розвитку креативних ідей та їх втілення у

життя. Це місце, де гармонійно поєдналися стиль, елегантність і водночас комфортні умови для життя і роботи [14].



Рисунок 1.26 – Фото ЖК Bartolomeo Resort Town

ЖК Bartolomeo Resort Town має наступні переваги:

1. Готова інфраструктура в одному місці: паркова зона, дитячі майданчики, спорт-комплекс, ресторанный комплекс, продуктовий супермаркет преміального рівня, яхт-клуб, басейн, унікальна спа-зона, пляж, підземний паркінг.
2. Відмінне місце розташування і не в центрі серед метушні, і також біля центру – в тиші серед природи. 5...7 хвилин їзди на авто – і ти у центрі, 15 хвилин їзди до аеропорту, 15 хвилин їзди до вокзалу.
3. Чудові видові характеристики на р. Дніпро відкривається вже з 4-го поверху висотного будинку.
4. Дворівневий паркінг на 250 місць в першій і другій Вежі. Так само

доступна безкоштовна гостьова парковка.

5. Для любителів клубних будинків і обмеженої кількості сусідів – «амфітеатр», триповерхова будівля, у під'їзді 6 апартаментів, з просторою терасою (від 18 м<sup>2</sup>).
6. Власникам яхт – яхт-клуб у будинку, перший і єдиний комплекс, який це пропонує.
7. Технологічність у будівництві: сучасна технологія будівництва – монолітно-каркасна, енергоефективні матеріали в будівництві (утеплення фасадів із необхідним запасом, якісне панорамне скління Reunaers, ультрасучасна дахова котельня), прилади обліку світла/води/тепла [16].

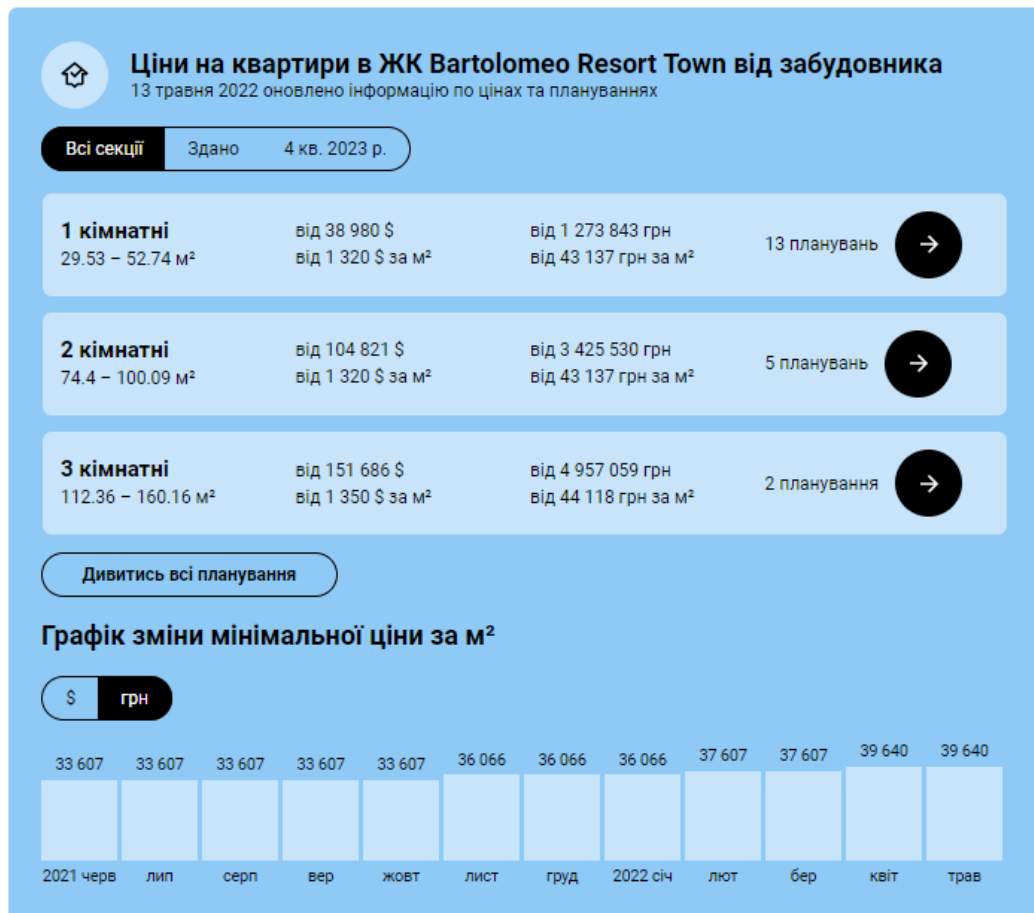


Рисунок 1.27 – Вартість житла у ЖК Bartolomeo Resort Town



## 1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

Одним з важливих напрямків успішного розвитку для житлового комплексу є автоматизація і диспетчеризація житлових, офісних і промислових приміщень.

Розумний житловий комплекс – це житловий комплекс з розвинутою цифровою інфраструктурою, що включає новітні інформаційні технології, розвинену інженерну мережу і сучасне обладнання.

Весь комплекс управляється єдиною цифровою системою, що дозволяє обслуговувати інжиніринг, а також надавати мешканцям всі необхідні послуги для комфортного проживання.

Цифрова система складається з набору підсистем, інтегрованих між собою:

- система життєзабезпечення будівлі, включаючи опалення, вентиляцію і дренаж,
- система управління, диспетчеризація будівель і обладнання, що дозволяє стежити за поточним станом техніки,
- система автоматизації однієї квартири,
- система безпеки та контролю доступу,
- мобільний додаток для зв'язку з комплексом управління та комерційними послугами,
- контроль за інженерним проектуванням зон загального користування, таких як вестибюль, паркінг, спортивний майданчик.

Управління всім комплексом відбувається через додаток, яке функціонально ділиться на дві частини:

- Частина для мешканців;
- Інтерфейс для управляючої компанії (збір і обробка даних про експлуатацію інженерних систем).

У сучасних реаліях, коли вартість часу значно зростає, розумна квартира дозволяє швидше виконувати домашні завдання.

Всі ми щомісяця стикаємося з тим, що необхідно передавати показання лічильника. Ті, хто живе в комплексах без автоматизації і спеціального додатка, роблять це вручну. Smart LCD дозволяє передавати всі дані автоматично.

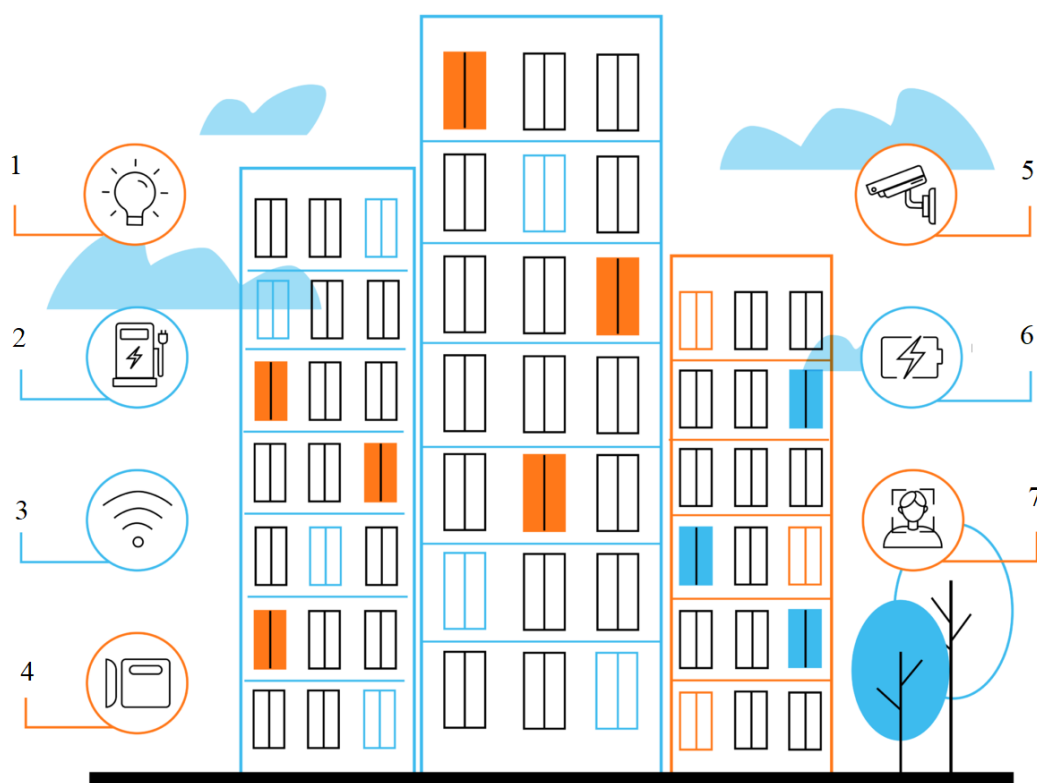


Рисунок 1.28 – Можливості розумного ЖК

- 1 – сценарії освітлення; 2 – зарядки для автомобілів;
- 3 – підсилювач Wi-Fi та сотової мережі у ліфтах та підземних паркінгах;
- 4 – домофона система; 5 – відеоспостереження (з доступом для мешканців);
- 6 – інформаційні сенсорні екрани, безпроводні і проводні зарядки;
- 7 – ідентифікація особи, обмеження доступу.

Головною перевагою для власників квартир в розумному житловому комплексі є швидкість вирішення побутових питань.

Найпопулярніші функції розумного РК-дисплея

Для мешканців:

- виклик майстра;
- замова абонементів на автомобілі гостей;
- оплата комунальних платежів і послуг.

Для керуючої компанії:

- надсилання сповіщень;
- збір запитів на виклик сервісних послуг;
- переглянути статистику платежів;
- управління орендою паркувальних місць.

У більшості квартир система «Розумний дім» – це всього лише набір розрізнених елементів, але в найближчому майбутньому єдина система розумного будинку стане звичною реальністю.

Перші прототипи розумних LCD були побудовані в 2010 роках. Від звичайної новобудови вона відрізнялася спеціальною енергозберігаючим системою, яка керувалася за допомогою комп'ютера.

Перший повноцінний розумний житловий комплекс був побудований в 2020 роках.

Однією з основних мотивацій забудовників до автоматизації інженерних систем житлового комплексу є здешевлення спожитих ресурсів в процесі експлуатації будівлі.

Окупності і забудовники, які думають про розумний житловий комплекс, цікавляться питанням ціни.

Точну вартість інтеграції назвати складно, вона залежить від сукупності факторів:

- концепція комплексу;
- кількість квартир;
- загальна площа;
- функціональність;

– побажання розробника.

Частка ринку розумних житлових комплексів зросте в найближчі п'ять років. І ця тенденція буде активно захоплювати масове будівництво. Обмеження в розвитку ринку можуть створити стандарти інтеграції розумної системи. Вимоги до розумних житлових комплексів в офіційних документах можуть не відображати необхідну «технічну начинку». Тому деякі новобудови з вбудованим обладнанням тільки номінально будуть вважатися розумним ЖК [20].

### **1.3 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань**

Інженерне обладнання може працювати в автономному режимі. Наприклад, може бути впроваджена автономна теплова станція. При цьому найпростіші засоби (найпростіший дисплей з текстовим екраном) передбачені для управління обладнанням і його управління. Ці найпростіші засоби управління і моніторингу можуть бути розширені, наприклад, у вигляді портативних консолей оператора або підключення ноутбука. Наступним етапом автоматизації є створення диспетчерської, яка являє собою, як правило, персональний комп'ютер серверного класу або робочу станцію з певним набором програмного забезпечення. В цьому випадку виникає питання вибору протоколу обміну інформацією.

Деякий час тому (приблизно до середини 1990–х років) виробники автоматичного обладнання використовували свої внутрішні закриті протоколи, тому після установки, наприклад, певного обладнання на тепловій станції замовник був змушений використовувати обладнання того ж виробника для автоматизації інших систем. Найширший спектр систем може бути автоматизований – від холодильних машин до обладнання для очищення води басейну, і жоден виробник не здатний виробляти весь спектр обладнання.

В результаті на будь-якому великому об'єкті буде встановлений певний комплект обладнання від різних виробників, кожен з яких добудує свої системи

окремими контролерами. Наприклад, холодильна машина – це повноцінний пристрій з власною системою управління, що працює в автономному режимі, але в процесі його експлуатації існує ряд параметрів, необхідних для роботи служби для контролю працездатності обладнання і виконання сервісних функцій.

Виникає питання про обмін інформацією між обладнанням різних виробників. Для вирішення цієї проблеми можна використовувати ряд протоколів – ModBus, RS485, ВАСnet. На цьому об'єкті був прийнятий протокол LON, розроблений незалежним виробником (Echelon, [www.echelon.com](http://www.echelon.com)) для уніфікації обладнання різних виробників. Цей протокол використовується сьогодні багатьма виробниками обладнання.

Використовувані протоколи обміну інформацією можуть бути визначені на рівні технічного завдання, або безпосередньо визначити виробника обладнання (так як замовник заздалегідь знає, з яким обладнанням він працює, він може визначити, наприклад, виробника панелей управління приводом насоса в технічному плані). Обладнання багатьох компаній дозволяє зробити вибір на момент установки – працювати за протоколом LON або за власним внутрішнім закритим протоколом. Якщо обладнання працює в автономному режимі, то неважливо, яким буде протокол обміну. Якщо є необхідність у створенні диспетчерської служби, системи повинні бути інтегровані і створити єдине інформаційне поле. При цьому пристрої, що поставляються, поставляються з певним набором файлів, створюється база даних пристроїв і надається доступ до будь-якого пристрою через шину зв'язку.

Найпростіша комунікаційна шина – це одна пара проводів. Автобус зв'язку має вимоги до імунітету. Існує програмне забезпечення різних рівнів. Залежно від типу системи буде обраний більш простий або більш складний (і більш дорогий) пакет, який підтримує розширений набір інтерфейсів. Вже на етапі складання технічного завдання замовник повинен визначити, яку структуру системи автоматизації він хоче отримати і в якій мірі деталізації він хоче реалізувати цю структуру, так як в деяких випадках достатньо автономного режиму роботи

інженерного обладнання. Наприклад, в даний час в Москві набула широкого поширення реконструкція старих будівель, наприклад, заводських будівель, для офісних приміщень або торгових площ.

Згідно зі стандартами, необхідно обладнати такі приміщення загальною обмінною вентиляцією. Для підтримки заданої температури припливного повітря в таких випадках зазвичай використовуються найпростіші контролери, які взагалі не підтримують ніяких протоколів обміну і працюють з одного датчика температури повітря подачі – система працює в автономному режимі. Інший варіант, якщо клієнт сам управляє об'єктом. В даному випадку він зацікавлений в зниженні експлуатаційних витрат і може реалізувати більш складну систему управління інженерним обладнанням, що дозволяє, завдяки більш гнучкому регулюванню параметрів мікроклімату, знизити витрати на енергію для кондиціонування об'єкта. Для забезпечення надійності та безпеки необхідно дотримуватися «правила цілісності системи». При цьому будь-який вентиляційний блок, кондиціонер розглядається як повноцінна система, яка може функціонувати автономна. Для цього кожна окрема система повинна управлятися одним контролером.

Сучасне обладнання автоматизації дає можливість управляти, наприклад, декількома кондиціонерами за допомогою одного контролера. З іншого боку, завжди можна розширити систему, коли кілька контролерів підключаються шиною зв'язку, наприклад, через протокол LON. Однак цикл опитування одного контролера набагато менше декількох контролерів на шині зв'язку, тобто при використанні декількох контролерів час відгуку системи збільшується. При проектуванні системи автоматизації враховуйте, чи є така затримка критичною для системи.

З'єднані системи повинні, по можливості, управлятися одним контролером, так як якщо різні контролери підключені шиною зв'язку, в разі розриву шини зв'язку система стане непрацездатною (необхідні параметри не можуть бути запитані і т. п.).

У разі використання одного контролера система може працювати в автономному режимі і при порушенні шини зв'язку. З тих же причин системи глобалізуються якомога менше – їх намагаються розділити на окремі сегменти, кожен з яких може працювати автономно. У разі виходу з ладу одного з сегментів системи інший сегмент залишається працездатним. З іншого боку, деякі системи вигідніше глобалізувати: наприклад, для вимірювання температури зовнішнього повітря немає сенсу ставити окремі датчики для кожної системи, для роботи яких потрібні такі дані. Зазвичай для вимірювання цього параметра використовуються два датчика, один з яких розташований на північній стороні будівлі, а другий – на південній. Виміряні температури усереднені за певним алгоритмом, враховуються час вимірювання (денні та нічні температури), час року (режими «зима» та «літній») тощо, що дозволяє уникнути різких змін режимів роботи обладнання у разі короткочасних коливань температури зовнішнього повітря. Ці дані про температуру на відкритому повітрі можуть бути використані всіма системами, які вимагають такої інформації.

Зі збільшенням кількості фізичних точок потік переданої інформації збільшується, тому у випадку з великими об'єктами для зниження трафіку використовується система розподілених серверів. Будівля розділена на сегменти. При використанні дерев'яної структури (сервера і декількох робочих станцій) сервер зарезервований для підвищення надійності – встановлюється резервний сервер з дзеркальною базою даних. При використанні розподілених серверів змінюється ідеологія побудови системи – виділяється окремий сегмент системи, і для цього сегмента сервер розміщується на певній кількості фізичних точок. Для цього сегмента можливий будь-який рівень деталізації. Перехресні запити по IP відправляються на сервер з робочих станцій, що зменшує трафік. При цьому пропускна здатність мережі набагато вище (рис. 1.28).

Розподілена серверна система: виділяється окремий сегмент системи, і для цього сегмента сервер розміщується на певній кількості фізичних точок. Для цього

сегмента можливий будь-який рівень деталізації. Перехресні запити по IP відправляються на сервер з робочих станцій, що зменшує трафік. у цьому випадку пропускна здатність мережі набагато вище.

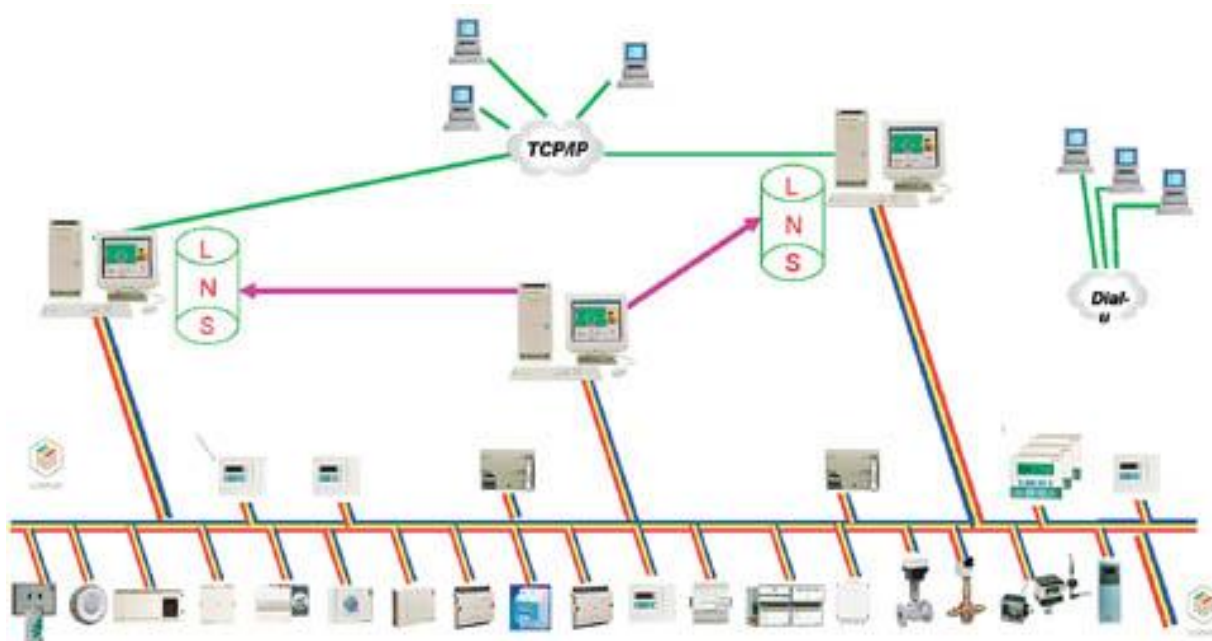


Рисунок 1.29 – Система розподілених серверів

В даний час серед фахівців немає єдиної думки, які будівлі можна назвати «розумними», і в чому різниця між «інтелектуальною будівлею» і високоавтоматизованою будівлею з розвиненою системою автоматизації і диспетчеризації. З іншого боку, часто немає реальної необхідності встановлювати високоавтоматизовані і тим більше «інтелектуальні» системи управління. В результаті в нашій країні реалізовано лише кілька об'єктів, які можна віднести до «інтелектуальних» об'єктів.

Наявність єдиного інформаційного поля (певного набору датчиків, сигналів і т. п.) дозволяє досягти будь-якого рівня «інтелекту» будівлі. Математична модель в даному випадку являє собою тривимірну матрицю, а варіант вибіркового дій з цієї матриці може бути доволно великим. Однак навіть у високоавтоматизованій будівлі деякі функції можуть не використовуватися через відсутність реальної потреби в них.



З точки зору автоматизації можна виділити три сегменти: автоматизація для малоповерхових житлових будинків (домашнє рішення), автоматизація для житлових і громадських будівель і споруд, автоматизація для промислових будівель.

Ідеологія систем автоматизації будівель для цих сегментів однакова. Ідеологія «розумного будинку» має на увазі, як правило, котедж «елітного» класу. Однак часто в організації єдиного інформаційного поля таких об'єктів немає необхідності. Для цього сегмента існують готові рішення, які не вимагають дорогої інженерії. Наприклад, котедж фактично можна розглядати як окремий пункт обігріву, що обслуговує кілька контурів (контур теплої підлоги, контури опалення першого і другого поверхів і т. п.), відповідно, є готовий контролер, призначений для вирішення цих проблем. Такі контролери мають на увазі фіксовану комбінацію підключеного периферійного обладнання і вимагають найпростішого введення в експлуатацію. У межах одного будинку немає необхідності в організації шини даних і т. п., хоча з технічної точки зору це цілком можливо.

