МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ЕЛЕКТРОНІКИ, РОБОТОТЕХНІКИ І ТЕХНОЛОГІЙ
МОНІТОРИНГУ ТА ІНТЕРНЕТУ РЕЧЕЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Шутко В.М.
«____»_____ 2020 р.

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА
ЗІ СПЕЦІАЛЬНОСТІ 153 «МІКРО- ТА НАНОСИСТЕМНА ТЕХНІКА»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ФІЗИЧНА ТА БІОМЕДИЧНА ЕЛЕКТРОНІКА»

Тема: «Система моніторингу комплексом аграрного призначення на базі інтернету речей»

Виконавець
студент групи МН-206М _____ Борсук Андрій Олегович

Керівник
д.т.н., доцент _____ Мельник Олександр Степанович

Консультант розділу
«Охорона праці» _____ Якимець І.В.

Консультант розділу
«Охорона навколишнього середовища» _____ Маджд С.М.

Нормоконтролер _____ Сініцин Р.Б.

КИЇВ 2020
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра електроніки, робототехніки і технологій моніторингу та інтернету речей
Освітньо-кваліфікаційний рівень Магістр
Напрям (спеціальність) 153 «МІКРО- ТА НАНОСИСТЕМНА ТЕХНІКА»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«ФІЗИЧНА ТА БІОМЕДИЧНА ЕЛЕКТРОНІКА»»

ЗАТВЕРДЖУЮ
Завідувач випускової кафедри
_____Шутко В.М.
«____»_____ 2020 р.

ЗАВДАННЯ
на виконання дипломного проекту (роботи) студента
Борсук Андрій Олегович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): «Система моніторингу комплексом аграрного призначення на базі інтернету речей» затверджена наказом ректора від «02» жовтня 2020 р. № 1900 / ст

2.Термін виконання проекту (роботи): 05.10.2020 по 27.12.2020

3.Вихідні дані: Структурна та функціональна схема проектованої системи моніторингу комплексом аграрного призначення на базі Інтернету речей.

4.Зміст пояснювальної записки (перелік питань, що підлягають обробці):
Аналіз технологій Інтернету речей
Огляд і аналіз існуючих рішень
Аналіз вузлів проектованої системи
Проектування системи безпеки
Розробка інфраструктури і програмного забезпечення

5.Перелік обов'язкового графічного матеріалу: таблиці, рисунки, графіки.

6.Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Робота над вступом	5.10.2020 р. – 10.10.2020 р.	Виконано
2.	Робота над розділом 1	10.10.2020 р. – 25.10.2020 р.	Виконано
3.	Робота над розділом 2	25.10.2020 р. – 10.11.2020 р.	Виконано
4.	Робота над розділом 3	10.11.2020 р. – 12.12.2020 р.	Виконано
5.	Робота над розділом 4 та 5	12.12.2020 р. – 16.12.2020 р.	Виконано
6.	Оформлення пояснювальної записки та презентації.	16.12.2020 р. – 20.12.2020 р.	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	Асистент кафедри ЦПБ, Якимець І.В.		
Охорона навколишнього середовища	Д.т.н., професор, доцент Мадж С.М.		

8.Дата видачі завдання: “_____”_____ 2020 р.

Керівник дипломної роботи (проекту) _____ Мельник О. С.

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Борсук А. О.

(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Магістерська дипломна робота: Система моніторингу комплексом аграрного призначення на базі Інтернету речей включає: 121 стор., 36 рис., 11 табл., 32 літературних джерела.

Метою роботи є дослідження методів та засобів побудови системи моніторингу комплексом аграрного призначення на базі Інтернету речей.

Об'єкт дослідження – технологія Інтернет речей.

Під час виконання роботи використовувались теоретичні методи досліджень із застосуванням апарату термодинаміки, фізики твердого тіла, електроніки, теорії ймовірності, математичної статистики, похибок.

У роботі:

1) Запропоновано комплексне рішення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.

2) Розроблені моделі використання системи комплексного моніторингу приміщень за допомогою технології Інтернет речей.

Результатом роботи є модель системи комплексного моніторингу приміщень за допомогою технології Інтернет речей. Модель зроблена щоб максимально знизити витрати на монтаж системи. Щодо моделі сучасної інтелектуальної системи комплексного моніторингу приміщень за допомогою технології Інтернет речей, то вона зроблена так, щоб за потребою у неї можна було вносити необхідні зміни не перериваючи її роботу та не припиняючи її.

Результати дослідження можуть бути впроваджені у рамках реального приміщення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.

Інтернет речей, моніторинг, комплекс аграрного призначення, технологія, модель.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

АВР	автомат введення резерву
ВРП	ввідно– розподільний пристрій
ДБЖ	джерело безперебійного живлення
ЕОМ	електроно обчислювальна машина
ІЧ– приймач	інфрачервоний приймач
ЛОМ	локально– обчислювальні мережі
ЦОД	центр обробки данних
ПАЗ	перетворювач амплітудних значень
ПК	персональний комп’ютер
Пульт ДУ	пульт дистанційного управління
СКС	структуровані кабельні системи
ФНЧ	фільтр низьких частот
ETS	Engineering Tool Software/Інструментальний програмний пакет для інженерного забезпечення.
Рлл	потужність люмінесцентних ламп
Рсд	потужність світлодіодних ламп
Р	питома усталена потужність штучного освітлення;
F	площа приміщення;
Т	річна кількість робочих годин джерел світла
k	кратність обміну повітря
KNX	відкритий уніфікований шинний протокол

ВСТУП

Актуальність теми. Інтернет речей (IoT - Internet of Things) є сучасною концепцією, що має на меті об'єднання об'єктів, «речей», в єдину всесвітню мережу, яка дозволяє речам бути розумними для взаємодії як з один з одним, так і з людиною в будь-який час і в будь-якому місці. На сьогоднішній день число пристроїв, підключених до мережі, перевищує число всіх жителів планети і продовжує стрімко збільшуватися, що піднімає питання про присвоєння кожному об'єкту унікальної адреси, забезпечення конфіденційності і безпеки при передачі даних. Незважаючи на це, до цих пір немає загальноприйнятого методу ідентифікації речей, який би задовольняв всім вимогам як для існуючих пристроїв і додатків Інтернету речей, так і для знову створюваних.

Ідентифікатор це виділений, публічно відомий атрибут або ім'я (або набір атрибутів та імен) для окремого пристрою. Як правило, ідентифікатори діють в межах певної області або мережі, що ускладнює ідентифікацію речей в глобальному масштабі. Зважаючи на складність і високу продуктивність сучасних пристроїв Інтернету речей вони можуть мати більше одного ідентифікатора. У той же час, існують різні методи ідентифікації, які не можуть використовуватися багатьма пристроями Інтернету речей з різних причин. Сучасні методи анонімізації і величезне число пристроїв Інтернету речей, підключених до мереж зв'язку загального користування, роблять сучасні мережі і системи зв'язку уразливими перед зловмисниками. Уразливість мережевої безпеки, що полягає в неможливості аутентифікації пристроїв Інтернету речей, відкриває для зловмисників можливість для виробництва фізичних і віртуальних речей.

Одним з напрямків забезпечення гарантованої і однозначної ідентифікації пристроїв Інтернету речей (IP) є використання унікального ідентифікатора пристрою IP в сукупності з параметрами самого пристрою. При цьому треба враховувати, що так званий універсальний ідентифікатор

повинен підтримувати (бути сумісний) з уже існуючими методами ідентифікації, такими як IMEI, MAC і інші.

Необхідно також відзначити, що від рівня до рівня ідентифікація пристроїв може підмінятися, тобто кінцевому пристрою інтернету речей з певною фізичною адресою на канальному рівні спочатку призначається відповідна логічна адреса на мережевому рівні, яка в подальшому може бути замінена на ідентифікатор на рівні платформи. При цьому дуже важливою властивістю є фіксованість співвідношення ідентифікатора з фактичним улаштуванням Інтернету речей (фізичною адресою), а також універсальність в застосуванні ідентифікатора в різних галузях.

Мета і завдання дослідження. Метою роботи є дослідження методів та засобів побудови системи моніторингу комплексом аграрного призначення на базі Інтернету речей.

Для досягнення поставленої мети вирішуються наступні задачі:

- описати призначення і область застосування;
- навести технічні характеристики;
- провести огляд існуючих рішень і обґрунтування вибору структури системи моніторингу комплексом аграрного призначення на базі Інтернету речей;
- розробити та описати структурну та функціональну схеми проектованої системи моніторингу комплексом аграрного призначення на базі Інтернету речей;
- здійснити вибір і обґрунтування окремих вузлів;
- розробити і описати принципову схему та алгоритм керуючої програми;
- дослідити систему моніторингу комплексом аграрного призначення на базі Інтернету речей.

Об'єкт дослідження – технологія Інтернет речей.

Предмет дослідження – розробка системи моніторингу комплексом аграрного призначення на базі Інтернету речей.

Методи дослідження. Під час виконання роботи використовувались теоретичні методи досліджень із застосуванням апарату термодинаміки, фізики твердого тіла, електроніки, теорії ймовірності, математичної статистики, похибок.

Наукова новизна отриманих результатів.

1) Запропоновано комплексне рішення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.

2) Розроблені моделі використання системи комплексного моніторингу приміщень за допомогою технології Інтернет речей.

Практичне значення отриманих результатів. Результати дослідження можуть бути впроваджені у рамках реального приміщення для комплексного моніторингу приміщень за допомогою технології Інтернет речей.

Структура роботи. Дана робота складається зі вступу, трьох розділів, висновків, переліку використаної літератури, що включає в себе 36 літературних джерела. Загальний обсяг роботи становить 135 сторінок.

РОЗДІЛ 1
ІНТЕРНЕТ РЕЧЕЙ ДЛЯ ФОРМУВАННЯ СИСТЕМИ МОНІТОРИНГУ КОМПЛЕКСОМ АГРАРНОГО ПРИЗНАЧЕННЯ

1.1 Сутність Інтернету речей

Інтернет речей (Internet of Things, IoT) – це концепція і парадигма, яка розглядає повсюдно присутність різних фізичних об'єктів («речей») в навколишньому середовищі. Термін «Інтернет речей» визначено як динамічну глобальну мережеву інфраструктуру з можливістю самонастроювання на основі стандартних і сумісних протоколів зв'язку, де фізичні та віртуальні «речі» мають ідентифікатори, фізичні атрибути, використовують інтелектуальні інтерфейси і інтегруються в інформаційну мережу [1].

Протягом останнього десятиліття Інтернет речей проникав в наше життя тихо і поступово, перш за все завдяки наявності систем бездротового зв'язку (наприклад, RFID, Wi-Fi, 4G, IEEE 802.15.x), які все частіше використовуються в якості рушійної сили для розвитку технології інтелектуального контролю та управління додатками [2]. Концепція IoT включає в себе безліч різних технологій, послуг, стандартів і сприймається як наріжний камінь на ринку інформаційно-комунікаційних технологій (ІКТ) принаймні на найближчі десять років. З логічної точки зору, система IoT може бути представлена як сукупність спільно взаємодіючих інтелектуальних пристроїв. З технічної точки зору, IoT може використовувати різні шляхи обробки даних, комунікації, технології та методології, ґрунтуючись на їх цільовому призначенны. Наприклад, система IoT може скористатися наявними можливостями бездротової сенсорної мережі (WSN), яка збирає екологічно значиму інформацію про навколишнє середовище [3]. Високий рівень неоднорідності в поєднанні з широкою гамою систем IoT, як очікується, збільшить число загроз безпеки власників пристроїв, які все частіше використовуються для взаємодії людей, машин і речей в будь-який варіації.

Традиційні заходи забезпечення безпеки і дотримання конфіденційності не можуть бути застосовані до технологій IoT, зокрема, через їх обмежену обчислювальну потужність. Крім того, велика кількість підключених пристроїв породжує проблему масштабованості. У той же час для досягнення визнання з боку користувачів необхідно в обов'язковому порядку забезпечити дотримання безпеки, конфіденційність і модель довіри, які підходять для контексту IoT [4-6].

Для запобігання несанкціонованого доступу користувачів (тобто людей і пристроїв) до системи повинні використовуватися механізми аутентифікації і авторизації, гарантована безпека, конфіденційність і цілісність персональних даних. Щодо персональних даних користувачів і інформації повинні забезпечуватися захист і конфіденційність, перш за все тому, що пристрої мають до неї доступ і здатні управляти нею (наприклад, відомості про звички користувачів). Нарешті, довіра (надійність, англ. Trust) – це основна проблема, оскільки IoT-середовище характеризується різними типами пристроїв, які повинні обробляти дані відповідно до потреб і прав користувачів.

Звернемо увагу, що адаптація і самовідновлення грають ключову роль в IoT інфраструктурах, які повинні бути в змозі протистояти несподіваним змінам у навколишньому середовищі. Відповідно, до питань конфіденційності та безпеки слід ставитися з високим ступенем гнучкості. Поряд з традиційними рішеннями для забезпечення безпеки необхідне використання спеціальних механізмів, вбудованих в самі пристрої з метою оперативної діагностики, ізоляції та профілактики порушень [7].

Що стосується аутентифікації, підхід, представлений в [8], передбачає використання механізму інкапсуляції, який настроюється користувачем, а саме протокол прикладного рівня для IoT під назвою – «інтелектуальна служба забезпечення безпеки» (англ. Intelligent Service Security Application Protocol). Він поєднує в собі крос-платформні зв'язки з шифруванням, підписом і аутентифікацією для підвищення ефективності розробки додатків IoT шляхом створення системи захищеного зв'язку між різними речами.

В роботі [9] представлена перша повністю реалізована двостороння схема перевірки справжності для IoT на основі існуючих стандартів, зокрема, протокол датаграм безпеки транспортного рівня (англ. Datagram Transport Layer Security, DTLS), який розташовується між транспортним і прикладним рівнями. Ця схема заснована на криптографічному алгоритмі RSA і призначена для IPv6 з використанням стандарту 6LoWPANs (англ. IPv6 over Low power Wireless Personal Area Networks) [10]. Аналіз результатів, заснованих на реальних системах IoT, показує, що така архітектура забезпечує цілісність повідомлення, конфіденційність, енергоефективність, низькі значення затримки пакетів і навантаження на пам'ять.

Щодо конфіденційності і цілісності в [11] наведено аналіз того, як існуючі системи управління ключами можуть бути застосовані в контексті IoT. Це дозволяє класифікувати протоколи систем управління ключами (англ. Key Management System, KMS) за чотирма основними категоріями: структура пулу ключів, математична база, механізм взаємодії і структура відкритого ключа. В роботі [12] автори стверджують, що більшість протоколів KMS не підходять для IoT. Однак протоколи KMS придатні для сценаріїв, в яких обчислювальні потужності є досить низькими в порівнянні з використанням криптографії з відкритим ключем (англ. Public Key Cryptography, PKC). Але для таких схем необхідне введення декількох контрзаходів для управління пристроєм аутентифікації і щоб уникнути MITM-атаки (англ. Man In The Middle).