Таке спрощення системи автоматизації знизило вартість системи – за невеликі гроші можна автоматизувати котедж площею понад 300 м<sup>2</sup>. В даний час при будівництві новобудов використовуються скляні фасади. котушки вентилятора, освітлення та жалюзі (рис. 1.30).

У будівлях зі скляними фасадами – щоб уникнути перегріву південно-орієнтованих приміщень влітку – використовуються спеціалізовані контролери, які поєднують в собі функції управління фан-котушками, освітленням і жалюзі. При впровадженні системи автоматизації на основі цих контролерів оцінюються вплив сонячної радіації, освітлення, температури, присутності людей в приміщенні, і в результаті обробки цієї інформації контролюються фан-котушки, освітлювальні прилади і жалюзі.



Рисунок 1.30 – Розташування компонентів системи автоматизації

При впровадженні системи автоматизації на основі цих контролерів оцінюються вплив сонячної радіації, освітлення, температури, присутності людей в приміщенні, і в результаті обробки цієї інформації контролюються фан–котушки, освітлювальні прилади і жалюзі. Набір цих функцій дозволяє дуже гнучко управляти мікрокліматом, підбираючи різні комбінації режимів роботи пристроїв, що запобігає перегріву приміщень і при цьому знижує навантаження на систему кондиціонування. Однак навряд чи реалізація цієї функції в окремій будівлі дозволяє назвати її «розумною».

Прикладом реалізації концепції «інтелектуального будівництва» можна вважати аеропорт Бориспіль. Ідеологія побудови системи автоматизації та диспетчеризації мала на увазі використання обладнання різних виробників, об'єднаного комунікаційною шиною. Завдяки відповідному програмному забезпеченню була створена єдина база даних, яка, в свою чергу, була підключена до системи управління розкладом польотів, тобто було створено єдине інформаційне поле. В аеропортовому комплексі досить високі вимоги до системи загальної обмінної вентиляції, але дуже великі площі призводять до значного споживання повітря. Була розроблена так звана «концепція оптимізації» – проект оптимізації роботи системи.

Залежно від розкладу польотів (планування польотів, звичайно, здійснюється спеціальною службою, яка жодним чином не пов'язана зі службою експлуатації інженерного обладнання), коефіцієнт умовного навантаження будівлі розраховується за кількістю пасажирів на годину (береться один з трьох станів цього коефіцієнта, що відповідає низькому, середньому і високому навантаженню), але не всієї будівлі в цілому, а окремих її зон.

Спочатку було визначено п'ять зон: зона вильоту, зона прибуття, зона очікування, дві окремі зони для міжнародних і внутрішніх рейсів, а потім ці великі зони були розділені на 27 менших підзон, мікроклімат яких забезпечувався окремими установками (зонування інженерної техніки). Ця «концепція оптимізації» була передбачена ще на етапі проектування інженерних систем, а обладнання забезпечувалося відповідними функціями (наприклад, вентиляційні установки були передбачені для багато-режимних). Реалізація концепції дозволила гнучко управляти інженерними системами в залежності від навантаження, щоб можна було, наприклад, взимку знизити температуру і відключити вентиляцію приміщень, в яких в даний час немає людей. В результаті створення єдиного інформаційного поля, інтеграції з «третьою стороною» у вигляді постачальника інформації та реалізації «концепції оптимізації» витрати на експлуатацію цього об'єкта знизилися, за попередніми оцінками, на 7...10 %.

Ще одним прикладом реалізації концепції «інтелектуальної будівлі» є одна з офісних будівель м. Києва. У цій будівлі створена система управління та диспетчеризації інженерного обладнання та офісного освітлення. Використовувалося обладнання автоматизації трьох різних виробників – система управління освітленням, автоматизація теплової станції, автоматизація іншого інженерного обладнання випускалася різними компаніями. Всі системи автоматизації були інтегровані за допомогою протоколу LON в єдину систему. У робочий час постійно вмикаються системи кондиціонування та освітлення. Через кілька годин або у вихідні дні, коли присутність людей не очікується, кондиціонер

працює в режимі очікування, а світло вимикається. Якщо в ці години в приміщенні знаходяться люди, їх наявність фіксується датчиками руху, а за сигналами від цих датчиків освітлення і відповідне обладнання в цій області включаються автоматично, без втручання оператора. При цьому на панель управління видається відповідний сигнал, і оператор може вносити корективи в режими роботи обладнання (наприклад, якщо будь-які роботи проводяться у великому приміщенні, то, незважаючи на наявність декількох робочих, система кондиціонування в ній може бути відключена) [21].

#### **1.4 Розробка схеми організаційної структури підприємства**

Організаційна структура житлового комплексу «Бартоломео» представлена на рисунку 1.31.

Житловий комплекс «Бартоломео» характеризується горизонтальним і вертикальним поділом праці обслуговуючого персоналу. Основним сенсом поділу праці є спеціалізація співробітників при виконанні окремих робіт, операцій, процедур. В основі розподілу лежить професійна риса.

Горизонтальний поділ праці – це поділ загального трудового процесу на різні приватні, безперервні, окремі види роботи зі спеціалізацією виробництва і виконавців. В основі цього поділу праці лежать функціональні, експлуатаційні та кваліфікаційні особливості.

Функціональний розподіл праці досягається за рахунок спеціалізації співробітників за видами діяльності. Розподіл праці на операційній основі пов'язаний зі спеціалізацією і обмеженнями при виконанні конкретних трудових операцій або роботи. Кваліфікаційний поділ праці базується на визначенні видів трудової діяльності, виходячи зі складності роботи і необхідної кваліфікації.

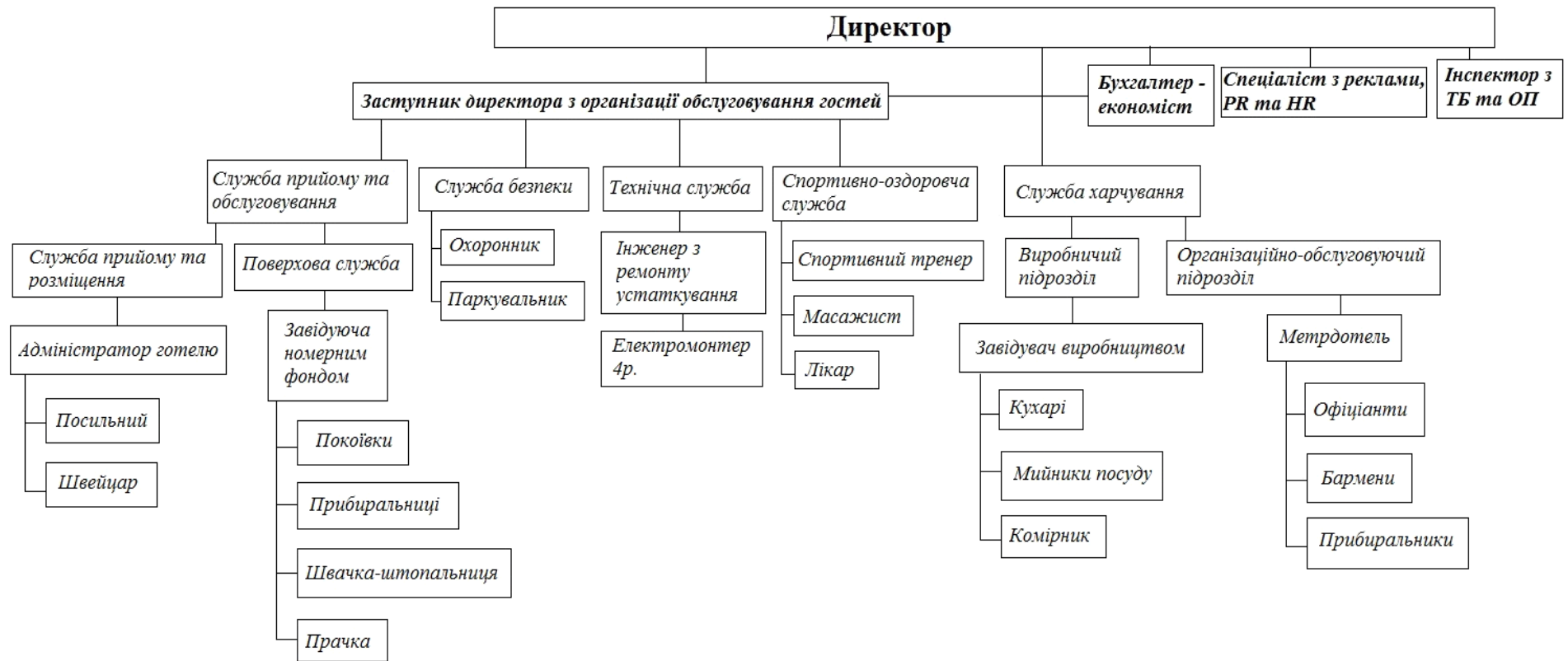


Рисунок 1.31 – Приклад організаційної структури управління підприємством

Вертикальний розподіл праці на підприємстві базується на принципах офіційного підпорядкування окремих служб і посадових осіб:

- загальне управління, спрямоване на розробку та реалізацію основних, перспективних напрямків діяльності підприємства;
- інноваційний менеджмент, завданням якого є розробка та впровадження передових технологій на основі впровадження сучасних форм управління виробництвом, комплексної механізації та автоматизації виробництва та окремих видів робіт (послуг); впровадження нових видів послуг та форм обслуговування;
- економічне управління, важливими функціональними обов'язками якого є розробка стратегічного і тактичного планування, аналіз господарської діяльності підприємства;
- оперативне управління, що полягає в підготовці і залученні до підрозділів (служб, змін, бригад і т. п.), а також окремих виконавців оперативних планів, розміщення виконавців на робочих місцях, їх інструктажу, організації систематичного контролю за ходом виробничо–технологічного процесу на підприємстві;
- управління персоналом, спрямоване на підбір і розміщення персоналу, розвиток і підвищення компетентності персоналу.

Певним чином обов'язки розподіляються між керівниками різних рівнів:

- менеджери нижчого рівня стежать за дотриманням виконавцями технологічної, трудової дисципліни та техніки безпеки;
- Менеджери середньої ланки забезпечують контроль і розробку певного кола питань, за які вони відповідають, і тим самим допомагають топ–менеджерам визначати управлінські рішення;
- топ–менеджери визначають стратегію розвитку підприємства, здійснюють загальне управління підприємством, приймають рішення з усіх питань, пов'язаних з його технічним, технологічним,

економічним і соціальним розвитком.

Відповідальна професійна організація колективу і організаційна структура підприємства дозволяє забезпечити ефективну роботу підприємства за допомогою:

- підбір і розміщення персоналу відповідно до технологічних процесів, обсягу робіт і посадових інструкцій, що регулюють права, обов'язки і обов'язки персоналу;
- визначення режиму їх роботи і відпочинку протягом дня, тижня відповідно до технологічного процесу, його складності і складності;
- підпорядкування певної кількості виконавців відповідним лінійним менеджерам певного рівня;
- виконання керівниками на всіх рівнях функцій планування, організації, контролю та мотивації роботи виконавців, що сприяє забезпеченню безперебійної роботи в покладених на них підрозділах;
- постійний пошук інноваційних методів роботи, що надає компанії конкурентні переваги в порівнянні з аналогічними підприємствами

### **1.5 Постановка завдання**

Завданням даної кваліфікаційної роботи є розробка кіберфізичної системи домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі.

Ураховуючи існуючу на підприємстві архітектуру мережі з попередньою кількістю підмереж, їх взаємозв'язками і кількістю комп'ютерів та обладнанням необхідно виконати розрахунок налаштувань для заданої топології мережі, здійснити вибір інтерфейсу каналів зв'язку та протоколу обміну, провести розрахунок топологічної схеми комп'ютерної системи, розрахунок налаштувань маршрутизації комп'ютерної мережі, а також виконати подальше моделювання і перевірки роботи комп'ютерної системи.

Окрім того необхідно провести аналіз проектування нової мережі підприємства, виконати вибір відповідного фізичного середовища, кабелів, портів і з'єднувачів для підключення мережевих пристроїв до інших пристроїв мережі і вузлів, вибір мережевих пристроїв і компонентів, необхідних для задоволення технічних вимог мережі і аналітичні розрахунки споживаної потужності, об'ємів і швидкостей передачі даних каналами мережі з урахуванням вибраних апаратних засобів, затримок на обробку даних на вузлах мережі.



## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА**

### **2.1 Технічні вимоги до комп'ютерної системи**

Кіберфізична система домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі – далі Система.

Система повинна забезпечувати можливість єдиного доступу користувачів до платформ, формування єдиної бази користувачів як авторів проектів, так і сервісу або їх підтримки.

Функціонування системи повинно відповідати наступним критеріям: забезпечити безперебійне функціонування системи; забезпечення мінімального часу обслуговування; забезпечити можливість роботи в різних режимах.

### **2.1 Найменування і сфера застосування системи**

Об'єкт: Об'єктом контролю є індивідуальне житло, гаражі, дачі, автомобілі і інші стаціонарні об'єкти приватної власності.

Мета: метою проекту є впровадження сучасних безпроводних комп'ютеризованих мереж передачі даних в технологію видаленого контролю стану об'єктів індивідуальної власності і завдання для них режимів охорони.

Сфера застосування : Охоронна GSM– система призначена для забезпечення охоронних відомств, приватної колективної охорони, приватних осіб програмно–апаратними засобами для проведення контролю і управління станом видалених стаціонарних об'єктів житлового і нежитлового фонду, таких як індивідуальне житло, гаражі, дачі, автомобілі і інші стаціонарні об'єкти приватної і державної власності.

## **2.2 Вимоги до системи в цілому**

### **2.2.1 Показники призначення**

Система призначена для організації охоронній і пожежній сигналізації на видалених об'єктах, таких як заміський будинок або дача, де неможлива постійна присутність людини. У разі виникнення позаштатних ситуацій, хазяїна або диспетчерський пункт інформуватиме автоматична система, на основі мікроконтролера і сигналів, що поступають на нього, з різних датчиків, пов'язаного з каналами передачі даних GSM. Така система допоможе запобігти збитку, нанесеному зловмисниками внаслідок проникнення і крадіжки цінностей, попередити займання об'єкту, або інших неприємних ситуацій. Усі ці заходи спрямовані на те, щоб зберегти матеріальні блага людей, їх майно, ну і, звичайно ж, здоров'я в психологічному плані.

При розробці системи слід враховувати наступні чинники:

- деякі, найбільш важливі технологічні процеси повинні контролюватися людиною;
- диспетчер несе відповідальність хід процесу охорони, його втручання в процес відбувається в обумовлених ситуаціях;
- у непередбачених ситуаціях час ухвалення рішень диспетчером обмежений секундами.

### **2.2.2 Вимоги до структури і функціонування системи**

Система розробляється на основі вивчення, аналізу і узагальнення досвіду експлуатації аналогічної апаратури, досягнень науки і техніки з урахуванням вітчизняного і зарубіжного досвіду, а також результатів і матеріалів другою виробничою і переддипломною практик.

Система повинна виконувати наступні основні функції:

- запиту стану для усіх ланцюгів контролю об'єкту, що охороняється;

- декілька каналів для підключення навантажень, забезпечивши управління ними як по безпроводному каналу, так і залежно від виміряних значень;
- підключення пасивних охоронних(магнітно–контактних) датчиків з нормально–замкнутими контактами, сполучених послідовно в ланцюг шлейфу сигналізації або датчиків з нормально–розімкненими контактами, сполученими паралельно;
- підключення датчиків з активним виходом до 24 В;
- забезпечення гнучкого налаштування режиму стеження за лінією;
- передбачити канали для підключення ліній дротяних датчиків стандарту 1Wire, з кількістю датчиків в кожній лінії – до 16 і довгою шлейфу до 100 м;
- передбачити канали для підключення ліній управління з параметрами комутації, не гірше ~220 В, 1 А;
- налаштування пристрою повинні задаватися за допомогою спеціальної програми, що встановлюється на будь–якому персональному комп'ютері з інтерфейсом USB.

Вимагається реалізувати можливість швидкого доступу до динамічно змінюваних даних, можливості їх аналізу і порівняння за які–небудь конкретні періоди часу. У цій розробці здійснення якісної обробки і зберігання внутрісистемної інформації пропонується реалізувати за допомогою використання спеціалізованої бази даних (БД).

Система повинна забезпечувати можливість:

- централізованого стеження за станом об'єкту в інтерактивному режимі;
- збір і зберігання даних, що поступають, про стан усіх об'єктів (стан датчиків, виконавчих механізмів), що охороняються;

- система повинна зберігати працездатність при заміні функціональних блоків запасними, при цьому допускається підстроювання за допомогою функцій коригування;
- система повинна реалізовувати двосторонній канал передачі даних від об'єктів, що охороняються, до диспетчера (серверу БД) без перебоїв.

До складу системи мають бути включені наступні функціональні структури:

- охоронні блоки – комплект програмно–апаратного устаткування, що забезпечує функції контролю і управління для об'єкту, що охороняється, а також наявністю безпроводного каналу зв'язку з диспетчерським пультом і дротяним або безпроводним каналом зв'язку з блоками розширення (охоронними);
- охоронні блоки розширення – комплект програмно–апаратного устаткування, що забезпечує додаткові функції контролю і управління для об'єкту, що охороняється, а також наявністю безпроводного каналу зв'язку з охоронними блоками;
- диспетчерський термінал або диспетчерський пункт управління, що має безпроводною двосторонній канал зв'язку для здійснення отримання, обробки і зберігання даних від охоронних блоків.

### **2.2.3 Склад системи**

Технічні засоби, що входять до складу мікропроцесорної індивідуальної охоронної системи з виходом на канал GSM, наступний :

#### **1) Устаткування робочого місця диспетчера:**

- IBM– сумісний комп'ютер для моніторингу стану об'єктів управління, що охороняються;
- IBM– сумісний комп'ютер в якості сервера;
- GPS– приймач диференціальної поправки з інтерфейсом RS – 232;

- програмований радіо–модем з можливістю підключення декількох пристроїв по інтерфейсу RS – 232 і Ethernet– адаптером для підключення до мережі;
- програмне забезпечення.

## 2) Об'єкт, що охороняється :

- охоронні блоки з необхідними датчиками і виконавчими пристроями;
- охоронні блоки розширення необхідними датчиками і виконавчими пристроями;
- диспетчерський термінал або диспетчерський пункт управління.

### 2.2.4 Технічні вимоги до системи

- GPRS, GPS– приймачі, радіо–модем повинні мати модульне виконання, щоб забезпечити максимальну гнучкість при експлуатації і наладці;
- застосування частоти радіоапаратури має бути ліцензоване державним органом нагляду частот;
- дозвіл на використання радіоустаткування;
- дозвіл на експлуатацію радіоустаткування.

### 2.2.5 Вимоги до структури для підсистеми передачі даних

- використовується деревовидна топологія;
- висока завадозахищеність;
- висока надійність передачі інформації;
- гнучкість конфігурації(для можливості швидкого і технічно зміни, що просто реалізовується, як складу мережі, так і зв'язків між окремими вузлами);
- можливість підключення до додаткових вузлів введення/виведення інформації.

### **2.2.6 Вимоги до функцій, що виконуються системою**

Система має бути виконана відкритою і повинна дозволяти здійснювати технічну і програмну модернізацію системи.

Система повинна забезпечувати виконання наступних функцій :

- постійний моніторинг ситуації – реєстрацію, обробку, запис, зберігання отримуваної інформації у базі даних комп'ютера, що знаходиться в диспетчерській;
- обробку запитів диспетчера – автоматизоване відтворення інформації;
- аналіз і редагування даних, виведення результатів на екран;
- безперервний контроль усіх параметрів безпеки;
- підвищення якості контролю параметрів і оперативності спрацьовування захист від неприпустимих режимів роботи.

### **2.2.7 Вимоги до безпеки і надійності**

Для забезпечення безпеки і надійності управління процесом контролю і управління система повинна задовольняти наступним вимогам:

- ніяка одинична відмова устаткування не повинна призводити до видачі неправдивої команди управління;
- ніяка одинична помилка оператора не повинна призводити до видачі неправдивої команди управління(реалізація механізмів виявлення і попередження критичної невідповідності між командами, що вводяться, і шаблонами основних системних налаштувань, що зберігаються у базі даних);
- усі операції управління мають бути інтуїтивно зрозумілі диспетчерові;
- забезпечення відмовостійкості усієї системи при виході з ладу устаткування одного або декількох охоронних пристроїв;
- використане радіоустаткування устаткування має бути рекомендоване виробником до використання на контрольованих і керованих об'єктах.

## **2.3 Вимоги до обслуговування і експлуатації системи**

### **2.3.1 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи**

Система призначена для безперервної роботи.

Виходячи з технічної і економічної доцільності, конструктивних рішень облаштувань системи, особливостей і умов експлуатації системи, прийняті наступні показники і вимоги надійності :

- середній час відновлення не більше 30 хв.(крупно–вузловий ремонт);
- середній термін служби системи не менше 5 років;
- вірогідність безвідмовної роботи не менше 10 000 ч. (по основних функціях).

Система повинна зберігати працездатність при заміні функціональних блоків запасними. При цьому допускається підстроювання за допомогою регулювальних елементів або функцій.

Складові частини системи мають бути піддані приробленню впродовж 12 годин.

У приміщенні диспетчерської, де розташовується обчислювальна техніка, необхідно забезпечити наступні кліматичні умови:

- температура навколишнього повітря 5...40 С;
- відносна вологість повітря 95 %;
- атмосферний тиск 84...106,7 кПа;
- для захисту обчислювальної техніки від дії сильних електромагнітних полів стіни, поли, стеля в приміщенні диспетчерської необхідно екранувати;
- приміщення має бути обладнане системою кондиціонування повітря;

- кліматичні умови, в яких повинне експлуатуватися устаткування системи :
- кліматичне виконання по ГОСТ 15150 – 69 УХЛ;
- категорія розміщення по ГОСТ 15150–69 5.
- електроживлення модулів здійснюється від джерел живлення з напругою живлення не більше 24 В;
- робочий діапазон температур від  $-30^{\circ}\text{C}$  до  $+70^{\circ}\text{C}$ ;
- вібростійка при 50 Гц з прискоренням  $50 \text{ м/с}^2$  впродовж 4 годин;
- удароміцність з максимальним прискоренням  $100 \text{ м/с}^2$  10 000 ударів.

### **2.3.2 Вимоги до упаковки і транспортування**

Система має бути піддана консервації відповідно до ГОСТ 9.014. Вироби системи, і документація, мають бути упаковані в ящики, масою брутто не більше 10 кг, виконані відповідно до ГОСТ 2991.

Система в упакованому виді повинна витримувати без ушкоджень транспортне трясіння з прискоренням  $30 \text{ м/с}^2$  при частоті від 80 до 120 ударів в хвилину впродовж 2 ч. чи 10 000 ударів з тим же прискоренням. На тарі, в яку упаковані вироби системи, має бути нанесена по трафарету транспортна маркіровка з вказівкою маніпуляційних знаків по ГОСТ 14192 «Обережно крихке», «Боїться вогкості», «Верх, не кантувати».

Транспортування дозволяється будь-яким видом критого транспорту, окрім відкритих палуб морського, річкового і в негерметизованих, не опалюваних відсіках повітряного транспорту, а також не допускається транспортування системи в райони з холодним кліматом в зимовий час. Розставлення і кріплення ящиків, з упакованою системою, повинні забезпечувати стійке положення при транспортуванні, зміщення, що виключає, і удари їх між собою. При



транспортуванні в контейнерах система має бути закріплена для запобігання ушкодженням. При цьому допускається ящикну упаковку не застосовувати.

При тривалості зберігання понад три роки система має бути піддана ревізії і пері–консервації.

### **2.3.3 Вимоги до чисельності і кваліфікації персоналу, який обслуговує систему і режими її роботи**

Підготовка фахівців, операторів по експлуатації, фахівців з програмного супроводу систем управління здійснюється на спеціалізованих курсах різних фірм, курсах підвищення кваліфікації. Нині в учбові плани ряду технічних університетів вводяться дисципліни, пов'язані з вивченням спеціалізованих систем управління об'єктами із складною(наприклад, виробничою) структурою. Спеціальна література по подібних системах відсутня; на даний момент є лише окремі статті і рекламні проспекти, велика частина яких розміщена в мережі інтернет.

## **2.4 Вимоги до програмної підсистеми**

### **2.4.1 Перелік функцій підсистеми занесення інформації у БД**

Підсистема використовується для організації автоматичного занесення інформації про зміни станів об'єкту, що охороняється, заноситься у базу даних і призначеною, передусім для:

- відображення стану датчиків і виконавчих механізмів на об'єкті, що охороняється;
- стійкості роботи в аварійних ситуаціях;
- забезпечення надійної роботи системи;
- накопичення технологічних параметрів за певний проміжок часу з можливістю побудови графіків за наявними даними;
- ведення журналу (бази даних) про події, що сталися.
- висновок повідомлень про втрату зв'язку або аварії.

### **2.4.2 Застосування систем управління базами даних**

В ході розробки системи було встановлено, що усі вимоги до функцій управління і зберігання інформації вже реалізовані в готових програмних продуктах, тому є сенс використати існуючі рішення, такі як MS SQL Server 2 000, при проектуванні структури баз даних, використовуюваної для роботи з внутрісистемною інформацією.

### **2.4.3 Вимоги до ПО**

Програма повинна забезпечити інтерактивне стеження за об'єктом, відображати усі зміни, що відбуваються, вносити усі дані про зміну стану датчиків і виконавчих механізмів у базу даних. Програмне забезпечення повинне точно відображати графічно місцезнаходження об'єктів управління і їх параметри і стан.

### **2.4.4 Вимоги до збереження інформації**

Програмне забезпечення рекомендується зберігати на будь-якому зручному носії інформації, зі збереженням резервної копії на знімному носії інформації. Рекомендується вводити обмеження доступу до програми, окрім персоналу, безпосередньо обслуговуючого програмний виріб.

### **2.4.5 Вимоги до захисту інформації від несанкціонованого доступу**

В цілях попередження аварій і нещасних випадків категорично забороняється допуск до монтажу, наладки, обслуговування і ремонту системи осіб, що не мають на те відповідного дозволу і що не ознайомилися з керівництвом, вносити зміни в апаратуру без узгодження із заводом виробником.

Має бути забезпечений програмний і апаратний захист від некваліфікованих дій користувача і від спроб несанкціонованого доступу користувачів до

внутрішньої інформації. Залежно від статусу користувача мають бути передбачені різні рівні доступу до внутрішньої інформації.

Цілісність даних передаваних по радіоканалу має бути захищена за допомогою засобів радіоапаратури і додаткового захисту не потребує.

## 3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

### 3.1 Розрахунок схеми адресації корпоративної мережі

Згідно технічних вимог до виконання КС житлового комплексу «Бартоломео», використаний адресний простір 10.68.0.0/22, а для адресації каналів між маршрутизаторами застосований блок адрес для: 10.0.10.0/24. Розподіл IP-адрес виконаний згідно до вимог, вказаних в таблиці 3.1.

Таблиця 3.1 – Кількість вузлів в підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
33	45	120	30	123

Таблиця 3.2 – Схема адресації мережі КС

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN4	123	10.68.0.0	255.255.255.128	10.68.0.1 – 10.68.0.126
LAN2	120	10.68.0.128	255.255.255.128	10.68.0.129–10.68.0.254
LAN1	45	10.68.1.0	255.255.255.192	10.68.1.1 – 10.68.1.62
LAN3	30	10.68.1.64	255.255.255.224	10.68.1.65 – 10.68.1.94
VLAN20	30	10.68.0.0	255.255.255.224	10.68.0.1 – 10.68.0.30
VLAN30	30	10.68.0.32	255.255.255.224	10.68.0.33 – 10.68.0.62
VLAN40	30	10.68.0.64	255.255.255.224	10.68.0.65 – 10.68.0.94
VLAN99	30	10.68.0.96	255.255.255.224	10.68.0.97 – 10.68.0.126
WAN1	2	10.0.10.0	255.255.255.252	10.0.10.1 – 10.0.10.2
WAN2	2	10.0.10.4	255.255.255.252	10.0.10.5 – 10.0.10.6
WAN3	2	10.0.10.8	255.255.255.252	10.0.10.9 – 10.0.10.10
WAN IPS	2	209.165.202.0	255.255.255.224	209.165.202.1– 209.165.202.2
WAN Remout	2	64.100.13.0	255.255.255.252	64.100.13.1–64.100.13.2

Таблиця 3.3 – Схема адресації пристроїв мережі

Ім'я пристрою	Інтер- фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключе ного пристрою
LAN3						
Gudakov_R1	G0/1	10.68.1.65	/27	–	–	G0/0
	S0/0/0	10.0.10.1	/30	–	–	S0/1/0
	S0/0/1	10.0.10.5	/30	–	–	S0/0/1
Gudakov_Sw1	Vlan1	10.68.1.66	/27	10.68.1.65	–	G0/0
ServerDNS	NIC	10.68.1.85	/27	10.68.1.65	–	Fa0/24
PC_L1–PC_L8	NIC	10.68.1.94– 10.68.1.82	/27	10.68.1.65	–	Fa0/1– Fa0/8
PrinterK	NIC	10.68.1.75	/27	10.68.1.65	–	Fa0/23
LAN2						
Gudakov_R2	G0/1	10.68.1.129	/25	–	–	G0/0
	S0/0/1	10.0.10.2	/30	–	–	S0/0/1
Gudakov_Sw2	Vlan1	10.68.1.130	/25	10.68.1.129		G0/1
PrinterA	NIC	10.68.1.139	/25	10.68.1.129		F0/23
PC_A1–PC_A7	NIC	10.68.0.254– 10.68.0.242	/25	10.68.1.129		F0/0–F0/7
Server_HTTP	NIC	10.68.0.149	/25	10.68.1.129		F0/24
LAN1						
Gudakov_R3	G0/0	10.68.1.1	/26	–	–	G0/1
	S0/0/0	10.0.10.6	/30	–	–	S0/0/0
	S0/0/1	10.0.10.10	/30	–	–	S0/0/1
	S0/1/0	209.165.202. 2	/27	–	–	S0/1/0
Gudakov_Sw3	Vlan1	10.68.1.2	/26	10.68.1.1	–	G0/1
PC_Gos1– PC_Gos8	NIC	10.68.1.62– 10.68.1.50	/26	10.68.1.1	–	Fa0/1– Fa0/8
PrinterGos	NIC	10.68.1.10	/26	10.68.1.1	–	Fa0/24
LAN4						
Gudakov_R4	G0/1	–	–	–	–	–
	G0/1.2 0	10.68.0.33	/27	–	20	G0/1
	G0/1.3 0	10.68.0.65	/27	–	30	G0/1
	G0/1.4 0	10.68.0.97	/27	–	40	G0/1
	G0/0.9 9	10.68.0.1	/27	–	99	G0/1
ServerTFTP.23	NIC	10.68.0.75	/27	10.68.0.65	–	Fa0/15
PC20.1–PC20.3	NIC	10.68.0.62– 10.68.0.59	/27	10.68.0.33	20	Fa0/4– Fa0/8

PC30.1–PC30.3	NIC	10.680.94– 10.68.0.90	/27	10.68.0.65	30	Fa0/10– Fa0/14
PC40.1–PC40.3	NIC	10.68.0.126– 10.68.0.124	/27	10.68.0.97	40	Fa0/21– Fa0/24
Gudakov_Sw4.1	F0/24	10.68.1.2	/27	10.68.1.1	99	–
Gudakov_Sw4.2	F0/1	10.68.1.3	/27	10.68.1.1	99	–
IPS						
Rout_IPS	S0/0/0	209.165.202. 1	/27	–	–	S0/0/0
Server_IPS	NIC	209.165.200. 5	/25	209.165.200.5	–	G0/0
LAN5						
Gudakov_R0	G0/1	10.68.1.65	/27	–	–	G0/0
	S0/0/0	10.0.10.1	/30	–	–	S0/1/0
	S0/0/1	10.0.10.5	/30	–	–	S0/0/1
Gudakov_Sw1	Vlan1	10.68.1.66	/27	10.68.1.65	–	G0/0
ServerDNS	NIC	10.68.1.85	/27	10.68.1.65	–	Fa0/24
PC_L1– PC_L8	NIC	10.68.1.94– 10.68.1.82	/27	10.68.1.65	–	Fa0/1– Fa0/8
PrinterK	NIC	10.68.1.75	/27	10.68.1.65	–	Fa0/23

### 3.2 Розробка топологічної схеми корпоративної мережі

Розроблена топологічна схема кберфізичної система домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі, яка містить ідентифікатор VLAN ID, представлена на рисунку. 3.1.

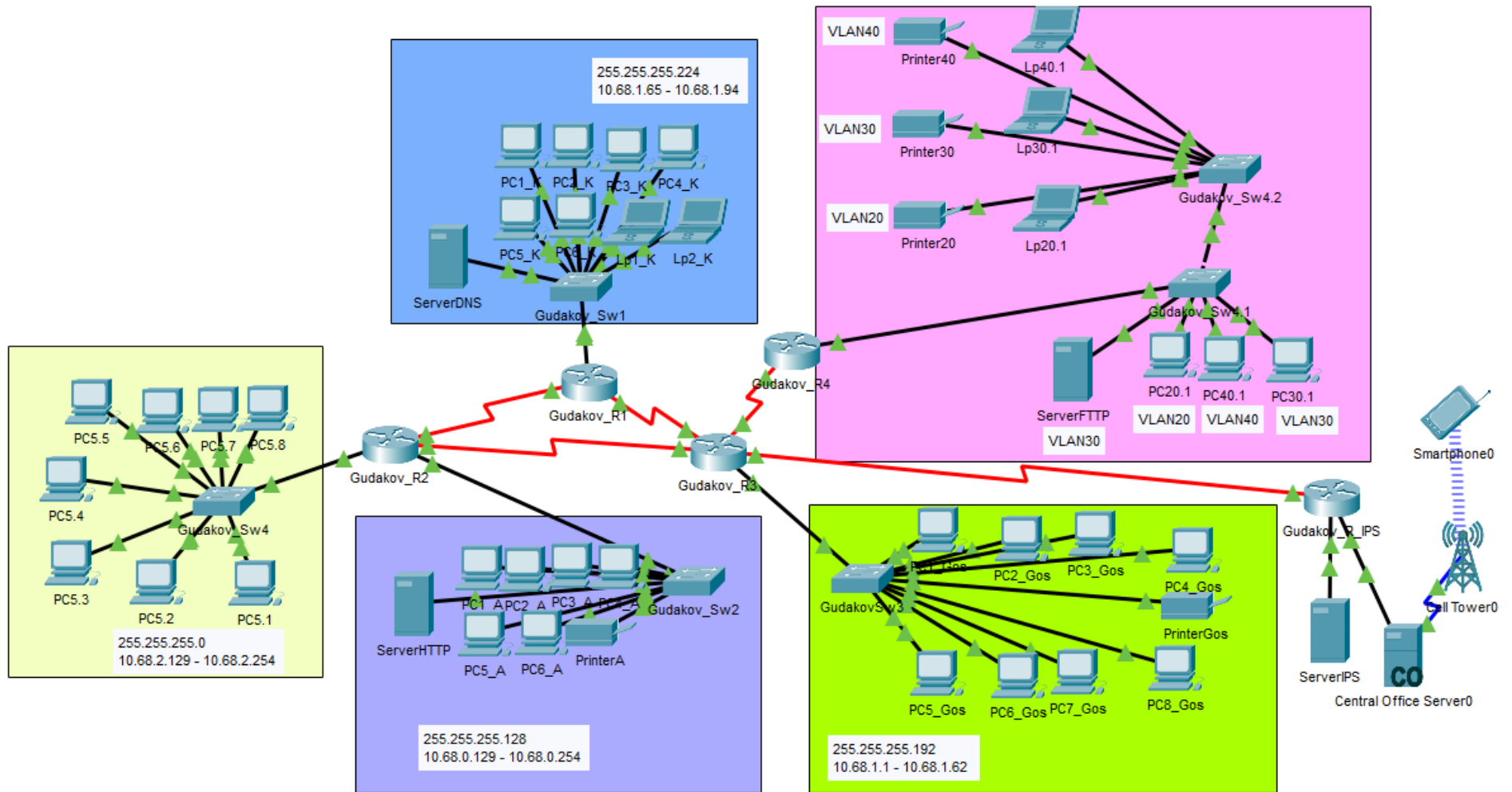


Рисунок 3.1 – Архітектура КС

### 3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

В КС житлового комплексу «Бартоломео», згідно технічних вимог, застосований протокол динамічної маршрутизації OSPF, який є дистанційно–векторним протоколом, з номером автономної системи 23.

При налаштуванні маршрутизації на роутерах даної КС, на serial–інтерфейсах, відповідно до технічних умов, встановлено пропускну спроможність 128 Кб/с , вартість метрики 7500 та швидкість каналу 128000.

```
Gudakov_R4(config)#interface s0/1/0
```

```
Gudakov_R4(config-if)#bandwidth 128
```

```
Gudakov_R4(config-if)# clock rate 128000
```

### 3.4 Налаштування та перевірка роботи комп'ютерної системи

#### 3.4.1 Базове налаштування конфігурації пристроїв

Процес базового налаштування конфігурації активних мережних пристроїв включає:

- застосування сервісу шифрування паролів;
- захист привілейованого режиму ОС, консольного порту та ліній vty;
- призначення банера MOTD;
- для віддаленого доступу до пристрою на лініях vty застосований протокол SSH;
- створено локальні облікові записи (*username 12318\_Gudakov*) з паролем *adminisco12318*;
- створено доменне ім'я пристрою (*ip domain-name Gudakov\_R1*);
- створено ключ RSA завдовжки 1024 біт для шифрування даних.

Приклад базових налаштувань на роутері R1.

Заборонено пошук DNS на маршрутизаторі:

```
Router(config)#no ip domain-lookup
```



Задання пристрою унікального імені:

```
Router(config)#hostname Gudakov_R1
```

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

```
Gudakov_R1(config)#service password-encryption
```

Встановлення паролю на вхід до привілейованого режиму:

```
Gudakov_R1(config)#enable secret class12318
```

Встановлено паролю на вхід до консольної лінії:

```
Gudakov_R1(config)#line console 0
```

```
Gudakov_R1(config-line)#password cisco12318
```

Налаштування запиту пароля при вході:

```
Gudakov_R1(config-line)#login
```

```
Gudakov_R1(config-line)#exit
```

Налаштування банера MOTD:

```
Gudakov_R1(config)#banner motd # 123-18 Gudakov. Enter only have key#
```

Налаштування протоколу SSH, Створення користувача:

```
Gudakov_R1(config)#username 12318_Gudakov password admincisco;
```

Створення домену:

```
Gudakov_R1(config)#ip domain-name Gudakov_R1
```

Для шифрування даних створено ключ RSA довжиною 1024 біт:

```
Gudakov_R1(config)#crypto key generate rsa
```

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Налаштування лінії VTY:

```
Gudakov_R1(config)#line vty 0 4
```

Встановлення необхідності введення логіну та пароля для входу лінії:

```
Gudakov_R1(config-line)#login local
```

Встановлення входу на лінію тільки по протоколу SSH:

```
Gudakov_R1(config-line)#transport input ssh
```

Встановлення IPv4-адрес відповідно до таблиці 3.3:

```
Gudakov_R1(config)#interface g0/1
```

```
Gudakov_R1 (config-if)# ip address 10.22.208.1 255.255.255.0
```

Для запуску інтерфейсу до роботи слід його обов'язково увімкнути:

```
Gudakov_R1(config-if)#no shutdown
```

### 3.4.2 Налаштування маршрутизаторів корпоративної мережі

Згідно технічних вимог, в мережі житлового комплексу «Бартоломео» використовується протокол динамічної маршрутизації OSPF 23. 23 – номер автономної системи, це сукупність мереж під єдиним адміністративним керуванням, що забезпечує загальну для всіх вхідних в автономну систему маршрутизаторів політику маршрутизації..

OSPF має такі переваги:

- висока швидкість збіжності в порівнянні з дистанційно-векторними протоколами маршрутизації;
- підтримка мережевих масок змінної довжини (VLSM);
- оптимальне використання пропускної здатності з побудовою дерева найкоротших шляхів.

Для кожного маршрутизатора оголошені безпосередньо підключені мережі і відключено поширення оновлень маршрутизації на інтерфейси в локальні мережі. На Gudakov \_R4 налаштований маршрут за замовчуванням в інтернет (ISP) і поширене його через оновлення маршрутизації OSPF.

Включити протокол OSPF на маршрутизаторі командою:

```
Gudakov _R4(config)#router ospf 23
```

Задати дентифікатор маршрутизатора (router ID) – унікальне 32-бітове число, яке унікально ідентифікує маршрутизатор в межах однієї автономної системи.

```
Gudakov _R4(config)#router-id 17.17.17.17
```

Протоколу потрібно об'явити мережі, підключені до маршрутизатора.

```
Gudakov_R4(config-router)#network 10.68.0.0 0.0.0.127 area 0
```

```
Gudakov_R4(config-router)#network 10.0.10.8 0.0.0.3 area 0
```

*area 0* – зона (area) – сукупність мереж і маршрутизаторів, що мають один і той же ідентифікатор зони.