Більш практичний підхід [13] пропонує модель передачі зі схемами шифрування підпису, в якій розглядаються вимоги безпеки IoT (тобто анонімність, надійність і стійкість до атак) за допомогою ONS-запитів (англ. Object Naming Service). Однак, з точки зору стійкості до атак, результати моделі передачі даних є дуже слабкими в зв'язку з використанням шифрування на базі «точка-точка» (англ. Hop-by-hop). Як і раніше відсутнє унікальне і чітко визначене рішення, яке може гарантувати конфіденційність в IoT. У цьому контексті багато зусиль було докладено для WSN (англ. WSN - Wireless Sensor Network) [14, 15].

В рамках WSN аутентифікація користувача і схема узгодження ключа для гетерогенних бездротових сенсорних мереж також запропонована, наприклад, в [17]. Це рішення дозволяє віддаленому користувачеві безпечно домовитися про сеансовий ключ з сенсорним вузлом за допомогою протоколу розподілу ключів. Таким чином, він забезпечує взаємну аутентифікацію між користувачами, сенсорними вузлами і шлюзовими вузлами (англ. Gate way node, GWN). Для того щоб застосувати таку схему для архітектури з обмеженими ресурсами, використовуються тільки прості хеш і XOR обчислення.

Метод перевірки автентичності і контроль доступу, представлений в [18], спрямований на створення ключа сеансу із застосуванням еліптичної криптографії (англ. Elliptic Curve Cryptography, ECC). Крім того, запропонований механізм захисту даних в хмарних сховищах, заснований на поєднанні «класичної» проблеми Діффі-Хеллмана і проблеми дискретного логарифмування в групі точок еліптичної кривої. Відзначається, що протокол, заснований на еліптичних кривих, має невеликий розмір ключа без шкоди криптостійкості, що робить еліптичну криптографію привабливою для використання в тих областях, де існують проблеми з-за обмеження пам'яті і обчислювальних потужностей.

Управління доступом відноситься до дозволів в галузі використання ресурсів, призначених для різних суб'єктів в мережі IoT. В [19] визначені два суб'єкти: власники даних і збирачі даних. Користувачі і речі, як власники даних, повинні дозволяти передавати тільки відомості, які необхідні для виконання конкретного завдання. У той же час збирачі даних повинні вміти ідентифікувати або підтвердити справжність (аутентифікувати) користувачів речей як законних власників даних, від яких вона збирається.

У IoT мають справу з обробкою потокових, а не дискретних даних, як в традиційних системах. Основні проблеми в цьому контексті відносяться до продуктивності і тимчасових обмежень. Зокрема, потік даних інтенсивніше,

ніж в традиційних системах управління базами даних (СУБД). Кілька робіт присвячено цим аспектам.

В [20] увага зосереджена на рівні, відповідальному за отримання і зберігання інформації. Велика кількість вузлів авторизованих користувачів використовує широкий спектр різних типів даних відповідних рівнях конфіденційності та безпеки. Тому в роботі представлена ієрархічна схема управління доступом для цього рівня. Схема враховує обмежену обчислювальну потужність і ємність пристрою зберігання. Кожному користувачеві і / або вузла дається тільки один ключ; інші необхідні ключі отримані за допомогою детермінованого алгоритму деривації ключа (англ. deterministic key derivation algorithm), підвищуючи рівень безпеки (так як обмін ключів обмежений) і скорочуючи витрати на зберігання для безлічі вузлів.

Інтернет речей концептуально належить до мереж наступного покоління, тому його архітектура багато в чому схожа з відомою чотиришаровою архітектурою NGN. IoT складається з набору різних інфокомунікаційних технологій, що забезпечують функціонування Інтернету речей, і його архітектура показує, як ці технології пов'язані один з одним.

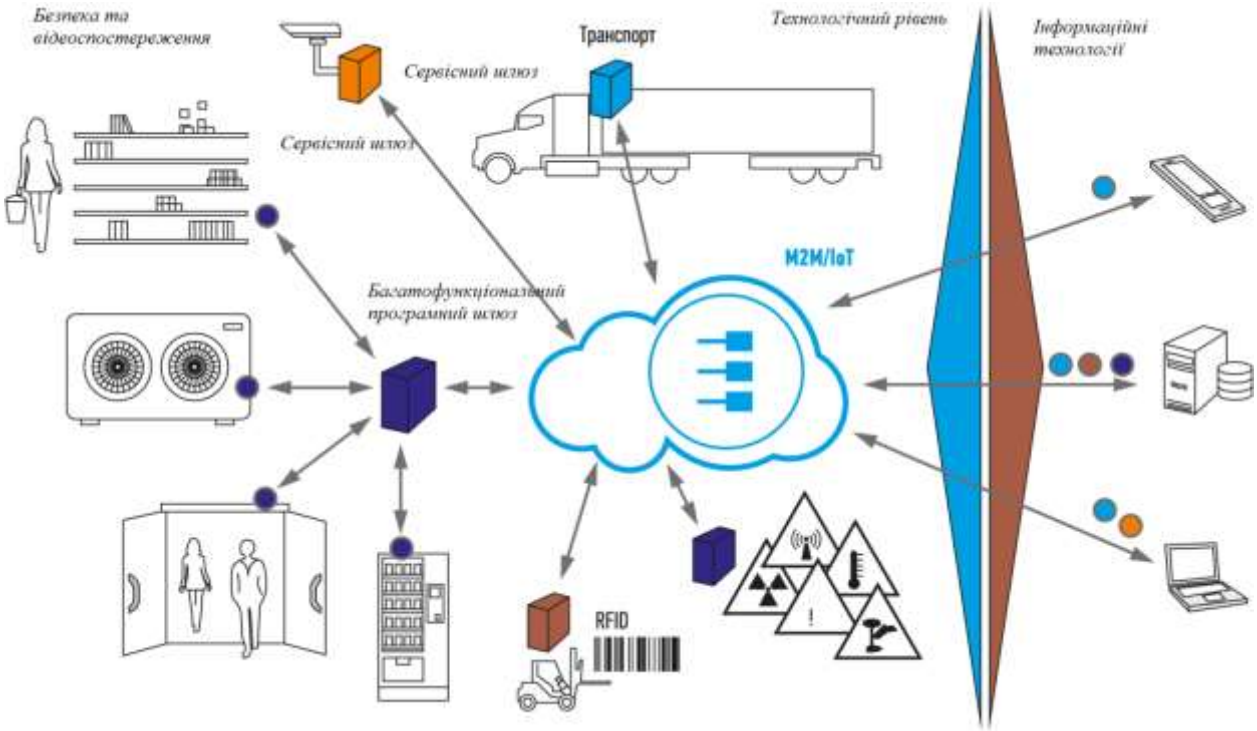


Рис. 1.1 Архітектура IoT

Архітектура IoT включає чотири функціональних рівня (рис. 1.1), описаних нижче.

1. Рівень сенсорів та сенсорних мереж.

Самий нижній рівень архітектури IoT складається з «розумних» (smart) об'єктів, інтегрованих з сенсорами (датчиками). Сенсори реалізують з'єднання фізичного та віртуального (цифрового) світів, забезпечуючи збір і обробку інформації в реальному масштабі часу. Мініатюризація, яка призвела до скорочення фізичних розмірів апаратних сенсорів, дозволила інтегрувати їх безпосередньо в об'єкти фізичного світу. Існують різні типи сенсорів для відповідних цілей, наприклад, для вимірювання температури, тиску, швидкості руху, місця розташування та ін. Сенсори можуть мати невелику пам'ять, даючи можливість записувати деяку кількість результатів вимірювань. Сенсор може вимірювати фізичні параметри контрольованого об'єкта/явища і перетворити їх в сигнал, який може бути прийнятий відповідним пристроєм. Сенсори класифікуються згідно з їх призначенням, наприклад, сенсори навколишнього середовища, сенсори для тіла, сенсори для побутової техніки, сенсори для транспортних засобів і т. д.

Більшість сенсорів потребує з'єднання з агрегатором сенсорів (шлюзом), які можуть бути реалізовані з використанням локальної обчислювальної мережі (LAN, Local Area Network), таких як Ethernet і Wi-Fi або персональної мережі (PAN, Personal Area Network), таких як ZigBee, Bluetooth і ультраширокополосного бездротового зв'язку на малих відстанях (UWB, Ultra-Wide Band). Для сенсорів, які не вимагають підключення до агрегатору, їх зв'язок з серверами/додатками може надаватися використанням глобальних бездротових мереж WAN, таких як GSM, GPRS і LTE.

Сенсори, які характеризуються низьким енергоспоживанням і низькою швидкістю передачі даних, утворюють широко відомі бездротові сенсорні мережі (WSN, Wireless Sensor Network). WSN набирають все більшу

популярність, оскільки вони можуть містити набагато більше сенсорів з підтримкою роботи від батарей і охоплюють великі площі.

2. Рівень шлюзів і мереж.

Великий обсяг даних, створюваних на першому рівні IoT численними мініатюрними сенсорами, вимагає надійної і високопродуктивної провідної або бездротової мережевої інфраструктури в якості транспортного середовища. Існуючі мережі зв'язку, що використовують різні протоколи, можуть бути використані для підтримки міжмашиних комунікацій M2M та їх додатків. Для реалізації широкого спектру послуг і додатків в IoT необхідно забезпечити спільну роботу безлічі мереж різних технологій і протоколів доступу в гетерогенній конфігурації. Ці мережі повинні забезпечувати необхідні значення якості передачі інформації, і перш за все по затримці, пропускної спроможності та безпеки. Цей рівень складається з конвергентної мережевої інфраструктури, яка створюється шляхом інтеграції різнорідних мереж в єдину мережеву платформу. Конвергентний абстрактний мережевий рівень у IoT дозволяє через відповідні шлюзи декільком користувачам використовувати ресурси в одній мережі незалежно і спільно без шкоди для конфіденційності, безпеки і продуктивності.

3. Сервісний рівень

Сервісний рівень містить набір інформаційних послуг, спрямованих автоматизувати технологічні і бізнес-операції в IoT: підтримки операційної та бізнес діяльності (OSS/BSS, Operation Support System/Business Support System), різної аналітичної обробки інформації (статистичної, інтелектуального аналізу даних і текстів, прогностична аналітика та ін), зберігання даних, забезпечення інформаційної безпеки, управління бізнес-правилами (BRM, Business Rule Management), управління бізнес-процесами (BPM, Business Process Management) і ін.

4. Рівень додатків

На четвертому рівні архітектури IoT існують різні типи додатків для відповідних промислових секторів і сфер діяльності (енергетика, транспорт,

торгівля, медицина, освіта та ін.). Додатки можуть бути «вертикальними», коли вони є специфічними для конкретної галузі промисловості, а також «горизонтальними», (наприклад, управління автопарком, відстеження активів та ін), які можуть використовуватися в різних секторах економіки.

Існують кілька еталонних архітектур і моделей і для M2M і IoT систем. Розглянемо архітектуру ETSI M2M високого рівня.

Архітектура високого рівня (рис.1.2) є комбінацією функціонального і топологічного огляду, який показує деякі функціональні групи, пов'язані з частинами фізичної інфраструктури (наприклад, пристроїв M2M, шлюзи) в той час як інші функціональні групи не мають конкретного топологічного розміщення. Основними елементами архітектури M2M систем є мережевий домен і домен пристроїв і шлюзів.

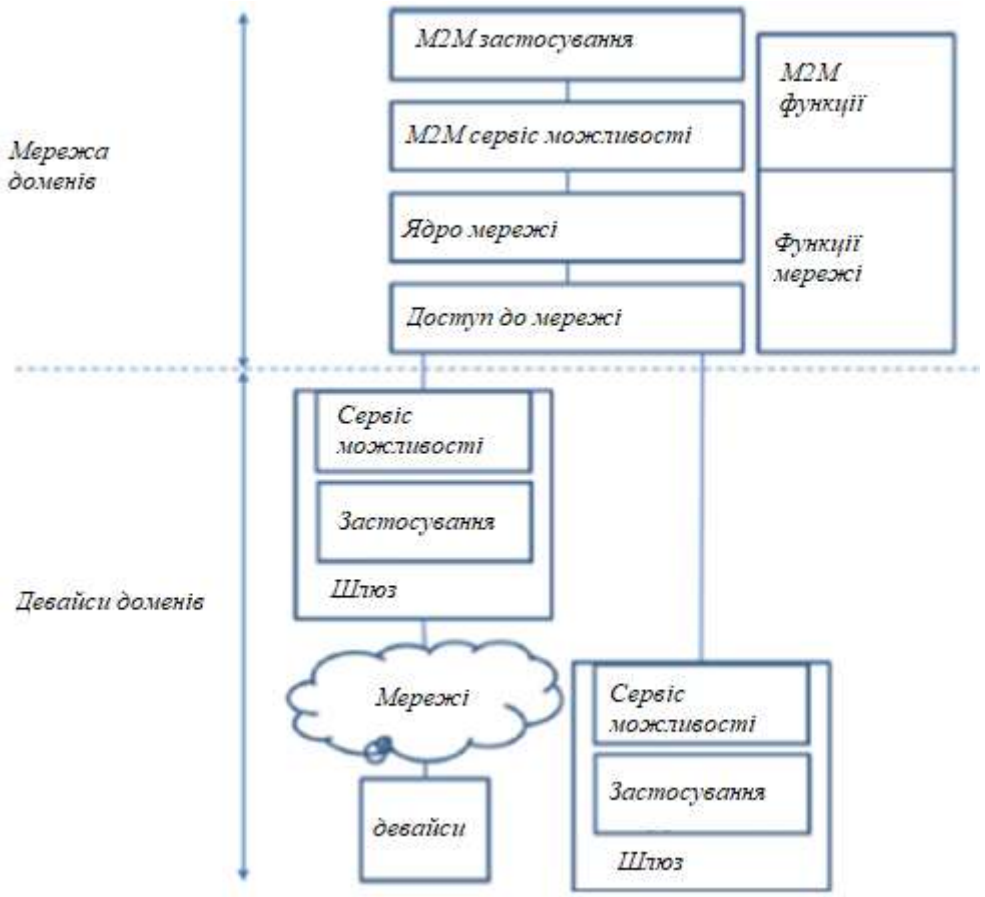


Рис. 1.2 Архітектура ETSI M2M високого рівня

Крім зазначених доменів до складу мережі M2M входять відповідна мережа доступу і транспортна мережа, які будуються на основі мереж 3GPP і NGN мереж.

Мережі доступу (Access Network) дозволяють домену пристроїв M2M забезпечувати з'єднання з ядром мережі M2M (базовою мережею). Функціональні можливості мереж доступу M2M базуються на можливостях існуючих мереж доступу (xDSL, HFC, PLC, VSAT, GERAN, UTRAN, LTE, W-LAN і WiMAX) та дозволяють розширити як перелік послуг, так і їх можливості.