Виконаємо перевірку таблиць маршрутизацій на маршрутизаторах (рисунок 4.2–4.6). Кожний маршрутизатор окрім безпосередньо підключених мереж з символом «С» має відомості про всі віддалені мережі, отримана по протоколу OSPF з символом «О». Також мають записи маршруту за замовчуванням, який складається з восьми нулів, для підключення до маршрутизатора IPS.

```
Gudakov_R4#sh ip ro
Gudakov_R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O       10.0.10.0/30 [110/15064] via 10.0.10.10, 00:03:06, Serial0/0/1
O       10.0.10.4/30 [110/7564] via 10.0.10.10, 00:03:16, Serial0/0/1
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.9/32 is directly connected, Serial0/0/1
C       10.68.0.0/27 is directly connected, GigabitEthernet0/1.99
L       10.68.0.1/32 is directly connected, GigabitEthernet0/1.99
C       10.68.0.32/27 is directly connected, GigabitEthernet0/1.20
L       10.68.0.33/32 is directly connected, GigabitEthernet0/1.20
C       10.68.0.64/27 is directly connected, GigabitEthernet0/1.30
L       10.68.0.65/32 is directly connected, GigabitEthernet0/1.30
C       10.68.0.96/27 is directly connected, GigabitEthernet0/1.40
L       10.68.0.97/32 is directly connected, GigabitEthernet0/1.40
O       10.68.0.128/25 [110/15065] via 10.0.10.10, 00:03:06, Serial0/0/1
O       10.68.1.0/26 [110/65] via 10.0.10.10, 00:03:16, Serial0/0/1
O       10.68.1.64/27 [110/7565] via 10.0.10.10, 00:03:06, Serial0/0/1
    209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7564] via 10.0.10.10, 00:03:16, Serial0/0/1
S*    0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.5– Таблиця маршрутизації на Gudakov\_R4

Виходячи з адресації маршрутизаторів ми бачимо, що всі наявні мережі вказані в таблицях, тому топологія повністю сходиться, а це значить, що з будь-якої мережі можна відправляти повідомлення до іншої, та це повідомлення буде обов'язково прийняте.

### 3.4.3 Налаштування роботи Інтернет

NAT на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 10.22.210.10 255.255.255.0 – адреса Server HTTP;
- номер списку доступу: 5;
- ім'я пулу: Internet.

Приклад налаштування NAT на Gudakov\_R3:

Список контролю доступу, що дозволяє всі адреси внутрішньої мережі:

```
Gudakov_R3(config)# access-list 5 permit 10.68.0.0 0.0.3.255
```

Пул для динамічного виділення інтернет адрес:

```
Gudakov_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30
netmask 255.255.255.224
```

Підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу:

```
Gudakov_R3(config)#ip nat inside source list 5 pool Internet
```

Адреса статичного NAT для серверу HTTP:

```
Gudakov_R3(config)#ip nat inside source static 10.68.0.149 209.165.200.5
```

Призначення інтерфейсу в якості вихідного для трафіку з мережі приватних адрес:

```
Gudakov_R3(config)#interface F4/0
```

```
Gudakov_R3(config-if)#ip nat outside
```

Призначення інтерфейсу в якості вхідного для трафіку з мережі приватних адрес:

```
Gudakov_R3(config-if)#interface Serial2/0
```

```
Gudakov_R3(config-if)#ip nat inside
```

Для перевірки роботи NAT отримаємо таблицю перетворювань.

NAT Table for Gudakov_R3					
Protocol	Inside Global	Inside Local	Outside Local	Outside Global	
icmp	209.165.202.12:1	10.68.0.140:1	209.165.202.1:1	209.165.202.1:1	
icmp	209.165.202.11:1	10.68.0.141:1	209.165.202.1:1	209.165.202.1:1	
icmp	209.165.202.8:1	10.68.1.15:1	209.165.200.5:1	209.165.200.5:1	
icmp	209.165.202.8:2	10.68.1.15:2	209.165.200.5:2	209.165.200.5:2	
icmp	209.165.202.9:1	10.68.1.79:1	209.165.200.5:1	209.165.200.5:1	
icmp	209.165.202.10:1	10.68.1.82:1	209.165.202.1:1	209.165.202.1:1	
---	209.165.200.5	10.68.0.149	---	---	

Рисунок 3.4 – Таблиця перетворювань NAT на Gudakov\_R3

#### 3.4.4 Перевірка роботи комп'ютерної системи

Пінгування хостів між підмережами LAN2 та LAN1.

```

PC2_Gos
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.68.0.99

Pinging 10.68.0.99 with 32 bytes of data:

Reply from 10.68.0.99: bytes=32 time=16ms TTL=126
Reply from 10.68.0.99: bytes=32 time=1ms TTL=126
Reply from 10.68.0.99: bytes=32 time=1ms TTL=126
Reply from 10.68.0.99: bytes=32 time=11ms TTL=126

Ping statistics for 10.68.0.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 7ms

C:\>

```

Рисунок 3.5 – Результат команди «ping» між підмережами КС

Для перевірки SSH зробимо підключення з командного рядка G1\_Engineer з підмережі «LAN4» до маршрутизатора Gudakov\_R1 від користувача 12318\_Gudakov з паролем admincisco12318 командою `ssh -l username ip-address`.

```

PC1_Gos
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l 12318_Gudakov 10.68.1.1

Password:

123-18 Gudakov. Enter only have key

Gudakov_R3>enable
Password: |

```

Рисунок 3.5– Перевірка підключення до маршрутизатора Gudakov\_R3 за допомогою протоколу SSH

В підмережах хости отримують мережні налаштування за протоколом DHCP.

Приклад налаштування DHCP на Gudakov\_R2.

```
Gudakov_R2(config)#interface g0/1
```

Активовано протокол DHCP:

```
Gudakov_R2(config-if)#service DHCP
```

Створений пул DHCP з ім'ям Organization\_department:

```
Gudakov_R2(config-if)#ip dhcp pool LAN1
```

Вилучено з пулу перші 10 адрес:

```
Gudakov_R2(config-if)#ip dhcp ex 10.68.0.32 10.68.0.42
```

Зазначена мережа і шлюз за замовчуванням:

```
Gudakov_R2(config-if)#net 10.68.0.32 255.255.255.224
```

```
Gudakov_R2(config-if)#def 10.68.0.33
```

```
Gudakov_R2(config-if)#dns 10.68.10.10
```

```
Gudakov_R4#sh ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
10.68.0.34	0002.1722.B3AD	--	Automatic
10.68.0.35	0007.EC39.1261	--	Automatic
10.68.0.36	0001.9720.2C99	--	Automatic
10.68.0.66	00E0.B016.BC25	--	Automatic
10.68.0.67	0000.0C78.964D	--	Automatic
10.68.0.68	0060.5C72.13EA	--	Automatic
10.68.0.99	000C.CF94.17A9	--	Automatic
10.68.0.98	00D0.BAA1.008D	--	Automatic
10.68.0.100	0060.7041.7427	--	Automatic

Рисунок 3.6 – Таблиця призначення IP-адрес вузлам за протоколом DHCP

### 3.5 Захист інформації в комп'ютерній системі від несанкціонованого доступу

#### 3.5.1 Розробка методів для захисту інформації в комп'ютерній системі

Комп'ютерна мережа є найбільш поширеним способом спілкування та обміну інформацією сьогодні. Всесвітня павутина зберігає гігабайти особистої

інформації про своїх користувачів. А ПК і сервери в локальній мережі – внутрішня інформація компанії. Ці дані повинні бути захищені від зовнішнього втручання.

Рівень захисту мережевих операційних систем дозволяє зберігати дані, протистояти загрозам і атакам, несанкціонованому доступу в мережу. Тим не менш, не варто говорити про виняткову, універсальну систему засобів захисту інформації. Бувають ситуації, коли він виходить з ладу, і пристрої уразливі для проникнення.

Інформаційна безпека полягає в наданні ряду факторів: захист інформації від несанкціонованого створення, часткової або повної втрати; конфіденційність;

Гарантії доступу для авторизованих користувачів – у певних сферах (банківська справа, фінанси, державне управління, оборона і правоохоронні органи) необхідно створити додаткову, більш надійну, систему інформаційної безпеки.

Захист інформації в інформаційних мережах – створені масштабні комп'ютерні лінії, а саме локальні, корпоративні, телекомунікаційні – ставлять перед собою завдання взаємодії великої кількості комп'ютерів, серверів, мереж і підмереж. Створюється проблема визначення найбільш ефективного методу захисту інформації.

Топологія системи, заснована на розташуванні міжкомп'ютерних посилань, залишається основною складовою всіх локальних і корпоративних мереж. Безпека даних в комп'ютерних мережах досягається шляхом обробки критичної інформації. Під цим терміном маються на увазі фактори, що сприяють ефективному управлінню основними структурними елементами мережі і максимально повному виконанню стратегічних завдань будь-якого рівня секретності (для особистого, службового користування, комерційної таємниці або інтелектуальної власності фізичної або юридичної особи).



Уразливість більшості інформаційних мереж пов'язана з кабельною системою. Є дані, що саме вона викликає збої і несправності. Це потрібно враховувати вже на етапі проектування мережевих з'єднань.

Так звані структуровані кабельні системи набули широкого поширення. Принцип їх пристрою полягає в наявності однотипних проводів для передачі всіх видів інформації (цифрових, телефонних, відео, сигналів охоронних систем).

Структурування полягає в можливості розділити всю систему кабелів на ряд рівнів за своїм призначенням і наявністю різних компонентів: зовнішніх, адміністративних, апаратних, магістральних, горизонтальних підсистем.

Зовнішня підсистема мідної та волоконна–оптичної включає в себе електрозахисні пристрої, заземлення і налагоджує комунікаційна–переробне обладнання в приміщенні. Він також включає в себе контактні пристрої для зовнішніх і внутрішніх кабельних систем. Обладнання необхідне для розміщення обладнання, яке підтримує роботу підсистеми адміністратора.

Основні проблеми в процесі захисту матеріалів. При вирішенні питання захисту інформації в корпоративних мережах варто звернути увагу на можливі перебої і порушення в процесі доступу, які можуть знищити або спотворити інформацію.

Можливі проблеми, пов'язані з порушенням безпеки в комп'ютерних мережах, можна розділити на кілька типів:

- Несправність системного обладнання: поломка кабелю, відключення електроенергії, збій в роботі дискової системи, порушення роботи серверів, мережевих карт, робочих станцій, системи архівування.
- Знищення даних внаслідок некоректної роботи програмного забезпечення: системні помилки, зараження комп'ютерними вірусами.
- Розслідування несанкціонованого доступу: піратське копіювання, усунення або фальсифікація даних, робота сторонніх осіб з

секретними матеріалами.

- Неграмотне збереження архівів.
- Помилки технічного персоналу і користувачів мережевого ресурсу: випадкове спотворення або знищення інформації, неправильне використання програмних продуктів.

У кожному з цих випадків необхідно усунути порушення і зміцнити систему безпеки комп'ютерної мережі.

Які засоби можуть бути використані для захисту інформації. Як показує практика, неавторизовані користувачі або програмні продукти вірусного типу можуть отримати доступ навіть до захищених мережевих ресурсів. Для цього вони повинні мати певний досвід роботи в області мережевого або системного програмування і бажання підключитися до певних файлів.

Для повної конфіденційності розроблені додаткові засоби захисту інформації:

Апаратне забезпечення (антивірусні програми, брандмауери, брандмауери та фільтри, пристрої шифрування протоколів).

Програмне забезпечення (моніторинг мережі, архівування даних, криптографія, ідентифікація та аутентифікація користувачів, контроль доступу, протокол та аудит).

Адміністративні (обмеження доступу до приміщень, розробка планів дій з надзвичайних ситуацій та стратегій безпеки компанії).

Будь-який з цих методів може обмежити доступ шкідливих програм і файлів або повністю відмовитися від нього. Для надійності бар'єру часто використовується поєднання декількох видів захисних засобів.

Архівування та дублювання інформації. Грамотна і надійна система архівування даних здатна зберігати інформацію в мережі. Якщо мережа невелика, система резервного копіювання встановлюється в доступний серверний слот. Великі корпоративні мережі краще оснастити окремим архівуючим сервером.

Такий пристрій архівує дані в автоматичному режимі і подає звіт із заданою періодичністю. Однак, можна керувати процесом резервного копіювання за допомогою консолі системного адміністратора.

Використовувати установку для архівування інформації можна через відсутність вільного місця на жорсткому диску або через вихід з ладу «дзеркального» диска сервера. Ця функція також може бути активована автоматично.

Як поставити бар'єр для вірусів. Поширення комп'ютерних вірусів в інформаційних мережах відбувається з неймовірною швидкістю. Тисячі вже відомих шкідливих програм регулярно оновлюються сотнями нових. Найдоступнішим засобом боротьби з ними є антивірусні програми.

Такі програмні пакети можуть блокувати доступ до інформації і вирішувати проблему з зараженими файлами. Кращий спосіб зберігання інформації про систему – використовувати комбінацію програмних і апаратних бар'єрів. Найчастіше це спеціалізовані дошки для боротьби з вірусами.

Захист ваших даних від несанкціонованого доступу. Питання захисту інформації в комп'ютерній системі від несанкціонованого проникнення пов'язане з широким охопленням інформаційного простору глобальними телекомунікаційними мережами. Найпростіші помилки самих користувачів завдають більш відчутної шкоди, ніж збій в системі або поломці обладнання. Щоб запобігти подібним ситуаціям, варто окреслити повноваження користувача.

Для цього використовуються вбудовані програми операційних систем мережі. Існують десятки каналів витоку даних і можливості несанкціонованого входу. Найбільш поширеними є:

- інформація, що залишилася після дозволеного запиту;
- злом системи захисту інформації та копіювання необхідних файлів;
- представництво зареєстрованим користувачем;

- імітувати системний запит;
- програмні пастки;
- недосконалість операційної системи;
- незатверджене підключення до мережевого обладнання;
- злом системи безпеки;
- введення вірусів.

З метою повного захисту інформації рекомендується використовувати ряд організаційно–технічних методів.

Організаційні заходи полягають, перш за все, в обмеженні доступності будівель і офісів, де працює інформація. Тільки сертифіковані і перевірені фахівці мають право взаємодіяти з ним. Всі носії інформації, журнали та записи повинні зберігатися в закритих сейфах. Необхідно виключити можливість перегляду матеріалів сторонніми особами через монітори або принтери. При передачі секретної інформації по каналах зв'язку краще використовувати криптографічне кодування. І, нарешті, потрібно стежити за тим, щоб всі відпрацьовані пристрої і носії, що містять цінні дані, були вчасно знищені.

До організаційно–технічних засобів захисту відноситься пристрій незалежного джерела живлення для системи обробки цінних файлів, оснащення вхідних дверей комбінованими замками і використання LCD або плазмових дисплеїв з високочастотним випромінюванням електромагнітних імпульсів. Крім того, відправляючи оргтехніку на ремонт, потрібно стерти всі наявні дані. Приміщення, в яких відбувається робота з секретними матеріалами, рекомендується обладнати сталевими екранами.

Технічне захисне обладнання включає в себе установку системи безпеки для операційних і організацію роботи контрольно–пропускних пунктів. Необхідно забезпечити контроль за можливістю проникнення в пам'ять комп'ютера, а також блокування інформації і використання ключів.

Архітектура програмного обладнання полягає в суворому контролі безпеки при вході в систему, реєстрації в спеціальних книгах, контролі дій користувача. Потрібно встановити систему реагування (в тому числі аудіо) для проникнення в корпоративну мережу.

Для надійності система безпеки і захисту даних повинна регулярно перевірятися, перевіряти готовність і роботу всіх її елементів. Велике значення має фіксація всіх маніпуляцій, які мають хоч якесь відношення до захисту системи.

Значно підвищити ступінь секретності можна за допомогою смарт-карт. Для цього сервер оснащений пристроєм для їх зчитування. Користувач, що увійшов до системи, вставляє в неї картку і вводить індивідуальний код доступу. Весь процес фіксує служба безпеки.

Механізми досягнення гарантованої безпеки. На сьогоднішній день розроблені і успішно використовуються різні методи захисту інформації. Найбільш актуальними і доступними з них є:

– Використання криптографії. Це використання шифру, який дозволяє змінювати вміст файлу, роблячи його нечитабельним. Дізнатися контент можна тільки за допомогою спеціальних ключів або паролів.

Для створення шифрування використовуються два взаємопов'язаних поняття: алгоритм і ключ. Перший визначає спосіб кодування, другий допомагає інтерпретувати повідомлення. Це просто і доступно без великих фінансових вкладень. Один алгоритм може бути використаний з декількома ключами для різних одержувачів. Крім того, при втраті секретності ключі можна відразу міняти, не порушуючи алгоритм. Безпека в даному випадку пов'язана тільки з ключами.

Для досягнення більшого ефекту ключі коду можна зробити довгими і складними. Існує дві схеми шифрування: симетрична (один ключ для відправника і одержувача) і асиметрична (ключ відкритого доступу).

– Застосування електронного цифрового підпису (ЕЦП). Він підтверджує особу відправника, створюється за допомогою його закритого ключа. Додатковим ступенем збереження ЕЦП є унікальний номер власника.

– Аутентифікація користувача. Мабуть, основний спосіб захисту даних в мережі. Щоб отримати доступ до ресурсу, користувач повинен підтвердити це право. Відповідний сервер приймає запит на використання ресурсу і пересилає його на сервер, відповідальний за аутентифікацію. Тільки після отримання позитивного результату доступ буде відкритий.

Однією з версій перевірки особистості є використання пароля. Це може бути будь-яке секретне слово, яке вводиться на початку роботи з системою. В особливих випадках сервер може попросити новий пароль на виході. І вони можуть бути різними.

Порушення можливе, якщо секретне слово перейняв хтось інший. Щоб цього не сталося, паролі краще робити одноразово. Навіть перехоплене кодове слово буде марним в наступному сеансі. Паролі можна генерувати за допомогою програм або спеціальних пристроїв, вставлених в слот комп'ютера.

– Захист інформації всередині корпоративної мережі. Корпоративні мережеві системи, як правило, підключені до Всесвітньої павутини. Це створює додаткові можливості, але також робить систему безпеки вразливою. Для захисту матеріалів у внутрішній мережі потрібні брандмауери (брандмауери), які можуть розділити трафік на кілька потоків і позначити умови для обміну даними з одного потоку в інший. Брандмауер аналізує прохідний трафік і, перевіряючи кожен пакет даних, вирішує, дозволяти його чи ні. Для цього формується алгоритм роботи програми, де прописуються правила і порядок проходження даних.

Брандмауери реалізуються в апаратному забезпеченні (як спеціалізований фізичний елемент) або як окрема програма, встановлена на комп'ютері. Для забезпечення безпечного функціонування брандмауера вносяться регулярні корективи в систему, що відповідає за її функціональність. У звичайних

користувачів немає можливості увійти в цю програму, вона доступна тільки для системного адміністратора.

Брандмауер складається з декількох компонентів, включаючи фільтри або захисні пристрої для блокування деякого трафіку. Можна виділити два типи таких елементів програми:

- застосовано – блокування доступу до окремих мережевих ресурсів;
- пакет – фільтрація інформаційних блоків за допомогою маршрутизаторів.

В результаті весь трафік від зовнішньої системи до внутрішньої системи і назад проходить через систему брандмауера. До місця призначення доходять лише дані, які відповідають стратегії безпеки.

### **3.5.2 Налаштування маршрутизаторів на підтримку служби AAA**

Приклад налаштування сервісу AAA та серверу RADIUS.

Запуск служби AAA:

```
Gudakov_R4(config)#aaa new-model
```

Налаштування методу аутентифікації з використання локальної бази користувачів:

```
Gudakov_R4(config)#aaa authentication login default local
```

Налаштування методу аутентифікації Login на сервері RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів:

```
Gudakov_R4(config)#aaa authentication login Login group radius local
```

Застосування методу аутентифікації Login на консольній лінії та vty:

```
Gudakov_R4(config)#line console 0
```

```
Gudakov_R4(config-line)#login authentication Login
```

```
Gudakov_R4(config)#line vty 0 4
```

```
Gudakov_R4(config-line)#login authentication default
```

Налаштування RADIUS-серверу:

```
Gudakov_R4(config)#radius-server host 10.68.10.10 auth-port 1645
```

```
Gudakov_R4(config)#radius-server key Radius+Gudakov123
```

Для доступу використовується доменне ім'я пристрою Gudakov\_R3 з паролем Radius+Gudakov123, що був налаштований на сервері RADIUS.

```
123-18 Gudakov. Enter only have key
```

```
User Access Verification
```

```
Username: Gudakov_R2
```

```
Password:
```

```
Gudakov_R2>enable
```

```
Password:
```

```
Gudakov_R2#|
```

Рисунок 3.9 – Аутентифікація на маршрутизаторі за допомогою служби AAA та сервера RADIUS



AAA

---

Service  On  Off      Radius Port

---

Network Configuration

Client Name       Client IP

Secret       ServerType

	Client Name	Client IP	Server Type	Key	
1	Gudakov_R2	10.68.0.129	Radius	R_Gudakov12318	<input type="button" value="Add"/>
2	Gudakov_R1	10.68.0.1	Radius	R_Gudakov12318	<input type="button" value="Save"/>
3	Gudakov_R4	10.68.2.1	Radius	R_Gudakov12318	<input type="button" value="Remove"/>

---

User Setup

Username       Password

	Username	Password	
1	Gudakov_R2	R_Gudakov12318	<input type="button" value="Add"/>
2	Gudakov_R1	R_Gudakov12318	<input type="button" value="Save"/>
3	Gudakov_R4	R_Gudakov12318	

Рисунок 3.10 – Налаштований RADIUS-сервер

На портах комутатора, де підключені сервери кіберфізичної системи домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі, налаштовані засоби безпеки: тільки одному вузлу дозволений доступ до порту; MAC-адреса пристрою додається статично в поточну конфігурацію; при порушенні системи безпеки порт виключається.

```

Gudakov_Sw2#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/22      2              0              0          Restrict
Fa0/23      2              0              0          Restrict
-----
Gudakov_Sw2#

```

Рисунок 3.10 – Перевірка безпеки портів GudakovSw2

### 3.5.3 Налаштування мережах VLAN та параметрів безпеки комутаторів

Згідно до технічних вимог в підмережі «Відділ Забезпечення діяльності голови суду» були створені 3 підмережі VLAN.

Таблиця 3.4 – Назви VLAN для підмережі

Номер VLAN	Ім'я VLAN
1	Default
20	Marketing
30	Postachanny
40	Sbutu
99	Management
100	Native

Налаштування на Gudakov\_Sw4.1:

Об'ява VLAN:

```

Switch (config)#hostname Gudakov_Sw4.1
Gudakov_Sw4.1(config)#vlan 20
Gudakov_Sw4.1(config-vlan)#name Marketing
Gudakov_Sw4.1(config-vlan)# vlan 30
Gudakov_Sw4.1(config-vlan)#name Postachanny
Gudakov_Sw4.1(config-vlan)#vlan 40
Gudakov_Sw4.1(config-vlan)#name Sbutu
Gudakov_Sw4.1(config-vlan)#vlan 99
Gudakov_Sw4.1(config-vlan)# name Management
Gudakov_Sw4.1(config-vlan)#vlan 100
Gudakov_Sw4.1(config-vlan)# name Native

```

Налаштування транкових каналів:

```

Gudakov_Sw4.1(config)#interface g0/1, f0/24, f0/24

```

```
Gudakov_Sw4.1(config-if)#switchport trunk native vlan 100
Gudakov_Sw4.1(config-if)#switchport mode trunk
Gudakov_Sw4.1(config-if)#exit
```

Налаштування портів доступу:

```
// включити режим access
Gudakov_Sw4.1(config-if)# switchport access vlan 20
// вказати інтерфейси для vlan 20
Gudakov_Sw4.1(config)#interface range f0/5-10
Gudakov_Sw4.1(config-if)#switchport mode access
Gudakov_Sw4.1(config-if)# switchport access vlan 40
Gudakov_Sw4.1(config)#interface range f0/15-20
Gudakov_Sw4.1(config-if)#switchport mode access
Gudakov_Sw4.1(config-if)# switchport access vlan 30
Gudakov_Sw4.1(config)#interface range f0/10-14
Gudakov_Sw4.1(config-if)#switchport mode access
Gudakov_Sw4.1(config-if)#exit
```

Налаштування SVI-інтерфейсу:

```
Gudakov_Sw4.1(config)# interface Vlan99
Gudakov_Sw4.1(config-if)# ip address 10.68.0.2 255.255.255.224
Gudakov_Sw4.1(config-if)#no shutdown
```

Port Status Summary Table for Gudakov_Sw4.2					Port Status Summary Table for Gudakov_Sw4.1				
Device Name: Gudakov_Sw4.2 Device Model: 2960-24TT Hostname: Gudakov_Sw4.2					Device Name: Gudakov_Sw4.1 Device Model: 2960-24TT Hostname: Gudakov_Sw4.1				
Port	Link	VLAN	IP Address	MAC Address	Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	0060.5C99.5001	FastEthernet0/1	Down	1	--	0001.6423.2401
FastEthernet0/2	Down	1	--	0060.5C99.5002	FastEthernet0/2	Down	1	--	0001.6423.2402
FastEthernet0/3	Down	1	--	0060.5C99.5003	FastEthernet0/3	Down	1	--	0001.6423.2403
FastEthernet0/4	Up	20	--	0060.5C99.5004	FastEthernet0/4	Up	20	--	0001.6423.2404
FastEthernet0/5	Up	20	--	0060.5C99.5005	FastEthernet0/5	Down	20	--	0001.6423.2405
FastEthernet0/6	Down	20	--	0060.5C99.5006	FastEthernet0/6	Down	20	--	0001.6423.2406
FastEthernet0/7	Down	20	--	0060.5C99.5007	FastEthernet0/7	Down	20	--	0001.6423.2407
FastEthernet0/8	Down	20	--	0060.5C99.5008	FastEthernet0/8	Up	20	--	0001.6423.2408
FastEthernet0/9	Down	1	--	0060.5C99.5009	FastEthernet0/9	Down	1	--	0001.6423.2409
FastEthernet0/10	Up	30	--	0060.5C99.500A	FastEthernet0/10	Up	30	--	0001.6423.240A
FastEthernet0/11	Up	30	--	0060.5C99.500B	FastEthernet0/11	Down	30	--	0001.6423.240B
FastEthernet0/12	Down	30	--	0060.5C99.500C	FastEthernet0/12	Down	30	--	0001.6423.240C
FastEthernet0/13	Down	30	--	0060.5C99.500D	FastEthernet0/13	Down	30	--	0001.6423.240D
FastEthernet0/14	Down	30	--	0060.5C99.500E	FastEthernet0/14	Down	30	--	0001.6423.240E
FastEthernet0/15	Up	40	--	0060.5C99.500F	FastEthernet0/15	Up	40	--	0001.6423.240F
FastEthernet0/16	Up	40	--	0060.5C99.5010	FastEthernet0/16	Down	40	--	0001.6423.2410
FastEthernet0/17	Down	40	--	0060.5C99.5011	FastEthernet0/17	Down	40	--	0001.6423.2411
FastEthernet0/18	Down	40	--	0060.5C99.5012	FastEthernet0/18	Down	40	--	0001.6423.2412
FastEthernet0/19	Down	40	--	0060.5C99.5013	FastEthernet0/19	Down	40	--	0001.6423.2413
FastEthernet0/20	Down	40	--	0060.5C99.5014	FastEthernet0/20	Down	40	--	0001.6423.2414
FastEthernet0/21	Down	1	--	0060.5C99.5015	FastEthernet0/21	Down	1	--	0001.6423.2415
FastEthernet0/22	Down	1	--	0060.5C99.5016	FastEthernet0/22	Down	1	--	0001.6423.2416
FastEthernet0/23	Down	1	--	0060.5C99.5017	FastEthernet0/23	Down	1	--	0001.6423.2417
FastEthernet0/24	Up	--	--	0060.5C99.5018	FastEthernet0/24	Up	--	--	0001.6423.2418
GigabitEthernet0/1	Down	1	--	0060.5C99.5019	GigabitEthernet0/1	Up	--	--	0001.6423.2419
GigabitEthernet0/2	Down	1	--	0060.5C99.501A	GigabitEthernet0/2	Down	1	--	0001.6423.241A
Vlan1	Down	1	<not set>	0090.2BDB.0042	Vlan1	Down	1	<not set>	0001.63C4.644D
Vlan99	Up	99	10.68.0.3/27	0090.2BDB.0001	Vlan99	Up	99	10.68.0.2/27	0001.63C4.6401

Рисунок 3.11 – Налаштування VLAN на Gudakov\_Sw4.1 та Gudakov\_Sw4.2

На рисунках наведено розподіл портів комутаторів за віртуальними мережами, які було створено та призначені інтерфейси керування.

Для здійснення передачі трафіку між VLAN необхідно налаштувати порт GigabitEthernet0/1 маршрутизатора Gudakov\_R0 на підтримку технології інкапсуляції 802.1Q.

```
Gudakov_R0(config)#interface g0/1
```

```
Gudakov_R0(config-if)#no shutdown
```

Налаштування підінтерфейсу для маршрутизації трафіку між VLAN.

```
Gudakov_R0(config)#interface g0/0.16
```

Тегування пакетів для даного підінтерфейсу.

```
Gudakov_R0(config-subif)#encapsulation dot1Q 16 //
```

```
Gudakov_R0(config-subif)#ip address 10.22.211.1 255.255.255.224
```

Port Status Summary Table for Gudakov_R4						
Device Name: Gudakov_R4						
Device Model: 2911						
Hostname: Gudakov_R4						
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address	
GigabitEthernet0/0	Down	--	<not set>	<not set>	00D0.58B6.C2D6	
GigabitEthernet0/1	Up	--	<not set>	<not set>	0090.2189.AA61	
GigabitEthernet0/1.20	Up	--	10.68.0.33/27	<not set>	0090.2189.AA61	
GigabitEthernet0/1.30	Up	--	10.68.0.65/27	<not set>	0090.2189.AA61	
GigabitEthernet0/1.40	Up	--	10.68.0.97/27	<not set>	0090.2189.AA61	
GigabitEthernet0/1.99	Up	--	10.68.0.1/27	<not set>	0090.2189.AA61	
GigabitEthernet0/2	Down	--	<not set>	<not set>	0060.5CCE.CA1B	
Serial0/0/0	Down	--	<not set>	<not set>	<not set>	
Serial0/0/1	Up	--	10.0.10.9/30	<not set>	<not set>	
Serial0/1/0	Down	--	<not set>	<not set>	<not set>	
Serial0/1/1	Down	--	<not set>	<not set>	<not set>	
Vlan1	Down	1	<not set>	<not set>	000C.859A.B825	

Рисунок 3.13 – Перевірка налаштування 802.1Q на Gudakov\_R0

Інкапсуляція 802.1Q Gudakov\_R0 на налаштована.

### 3.5.4 Налаштування віртуальної приватної мережі VPN

В кіберфізична система домашнього Інтернету речей житлового комплексу «Бартоломео» VPN передається трафік між підмережою «LAN2» (шлюзом для неї є інтерфейс роутера Gudakov\_R0) та підмережою «LAN3» (шлюзом для неї є інтерфейс роутера Gudakov\_R4).

Для перевірки створеного VPN тунелю передачі трафіку між підмережами застосовується команда *show crypto ipsec sa*.

```
Gudakov_R3#show crypto ipsec sa

interface: Serial0/0/0
  Crypto map tag: VPN-MAP, local addr 10.0.10.6

protected vrf: (none)
local ident (addr/mask/prot/port): (10.68.1.0/255.255.255.192/0/0)
remote ident (addr/mask/prot/port): (10.68.1.64/255.255.255.224/0/0)
current_peer 10.0.10.5 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.10.6, remote crypto endpt.:10.0.10.5
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)
```

Рисунок 3.14 – Перевірка стану IPSec SA на роутері Gudakov\_R3

## 4 КІБЕРФІЗИЧНА СИСТЕМА

### 4.1 Загальна інформація

У час високих технологій багато уваги приділяється видаленому контролю за допомогою мобільної системи передачі даних. За допомогою зв'язку мікроконтролера і GSM – модуля можна виконувати багато функцій, які значно допомагають в побутовому житті.

Охоронні GSM системи, як і виходить з назви, застосовуються для охорони території і майна з використанням GSM технологій. Основним завданням охоронної GSM сигналізації, обладнаної GSM модулем, є визначення факту вторгнення на підконтрольну територію і сповіщення власника по стільниковому телефону. Принцип роботи системи GSM сигналізації: підконтрольна територія обладналася усіма необхідними датчиками і GSM модулем. Усі пристрої підключаються до контрольної панелі. При виникненні несанкціонованого вторгнення, тобто при спрацьовуванні будь якого з датчиків, по радіоканалу активується GSM модуль, який передає тривожні SMS повідомлення на стільниковий телефон відповідального за охорону майна і його власникові. Сучасні GSM системи обладнані голосовим модулем для дзвінків на заздалегідь задані телефонні номери. Постановка і зняття GSM сигналізації з охорони відбувається за допомогою брелка або безпосередньо із стільникового телефону.

У кваліфікаційній роботі на тему «Кіберфізична система домашнього Інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі» розробляється облаштування охоронної і пожежної сигналізації на видалених об'єктах, таких як причали, складські приміщення де можлива не постійна присутність людини. У разі виникнення позаштатних ситуацій, диспетчерський пункт інформуватиме автоматична система, по каналами передачі даних GSM. Така система допоможе запобігти збитку, нанесеному зловмисниками внаслідок проникнення і крадіжки

цінностей, попередити займання об'єкту, або інших неприємних ситуацій. Усі ці заходи спрямовані на те, щоб зберегти матеріальні блага людей, їх майно, ну і, звичайно ж, здоров'я в психологічному плані.

Орієнтовна структурна схема охоронної системи з виходом на канал GSM представлена на рисунку 4.1.

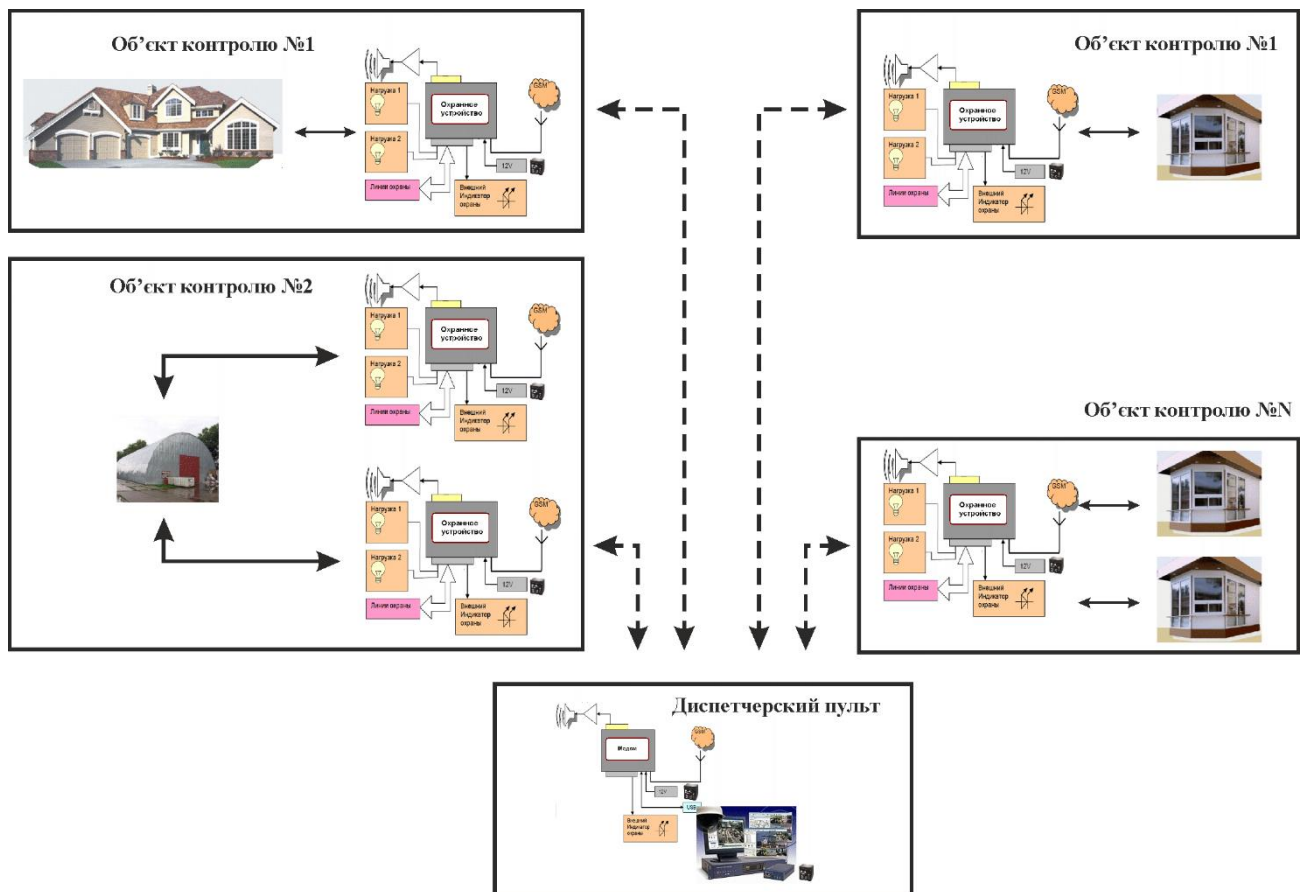


Рисунок 4.1 – Орієнтовна структурна схема охоронної системи з виходом на канал GSM

#### 4.2 Апаратна частина системи автоматичного управління

Охоронно–пожежні сигналізації використовуються для виявлення займань і несанкціонованих вторгнень на об'єкти, що охороняються. Для управління системами сигналізації використовуються приймально–контрольні охоронно–пожежні прилади. На великих і середніх об'єктах використовуються окремо



охоронні і пожежні прилади. Це пов'язано з різними режимами постановки / зняття з охорони і, в деяких випадках, розділенням відповідальності між службою безпеки і протипожежною службою підприємства.

Прилади приймально–контрольні охоронно–пожежні – розрізняють прилади променеві, адресні і адресно–аналогові.

Променеві прилади використовують окрему лінію зв'язку(промінь) для кожного шлейфу сигналізації, який підключається безпосередньо до приладу. Цей вид устаткування має широке поширення, але поступово його доля в середніх і великих об'єктах скорочується.

Адресні прилади використовують адресні датчики або адресні блоки (мітки) для побудови системи. При цьому від приладу йде один двопровідний дріт, до якого підключаються адресні блоки, до яких підключаються датчики (якщо датчики – адресні, блоки виключаються). Адресні системи можуть покривати об'єкти з великими відстанями, мають великий набір функцій.

Адресно–аналогові прилади найбільш перспективні, але доки мало поширені. Вони в середньому дорожче за адресні і променеві прилади, при цьому дозволяють виявляти виникнення пожеж на більше ранніх стадіях.

Сучасні вироби мають можливість підключення до комп'ютера. У багатьох випадках комп'ютер служить в якості основного облаштування моніторингу, а прилад в якості допоміжного.

Комп'ютер, що управляє, або мікроконтролер дозволяє комфортно вносити налаштування в підключений прилад або прилади, здійснювати моніторинг стану датчиків, вести архів подій, задавати правила постановки/зняття з охорони по графіку, при тому, що піднесло карт, розподіляти повноваження між оперативними співробітниками, відображати події на планах об'єкту, передавати інформацію на пульт озорони.

Для побудови охоронно–пожежної сигналізації зазвичай застосовують наступні сповіщувачі.

Оптичний димовий датчик. Один з найбільш поширених типів датчиків. Принцип дії заснований на аналізі рівня прозорості середовища між випромінювачем і фотоприймачем.

Димовий датчик радіоізотопний в побутових приміщеннях застосовується набагато рідше, ніж оптичний інфрачервоний датчик. При цьому він незамінний в промислових приміщеннях, в приміщеннях з великою кількістю пилу. Димовий променевий датчик застосовується в приміщеннях з високою стелею, в атриумах. По суті, в чомусь повторює принцип дії оптичного димового датчика : аналізує стан середовища між приймачем і передавачем. Димовий аспіраційний датчик. Датчик використовується в різних каналах або в приміщеннях з дуже красивим інтер'єром (наприклад, театрах). Датчик всмоктує повітря і аналізує воно на предмет наявності диму.

Тепловий датчик отримав широке поширення завдяки своїй невисокій вартості. Принцип дії : спрацьовування датчика при нагріванні термо-чутливого елемента до заданої температури. Теплові сповіщувачі застосовуються у випадках обмеженості бюджету або неможливості застосування димових сповіщувачів.

Ручні сповіщувачі застосовуються для ручного сповіщення про пожежу.

Сповіщувачі охоронної сигналізації – як правило, це об'ємний інфрачервоний датчик. Об'ємний інфрачервоний датчик призначений для визначення переміщень у рамках території, що охороняється. Принцип дії заснований на аналізі відбитого променя, що випромінюється сповіщувачем. Залежно від типу діаграми випромінювання розрізняють датчики типу «стіна» або «штора», з круговою і секторною діаграмою. Об'ємні радіохвильові датчики використовуються для прихованої установки, для вуличного застосування. Ці датчики в середньому дорожче об'ємних інфрачервоних і складніші в налаштуванні.

Датчик розбиття скла реагує на звук відповідної частоти і застосовується для захисту вікон, вітрин і ін.

Магнітно–контактний датчик. Найбільш поширений вид датчика. Принцип дії заснований на замиканні шлейфу при зникненні магнітного поля (відкритті вікна або дверей).

#### **4.2.1 Розробка структурної схеми системи управління**

Згідно з технічним завданням на розробку мікропроцесорної індивідуальної охоронної системи з виходом на канал GSM, була розроблена структурно схемо (рис. 4.2).

Охоронні блоки для одного контрольованого об'єкту, що складається з декількох охоронних підоб'єктів (окремі будови, наприклад будинок охорони, гостьовий будинок, гараж, службові приміщення на причалі і тому подібне), спрощено декількома однаковими структурними елементами, насправді складаються з одного основного блоку і декількох додаткових блоків, кількість яких визначається по кількості охоронних підоб'єктів.

Охоронний блок забезпечує основні пожежна–охоронні функції системи і додаткові сервісні функції, двосторонній зв'язок по GSM– каналу з пультом диспетчера і по радіоканалу з додатковими охоронними блоками. На структурній схемі умовно не показано джерело безперебійного живлення і кнопку виклику «Тривога» («Пожежа»).

Канали телемеханічного управління, що відносяться до сервісної групи, призначені для забезпечення видаленого управління різними об'єктами, наприклад, автономною автоматичною системою опалювання, провітрювання або кондиціонування і тому подібне.

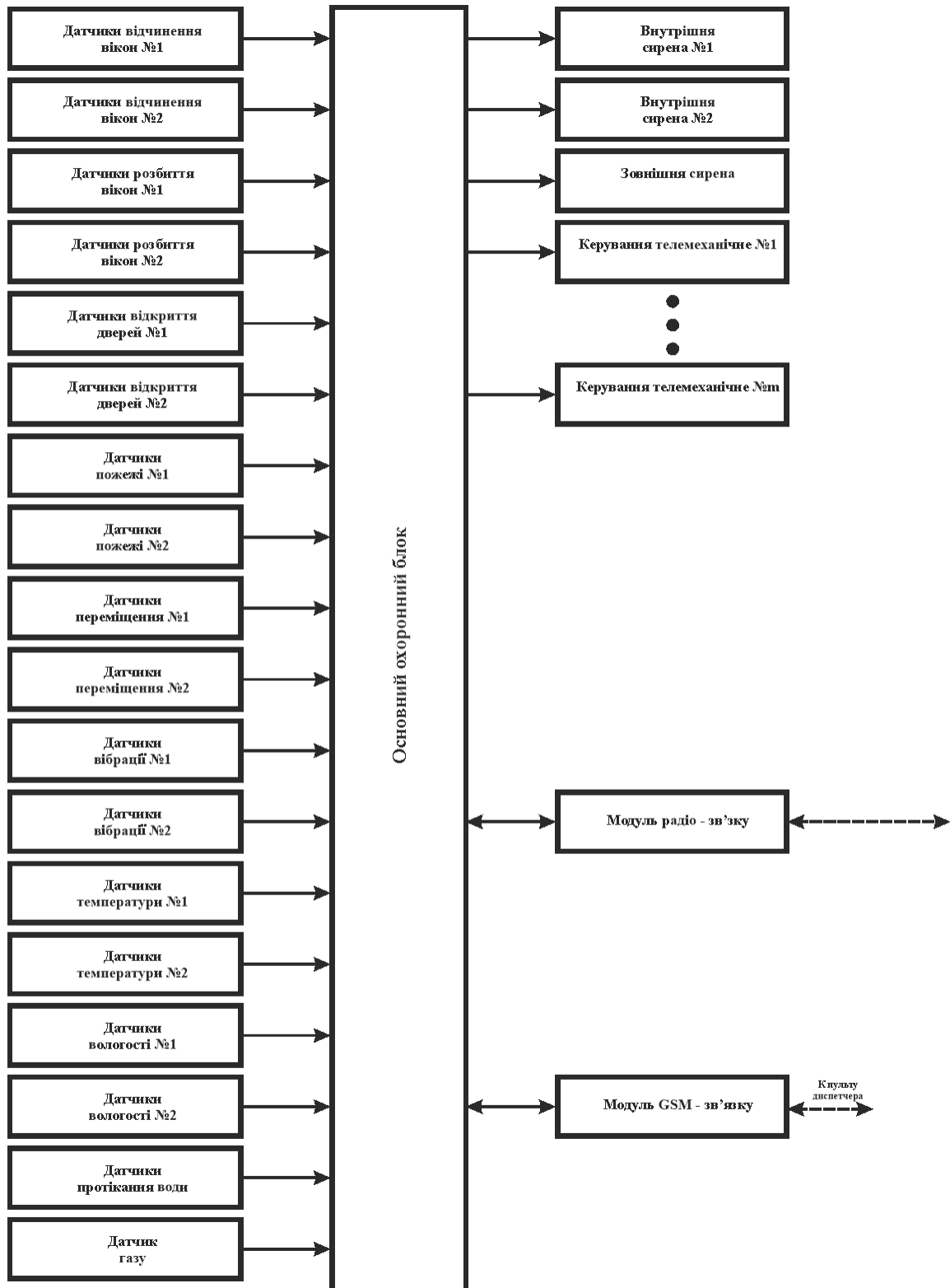


Рисунок 4.2 – Структурна схема основного охоронного блоку

## 4.2.2 Вибірання технічних засобів і елементної бази

Варіанти датчиків і виконавчих пристроїв, вживані для пожежників і охоронних систем представлені на листі 3 графічних частини ДП і на малюнках далі, нижче за текстом.