Транспортна мережа (Core Network) забезпечує транспортування даних між мережевим доменом і доменом додатків. Функціональні можливості трасування мереж в мережах M2M базуються на можливостях існуючих мереж трасування і так само, як мережі доступу, дозволяють розширити перелік послуг M2M і їх можливості.

Базова мережа M2M (M2M Service Capabilities) надає функціональні можливості IP-з'єднання елементів мережі M2M, сервісні та мережеві функції управління, між мережеву взаємодію, роумінг та забезпечує безпеку мережі. Функціональні можливості базової мережі M2M ґрунтуються на відповідних функціональних можливостях існуючих базових мереж 3GPP CN (наприклад, GPRS, EPC), ETSI TISPAN CN.

Пристрої M2M (M2M Device) дозволяють швидко скористатися послугами M2M і функціями доменної мережі. Пристрій M2M може бути пов'язаний з мережею доступу або безпосередньо, або через локальну мережу M2M і шлюз M2M.

Локальні мережі M2M (M2M Area Network) надають з'єднання між пристроями M2M і шлюзами M2M з використанням PAN-технологій (IEEE 802.15, SRD, UWB, Zigbee, Bluetooth) або локальних мереж (PLC, M-BUS, Wireless M-BUS).

Шлюзи M2M (M2M Gateway) забезпечують пристроям M2M гарантовану міжмережеву взаємодію і підключення до мережі і прикладних

доменів. Шлюз M2M може використовуватися для різних додатків пристроїв M2M. Функціонально шлюз M2M може бути об'єднаний в одному модулі с пристроєм або групою пристроїв M2M.

Функціональні можливості мережі M2M можуть бути як спеціальними, що підтримують додатки M2M, так і загальними, що підтримують загальномережеві можливості: збір та агрегацію даних, доставку багато адресних повідомлень і ін.

Однак є фактори, здатні уповільнити розвиток Інтернету речей. Одним з найважливіших вважається відсутність прийняття загальних стандартів. У структурі головного європейського органу зі стандартизації в області телекомунікацій – Європейського інституту стандартизації електрозв'язку (ETSI) в 2009 році був створений технічний комітет ТК M2M. За час роботи ТК M2M / ETSI була розроблена нормативно-технологічна база, що включає кілька технічних звітів і стандартів ETSI, які визначили вимоги до функціональної архітектури мереж M2M, пристроїв, інтерфейсів і основних бізнес-моделей послуг M2M.

В рамках діяльності Комітету з електронних комунікацій ECC / CEPT адміністрацій зв'язку країн Європи прийнято ряд рішень і рекомендацій по використанню радіочастотного спектру для пристроїв M2M [3, 4].

1.2 Співставний аналіз систем моніторингу комплексом аграрного призначення

На сьогодні, на ринку програмного забезпечення представлено широкий асортимент програм для забезпечення моніторингу комплексів аграрного призначення.

AGS – система моніторингу комплексом аграрного призначення

Функціональні можливості системи:

- моніторинг роботи сільгосптехніки в режимі реального часу;

– контроль місцеположення транспорту і сільгосптехніки, їх напрямку і швидкості руху;

– контроль траєкторії розташування транспорту і сільськогосподарської техніки в режимі on-line. Відображення інформації на електронній карті в режимі реального часу;

– контроль за дотриманням технологічної швидкості агрегатів при проведенні польових робіт;

– планування полів, збір інформації для складання паспорта поля, визначення чітких меж полів, вимірювання площі сільгоспугідь, картування врожайності (щільність врожаю та ін.);

– розрахунок маршрутів, планування розкладу робіт і контроль його виконання. Виявлення несанкціонованих простоїв техніки з вини працівників;

– облік кількості рейсів, пройденого кілометражу, робочого часу автомобілів і спецтехніки. Виявлення «приписок» в дорожніх листах;

– контроль знаходження об'єкта в межах позначеної ділянки (поля), час входу / виходу на об'єкт;

– контроль руху техніки по полю (якість обробки країв при посіві, обробці гербіцидами);

– планування і контроль дотримання маршруту руху: знаходження техніки в межах позначеного поля, проходження техніки перевозить зібраний урожай строго на місце розвантаження. Виявлення «лівих» рейсів;

– планування і контроль графіка роботи техніки на поле;

– виявлення несанкціонованих простоїв. Мінімізація простоїв техніки з вини працівників;

– отримання диспетчером або керівником тривожного повідомлення про відхилення від маршруту руху, графіка виконання робіт і інших позаштатних ситуаціях.

Диспетчер має можливість зі свого пульта управління дистанційно заблокувати двигун при виході техніки на інше поле або при спробі угону.

Забезпечення збереження вантажів, контроль прибуття автомобіля на об'єкт розвантаження, отримання інформації про точне місце вивантаження врожаю.

Cropio.

Система моніторингу Cropio спрямована на оптимізацію добрива і зрошення ґрунту і таким чином знижується кількість використовуваних добрив і води. Cropio, разом з інформацією про погоду і даними з супутника, також робить можливим моніторинг посівів і прогноз врожайності.

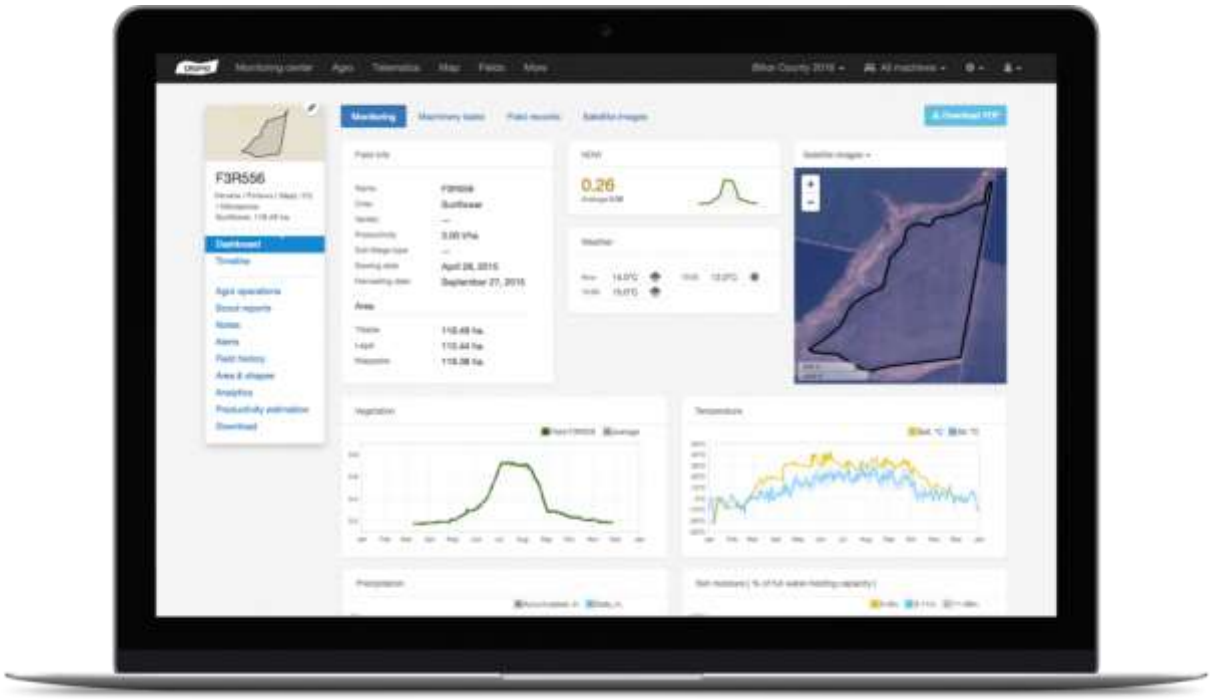


Рис. 1.3 Система дистанційного контролю сільськогосподарських угідь

Cropio – це система дистанційного контролю сільськогосподарських угідь, яка включає оперативний моніторинг стану посівних площ, автодокументування, прогнозування і планування сільськогосподарських операцій.

Система управління агропідприємством

Система веде облік активів, планування робіт, GPS-трекінг техніки, моніторинг вегетації – всі аспекти господарства зібрані в одному місці і доступні з будь-якого пристрою.

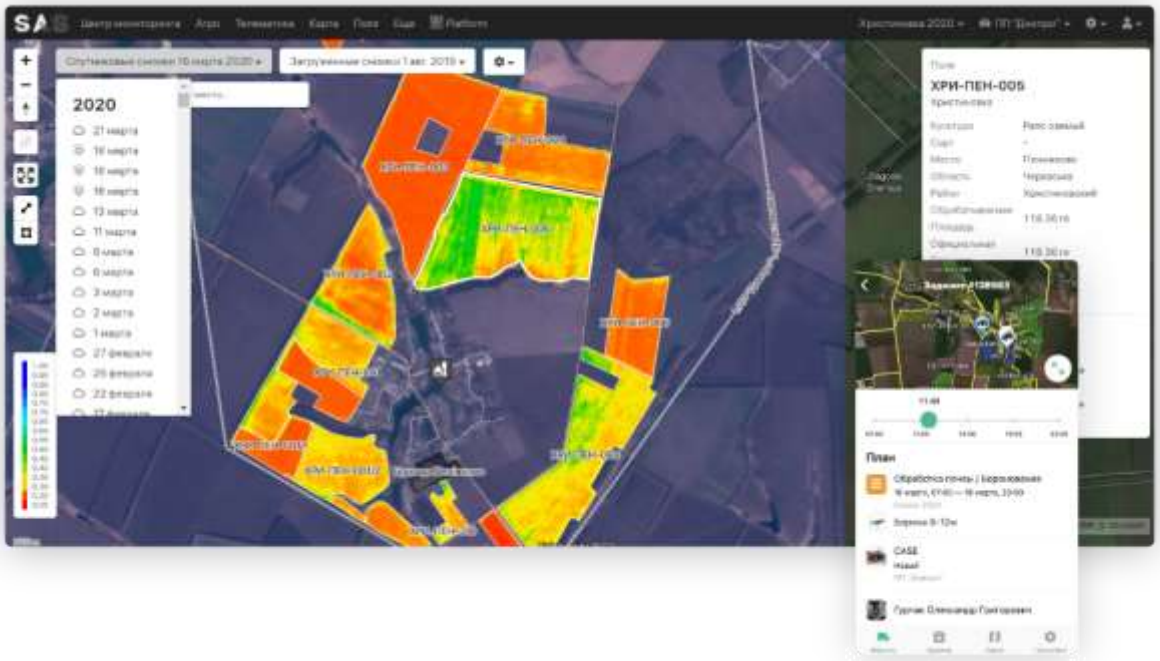


Рис. 1.4 Система управління агропідприємством

Система управління агропідприємством має можливість здійснювати та аналізувати супутникові знімки посівів, знаходити проблемні зони на полі. Програма дє прогноз врожайності культур, аналізчиую дані за поточний сезон та порівнюючи їх з минулим роком.

1.3 Технічне завдання на проект системи

Підприємство яке обрано за для впровадження системи моніторингу комплексом аграрного призначення на базі Інтернету речей, розробка якої передбачена у межах даної дипломної роботи, займається агропромисловим бізнесом. Структура підприємства наведена на рис. 1.5.

Компанія має у Києві три магазини та один склад з якого і відбувається перевезення вантажів у магазини за їхнім замовленням.

Компанія, яка займає 60.000 м^2 закритих площ вважається найбільшим виробництвом та пропонує рішення у галузі агропромислового виробництва.

Компанія, яка пропонує виключно якісну продукцію, приділяє велику увагу обслуговуванню клієнтів та розробляє проекти, які дають змогу бути лідером у своєму секторі. Компанія отримала багато нагород за якість, як на місцевому так і на міжнародному рівнях.

Компанія, яка в процесі досягнення своїх цілей орієнтується на політику розуміння потреб клієнта, поєднує в своїй роботі технологічну міць, динамічний розвиток своїх співробітників та постійний розвиток компанії, що дозволяє розробляти, впроваджувати та пропонувати рішення, які значною мірою полегшують життя людини.

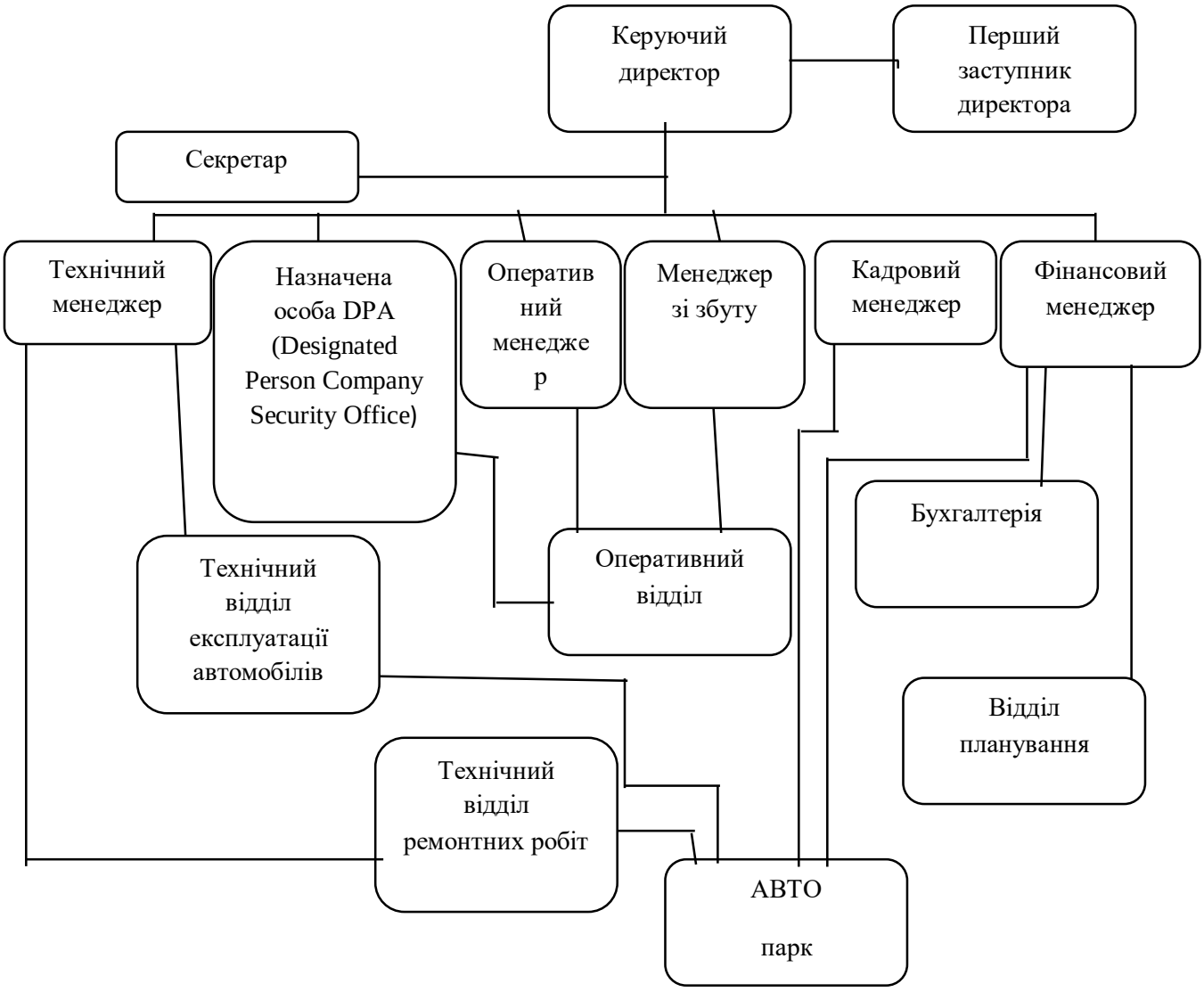


Рис. 1.5 Структура підприємства

Для розробки системи моніторингу комплексом аграрного призначення на базі Інтернету речей необхідно усвідомити функції і завдання які вирішує менеджер в процесі виконання функціональних обов'язків.