### 4.2.2.1 Датчики

#### 4.2.2.1.1 Контактні датчики

Контактні реагують на несанкціоноване відкривання дверей, вікон, комір і тому подібне і складаються з геркона (герметичного контакту), який встановлюють на нерухому частину конструкції(наприклад, на одвірок), і магніту, який стоїть на самих дверях.

На рис. 3.3 показаний врізний магнітоконтактний датчик, призначений для установки на металеві, дерев'яні і пластикові двері.



Рисунок 4.3 – Датчик магнітоконтактний (відкриття дверей, вікна) СМК–5

Технічні характеристики СМК–5:

- тип виходу : сухий контакт;
- здатність навантаження : 220 В, 0,5 А;



Рисунок 4.4 – Кінцевий вимикач (відкриття воріт) СК–100

Технічні характеристики СК–100:

- тип виходу : сухий контакт;
- здатність навантаження : 220 В, 10 А;



Рисунок 4.5 – Індуктивний датчик (відкриття воріт) TELETRACK LS– 10–25.1К

Основні технічні параметри TELETRACK LS– 10–25.1К:

- діапазон температури : – 40.+85 С;
- параметри живлення : 12.48 В, 25 мА;
- діапазон чутливості: 5...35 мм;
- вихідний сигнал: відкритий колектор: 48 В, 100 мА;
- габаритні розміри: 50×16 мм.

Безпроводною датчик відкриття дверей / вікна призначений для детектування відкриття дверей, вікон, люків, воріт і так далі. Датчик складається з двох частин – магніту і блоку з герконом. Принцип роботи датчика відкриття заснований на властивостях геркона – елементу, що проводить струм під дією

змінного магнітного поля. У нормальному стані магніт і блок з герконом зімкнуті. Як тільки двері, на яких встановлений датчик, відкриваються – магніт віддаляється від геркона, геркон замикається, починає проводити струм – датчик спрацьовує. Безпроводний датчик відкриття використовується для охорони будинку, магазину, готелю, ресторану, офісної будівлі, школи, банку, бібліотеки, складу і так далі



Рисунок 4.6 – Безпроводний датчик відкриття дверей / вікна Д–308

Технічні характеристики Д–308:

- елемент живлення : 12 В (тип 23 А);
- діапазон робочих температур : – 10°C.+50°C;
- робоча вологість: до 90%;
- робоча частота: 433 МГц;
- протокол зв'язку : MODBUS RTU;
- розміри: 71×36×15 мм;
- споживання струму в робочому режимі: не більше 15 мА;
- термін роботи датчика від однієї батареї: до 12 місяців
- поріг спрацьовування : 1 см
- максимальна відстань передачі : 100 м  
(пряма видимість).

#### 4.2.2.1.2 Інфрачервоні датчики руху

Безпроводною датчик руху М-303УБП призначений для виявлення руху людини поза приміщенням.

Датчик складається з мікрохвильового модуля, сенсора інфрачервоного випромінювання і передавача радіосигналу. Принцип роботи датчика руху заснований на уловлюванні інфрачервоного випромінювання, яке випромінює кожна живу істоту. ГИК – випромінювання, яке приймають датчики руху, фокусується на пироприймачі, як яке використовується надчутливий напівпровідниковий піроелектричний перетворювач, здатний зареєструвати різницю декілька десятих градуса між температурою тіла людини і температурою фону. Різниця температур перетвориться в електричний сигнал, який передається на центральний блок. Проте після спрацювання ІК-сенсора руху, автоматично включається СВЧ-сенсор. Якщо мікрохвильовою канал не підтвердить тривожний сигнал, датчик розцінить цю подію як неправдиве, і система повернеться до чергового режиму роботи. Таким чином, пальто, що впало, в зоні дії датчика не спровокує відправку тривожного сигналу датчика, а ось щонайменше рухи людини датчик руху відразу ж засіче.



Рисунок 4.7 – Безпроводної датчик руху М-303УБП

Технічні характеристики:

- елемент живлення : 3 В (літієва батарея);
- діапазон робочих температур : – 50 С – +65 С;



- протокол зв'язку : MODBUS RTU;
- робоча вологість: до 90%;
- захист від білого світлу: більше 1 000 000 лм;
- робоча частота: 433 МГц;
- розміри: 138x75x46 мм;
- термін роботи від однієї батареї: 6...12 місяців;
- дальність детектування : до 18 м;
- кут детектування : 110°;
- висота інсталяції : від 2 м до 2,5 м;
- максимальна відстань передачі : 100 м (пряма видимість).

#### 4.2.2.1.3 Датчик вологості

Датчики вологості вимірюють відносну вологість повітря.

Датчик вологості TELETRACK AS100 – I4 – 20 призначений для виміру відносній вологості повітря в діапазоні 0...100% (без конденсату), має вбудований перетворювач сигналу вологості в струм 4...20 мА змонтований в корпусі датчика.



Рисунок 4.8 – Датчики вологості TELETRACK AS100 – I4 – 20

Технічні характеристики TELETRACK AS100 – I4– 20:

- показник інерції : 30 с;
- робоча температура експлуатації : 0.+85°З;

– параметри живлення :	12.24 В, 50 мА;
– вихідний сигнал:	4.20 мА;
– клас точності в діапазонах:	0...10% – 6 11...89% – 2, 90...100% – 3;
– варіанти виконання :	погружної і настінний;
– габаритні розміри:	40×63×30 мм з штирем з фільтром 30 мм, для настінного виконання;
– довжина погружної частини:	L = 80.250 мм.

#### 4.2.2.1.4 Акустичні датчики

Акустичні датчики – реагують на звук розбитого скла, тому їх встановлюють на стіну або стелю біля вікна.

Безпроводний датчик розбиття скла М-601 призначений для виявлення розбиття скла в приміщенні, що охороняється. Детектувальний елемент датчика – акустичний мікрофон. За допомогою його датчик виявляє поле акустичних хвиль, що утворюються при руйнуванні заклої конструкції (вікно, вітрина), що охороняється. Уловлені хвилі датчик перетворить в електричні сигнали, і передає у блок обробки. У цьому блоці здійснюється посилення сигналів і їх аналіз.

Якщо частота звукового сигналу співпала з частотою звуку розбиття скла, то на датчику спалахує світловий індикатор і датчик посиляє повідомлення на центральний блок.

Датчик використовується для виявлення розбиття скла у будинку, магазині, готелі, ресторані, офісній будівлі, школі, банці, бібліотеці, складі і так далі.

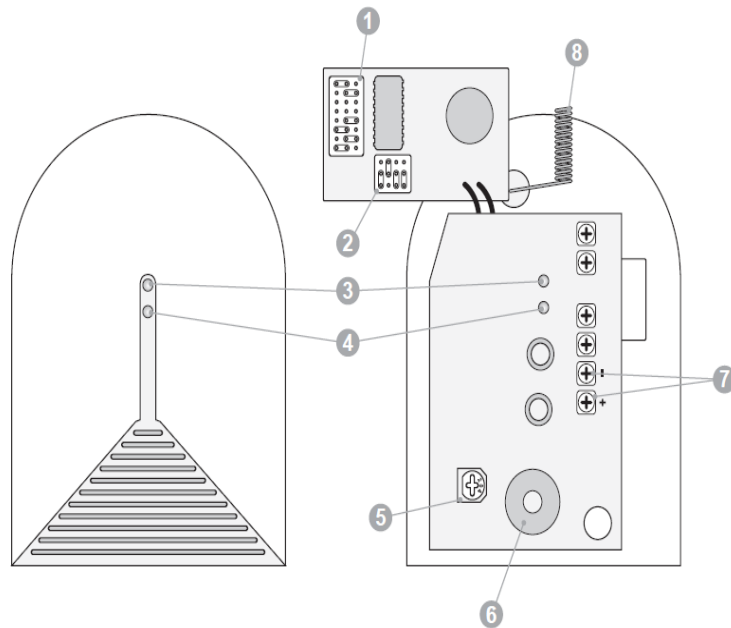


Рисунок 4.9 – Безпроводний датчик розбиття скла М–601

1. Перемички для установки адресної інформації центрального блоку.
2. Перемички для установки зони датчика.
3. Індикатор «Тестування»(зелений).
4. Індикатор «Тривога»(червоний).
5. Регулятор рівня чутливості датчика.
6. Акустичний мікрофон.
7. Клеми для підключення кабелю електроживлення.
8. Антена для передачі сигналу з датчика на центральний блок.

Технічні характеристики М–601:

- живлення: 12 В;
- дальність детектування: 9 м;
- спожив. струму в режимі «БЕЗДІЯЛЬНІСТЬ»: 5 мА;
- споживання струму в режимі «ТРИВОГА»: 80 мА;
- діапазон робочих температур : – 10°С.+50°С;
- робоча вологість: до 95%;
- частота передавача : 433 МГц;

- протокол зв'язку : MODBUS RTU;
- відстань зв'язку, (пряма видимість): 100 м;
- розмір: 90x65x25 мм.

#### 4.2.2.1.5 Вібраційні датчики

Вібраційні датчики М-4402 реагують на вібрацію поверхні, на якій встановлені. Спрацьовують, наприклад, при спробі відкрити вікно, дверці сейфа, проломити стіну і тому подібне. Встановлюються на рами, двері, стіни, дахи.



Рисунок 3.10 – Вібраційний датчик М-4402

Технічні характеристики М-4402:

- робоча напруга: ~220 В;
- чутливість: від 0,3 дБ;
- струм в режимі «Бездіяльність»: не більше 9 мА;
- струм в режимі «Тривога»: не більше 100 мА;
- рівень звуку вбудованої сирени : 85 дБ/м;
- діапазон робочих температур : – 10°C +50°C;
- робоча вологість: до 95%;
- спосіб установки : настінний;
- частота передавача : 433 МГц;

- протокол зв'язку : MODBUS RTU;
- відстань передачі (безпроводною): 100 м (пряма видимість);
- розміри: 99×70×60 мм.

#### 4.2.2.1.6 Датчики газу

Дротяною або безпроводною датчик виявлення газу М-502 використовується для виявлення витoku горючих газів(природний газ, побутовий газ, пропан, Бутан і ін.). Основний елемент датчика – детектор газу. Поверхня детектора покрита тонким шаром каталізатора, як який використовується, платина, паладій або діоксид олова. Газ, що потрапляє на шар каталізатора, окислюється киснем повітря і викликає додатковий нагрів цього шару. Зміна температури призводить до появи електричного сигналу, який посилюється електронною схемою. При перевищенні певного порогового значення концентрації газу датчик посилає повідомлення про пожежну тривогу на центральний блок і включається вбудована в датчик звукова сирена.



Рисунок 4.11 – Дротяної або безпроводної датчик виявлення газу М-502

Дротяний / безпроводною датчик виявлення газу підходить для використання у будинку, магазині, готелі, ресторані, офісній будівлі, школі, банці, бібліотеці, складі і так далі

Технічні характеристики М-502:

- робоча напруга: ~220 В;

- струм в режимі «Бездіяльність»: не більше 9 мА;
- струм в режимі «Тривога»: не більше 100 мА;
- час прогрівання : близько 180 с;
- рівень звуку вбудованої сирени : 85 дБ/м;
- діапазон робочих температур :  $-10^{\circ}\text{C} +50^{\circ}\text{C}$ ;
- робоча вологість: до 95%;
- спосіб установки : настінний;
- частота передавача : 433 МГц;
- протокол зв'язку : MODBUS RTU;
- відстань передачі(безпроводною) : 100 м (пряма видимість);
- розміри:  $107 \times 72 \times 41$  мм.

#### 4.2.2.1.7 Теплові і пожежні датчики

Теплові датчики повідомляють про підвищення температури в приміщенні (у зоні, що охороняється).



Рисунок 4.12 – Датчик температури TELETRACK PT100 – I4 – 20

Датчик температури TELETRACK PT100 – I4 – 20 застосовується для виміру температури повітря, має вбудований перетворювач сигналу опору Pt100 в струм 4–20 мА, змонтований в корпусі датчика.

Основні технічні параметри TELETRACK PT100 – I4– 20:

- діапазон температури :  $-40 \dots +85$  C;
- параметри живлення : 12.24 В, 50 мА;

- вихідний сигнал: 4...20 мА;
- клас точності : 0,5;
- варіанти виконання: занурюваний і настінний;
- габаритні розміри: 40×63×30 мм з штирем 30 мм для настінного виконання і під замовлення для занурюваного виконання.

Димові датчики реагують на задимлення, призначені для контролю займань.

Безпроводний пожежний датчик ПД714–09 призначений для визначення пожежі в приміщенні, що охороняється. Датчик виявляє дим за допомогою інфрачервоного випромінювача і фотоприймача. Елементи змонтовані в спеціальній димовій камері. Фотоприймач орієнтований так, щоб при роботі в штатних умовах ГИК випромінювання їм не фіксувалося. При попаданні частинок диму в оптичну камеру пожежного датчика на них відбувається хаотичне розсіювання ГИК випромінювання. І частина цього випромінювання потрапляє на фотоприймач, збуджуючи електричний сигнал. Чим вище концентрація диму в повітрі, тим вище рівень електричного сигналу. При перевищенні їм певного порогового значення датчик диму посилає повідомлення про пожежну тривогу на центральний блок і включається вбудована в датчик звукова сирена. Датчик використовується для виявлення диму у будинку, магазині, готелі, ресторани, офісній будівлі, школі, банці, бібліотеці, складі і так далі



Рисунок 4.13 – Безпроводний пожежний датчик ПД714–09

Технічні характеристики ПД714–09:

- елемент живлення : 9 В (тип РРЗ «Крона»);
- споживання струму в робочому режимі: не більше 10 мкА;
- світлова індикація: черв. спалах на діоді;
- рівень звуку вбудованої сирени : 85 дБ/м;
- діапазон робочих температур : – 10°З +50°З;
- робоча вологість: до 95%;
- площа, що покривається : 20 м<sup>2</sup>;
- частота передавача : 433 МГц;
- відстань передачі : 100 м  
(пряма видимість);
- розміри: діаметр 107 мм  
висота 35 мм.

#### 4.2.2.1.8 Датчик витоку води

Датчик витоку води Waterguard 1000 – H2OS представляє серію недорогих порогових датчиків витоку води, які можна використати у складі стандартних систем охоронно–пожежної і аварійної сигналізації.

Таблиця 4.1 – Технічні характеристики Waterguard 1000 – H2OS

Параметр	Значення
Напруга живлення	5...24 В
Споживання в черговому режимі	1 мкА
Споживання в режимі тривоги	до 200 мА
Контакти	Нормально відкриті
Розміри	6x1, 2x1, 2 см
Підключення	18 см двожильний кабель
Колір	Білий



Датчики поєднаємо з більшістю приймально–контрольних панелей (Paradox Security Systems, Detection Systems, Ademco, DSC, Texcom, Napco, Pyronix і так далі).



Рисунок 4.14 – Датчик витоку води Waterguard 1000 – H2OS

Підключаються просто паралельно крайовому опору шлейфу, єдина умова – панель повинна обмежувати струм в шлейфі значенням в 50 мА. Коли рівень води досягне зовнішніх контактів датчика, вихід датчика замкнеться. При падінні рівня води датчик саме – відновлюється. Моделі датчиків розрізняються діапазоном робочої напруги і зовнішнім виглядом.

#### 4.3.2.2 Виконавчі пристрої

##### 4.2.2.2.1 Звукова сирена

Звукова сирена внутрішньої установки SA 107 призначена для звукового сповіщення про тривогу.

Технічні характеристики SA 107:

- |  |                  |
|--|------------------|
| – параметри живлення :                 | 12 В;            |
| – споживання струму в робочому режимі: | не більше 20 мА; |
| – рівень звуку вбудованої сирени :     | 85 дБ/м;         |
| – діапазон робочих температур :        | – 10°C +50°C;    |
| – робоча вологість:                    | до 95%;          |
| – розміри:                             | діаметр 80 мм;   |
|  | висота 90 мм.    |



Рисунок 4.15 – Сирена для внутрішньої установки SA 107

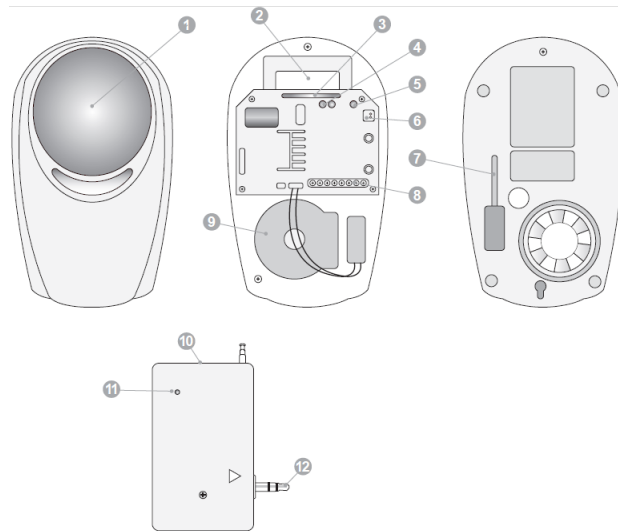


Рисунок 4.16 – Безпроводна вулична звукова сирена М-204 УБП

1. Лінза світлового сповіщення.
2. Вбудований акумулятор.
3. Лампа для світлового сповіщення.
4. Індикатори «Тривога».
5. Індикатор «Прийом сигналу».
6. Роз'єм для підключення вбудованого акумулятора.
7. Темпер.
8. Клеми для підключення мережі електроживлення.
9. Динамік.
10. Зовнішня антена для передачі сигналу тривоги з центрального блоку на рупор.
11. Індикатор «Передача сигналу».
12. Штекер для підключення до охоронної системи.

Безпроводна вулична звукова сирена М-204 УБП призначена для світлового і звукового сповіщення про тривогу, гучністю 110 дБ. Сирена має вбудований акумулятор для автономної роботи. Завдяки міцним матеріалам корпусу безпроводну вуличну світлозвукову сирену можна використати поза приміщенням.

Технічні характеристики М-204 УБП:

– робоча напруга:	12 В;
– діапазон робочих температур :	– 10°С.+50°С;
– робоча вологість:	до 90%;
– робоча частота:	433 МГц;
– протокол зв'язку :	MODBUS RTU;
– розміри:	80 x 110 x 200 мм;
– споживання струму в робочому режимі:	не більше 12 мА;
– гучність:	110 дБ;
– роботи від вбудованого акумулятора:	до 12 місяців.

#### 4.2.2.2.2 Магнітний пускач

Для управління різними дискретними навантаженнями, застосуємо контактно – модульні пускачі фірми TERASAKI, які застосуються для комутації силових електричних ланцюгів. Завдяки модульній конструкції контактори є незамінними при монтажі в модульних щитах спільно з іншим модульним електроустаткуванням.

Технічні характеристики пускача TERASAKI CDI 406/63:

– кількість контактних груп :	3, що замикають;
– номінальний комутований струм:	25–63 А;
– номінальна комутувана напруга:	440 В;
– напруга ланцюга управління :	12 В.

– струм ланцюга управління : 0,1 А.



Рисунок 4.17 – Контактор модульний CDI 406/63

### 4.2.2.3 Додаткові пристрої

#### 4.2.2.3.1 Акумулятори

Акумулятори призначені для блоків безперебійного живлення і модулів охоронно–пожежної сигналізації.



Рисунок 4.18 – Li-ion 12 В акумулятори, місткістю 1,3 А-ч; 4 А-ч; 7 А-ч;

#### 4.2.2.4 Мікроконтролер

Нині на світовому ринку представлений широкий спектр мікроконтролерів різних виробників (Atmel, Dallas Semiconductor, Philips Semiconductor, Winbond, Silicon Laboratories, Texas Instruments і Cypress Semiconductor, Microchip Technology Inc.).

Майже усі сучасні мікроконтролери мають гарвардську архітектуру і побудовані на CMOS– технології – це означає, що схеми самих мікроконтролерів мають високу швидкість і невелике енергоспоживання.

У номенклатурі Microchip Technology Inc. представлений широкий спектр 8-и, 16-и і 32-битних мікроконтролерів і цифрових сигнальних контролерів під маркою PIC. Відмітною особливістю PIC- контролерів є хороша спадкоємність різних сімейств. Це і програмна сумісність (єдине безкоштовне середовище розробки MPLAB IDE, C-компілятори від GCC, HTPIC), і сумісність по виведенню, по периферії, по напрузі живлення, по засобах розробки, по бібліотеках і стеках найбільш популярних комунікаційних протоколів. Номенклатура налічує більше 500 різних контролерів зі всілякими варіаціями периферії, пам'яті, кількістю виведень, продуктивністю, діапазонами живлення і температури і так далі

Таким чином, PIC- мікроконтролери – це універсальні пристрої, які застосовні практично в усіх сферах електроніки. Наявність великої кількості готових програмних бібліотек, довідкової літератури, безкоштовного програмного забезпечення, готових тестових учбових плат вигідно відрізняє мікроконтролери сімейства PIC серед інших.

PIC18F452(PIC18F252) – це багатофункціональний контролер, розроблений фірмою «Microchip»<sup>®</sup> спеціально для застосування в системах автоматики, який має усі необхідні функції, необхідні для створення апаратної частини охоронного блоку. А саме: низьке енергоспоживання, достатня швидкість обробки даних, наявність достатньої кількості портів введення / виведення і процедур обробки різноманітних переривань(від таймерів, зовнішніх пристроїв), підтримка стандартних інтерфейсів зв'язку для комунікації з периферійними пристроями, можливість переходу в економічний режим роботи (SLEEP mode) та ін.

Доступність на ринку України і низька вартість дозволяє створювати додатки високого рівня інтеграції з невеликими економічними витратами.

Основні характеристики контролера PIC18F252:

- час виконання інструкції: 100 нс;

- достатній об'єм програмної, оперативної і енергонезалежної пам'яті;
- підтримка переривань (до 14–джерел);
- підтримка «сплячого режиму» (SLEEP mode);
- широкий діапазон напруги живлення: 2,0...5,5 В;
- комерційне, промислове або військове виконання;
- низьке енергоспоживання:
  - < 0,6 мА при 3 В і 4 МГц;
  - 20 мкА при 3 В і 32 кГц;
  - < 1 мкА в режимі очікування.

Основні апаратні частини контролера, необхідні для створення проекту :

- апаратні таймери (Timer 0, Timer 1, Timer 2);
- багатоканальне 10–розрядне АЦП;
- синхронний послідовний порт (SSP) з підтримкою SPI;
- універсальний синхронний / асинхронний приймач (USART/SCI) з підтримкою 9–бітової адресації.

Однією з основних вимог до вибраного контролера є наявність апаратної підтримки USART, оскільки цей інтерфейс використовуватиметься для організації комунікації з GSM– модемом і іншими блоками, працюючими по протоколу MODBUS RTU.

#### **4.2.2.5 Безпроводні засоби передачі інформації**

##### **4.2.2.5.1 GSM– модуль SIM300DZ, SIM300C**

Якщо проаналізувати GSM– пристрою, то видно, що практично в кожному з них головну роль грають GSM– модулі. Це цегла, з якої збираються складніші системи. У нашому пристрої використовується модуль китайської фірми «SimCom». У GSM– модулі сконцентрована практично уся інтелектуальна начинка мобільного пристрою.



Рисунок 4.19 – GSM модуля SIM300DZ

SIM300DZ – трьох-діапазонний GSM/GPRS модуль, виробництва «SimCom», який призначений для передачі голосу, даних, SMS повідомлень, факсимільних повідомлень. Маленькі розміри форм-фактору і висока функціональність модуля SIM300DZ ідеально підходить для вбудовуваних рішень, де важливі розміри кінцевого пристрою. SMD форм-фактор модуля SIM300DZ дає можливість інтегрувати модуль на автоматичній лінії в пристрій(на друковану плату) без застосування дорогого устаткування, дорогих методів перевірки припою по порівнянню з BGA корпусом. SIM300DZ має вбудований повнофункціональний TCP/IP стек, можливість контролю і управління зарядом Liон- акумулятора. Застосування GSM / GPRS модуля SIM300DZ скорочує час виробництва і здешевлює кінцевий виріб.

Основні характеристики:

- діапазон частот : 900/1800/1900 МГц;
- протокол: вбудований TCP/IP;
- управління: за допомогою AT – команд;
- напруга живлення : 3,4...5,5 В;
- стандарт: сумісність GSM Phase 2/2+;
- вихідна потужність: 2 Вт/900 МГц, 1 Вт/1800/1900 МГц;
- робоча температура: – 20°C.+55°C (SIM 300C)  
–30°C.+70°C (SIM300DZ);

- розміри: 40 x 33 x 2,85 мм (SIM 300C)  
50 x 33 x 6,2 мм (SIM300DZ);
- вага: 8 г (SIM 300C)  
13,8 г (SIM300 DZ).

Інтерфейси GSM модуля (SIM300DZ, SIM300C) :

- зовнішній інтерфейс: SIM– карта 1,8.3 В;
- роз'єм: 60 виведень;
- інтерфейси: 2 аналогових аудіо  
клавіатура  
LCD– дисплей.

Передача даних GSM модуля (SIM300DZ, SIM300C):

General Packet Radio Service (GPRS) Class 10 забезпечує роботу GSM–модулю в режимі голосового з'єднання або пакетної передачі даних, з можливістю автоматичного перемикання між режимами. Модуль дозволяє передавати дані зі швидкістю до 9 600 біт/с, а приймати зі швидкістю до 38 400 біт/с.

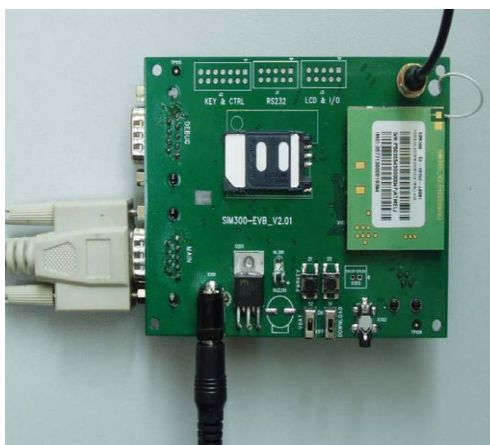


Рисунок 4.20 – Налагоджувальний комплект SIM300CEVBKIT

SMS сервіс GSM модуля (SIM300DZ, SIM300C) :

- прийом текстових і PDU повідомлень (MT);
- передача текстових і PDU повідомлень (MO);



- прийом широкомовних повідомлень;
- підтвердження про отримання SMS.

Максимальна довжина одного повідомлення 160 символів при використанні 7-біт кодування і 140 символів при 8-біт кодуванні. При використанні так званого кириличного кодування UCS2 можливо читати і посилати повідомлення по-російськи і тоді максимальна довжина повідомлення скорочується до 70 символів через те, що на кожен символ цього кодування потрібно 2 байти. З'єднання до 6 повідомлень при одній відправці.

Для роботи з GSM-модулем є налагоджувальний комплект SIM300CEVBKIT – спеціально розроблений для цього модуля.

#### **4.2.2.5.2 Радіо-облаштування приймача даних TRC101**

Фірма «RF Monolithic»® є одним зі світових лідерів з виробництва радіо-компонентів і радіопристроїв. На сайті фірми представлений спектр продукції, що випускається, з усією супутньою літературою і технічною документацією, яка може згодитися на етапах проектування нових пристроїв або впровадженні в існуючі системи автоматики і телемеханіки. Так само представлені у вигляді прикладів друковані плати і частини програмного коду, які можуть бути використані як зразок.

Поставленим технічним завданням до радіопередавача системи, що розробляється, задовольняють багато частотних маніпуляторів різних виробників, тому вибір радіопередавача по виробникові не критичний, а по функціональних можливостях найбільш відповідним є сімейство TRC фірми «RF Monolithic»®.

TRC101 – це малопотужний радіочастотний приймач, який був спеціально розроблений фірмою «RF Monolithic»® для застосування в системах збору, обробки і передачі інформації і має безліч вбудованих функцій(програмних і

апаратних), що дозволяють розробляти короткохвильову радіоапаратуру з відносно низькими витратами трудових ресурсів.

Низька споживана потужність при роботі приймача і наявність функцій сплячого режиму ідеально підходить для створення систем з жорсткими вимогами до енергоспоживання.

Доступність на ринку України і низька вартість дозволяє створювати додатки високого рівня інтеграції з малими економічними витратами.

Проведення детального аналізу функціональних можливостей і сфер застосування TRC101 показало, що використання цієї мікросхеми задовольняє поставленим завданням.

Основні характеристики мікросхеми TRC101 :

- модуляція: FSK(частотна маніпуляція);
- частотний діапазон: 300.1000 МГц;
- чутливість: – 105 дБ;
- швидкість передачі даних : до 256 кбод;
- низьке енергоспоживання: ~8.5 мА (Rx), ~20 мА (Tx);
- широкий діапазон напруги живлення: 2,2...5,4 В;
- низьке енергоспоживання в режимі очікування: 0,2 мкА;
- вбудовані PLL (фазове автоматичне підстроювання частоти), IF (проміжна частота), Baseband Circuitry (ланцюги генерації частоти, що несе);

Однією з основних вимог до вибраного радіопристрою є наявність апаратної підтримки SPI- інтерфейсу, оскільки цей інтерфейс використовуватиметься для організації комунікації з контролером.

### 4.3 Розробка схеми автоматизації

Для перевірки функціональних можливостей схемотехніки і програмних охоронного блоку мікропроцесорної індивідуальної охоронної системи з виходом на GSM- канал був розроблений спрощений варіант макету функціональної схема основного охоронного блоку.

На рисунку 4.21 представлена функціональна схема макету основного охоронного блоку.

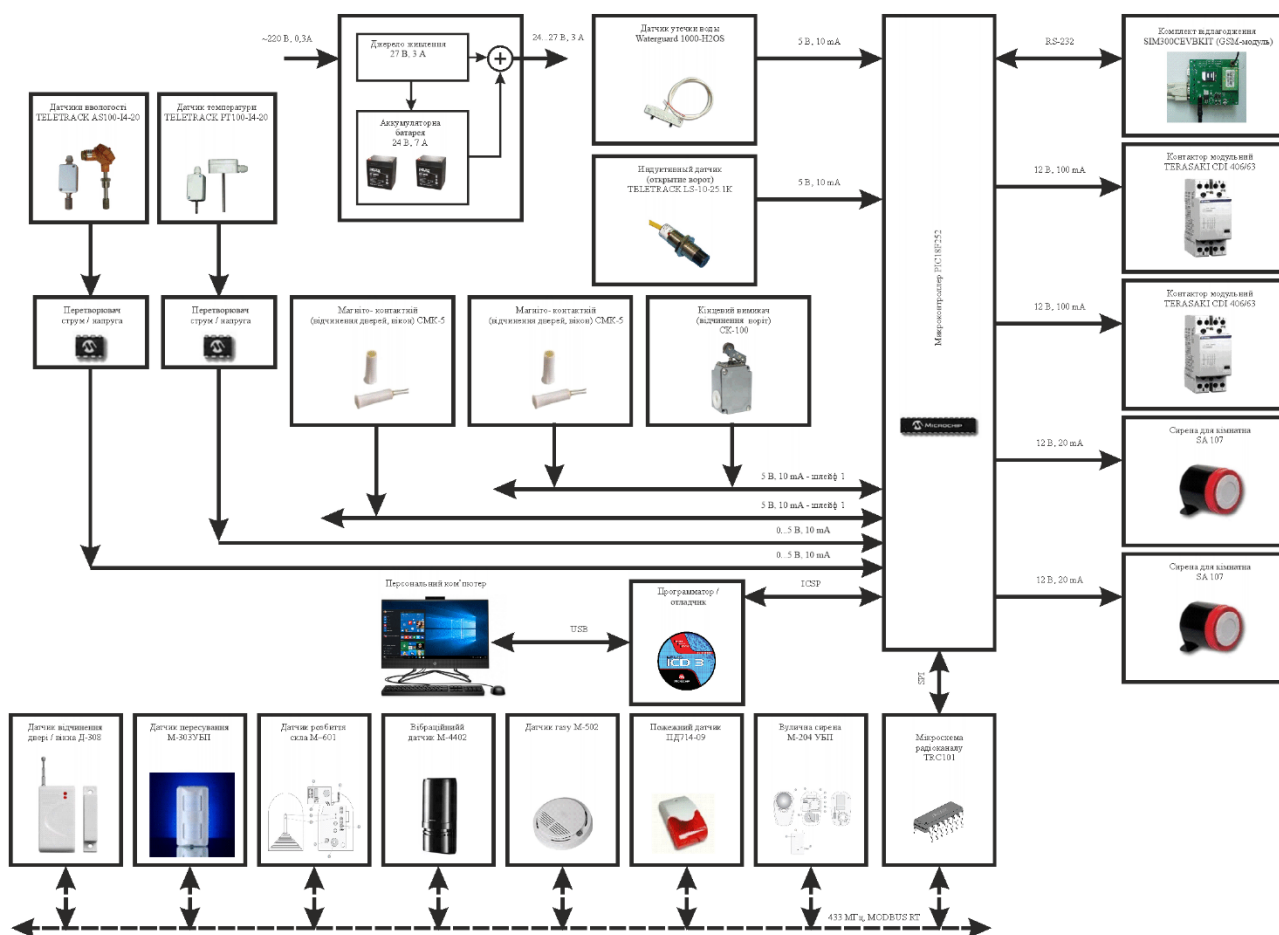


Рисунок 4.21 – Функціональна схема макету основного охоронного блоку

Розроблена функціональна схема містить усі основні компоненти:

- мікроконтролер;
- модуль GSM- каналу;

- модулі для підключення дискретних датчиків – шлейфи датчиків вікон і дверей;
- модулі для підключення аналогових датчиків;
- модулі для підключення радіо – датчиків, радіо – виконавчих пристроїв і каналу розширення – для підключення додаткового охоронного блоку;
- джерело безперебійного живлення;
- модуль для підключення програматора.

#### **4.3.1 Функціональна схема контролера**

Згідно з функціональною схемою основного охоронного блоку розроблена електрична принципова схема макету основного охоронного блоку.

Для проєктованого основного охоронного блоку, зібраного на мікроконтролері PIC128F252, для забезпечення введення сигналів з датчиків і виведення на облаштування управління необхідно, потрібні наступні рішення схемотехніки облаштувань узгодження з об'єктом:

- 2 однакові схеми узгодження : з датчиком температури TELETRACK PT100 – I4 – 20 і датчиком вологості TELETRACK AS100 – I4 – 20
- 2 схеми управління пускачами TERASAKI – CDI 406/63;
- 2 схеми управління сиренами SA 107.

Інші сигнали, необхідні для контролю і управління не вимагають спеціальних рішень схемотехніки.

Розглянь перераховані схеми детальніше.

Схема, призначена для узгодження з датчиками температури і вологості, і реалізована таким чином (рис. 4.22).

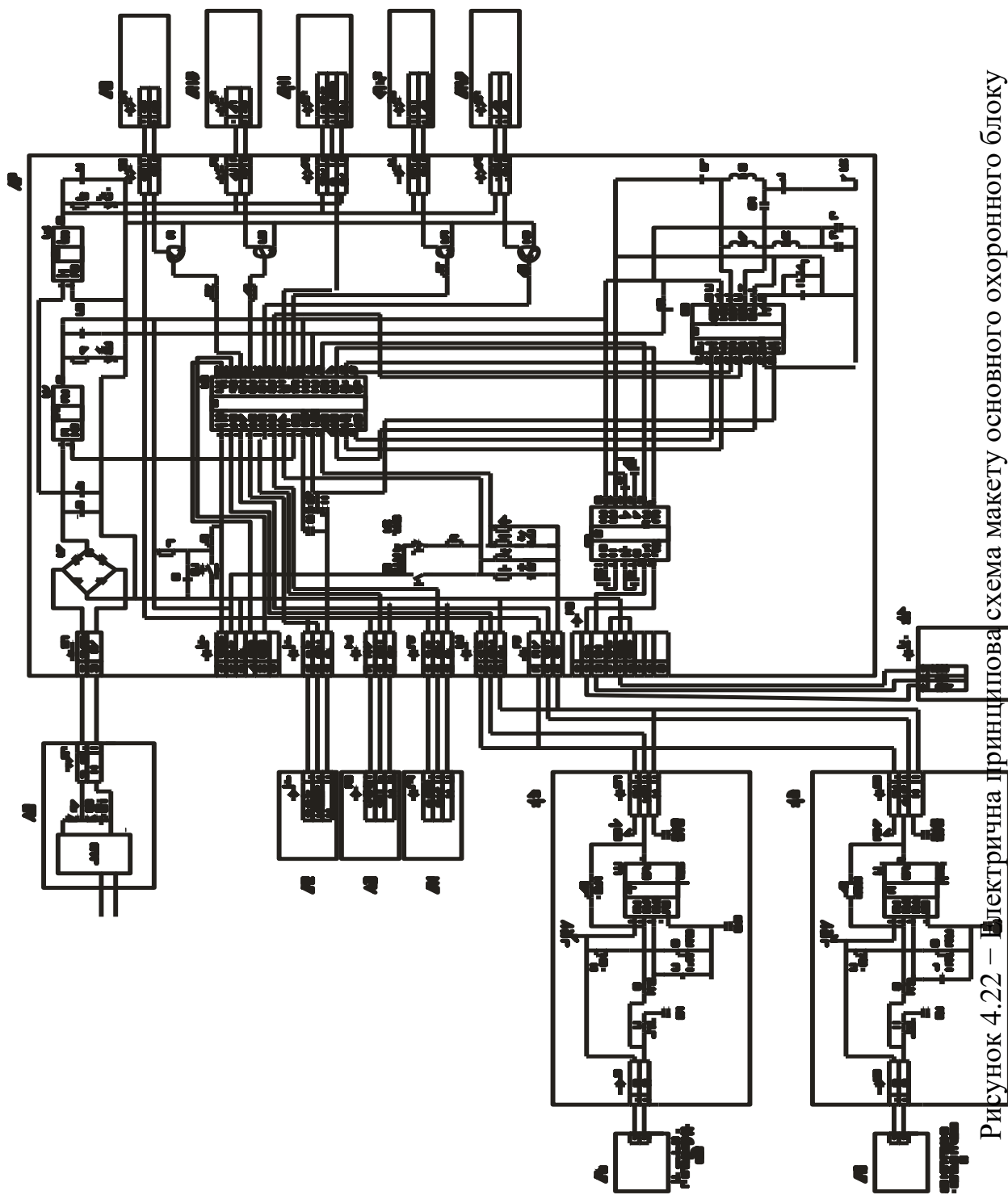


Рисунок 4.22 – Принципова електрична схема макету основного охоронного блоку

Пряме підключення датчиків з номінальним опором на вхід АЦП мікроконтролера не дозволить отримати бажаного результату вимірів, оскільки амплітуда змін вихідного сигналу з датчика буде занадто мала, що приведе до того, що цифрований сигнал матиме великий відсоток погрішності.

Включення в схему підсилювача сигналу, дозволить збільшити амплітуду вихідного сигналу датчика. Схема підсилювача сигналу датчика представлена на рис. 4.23. Ця схема побудована на операційному підсилювачі MCP6002. Коефіцієнт посилення ( $\alpha$ ) при такому включенні операційного підсилювача обчислюється за формулою 4.1.

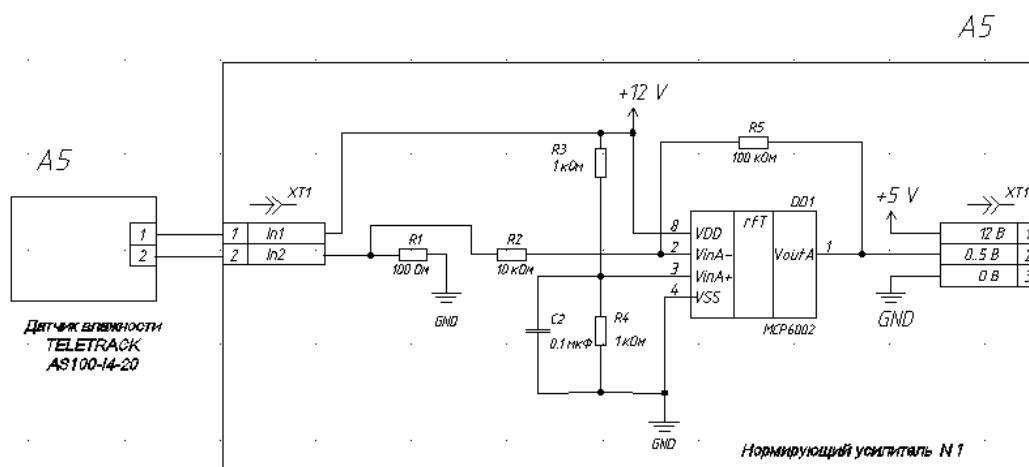


Рисунок 4.23 – УСО з датчиками температури і вологості

$$\alpha = R5/R2 \quad (3.1)$$

Друга схема, призначена для узгодження з пускачами засувки (рис. 4.24), зібрана за класичною схемою силового ключа, виконаного на біполярному транзисторі.

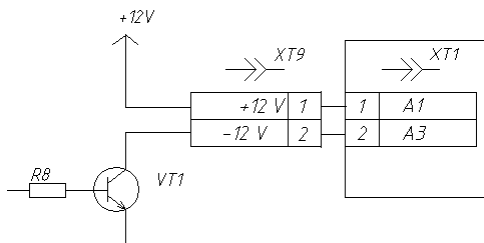


Рисунок 4.24 – УСО з пускачами TERA SAKI – CDI 406/63

Частина схеми електричної, яка відповідає за стабілізацію живлячої напруги для апаратної частини представлена на рис. 4.25.

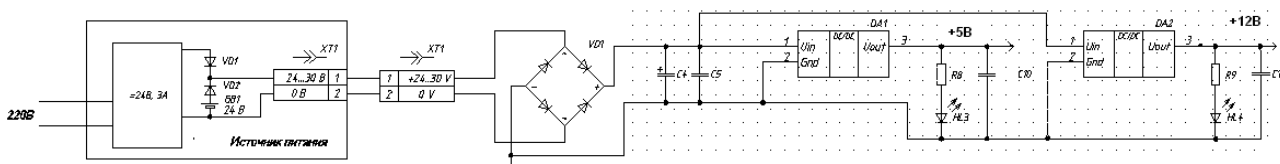


Рисунок 4.25 – Стабілізаторів напруги на +5 В і +12 В

XT1 – це монтажна клема, призначена для підключення джерела живлення (стабілізованого або нестабілізованого) з вихідною напругою 15...30 В. Полярність живлячої напруги на клемі XT1 не має значення, оскільки використовується діодний міст VD1. Місткості C4, C5 і C6 служать для виключення пульсації живлення на вході і виході перетворювача напруги DA1, який відповідає за стабілізацію живлення іншої частини схеми на рівні 5 В, а DA2, який відповідає за стабілізацію живлення іншої частини схеми на рівні 12 В.