Менеджер, що формує вантажні перевезення відноситься до категорії технічних виконавців. Він повинен знати:

- Нормативні правові акти, методичні матеріали з питань виробничого планування і оперативного управління підприємства по вантажним перевезенням;
- Організацію виробничого планування на підприємстві по вантажним перевезенням;
- Виробничі потужності підприємства;
- Спеціалізацію підрозділів підприємства і виробничі зв'язки між ними;
- Види надання підприємством послуг;
- Організацію роботи сервісу по ремонту;
- Засоби обчислювальної техніки, комунікацій та зв'язку;
- Основи економіки, організації виробництва, праці та управління;
- Порядок оформлення та обробки шляхових листів;
- Положення та інструкції про порядок організації вантажних перевезень і оперативного управління процесом перевезень;
- Правила експлуатації автомобілів;
- Правила експлуатації застосовуваних технічних засобів обробки і передачі інформації;
- Правила і норми охорони праці, виробничої санітарії, техніки безпеки і протипожежного захисту[7].

Оператор підприємства відноситься до категорії технічних виконавців. На посаду оператора призначається особа, яка має середню професійну освіту без пред'явлення вимог до стажу роботи або професійно-технічну освіту і стаж роботи за фахом не менше 6 місяців. Призначення на посаду і звільнення з неї здійснюється наказом.

Оператор повинен знати:

Положення, інструкції, інші керівні матеріали і нормативні документи, що стосуються діяльності диспетчерської руху і вантажно-розвантажувальних робіт.

Статут автомобільного транспорту.

Порядок оформлення та обробки шляхових листів і товарно-транспортної документації.

Положення та інструкції про порядок організації перевезень і оперативного управління перевізним процесом на агропідприємстві.

Порядок виконання вантажно-розвантажувальних робіт на агропідприємстві.

Правила експлуатації автомобілів.

Правила експлуатації застосовуваних технічних засобів обробки і передачі інформації на агропідприємстві.

Основи організації праці на агропідприємстві.

Законодавство про працю.

Правила внутрішнього трудового розпорядку.

Правила і норми охорони праці, техніки безпеки, виробничої санітарії та протипожежного захисту.

На час відсутності оператора на агропідприємстві (хвороба, відпустка, ін.) Його обов'язки виконує особа, призначена наказом директора підприємства. Дана особа набуває відповідних прав і несе відповідальність за належне виконання покладених на нього обов'язків.

Оператор на агропідприємстві:

− вживає заходів щодо виконання плану перевезень, змінного завдання водіями автомобілів, навантажувачів, електро- і автовізків і ін.;

− виконує розпорядження диспетчера транспорту;

− заповнює, видає і приймає подорожні листи і товарно-транспортні накладні;

– перевіряє правильність їх оформлення, наявність реквізитів і штампів у товарно-транспортних накладних, позначок про здавання вантажу в повному обсязі;

– контролює дотримання графіків випуску на лінію та рух транспортних засобів на маршрутах, виконання замовлень на таксомотори;

– здійснює реєстрацію шляхової документації та облік роботи транспортних засобів;

– контролює правильність записів показань спідометра, одержання і залишків паливно-мастильних матеріалів (ПММ);

– виявляє в дорожніх листах записи про допущені водіями порушення правил дорожнього руху і доповідає про них керівництву;

– зіставляє отримані дані про роботу транспортних засобів зі змінно-добовими завданнями, виявляє відхилення і причини їх виникнення;

– контролює дотримання водіями (машиністами) транспортних засобів дорожньо-транспортної дисципліни, веде облік роботи транспортних засобів;

– здійснює оперативний зв'язок з клієнтурою, вантажно-розвантажувальними та лінійними диспетчерськими пунктами, автовокзалами, автостанціями та касами;

– сповіщає вантажоодержувачів про час прибуття вантажів на їхню адресу;

– збирає й обробляє інформацію, в тому числі з використанням комп'ютерної техніки, про наявність вантажів на об'єктах, пунктах навантаження і розвантаження;

– веде оперативний облік ходу перевізного процесу, виконання вантажно-розвантажувальних робіт;

– координує роботу вантажних транспортних засобів;

– здійснює контроль за рухом автобусів на лінії, якістю перевезень і обслуговування пасажирів;

– отримує і доводить до водіїв повідомлення про умови та особливості перевезень на маршрутах, стан доріг, особливості руху на окремих ділянках, а також зведення метеослужби та прогнози погоди;

– веде журнал оперативних розпоряджень.

Як випливає з вище описаного, на оператора покладено обов'язки ведення великої кількості паперової документації, частина якої складається з документів, які повторюється або не сильно змінюється змістовною частиною[8]. Крім того він повинен володіти оперативною і поточною інформацією, яка схильна до швидких змін.

У зв'язку з наведеними аргументами, робоче місце оператора потребує автоматизації. У першу чергу необхідна оптимізація витрат робочого часу при отриманні оперативної та поточної інформації, збільшення застосування без паперового ведення журналів і табелів, зменшення часу на оформлення шляхових листів.

Метою автоматизації є створення автоматизованої системи, що дозволяє моніторити комплекс аграрного призначення на базі інтернету речей. Впровадження програмного забезпечення, що дозволяє своєчасно отримувати інформацію про наявність та роботі транспортних засобів, вести зведену інформацію про формування замовлення та розподіл його між машинами, оперативний журнал з контролю за рухом по заданому маршруту.

Таким чином, програмний додаток (системи моніторингу комплексом аграрного призначення на базі інтернету речей), що проектується в рамках даної дипломної роботи, повинен забезпечувати вирішення наступних завдань:

– автоматично формувати і обробляти поточні планові листи роботи;

– формувати маршрути руху техніки;

– вести журнали обліку роботи сільськогосподарської техніки;

– пропонувати найбільш оптимальні варіанти розподілу праці.

Висновок до розділу

У межах першого розділу здійснено дослідження поняття «Інтернет речей», розкрито сутність та наведено аналіз систем моніторингу комплексом аграрного призначення.

Інтернет речей (Internet of Things, IoT) – це концепція і парадигма, яка розглядає повсюдно присутність різних фізичних об'єктів («речей») в навколишньому середовищі. Термін «Інтернет речей» визначено як динамічну глобальну мережеву інфраструктуру з можливістю самонастроювання на основі стандартних і сумісних протоколів зв'язку, де фізичні та віртуальні «речі» мають ідентифікатори, фізичні атрибути, використовують інтелектуальні інтерфейси і інтегруються в інформаційну мережу.

Для розробки системи моніторингу комплексом аграрного призначення на базі Інтернету речей необхідно усвідомити функції і завдання які вирішує менеджер в процесі виконання функціональних обов'язків.

РОЗДІЛ 2
АПАРАТНО-ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ МОНІТОРИНГУ КОМПЛЕКСОМ АГРАРНОГО ПРИЗНАЧЕННЯ

2.1 Цільове призначення системи моніторингу агрокомплексом на базі Інтернету речей

Завдання системи моніторингу комплексом аграрного призначення на базі Інтернету речей полягає у комплексному моніторингу роботи аграрного підприємства. Реалізація даного завдання полягає у виборі оптимально працездатної і недорогої конфігурації мережі здатної здійснювати повний моніторинг роботи підприємства.

Одним з варіантів такої організації локальної мережі є мережа на базі тонких клієнтів плюс бездротова мережа Wi-Fi плюс стандартна дротова мережа. Призначення у кожній частині локальної мережі наступні: Бездротова мережа призначена для вільного доступу до даних несекретного характеру, вона з'єднана з мережею на базі тонких клієнтів. Стандартна дротова мережа об'єднує користувачів, що працюють з секретною інформацією.

Розглянемо локальну мережу аграрного підприємства. На поверсі є п’ять кабінетів, обладнаних обчислювальною технікою, та два кабінети, є адміністративними - директора, заступників. У робочих кабінетах стоять робочі станції, які час від часу виходять з ладу. Для більшої надійності функціонування краще встановити мережу на базі тонких клієнтів. При цьому не треба буде встановлювати ПЗ на кожну РС, досить буде ПЗ сервера, спрощується обслуговування, підвищується надійність функціонування класів, знижується ризик псування устаткування. У кабінетах бажаного використання ВТ можна використовувати ноутбуки, налаштовані на роботу з Wi-Fi в бездротовій мережі. Адміністративний сегмент локальної мережі є дротовою мережею з усіма вимогами захисту, викладеними вище.

2.2 Проектування системи моніторингу комплексом аграрного призначення на базі Інтернету речей

Принципи організації доступу до сервісів мережі з Інтернет можуть бути реалізовані за п’ятьма варіантами, кожен з яких аналізується на предмет безпеки і можливості бути реалізованим.

При розгляді варіантів в якості прикладу візьмемо мережу, в якій потрібно опублікувати:

Корпоративний поштовий сервер (Web-mail).

Корпоративний термінальний сервер (RDP).

Extranet сервіс для контрагентів (Web-API).

Варіант 1. Плоска мережа

В даному варіанті всі вузли корпоративної мережі містяться в одній, загальній для всіх мережі («Внутрішня мережа»), в рамках якої комунікації між ними не обмежуються. Мережа підключена до Інтернет через прикордонний маршрутизатор / міжмережевий екран (далі - IFW).

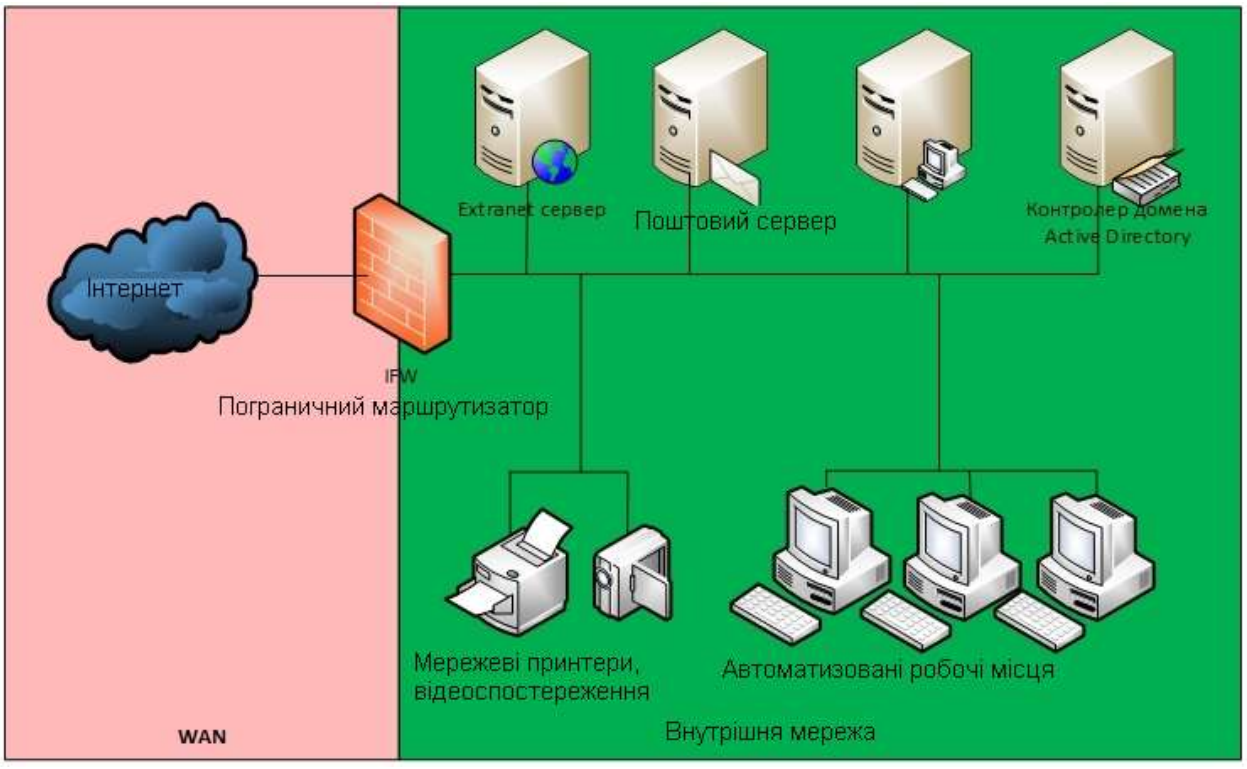


Рис. 2.1 Структура плоскої мережі

Доступ вузлів в Інтернет здійснюється через NAT, а доступ до сервісів з Інтернет через Port forwarding.

Переваги варіанту:

Мінімальні вимоги до функціоналу IFW (можна зробити практично на будь-якому, навіть домашньому роутері).

Мінімальні вимоги до знань спеціаліста, який здійснює реалізацію варіанту.

Недоліки варіанту:

Мінімальний рівень безпеки. У разі злому, при якому Порушник отримає контроль над одним з опублікованих в Інтернеті серверів, йому для подальшої атаки стають доступні всі інші вузли і канали зв'язку корпоративної мережі.

Аналогія з реальним життям

Подібну мережу можна порівняти з компанією, де персонал і клієнти знаходяться в одній загальній кімнаті (open space)

Рис. 2.2 Практичне застосування плоскої мережі

Варіант 2. DMZ

Для усунення зазначеної раніше нестачі вузли мережі, доступні з Інтернет, поміщають в спеціально виділений сегмент - демілітаризовану зону (DMZ). DMZ організовується за допомогою міжмережевих екранів, що відокремлюють її від Інтернет (IFW) і від внутрішньої мережі (DFW).

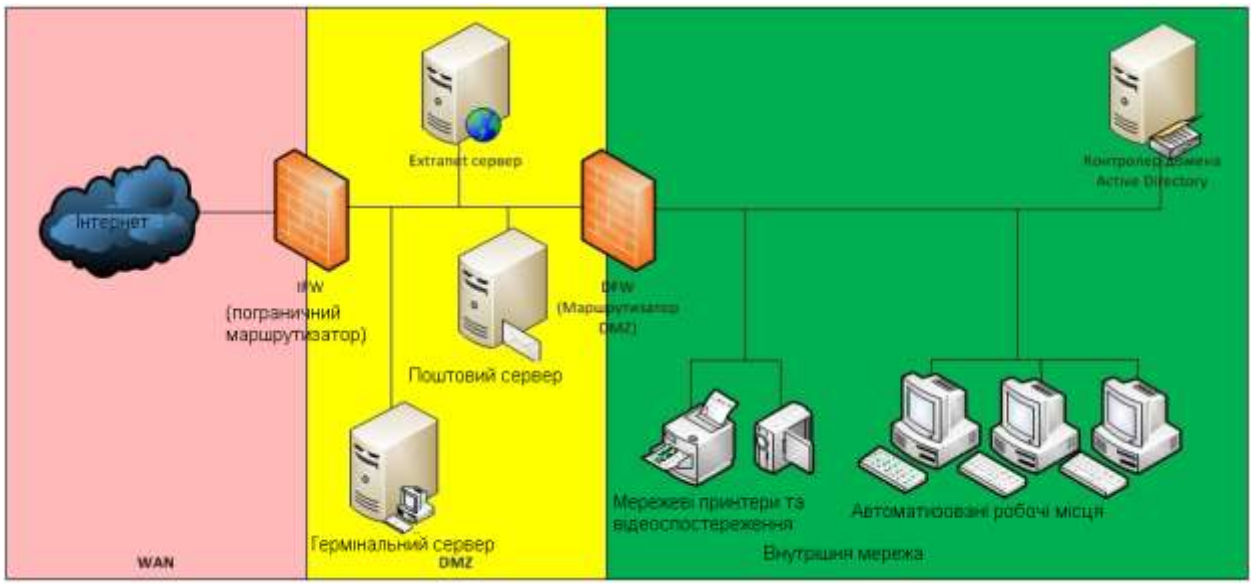


Рис. 2.3 Структура мережі DMZ

При цьому правила фільтрації міжмережевих екранів виглядають наступним чином:

З внутрішньої мережі можна ініціювати з'єднання в DMZ і в WAN (Wide Area Network).

З DMZ можна ініціювати з'єднання в WAN.

З WAN можна ініціювати з'єднання в DMZ.

Ініціація з'єднань з WAN і DMZ до внутрішньої мережі заборонена.

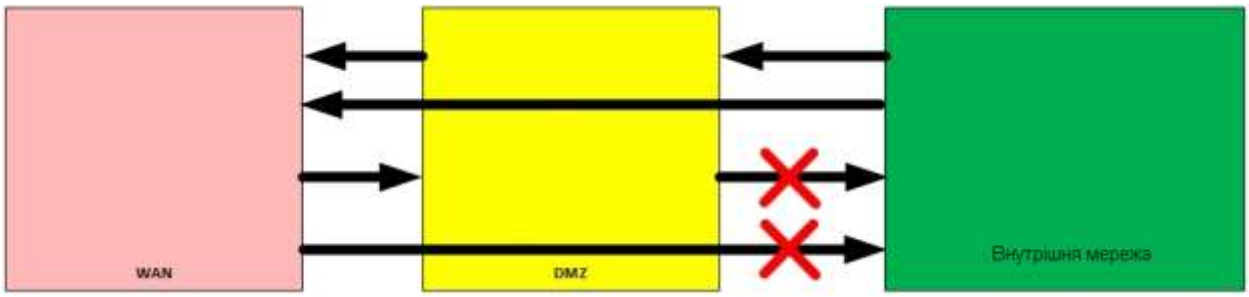


Рис. 2.4 Правила фільтрації міжмережевих екранів

Переваги варіанти:

Підвищена захищеність мережі від зломів окремих сервісів. Навіть якщо один з серверів буде зламаний, Порушник не зможе отримати доступ до ресурсів, що знаходяться у внутрішній мережі (наприклад, мережевих принтерів, систем відеоспостереження і т.д.).

Недоліки варіанту:

Саме по собі винесення серверів в DMZ не підвищує їх захищеність.

Необхідний додатковий МЕ для відділення DMZ від внутрішньої мережі.

Аналогія з реальним життям

Даний варіант архітектури мережі схожий на організацію робочої і клієнтської зон в компанії, де клієнти можуть перебувати тільки в клієнтській зоні, а персонал може бути як в клієнтській, так і в робочих зонах. DMZ сегмент - це якраз і є аналог клієнтської зони.

Рис. 2.5 Приклад реалізації сегменту мережі DMZ

Варіант 3. Поділ сервісів на Front-End і Back-End

Як вже зазначалося раніше, розміщення сервера в DMZ жодним чином не покращує безпеку самого сервісу. Одним з варіантів виправлення ситуації є поділ функціоналу сервісу на дві частини: Front-End і Back-End. При цьому кожна частина розташовується на окремому сервері, між якими організовується мережева взаємодія. Сервера Front-End, що реалізують функціонал взаємодії з клієнтами, що знаходяться в Інтернет, розміщують в DMZ, а сервера Back-End, що реалізують решті функціонал, залишають у внутрішній мережі. Для взаємодії між ними на DFW створюють правила, що дозволяють ініціацію підключень від Front-End до Back-End.

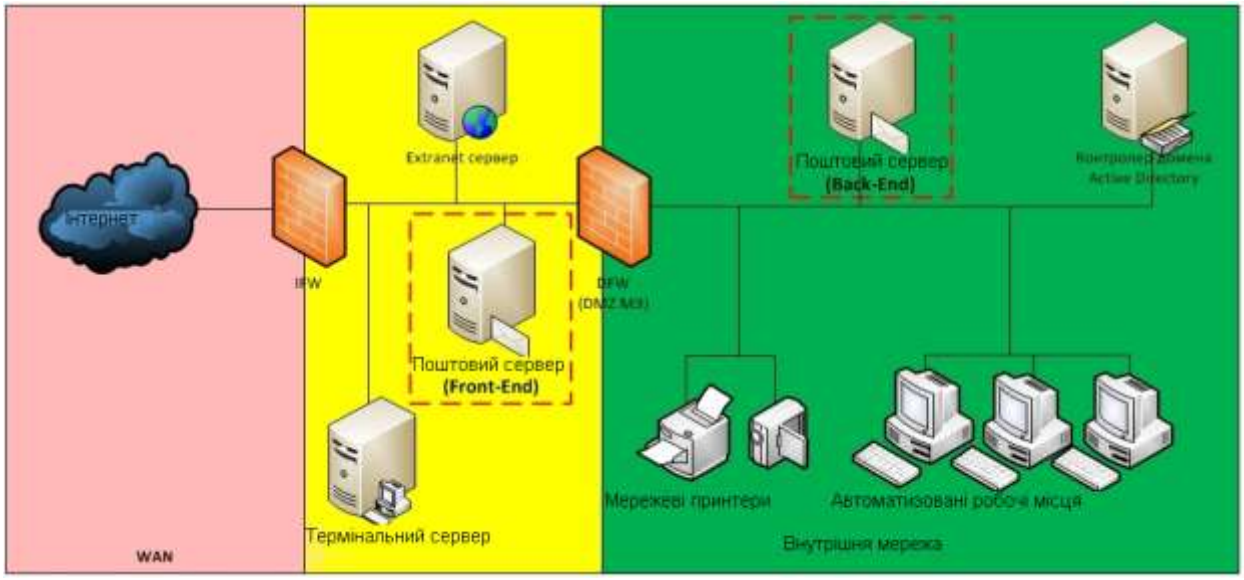


Рис. 2.6 Структура мережі поділу сервісів на Front-End і Back-End

Як приклад розглянемо корпоративний поштовий сервіс, який обслуговує клієнтів як зсередини мережі, так і з Інтернет. Клієнти зсередини використовують POP3 / SMTP, а клієнти з Інтернет працюють через Web-інтерфейс. Зазвичай на етапі впровадження компанії вибирають найбільш простий спосіб розгортання сервісу і ставлять всі його компоненти на один сервер. Потім, у міру усвідомлення необхідності забезпечення інформаційної безпеки, функціонал сервісу поділяють на частини, і та частина, що відповідає за обслуговування клієнтів з Інтернет (Front-End), виноситься на окремий сервер, який по мережі взаємодіє з сервером, які реалізують функціонал (Back

-End). При цьому Front-End розміщують в DMZ, а Back-End залишається у внутрішньому сегменті. Для зв'язку між Front-End і Back-End на DFW створюють правило, яке дозволяє, ініціацію з'єднань від Front-End до Back-End.

Переваги варіанти:

У загальному випадку атаки, спрямовані проти сервісу, що захищається, можуть «спіткнутися» про Front-End, що дозволить нейтралізувати або істотно знизити можливі збитки. Наприклад, атаки типу TCP SYN Flood або slow http read , спрямовані на сервіс, приведуть до того, що Front-End сервер може виявитися недоступним, в той час як Back-End буде продовжувати нормально функціонувати і обслуговувати користувачів.

У загальному випадку на Back-End сервері може не бути доступу в Інтернет, що в разі його злому (наприклад, локально запущеним шкідливим кодом) утруднить віддалене керування ним з Інтернет.

Front-End добре підходить для розміщення на ньому брандмауера рівня додатків (наприклад, Web application firewall) або системи запобігання вторгнень (IPS, наприклад snort).

Недоліки варіанту:

Для зв'язку між Front-End і Back-End на DFW створюється правило, яке дозволяє ініціацію з'єднання з DMZ у внутрішню мережу, що породжує загрози, пов'язані з використанням даного правила з боку інших вузлів в DMZ (наприклад, за рахунок реалізації атак IP spoofing, ARP poisoning і т. д.)

Не всі сервіси можуть бути розділені на Front-End і Back-End.

У компанії повинні бути реалізовані бізнес-процеси актуалізації правил міжмережевого екранування.

У компанії повинні бути реалізовані механізми захисту від атак з боку Порушників, які отримали доступ до сервера в DMZ.

Примітки

У реальному житті навіть без поділу серверів на Front-End і Back-End серверів з DMZ дуже часто необхідно звертатися до серверів, що знаходяться

у внутрішній мережі, тому зазначені недоліки даного варіанту будуть також справедливі і для попереднього розглянутого варіанту.

Якщо розглядати захист додатків, що працюють через Web-інтерфейс, то навіть якщо сервер не підтримує рознесення функцій на Front-End і Back-End, застосування http reverse proxy сервера (наприклад, nginx) в якості Front-End дозволить мінімізувати ризики, пов'язані з атаками на відмову в обслуговуванні. Наприклад, атаки типу SYN flood можуть зробити http reverse proxy недоступним, в той час як Back-End буде продовжувати працювати.

Аналогія з реальним життям Даний варіант по суті схожий на організацію праці, при якій для високо завантажених працівників використовують помічники - секретарі. Тоді Back-End буде аналогом завантаженого працівника, а Front-End аналогом секретаря.

Варіант 4. Захищений DMZ

DMZ це частина мережі, доступна з Internet, і, як наслідок, підвладна максимальному ризику компрометації вузлів. Дизайн DMZ і підходи в ній повинні забезпечувати максимальну живучість в умовах, коли Порушник отримав контроль над одним з вузлів в DMZ. В якості можливих атак розглянемо атаки, до яких схильні практично всі інформаційні системи, що працюють з настройками за замовчуванням:

CAM-table overflow

ARP poisoning

Rogue DHCP Server

DHCP starvation

VLAN hopping

MAC flood

UDP flood

TCP SYN flood

TCP session hijacking

TCP reset

Атаки на Web-додатки

Атаки на обхід засобів аутентифікації і авторизацію від імені легітимного користувача (наприклад, підбір паролів, PSK і т.д.)

Атаки на уразливості в мережевих службах, наприклад:

Атака на Web-сервер - slow reading

DNS cache poisoning

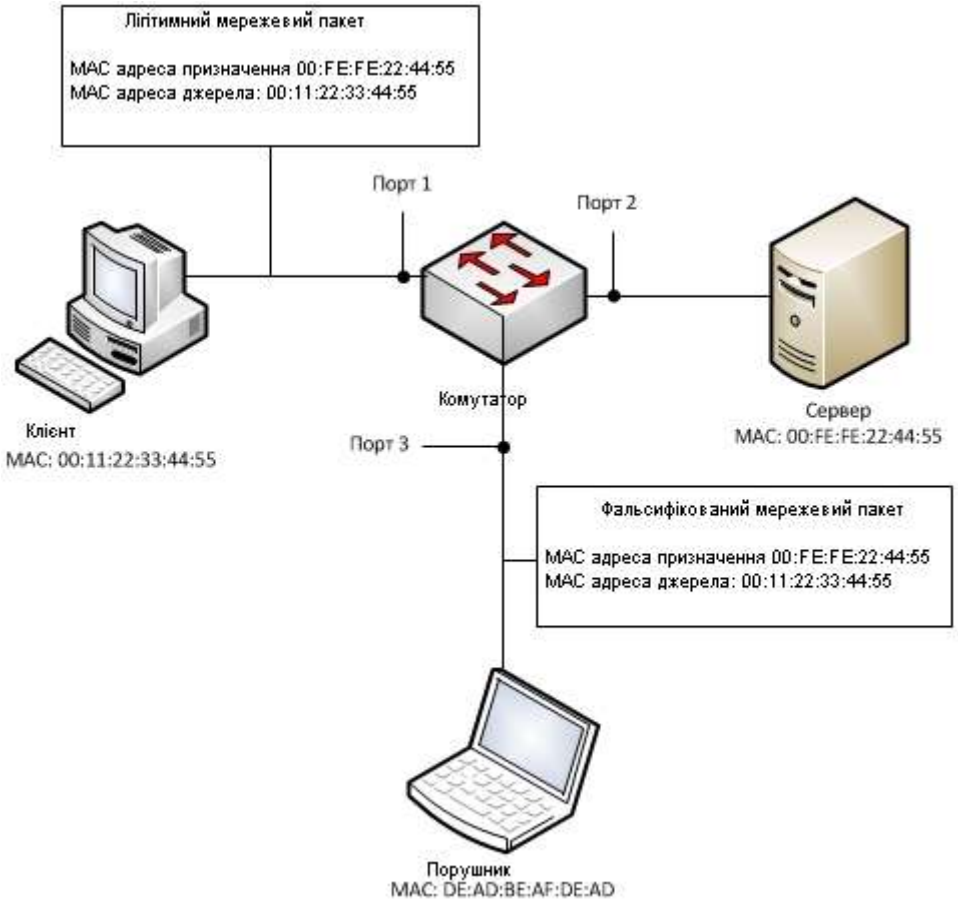


Рис. 2.7 Схема здійснення атаки

Велика частина зазначених атак (принаймні з 1 по 10) базується на вразливості архітектури сучасних Ethernet / IP мереж, що полягають в можливості Порушника підробляти в мережевих пакетах MAC і IP адреси. Експлуатацію даних вразливостей іноді виділяють в окремий види атак:

MAC spoofing ;

IP spoofing .

Тому побудову системи захисту DMZ почнемо з розгляду способів захисту від IP і MAC spoofing.

Наведені нижче способи захисту від даних атак не є єдино можливими. Існують і інші способи.

Захист від MAC spoofing

Схематично атаки, пов'язані з підміною MAC адреси, можна проілюструвати наступним чином:

Нейтралізацією даної атаки може бути фільтрація MAC-адрес на портах комутатора. Наприклад, трафік по порту 3 повинен проходити тільки в разі, якщо в адресі джерела або в адресі призначення вказано MAC-адресу DE: AD: BE: AF: DE: AD або широкомовну адресу (в деяких випадках).

Захист від IP spoofing

Схема атаки IP spoofing схожа на попередню, за винятком того, що Порушники підробляють не MAC, а IP-адресу. Захист від IP spoofing може бути реалізовано шляхом поділу IP-мережі DMZ на більш дрібні IP-підмережі і подальшу фільтрацією трафіку на інтерфейсах маршрутизатора за аналогією з розглянутою раніше MAC-фільтрацією. Нижче приклад дизайну DMZ, що реалізує даний принцип:

У DMZ розташовується 3 вузли:

Термінальний сервер (192.168.100.2)

Поштовий сервер (192.168.100.5)

Extranet сервер (192.168.100.9)

Для DMZ виділена IP-мережа 192.168.100.0/24, в даній мережі виділяються 3 IP-підмережі (по числу серверів):

Підмережа 1 - 192.168.100.0/30 для термінального сервера (192.168.100.2)

Підмережа 2 - 192.168.100.4/30 для поштового сервера (192.168.100.5)

Підмережа 3 - 192.168.100.8/30 для поштового сервера (192.168.100.9)

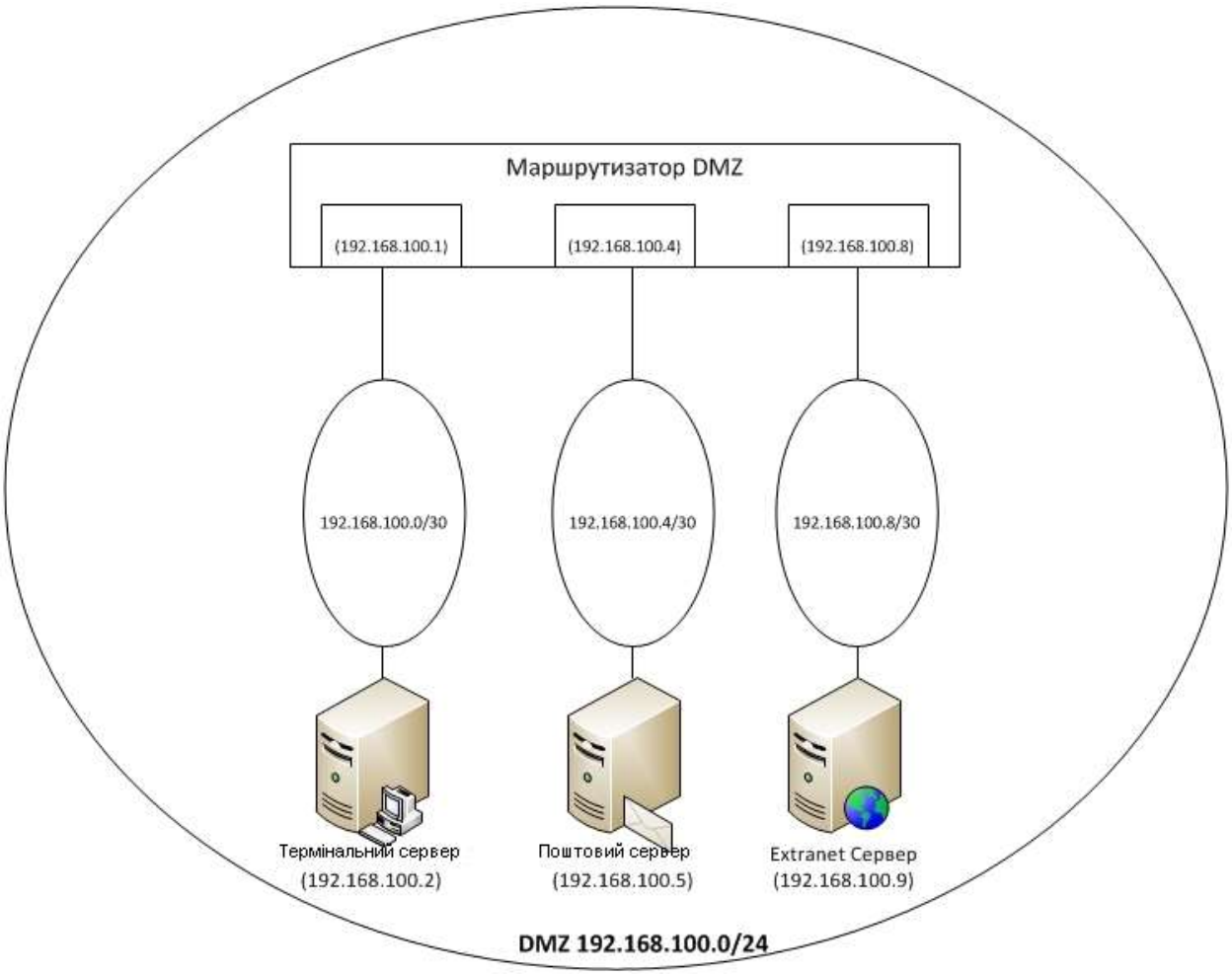


Рис. 2.8 Схема поділу IP-мережі DMZ на більш дрібні IP-підмережі і подальшу фільтрацією трафіку на інтерфейсах маршрутизатора

На практиці поділ мережі на подібні підмережі реалізують за допомогою технології VLAN. Однак, її застосування породжує ризики.

Захист від VLAN hopping

Для захисту від цієї атаки на комутаторі відключають можливість автоматичного узгодження типів (trunk / access) портів, а самі типи адміністратор призначає вручну. Крім того, організаційними заходами забороняється використання так званого native VLAN .

Захист від атак, пов'язаних з DHCP

Не дивлячись на те, що DHCP призначений для автоматизації конфігурації IP-адрес робочих станцій, в деяких компаніях зустрічаються

випадки, коли через DHCP видаються IP-Адреса для серверів, але це досить погана практика. Тому для захисту від Rogue DHCP Server , DHCP starvation рекомендується повна відмова від DHCP в DMZ.

Захист від атак MAC flood

Для захисту від MAC flood проводять настройку на портах комутатора на предмет обмеження граничної інтенсивності широкомовного трафіка (оскільки зазвичай при даних атаках генерується широкомовний трафік (broadcast)). Атаки, пов'язані з використанням конкретних (unicast) мережевих адрес, будуть заблоковані MAC фільтрацією.

Захист від атак UDP flood

Захист від даного типу атак проводиться аналогічно захисту від MAC flood, за винятком того, що фільтрація здійснюється на рівні IP (L3).

Захист від атак TCP SYN flood

Для захисту від даної атаки можливі варіанти:

Захист на вузлі мережі за допомогою технології TCP SYN Cookie .

Захист на рівні брандмауера (за умови поділу DMZ на підмережі) шляхом обмеження інтенсивності трафіку, що містить запити TCP SYN.

Захист від атак на мережеві служби і Web-додатки

Універсального рішення даної проблеми немає, але усталеною практикою є впровадження процесів управління уразливими ПЗ (виявлення, установка патчів і т.д.,), а також використання систем виявлення і запобігання вторгнень (IDS / IPS).

Захист від атак на обхід засобів аутентифікації

Як і для попереднього випадку універсального рішення даної проблеми немає.

Зазвичай у разі великого числа невдалих спроб авторизації облікові записи, для уникнення підбирань аутентифікаційних даних (наприклад, пароля) блокують. Але подібний підхід досить спірний, і ось чому.

По-перше, Порушник може проводити підбір аутентифікаційної інформації з інтенсивністю, що не приводить до блокування облікових записів

(зустрічаються випадки, коли пароль підбирався протягом кількох місяців з інтервалом між спробами в кілька десятків хвилин).

По-друге, цю особливість можна використовувати для атак типу відмова в обслуговуванні, при яких Порушник буде навмисне проводити велику кількість спроб авторизації для того, щоб заблокувати облікові записи.

Найбільш ефективним варіантом від атак даного класу буде використання систем IDS / IPS, які при виявленні спроб підбору паролів блокуватимуть не обліковий запис, а джерело, звідки даний підбір відбувається (наприклад, блокувати IP-адресу Порушника).

Підсумковий перелік захисних заходів за цим варіантом:

DMZ розділяється на IP-підмережі з розрахунку окрема підмережа для кожен вузол.

IP адреси призначаються вручну адміністраторами. DHCP не використовується.

На мережеві інтерфейси, до яких підключені вузли DMZ, активується MAC і IP фільтрація, обмеження по інтенсивності широкомовного трафіка і трафіку, що містить TCP SYN запити.

На комутаторах відключається автоматичне узгодження типів портів, забороняється використання native VLAN.

На вузлах DMZ і серверах внутрішньої мережі, до яких дані вузли підключаються, налаштовується TCP SYN Cookie.

Відносно вузлів DMZ (і бажано іншої мережі) впроваджується управління уразливими ПЗ.

У DMZ-сегменті впроваджуються системи виявлення та запобігання вторгнень IDS / IPS.

Переваги варіанту:

Високий ступінь безпеки.

Недоліки варіанту:

Підвищені вимоги до функціональних можливостей обладнання.

Трудовитрати у впровадженні та підтримці.

Варіант 5. Back connect

Розглянуті в попередньому варіанті заходи захисту були засновані на тому, що в мережі був присутній пристрій (комутатор / маршрутизатор / міжмережевий екран), здатний їх реалізовувати. Але на практиці, наприклад, при використанні віртуальної інфраструктури (віртуальні комутатори часто мають дуже обмежені можливості), подібного пристрою може і не бути.

У цих умовах Порушнику стають доступні багато з розглянутих раніше атак, найбільш небезпечними з яких будуть:

атаки, що дозволяють перехоплювати і модифікувати трафік (ARP Poisoning, CAM table overflow + TCP session hijacking і ін.);

атаки, пов'язані з експлуатацією вразливостей серверів внутрішньої мережі, до яких можна ініціювати підключення з DMZ (що можливо шляхом обходу правил фільтрації DFW за рахунок IP і MAC spoofing).

Наступною важливою особливістю, є те, що автоматизовані робочі місця (АРМ) користувачів теж можуть бути джерелом (наприклад, при зараженні вірусами або троянами) шкідливого впливу на сервер.

Таким чином, перед нами постає завдання захистити сервера внутрішньої мережі від атак Порушника як з DMZ, так і з внутрішньої мережі (зараження АРМа трояном можна інтерпретувати як дії Порушника з внутрішньої мережі).

Пропонований далі підхід спрямований на зменшення числа каналів, через які Порушник може атакувати сервера, а таких каналів як мінімум два. Перший це правило на DFW, яке дозволяє доступ до сервера внутрішньої мережі з DMZ (нехай навіть і з обмеженням по IP-адресами), а другий - це відкритий на сервері мережевий порт, по якому очікуються запити на підключення.

Закрити зазначені канали можна, якщо сервер внутрішньої мережі буде сам будувати з'єднання до сервера в DMZ і буде робити це за допомогою крипто захищених мережевих протоколів. Тоді не буде ні відкритого порту, ні правила на DFW.

Але проблема в тому, що звичайні серверні служби не вміють працювати так само, і для реалізації зазначеного підходу необхідно застосовувати мережеве тунелювання, реалізоване, наприклад, за допомогою SSH або VPN, а вже в рамках тунелів дозволяти підключення від сервера в DMZ до сервера внутрішньої мережі .

Загальна схема роботи даного варіанту виглядає наступним чином:

На сервер в DMZ інсталюється SSH / VPN сервер, а на сервер у внутрішній мережі інсталюється SSH / VPN клієнт.

Сервер внутрішньої мережі ініціює побудову мережевого тунелю до сервера в DMZ. Тунель будується з взаємною аутентифікацією клієнта і сервера.

Сервер з DMZ в рамках побудованого тунелю ініціює з'єднання до сервера у внутрішній мережі, по якій передаються дані, що захищаються.

На сервері внутрішньої мережі налаштовується локальний міжмережевий екран, фільтруючий трафік, що проходить по тунелю.

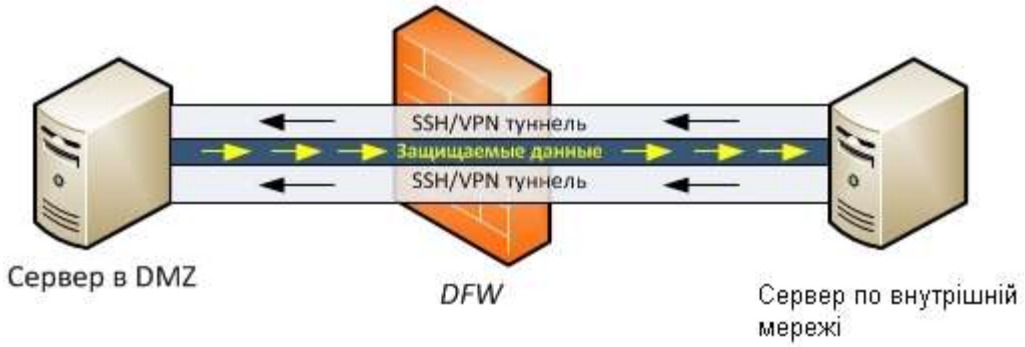


Рис. 2.9 Схема реалізації

Використання даного варіанта на практиці показало, що мережеві тунелі зручно будувати за допомогою OpenVPN , оскільки він володіє наступними важливими властивостями:

Кросплатформеність. Можна організовувати зв'язок на серверах з різними операційними системами.

Можливість побудови тунелів з взаємною аутентифікацією клієнта і сервера.

Можливість використання сертифікованої криптографії

На перший погляд може здатися, що дана схема надмірно ускладнена і що, раз на сервері внутрішньої мережі все одно потрібно встановлювати локальний міжмережевий екран, то простіше зробити, щоб сервер з DMZ, як зазвичай, сам підключався до сервера внутрішньої мережі, але робив це по шифрованому з'єднанню. Дійсно, даний варіант закриє багато проблем, але він не зможе забезпечити головного - захист від атак на вразливості сервера внутрішньої мережі, що здійснюються за рахунок обходу брандмауера за допомогою IP і MAC spoofing.

Переваги варіанту:

Архітектурне зменшення кількості векторів атак на сервер, що захищається внутрішньої мережі.

Забезпечення безпеки в умовах відсутності фільтрації мережевого трафіку.

Захист даних, що передаються по мережі, від несанкціонованого перегляду та зміни.

Можливість виборчого підвищення рівня безпеки сервісів.

Можливість реалізації двоконтурної системи захисту, де перший контур забезпечується за допомогою міжмережевого екранування, а другий організовується на базі даного варіанту.

Недоліки варіанту:

Впровадження і супровід даного варіанту захисту вимагає додаткових трудових витрат.

Несумісність з мережевими системами виявлення та запобігання вторгнень (IDS / IPS).

Додаткове обчислювальне навантаження на сервер.

Аналогія з реальним життям

Основний сенс даного варіанту в тому, що довірена особа встановлює зв'язок з не довіреною, що схоже на ситуацію, коли при видачі кредитів Банки самі передзвонюють потенційному позичальникові з метою перевірки даних.

2.3 Захист інформаційного забезпечення мереж

У зв'язку з бурхливим розвитком локальних і глобальних обчислювальних мереж широкий розвиток отримали і методи розвідки (промислового шпигунства), спрямовані на перехоплення інформації, що обробляється (переданої, що зберігається) в локальних мережах [18].

Проникнення в локальну мережу будь-якої організації можливо тільки при недостатньо кваліфікованому налаштуванні всіх елементів локальної мережі адміністратором системи. У разі ж грамотного налаштування, зловмисникам необхідно шукати способи добування інформації, не пов'язані з проникненням в локальну мережу. Для цього використовуються методи перехоплення інформації з каналів побічних випромінювань і наведень (ПЕМВН) елементів локальної мережі. Методика захисту окремих комп'ютерів досить добре опрацьована, підкріплена необхідними нормативними документами. Завдання ж захисту інформації від витоку каналами ПЕМВН в локальній мережі істотно складніше, ніж для автономно використовуваних пристроїв.

Джерелами електромагнітних випромінювань в локальній мережі є робочі станції і активне мережеве обладнання. Для захисту від витоку інформації по каналах побічних випромінювань і наведень застосовується екранування цього обладнання. Для зниження рівня випромінювань активного обладнання локальної мережі обладнання та сервери найкраще розміщувати в екранованому шафі.

Для комп'ютерів в даний час доступні корпуси, які відповідають вимогам Європейської Директиви щодо електромагнітної сумісності (European EMS Directive 89/336 / EEC). Сучасні корпуси дозволяють значно

послабити випромінювання елементів комп'ютера, але більшість вимагає додаткового доопрацювання. Якість екранування корпусу системного блоку комп'ютера впливає на рівень випромінювання всіх пристроїв, підключених до системного блоку (наприклад, клавіатури). Стандартна клавіатура зазвичай має дуже високий рівень випромінювання. У той же час з клавіатури вводяться дуже критичні з точки зору безпеки дані, включаючи паролі користувачів і адміністратора системи. Для перехоплення випромінювання клавіатури може використовуватися простий короткохвильовий приймач. З огляду також на те, що дані, що вводяться з клавіатури, вводяться в послідовному коді і тому можуть бути легко інтерпретовані, випромінювання, створювані клавіатурою, слід вважати найбільш небезпечними. Результати вимірювань рівня електричної (рис.2.10) і магнітної (рис.2.11) складових показав, що у комп'ютерів з різними корпусами системних блоків потужність побічних випромінювань від клавіатури може відрізнятися більш ніж в 100 разів.

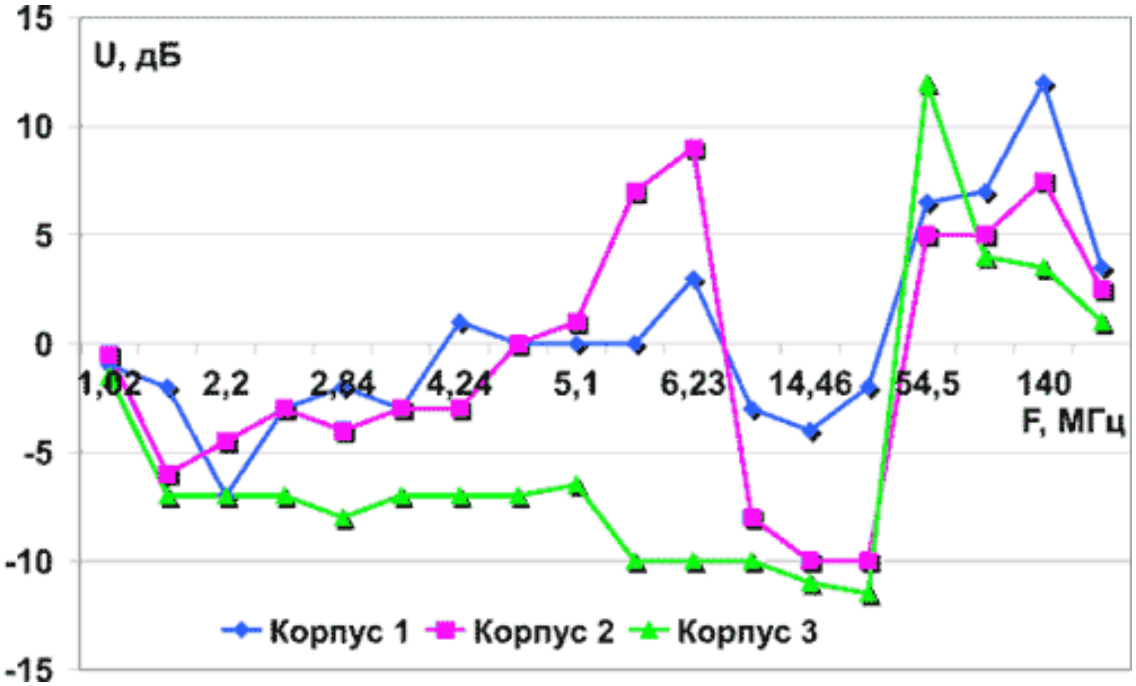


Рис. 2.10 Рівні електричної складової

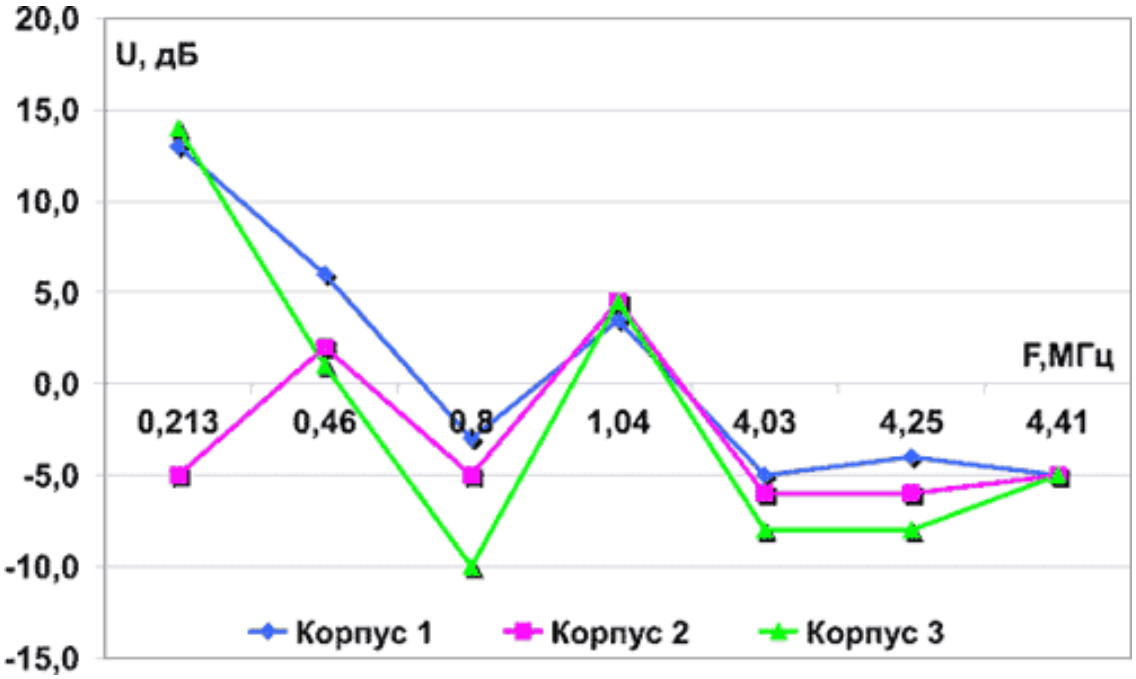


Рис. 2.11 Рівні магнітної складової

Аналогічні співвідношення виходять і для інших пристроїв, що входять до складу ПК.

Завдання доопрацювання стандартних корпусів і шаф:

По-перше, в місцях з'єднання окремих конструкцій корпусу завжди є щілини, які істотно погіршують екрануючі властивості.

По-друге, корпус електронного приладу не може бути герметичним так як потрібні вентиляційні отвори для відведення тепла.

По-третє, конструкція екрануючого корпусу не може бути розрахована заздалегідь. Тому доопрацювання стандартного корпусу з метою поліпшення його властивостей це завжди експериментальна робота.

Зараз існує безліч матеріалів, призначених для поліпшення властивостей корпусів - всілякі пружні ущільнювачі, електропровідні еластомери, самоклеючі металізовані покриття.

Джерелом випромінювання є блок живлення. Всередину живлення подається через фільтр, що перешкоджає поширенню побічних випромінювань уздовж проводів. Але розрахувати фільтр для повного

придушення випромінювань практично неможливо, так як на його характеристики впливають дуже багато параметрів зовнішньої мережі. Жоден фільтр, що серійно виготовляється не може повністю виконувати свої функції в широкій смузі частот. Хороші фільтри - це компромісне рішення, яке тільки в більшості випадків задовольняє пропонованим до фільтру вимог.

Залежно від цього характеристики щодо захисту інформації від витоку каналами ПЕМВН автономного комп'ютера або комп'ютера в складі мережі, можуть істотно відрізнятися. І основним чинником, що призводить до відмінності характеристик, є заземлення пристроїв.

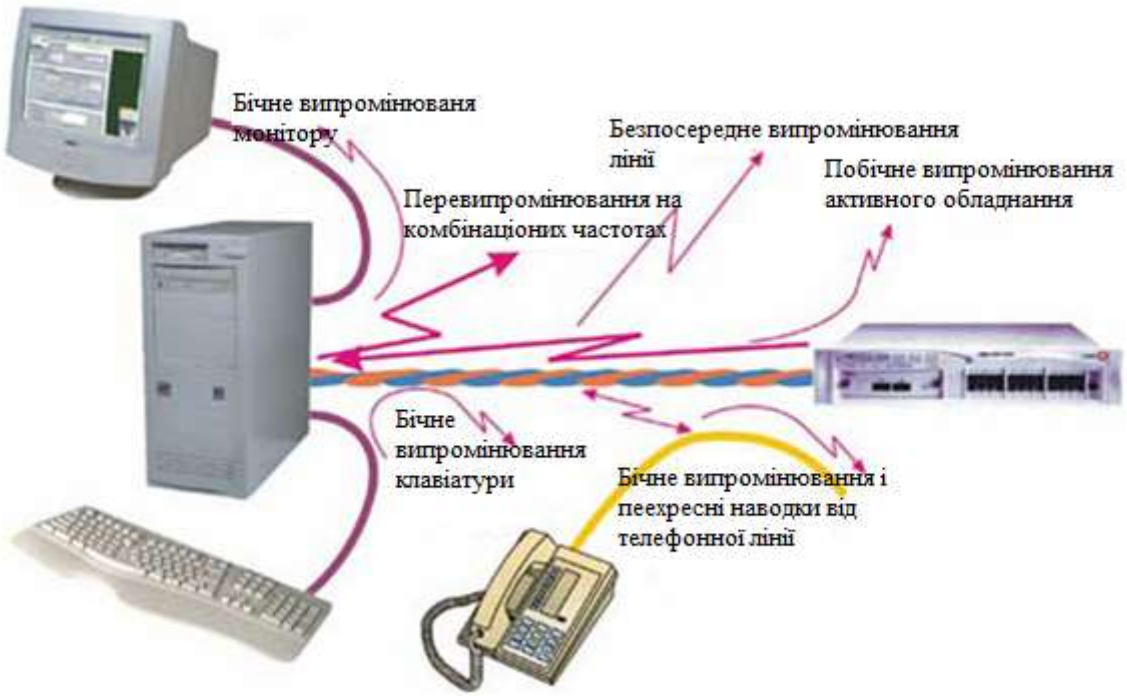


Рис. 2.12 Побічні електромагнітні випромінювання

В автономних пристроях заземлення не покращує і не погіршує їх екрануючих властивостей. Заземлення необхідно тільки за вимогами техніки електробезпеки. При грамотно виконаному заземленні рівень побічних випромінювань дещо знижується. Але в деяких випадках при підключенні заземлення рівень побічних випромінювань може і збільшитися.

Кабельна система не містить активних елементів, тому сама по собі вона не може бути джерелом побічних випромінювань. Однак кабельна система пов'язує між собою всі елементи комп'ютерної мережі. По ній передаються мережеві дані і вона є також приймачем всіх наведень і середовищем для перенесення побічних електромагнітних випромінювань (рис. 2.12).

Тому слід розрізняти:

Побічне випромінювання, викликане переданими по даній лінії сигналами (трафіком локальної мережі);

Прийом і подальше перевипромінювання побічних випромінювань від розташованих поблизу інших ліній і пристроїв;

Випромінювання кабельною системою побічних коливань від елементів мережевого активного обладнання і комп'ютерів, до яких підключений кабель.

Найчастіше при оцінці захищеності кабельної системи цікавляться тільки тим, наскільки послаблюється побічне випромінювання, викликане сигналами, що передаються по кабелю в процесі мережевого обміну інформацією.

Якщо по радіовипромінюванню кабельної системи можна відновити трафік в локальній мережі, то це становить велику небезпеку. Насправді трафік локальної мережі досить добре захищений від витоку інформації каналами ПЕМВН. Сучасні кабелі для локальних мереж мають дуже низький рівень випромінювання переданих сигналів. У цих кабелях сигнали передаються по кручений парі проводів, причому кількість скруток на одиницю довжини строго постійно. В принципі така система взагалі не повинна випромінювати. Більш того, наявність екрану у крученій парі дуже мало впливає на рівень випромінювання сигналів, які передаються по кручений парі. У реальній системі завжди мають місце окремі неоднорідності кабелю які впливають на рівень побічного випромінювання, що виникає в процесі мережевого обміну. Реально на відстані буквально одиниць метрів вже неможливо по електромагнітному випромінюванню сучасного кабелю перехопити передану по ньому інформацію. Але в більшості практичних випадків кабельна система

- це відмінна антена для всіх побічних випромінювань обладнання, підключеного до мережі. Побічні випромінювання, що виникають в елементах комп'ютера, наводяться на всі дроти кабелю локальної мережі (рис. 2.13).

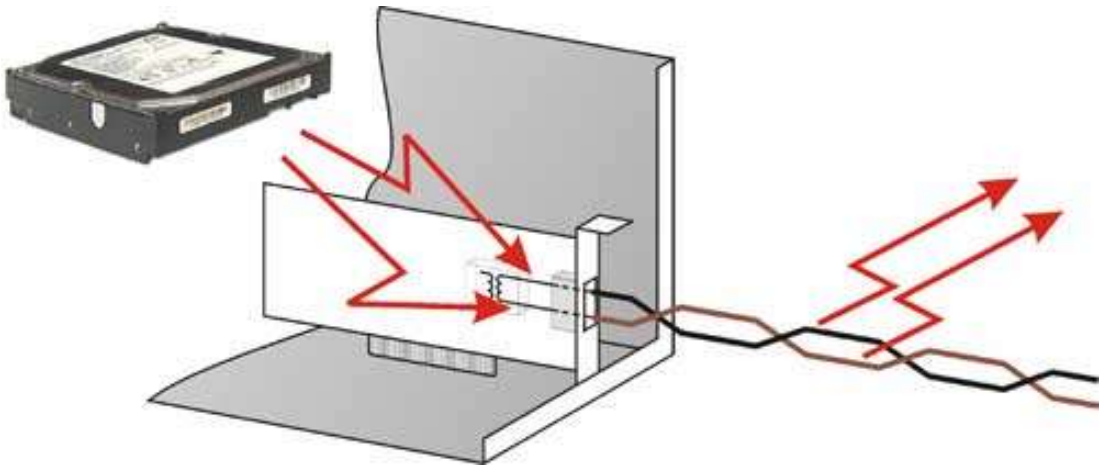


Рис. 2.13 Побічні випромінювання в елементах комп'ютера

Внаслідок цього для побічних випромінювань елементів комп'ютера кабель локальної мережі необхідно розглядати просто як одиночний багатожильний провід, що виходить за межі екранованого обсягу. Поставити для цих проводів фільтр, що пригнічує побічні випромінювання, неможливо. Таким чином, якщо комп'ютер із захистом інформації включити в локальну мережу на неекранованій кручений парі, то дроти витої пари, граючи роль антени, можуть посилити напруженість поля, створюваного, наприклад, клавіатурою комп'ютера (рис. 2.12, рис. 2.13), в десятки тисяч раз. Тому неекранована кручена пара не може застосовуватися в локальній мережі, в якій обробляється інформація з обмеженим доступом. Застосування ж екранованої крученої пари значно покращують ситуацію.

Локальна комп'ютерна мережа в даний час вже не може експлуатуватися автономно, без взаємодії з іншими мережами. Зокрема, будь-яка організація, будь то приватне підприємство, орган державного управління або відділ МВС, повинна бути активно представлена в глобальній мережі Інтернет. Це і власний сайт, і загальнодоступна електронна пошта, і доступ співробітників до інформації глобальної мережі. Така тісна взаємодія вступає в конфлікт з

вимогами забезпечення безпеки. При взаємодії кількох мереж можуть виникати різні загрози безпеки. Наприклад, при підключенні до глобальної мережі найбільш невинною з можливих загроз є злом мережі з хуліганських спонукань. У комп'ютерних мережах державних органів влади циркулює інформація, що представляє інтерес для іноземних розвідок. У комп'ютерних мережах МВС циркулює інформація, що представляє інтерес для криміналу. Ця інформація може і не мати грифа секретності. Однак в сукупності дозволяє отримати досить важливу інформацію. Тому, в разі об'єднання комп'ютерних мереж державних органів з глобальною мережею Інтернет крім хуліганських зломів слід припускати і більш кваліфіковані спроби проникнення в мережу зловмисників. Протистояти таким спробам вкрай складно. Тому мережу Інтернет необхідно ізолювати від внутрішньої мережі, в якій зосереджені великі цифри. Відомо кілька способів ізоляції власної комп'ютерної мережі від глобальної мережі Інтернет з метою забезпечення безпеки. У мережах, в яких не циркулює інформація з обмеженим доступом, для ізоляції мереж як правило досить використовувати маршрутизатор. Але серйозний захист від вторгнення з глобальної мережі можна забезпечити тільки при застосуванні міжмережевих екранів (FireWall). Тому для захисту корпоративної інформації комерційних фірм необхідне застосування міжмережевих екранів. Однак, для захисту інформації в державних органах як правило міжмережевий екран не забезпечує необхідного рівня захисту. Найбільш повно безпека забезпечується тільки в разі фізичної ізоляції мережі Інтернет від власної локальної мережі. Безумовно, це створює певні незручності в роботі і вимагає додаткових витрат при створенні комп'ютерної мережі. Однак в умовах необхідності протидії криміналу це виправданий захід.

При побудові мереж з фізичною ізоляцією також необхідно враховувати питання захисту від витоку інформації каналами ПЕМВН. У багатьох випадках співробітникові, що працює з інформацією обмеженого доступу необхідна і можливість виходу в Інтернет. На робочому місці встановлюється два комп'ютери, один з яких підключений до локальної мережі підприємства

(організації), а другий до мережі Інтернет. В цьому випадку кабелі власної мережі з захистом інформації та кабелі відкритої мережі Інтернет дуже важко рознести на достатню відстань. Внаслідок цього інформація, що циркулює в локальній мережі, а також всі побічні випромінювання комп'ютерів, наведені на кабелі локальної мережі, можуть наводитися і на кабелі відкритої мережі Інтернет. Мало того, що кабель відкритої мережі це досить довга антена (особливо коли відкрита мережа прокладена неекранованим кабелем). Кабелі відкритої мережі як правило виходять за межі території, що охороняється, тому зняти інформацію можна не тільки шляхом перехоплення випромінювань, але і шляхом безпосереднього підключення до кабелів відкритої мережі. Тому кабелі відкритої мережі також повинні бути прокладені у відповідності з усіма рекомендаціями, виконуваними при побудові мережі із захистом інформації.

Висновок до розділу

У межах другого розділу розкрито цільове призначення системи моніторингу комплексом аграрного призначення на базі Інтернету речей, проведено проектування системи та описано принципи проектування системи моніторингу комплексом аграрного призначення на базі Інтернету речей. Розглянуто всі п'ять заявлених варіантів організації доступу до сервісів корпоративної мережі з Інтернет. Який з них краще, який гірше – сказати складно, оскільки все залежить, в кінцевому рахунку, від тієї інформації, яку необхідно захистити, і тих ресурсів, якими компанія володіє для захисту. Якщо ні ресурсів, ні знань немає, то оптимальним буде перший варіант. Якщо ж інформація дуже цінна, то комбінація четвертого і п'ятого варіантів дасть неперевершений рівень безпеки.

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНА СИСТЕМА МОНІТОРИНГУ КОМПЛЕКСОМ АГРАРНОГО ПРИЗНАЧЕННЯ НА БАЗІ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Етапи розробки системи моніторингу

Незважаючи на величезну різноманітність різних систем, що реалізують механізм системи управління приміщеннями загального користування, єдиних стандартів для побудови таких систем не існує до теперішнього часу. Тому, переглянувши безліч різних реалізацій подібних проектів (елеватора, тваринницького комплексу, пасіки, тощо), було прийнято рішення створити систему комплексного моніторингу приміщення двоповерхової адміністративної будівлі аграрного призначення, що стоїть окремо з урахуванням технології Інтернет речей з використанням широко поширених інтерфейсів і протоколів, яка б відповідала технічному завданню. Це дозволяє отримати повну незалежність від стороннього розробника (що є ключовим моментом) і в подальшому модернізувати систему виходячи зі своїх запитів і потреб, а використання стандартних рішень дозволяє відносно просто інтегрувати їх в розроблювану систему.

У більшості випадків існуючі системи працюють на «інформаційно–керуючому рівні». Припустимо, це управління освітленням, контроль температури в приміщеннях (клімат-контроль), включення певного навантаження. При побудові подібних систем, обов'язково повинен бути використаний принцип автоматизованості.

Це мають бути системи енергопостачання, контролю різних параметрів і управління виконавчими пристроями, пов'язаними в єдину мережу, керовану центральним контролером і можливістю безпосереднього та віддаленого доступу користувача до цієї мережі. Рівні інтеграції системи управління приміщенням з урахуванням технології Інтернет речей представлено на рис. 3.1

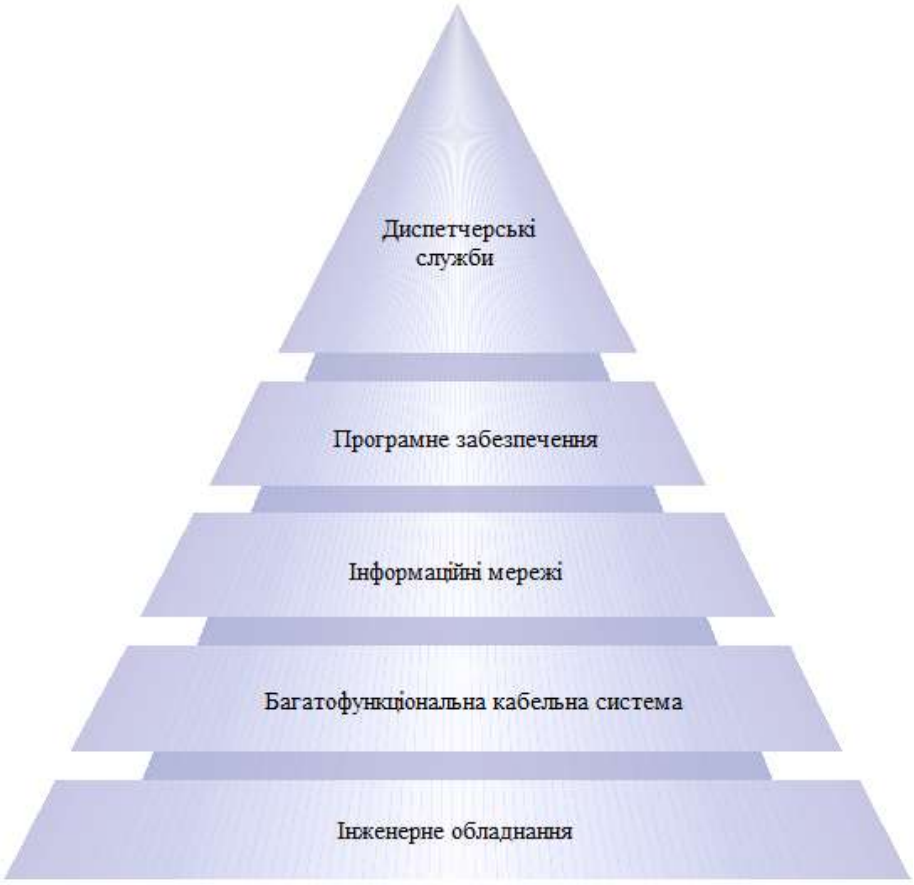
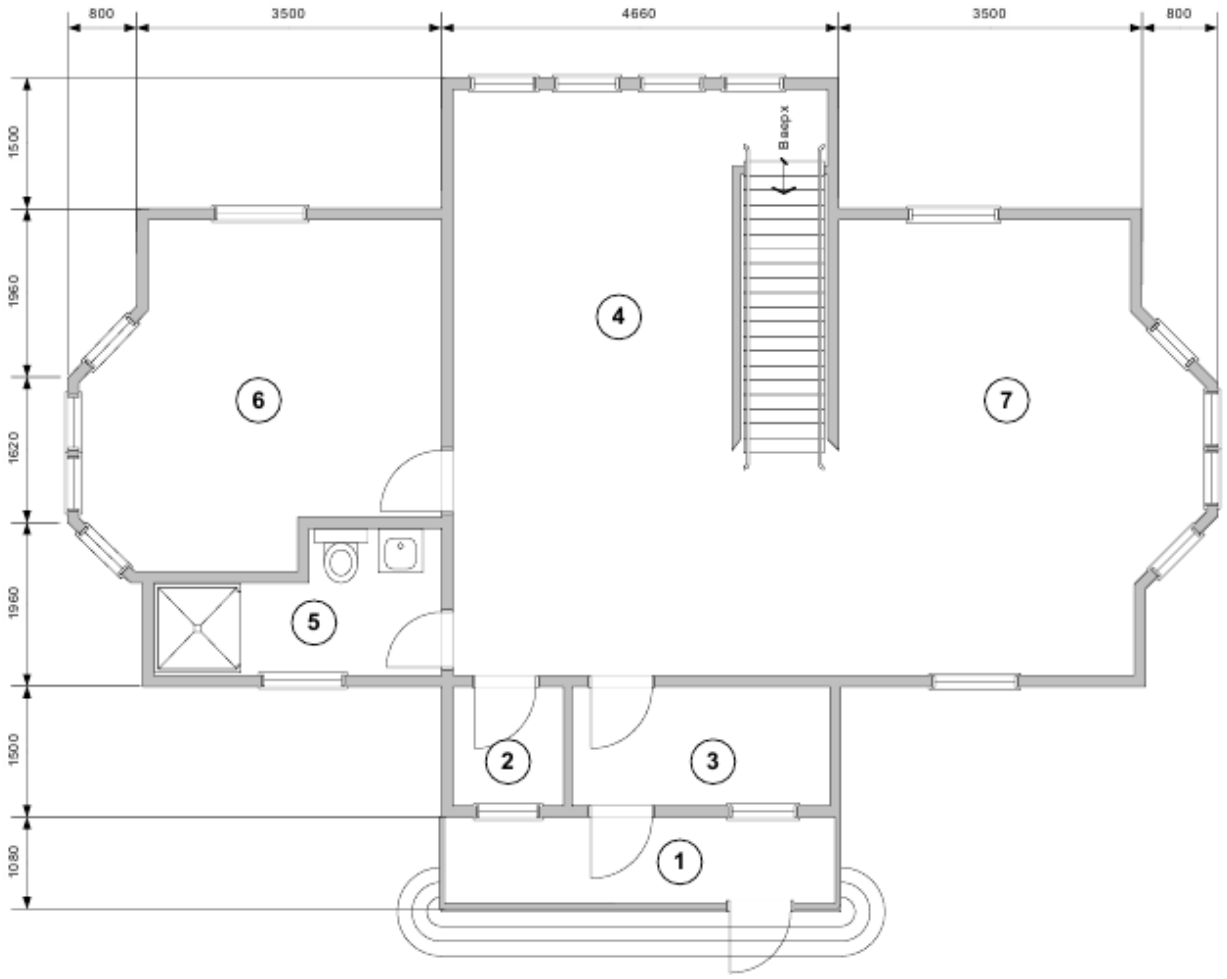