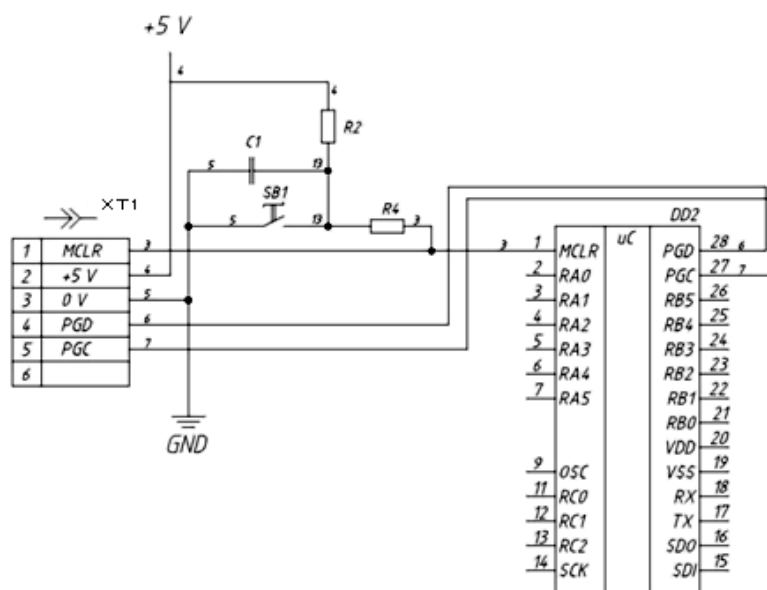


Рисунок 4.26 – Роз'єм підключення програматора і кнопка апаратного скидання мікроконтролера

Для того, щоб було можливо програмувати мікроконтролер безпосередньо на платі проектованого пристрою(забезпечити можливість підключення програматора), в апаратну частину були додані додаткові елементи (роз'єм ХЕ1, резистори R2, R4 – рис. .427) згідно з керівництвом по експлуатації використовуваного мікроконтролера. Таким чином, на етапі проектування програмного забезпечення для мікроконтролера при виявленні помилок буде обпечена можливість зміни програми мікроконтролера. Кнопка SB1 – апаратне скидання мікроконтролера.

Для підключення підсистеми регулювання до комп'ютера використовуємо зовнішній послідовний інтерфейс COM. Функції управління передачею даних з боку вузла по RS232 бере на себе модуль USART вибраного мікроконтролера PIC18F252. Для узгодження рівнів сигналів COM– порту комп'ютера і мікроконтролера використовується мікросхема MAX232A.

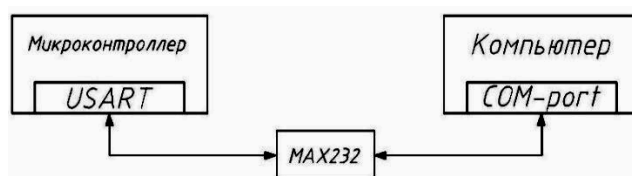


Рисунок 4.27 – Структурна схема модуля підключення до комп'ютера

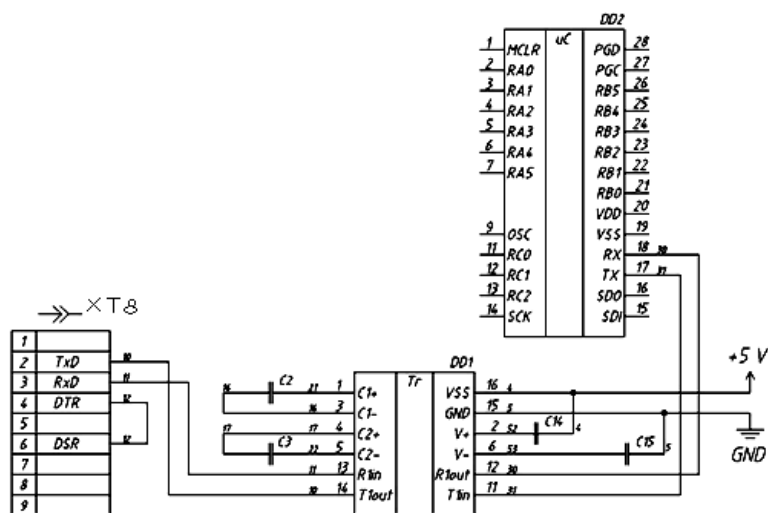


Рисунок 4.28 – Організація комунікації мікроконтролера з ЕОМ



Частина електричної схеми, яка відповідає за зв'язок з комп'ютером по RS232, представлена на рис. 4.29. DD1 (мікросхема MAX232A) – це драйвер RS232 для додатків, де недоступна напруга  $\pm 12$  В, яке використовується в ЕОМ при зв'язку через СОМ– порт. Роз'єм XT8 – це стандартний 9–контактний DE – 9 (D – Sub) роз'єм, який забезпечує пряме підключення до комп'ютера стандартним кабелем.

## ВИСНОВКИ

Виконана розробка кіберфізичної системи домашнього інтернету речей житлового комплексу «Бартоломео» з детальною розробкою побудови та безпеки комп'ютерної мережі на основі мережевого обладнання Cisco™ для основних мережевих вузлів. Виконано розрахунок налаштувань для заданої топології мережі, обрано інтерфейси каналів зв'язку та протоколи обміну, розрахована топологічна схема комп'ютерної системи, розраховані налаштування маршрутизації комп'ютерної мережі, а також виконане подальше моделювання і перевірка роботи комп'ютерної системи.

У кваліфікаційній роботі розроблено облаштування охоронної і пожежної сигналізації для видалених об'єктів, таких як заміський будинок або дача, де неможлива постійна присутність людини. У разі виникнення позаштатних ситуацій, хазяїна або диспетчерський пункт інформуватиме автоматична система, на основі мікроконтролера і сигналів, що поступають на нього, з різних датчиків, пов'язаного з каналами передачі даних GSM. Така система допоможе запобігти збитку, нанесеному зловмисниками внаслідок проникнення і крадіжки цінностей, попередити займання об'єкту, або інших неприємних ситуацій. Усі ці заходи спрямовані на те, щоб зберегти матеріальні блага людей, їх майно, ну і, звичайно ж, здоров'я в психологічному плані.

Детально розглянуті недоліки існуючих дистанційних охоронних систем, визначена структура системи і приведені принципи, закладені в основу пристрою, що розробляється. Розроблено технічне завдання для усієї охоронної системи. Розроблена деталізована структурна схема системи, здійснений детальний вибір елементної бази, розроблена функціональна схема макету основного охоронного блоку і згідно з нею, зроблений синтез електричної принципової схеми макету основного охоронного блоку. Розроблений комплект документації для програмного забезпечення.

## ПЕРЕЛІК ПОСИЛАНЬ

1. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 62 с.
2. Положення про організацію атестації здобувачів вищої освіти НТУ «Дніпровська політехніка» / М-во освіти і науки України, Нац. техн. ун-т. – Д.: НТУ «ДП», 2018. – 40 с
3. Цвіркун Л.І. Розробка програмного забезпечення комп'ютерних систем. Програмування: навч. посіб. [Електронний ресурс] / Л.І. Цвіркун, А.А. Євстігнеєва, Я.В. Панферова; під заг. ред. проф. Л.І. Цвіркуна ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка».
4. Цвіркун Л.І. Інженерна та комп'ютерна графіка. AutoCAD : навч. посіб. / Л.І. Цвіркун, Л.В. Бешта; під. заг. ред. Л.І. Цвіркуна; М-во освіти і науки України, НТУ «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 209 с. – ISBN 978-966-350-663-0.
5. Цвіркун Л.І. Розробка програмного забезпечення комп'ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнеєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с. – ISBN 978-966-350-595-4.
6. Цвіркун Л.І. Глобальні комп'ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с. – ISBN 978-966-350-417-9.

7. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія /Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М–во освіти і науки України, Нац. техн. ун–т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.
8. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова; М–во освіти і науки України, Нац. техн. ун–т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.
9. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова; М–во освіти і науки України, Нац. техн. ун–т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.
10. Morrow K. Rio–20, the Green Economy and Re–orienting Sustainable Development // Environmental Law Review. 2012. № 14. P. 279–297.
11. Куличкан А.В., Щербаченко П.С. Экоинновации как инструмент устойчивого развития современного общества // Современные корпоративные стратегии и технологии в России : сб. научных статей : в 3 ч. / под ред. проф. И.Ю. Беляева. М., 2015. С. 97–106.
12. Калинина К.Д. инновации для объектов недвижимости: понятие, компоненты (социальная и экологическая) // Научный альманах. 2016. № 3–1 (17). С. 141–144 с.
13. Мингалева Ж.А. Современные подходы в исследовании эколого–экономических аспектов решения проблем урбанистики // Экономика и предпринимательство. 2014. Т. 8, № 4 (ч. 2). С. 725–727.

14. ЖК Bartolomeo Resort Town (Бартоломео Резорт Таун). Режим доступа: [https://dom.ria.com/uk/novostroyka-zhk-bartolomeo-resort-town-5881/?r\\_source=g\\_ads&r\\_medium=search&r\\_audience=ppc\\_buyers&r\\_options=targeting&r\\_campaign=15561928526&r\\_project=newbuilding&gclid=Cj0KCQjwqPGUBhDwARIsANNwjV77cHhxotcQ9mw4Hoct9fBj7M06nJDuHUSDnJmAlQiRx7wOE6kuxJYaAl3rEALw\\_wcB](https://dom.ria.com/uk/novostroyka-zhk-bartolomeo-resort-town-5881/?r_source=g_ads&r_medium=search&r_audience=ppc_buyers&r_options=targeting&r_campaign=15561928526&r_project=newbuilding&gclid=Cj0KCQjwqPGUBhDwARIsANNwjV77cHhxotcQ9mw4Hoct9fBj7M06nJDuHUSDnJmAlQiRx7wOE6kuxJYaAl3rEALw_wcB)
15. Bartolomeo resort town, житло, де все обертається навколо тебе. Режим доступа: <https://bartolomeo-town.com.ua/ua>
16. Особенности строительства жилых комплексов. Режим доступа: <http://www.realto.ru/journal/articles/osobennosti-stroitelstva-zhilyh-kompleksov/>
17. Проектирование жилого комплекса. Цены, особенности и основные этапы при проектировании жилых комплексов. Режим доступа: [http://www.ovikv.ru/%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5\\_%D0%B6%D0%B8%D0%BB%D1%8B%D1%85\\_%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BE%D0%B2.htm](http://www.ovikv.ru/%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B6%D0%B8%D0%BB%D1%8B%D1%85_%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BE%D0%B2.htm)
18. Особенности строительства новых жилых комплексов. Режим доступа: <http://pro-tools.eu/news/334-osobennosti-stroitelstva-novyh-zhilyh-kompleksov.html>
19. Обзор жилых комплексов элитных новостроек Днепропетровска. Режим доступа: <https://dd.net.ua/obzor-zhilyih-kompleksov-elitnyih-novostroek-dnepropetrovska/>
20. 20 – Самые востребованные функции умного ЖК. Режим доступа: <https://digitaldeveloper.ru/blog/tpost/t9dduf3521-samie-vostrebovannie-funksii-umnogo-zhk>

21. Системы автоматизации и диспетчеризации высотных жилых комплексов. Режим доступа: [https://www.abok.ru/for\\_spec/articles.php?nid=2857](https://www.abok.ru/for_spec/articles.php?nid=2857)
22. Формування організаційної структури підприємства. Режим доступу: <https://studfile.net/preview/5127858/page:58/>

**ДОДАТОК А**  
**ТЕКСТ ПРОГРАМИ**

**Міністерство освіти і науки України**  
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**  
**“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ**  
**НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ**

Текст програми

804.02070743.22005–01 12 01

Листів 6

**2022**



## АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп'ютерної системи третього апеляційного адміністративного суду. Програма призначена для забезпечення налаштування динамічної маршрутизації, DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и SSH комп'ютерної системи.

## ЗМІСТ

	Стор.
1. Налаштування роутера Gudakov_R2	4
2. Налаштування комутатора Gudakov_SwV4.1	6

```

1      Налаштування роутера Gudakov_R2
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Gudakov_R2
!
enable                secret                5
$1$mERr$hX5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 10.68.0.129
10.68.0.139
!
ip dhcp pool POOL_LAN2
network 10.68.0.128 255.255.255.128
default-router 10.68.0.129
dns-server 10.68.1.85
!
aaa new-model
!
aaa authentication login Login group radius
local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius
local

!
license udi pid CISCO2911/K9 sn
FTX1524602K-
!
no ip domain-lookup
ip domain-name Shchetinin_R1
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description LAN Admin
ip address 10.68.0.129 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
!
interface Serial0/0/1
description WAN R1
bandwidth 128
ip address 10.0.10.2 255.255.255.252
ip ospf cost 7500
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 23
router-id 15.15.15.15
log-adjacency-changes
passive-interface GigabitEthernet0/0
network 10.0.10.0 0.0.0.3 area 0
network 10.68.0.128 0.0.0.127 area 0
default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
banner motd #123-18 Gudakov. Enter only
have key#
!
radius-server host 10.68.0.150 auth-port 1645
radius-server key Gudakov

```

```

!
radius server 10.68.0.150
  address ipv4 10.68.0.150 auth-port 1645
!
!
!
line con 0
  password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
  password 7 0822455D0A16
  login authentication SSH-LOGIN
  transport input ssh
line vty 5 15
  password 7 0822455D0A16
  transport input ssh
!
!
!
end

1      Налаштування      комутатора
Gudakov_Sw4.1
!
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Gudakov_Sw4.1
!
enable      secret      5
$1$mERr$hX5rVt7rPNoS4wqbXKX7m0
!
ip domain-name Shchetynin_SW_Gosp
!
username 12316z_Shchetynin privilege 1
password 7 082048430017061E010803
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  shutdown
!
interface FastEthernet0/2
  shutdown
interface FastEthernet0/4
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/5
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/6
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/7
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/8
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/9
  shutdown
!
interface FastEthernet0/10
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/11
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/12
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/13
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/14
  switchport access vlan 30
  switchport mode access
!

```

```

interface FastEthernet0/15
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/16
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/17
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/18
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/19
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/20
  switchport access vlan 40
  switchport mode access
  switchport port-security
  switchport port-security maximum 2
  switchport port-security mac-address sticky
  switchport port-security violation restrict
!
interface FastEthernet0/21
  shutdown
!
interface FastEthernet0/22
  shutdown
!
interface FastEthernet0/23
  shutdown
!
interface FastEthernet0/24
  switchport trunk native vlan 100
  switchport trunk allowed vlan 20,30,40,99
  switchport mode trunk
!
interface GigabitEthernet0/1
  switchport trunk native vlan 100
  switchport trunk allowed vlan 20,30,40,99
  switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan99
  description LAN Menag
  ip address 10.68.0.2 255.255.255.224
!
ip default-gateway 10.68.0.1
!
banner
-----123-18
Gudakov.      Enter      only      have
key-----
!
line con 0
  password 7 0822455D0A16
  login
!
line vty 0 4
  password 7 0822455D0A16
  login local
  transport input ssh
line vty 5 15
  password 7 0822455D0A16
  login local
  transport input ssh
!
end

```

**ДОДАТОК Б**  
**ТАБЛИЦІ МАРШРУТИЗАЦІЇ**

**Міністерство освіти і науки України**  
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**  
**“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ**  
**НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ**

Таблиці маршрутизації

Листів 5

**2022**

## Таблиця маршрутизації на Gudakov\_R1

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
C       10.0.10.0/30 is directly connected, Serial0/0/1
L       10.0.10.1/32 is directly connected, Serial0/0/1
C       10.0.10.4/30 is directly connected, Serial0/0/0
L       10.0.10.5/32 is directly connected, Serial0/0/0
O       10.0.10.8/30 [110/15000] via 10.0.10.6, 02:51:55, Serial0/0/0
O       10.68.0.0/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.32/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.64/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.96/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.128/25 [110/7501] via 10.0.10.2, 03:57:06, Serial0/0/1
O       10.68.1.0/26 [110/7501] via 10.0.10.6, 03:57:06, Serial0/0/0
C       10.68.1.64/27 is directly connected, GigabitEthernet0/1
L       10.68.1.65/32 is directly connected, GigabitEthernet0/1
    209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/15000] via 10.0.10.6, 03:53:53, Serial0/0/0
S*    0.0.0.0/0 [1/0] via 209.165.202.1

```



## Таблиця маршрутизації на Gudakov\_R2

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 209.165.202.1 to network 0.0.0.0
```

```
10.0.0.0/8 is variably subnetted, 12 subnets, 5 masks
C    10.0.10.0/30 is directly connected, Serial0/0/1
L    10.0.10.2/32 is directly connected, Serial0/0/1
O    10.0.10.4/30 [110/15000] via 10.0.10.1, 03:57:56, Serial0/0/1
O    10.0.10.8/30 [110/22500] via 10.0.10.1, 02:52:45, Serial0/0/1
O    10.68.0.0/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O    10.68.0.32/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O    10.68.0.64/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O    10.68.0.96/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
C    10.68.0.128/25 is directly connected, GigabitEthernet0/0
L    10.68.0.129/32 is directly connected, GigabitEthernet0/0
O    10.68.1.0/26 [110/15001] via 10.0.10.1, 03:57:56, Serial0/0/1
O    10.68.1.64/27 [110/7501] via 10.0.10.1, 03:57:56, Serial0/0/1
209.165.202.0/27 is subnetted, 1 subnets
O    209.165.202.0/27 [110/22500] via 10.0.10.1, 03:54:48, Serial0/0/1
S*  0.0.0.0/0 [1/0] via 209.165.202.1
```

## Таблиця маршрутизації на Gudakov\_R3

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default, U - per-user static route, o - ODR  
 P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
O    10.0.10.0/30 [110/15000] via 10.0.10.5, 03:58:34, Serial0/0/0
C    10.0.10.4/30 is directly connected, Serial0/0/0
L    10.0.10.6/32 is directly connected, Serial0/0/0
C    10.0.10.8/30 is directly connected, Serial0/0/1
L    10.0.10.10/32 is directly connected, Serial0/0/1
O    10.68.0.0/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O    10.68.0.32/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O    10.68.0.64/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O    10.68.0.96/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O    10.68.0.128/25 [110/15001] via 10.0.10.5, 03:58:24, Serial0/0/0
C    10.68.1.0/26 is directly connected, GigabitEthernet0/1
L    10.68.1.1/32 is directly connected, GigabitEthernet0/1
O    10.68.1.64/27 [110/7501] via 10.0.10.5, 03:58:34, Serial0/0/0
209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.202.0/27 is directly connected, Serial0/1/0
L    209.165.202.2/32 is directly connected, Serial0/1/0
S*  0.0.0.0/0 [1/0] via 209.165.202.1

```

## Таблиця маршрутизації на Gudakov\_R4

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default, U - per-user static route, o - ODR  
 P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O    10.0.10.0/30 [110/15064] via 10.0.10.10, 02:54:02, Serial0/0/1
O    10.0.10.4/30 [110/7564] via 10.0.10.10, 02:54:02, Serial0/0/1
C    10.0.10.8/30 is directly connected, Serial0/0/1
L    10.0.10.9/32 is directly connected, Serial0/0/1
C    10.68.0.0/27 is directly connected, GigabitEthernet0/1.99
L    10.68.0.1/32 is directly connected, GigabitEthernet0/1.99
C    10.68.0.32/27 is directly connected, GigabitEthernet0/1.20
L    10.68.0.33/32 is directly connected, GigabitEthernet0/1.20
C    10.68.0.64/27 is directly connected, GigabitEthernet0/1.30
L    10.68.0.65/32 is directly connected, GigabitEthernet0/1.30
C    10.68.0.96/27 is directly connected, GigabitEthernet0/1.40
L    10.68.0.97/32 is directly connected, GigabitEthernet0/1.40
O    10.68.0.128/25 [110/15065] via 10.0.10.10, 02:54:02, Serial0/0/1
O    10.68.1.0/26 [110/65] via 10.0.10.10, 02:54:02, Serial0/0/1
O    10.68.1.64/27 [110/7565] via 10.0.10.10, 02:54:02, Serial0/0/1
209.165.202.0/27 is subnetted, 1 subnets
O    209.165.202.0/27 [110/7564] via 10.0.10.10, 02:54:02, Serial0/0/1
S*  0.0.0.0/0 [1/0] via 209.165.202.1

```

## Таблиця маршрутизації на Gudakov\_R0

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default, U - per-user static route, o - ODR  
 P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O    10.0.10.0/30 [110/15064] via 209.165.202.2, 03:54:58, Serial0/1/0
O    10.0.10.4/30 [110/7564] via 209.165.202.2, 03:54:58, Serial0/1/0
O    10.0.10.8/30 [110/7564] via 209.165.202.2, 02:54:50, Serial0/1/0
O    10.68.0.0/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O    10.68.0.32/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O    10.68.0.64/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O    10.68.0.96/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O    10.68.0.128/25 [110/15065] via 209.165.202.2, 03:54:58, Serial0/1/0
O    10.68.1.0/26 [110/65] via 209.165.202.2, 03:54:58, Serial0/1/0
O    10.68.1.64/27 [110/7565] via 209.165.202.2, 03:54:58, Serial0/1/0
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/27 is directly connected, GigabitEthernet0/0
L    209.165.200.1/32 is directly connected, GigabitEthernet0/0
209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.202.0/27 is directly connected, Serial0/1/0
L    209.165.202.1/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 209.165.202.2, 03:54:58, Serial0/1/0

```

**ВІДГУКИ КОНСУЛЬТАНТІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ**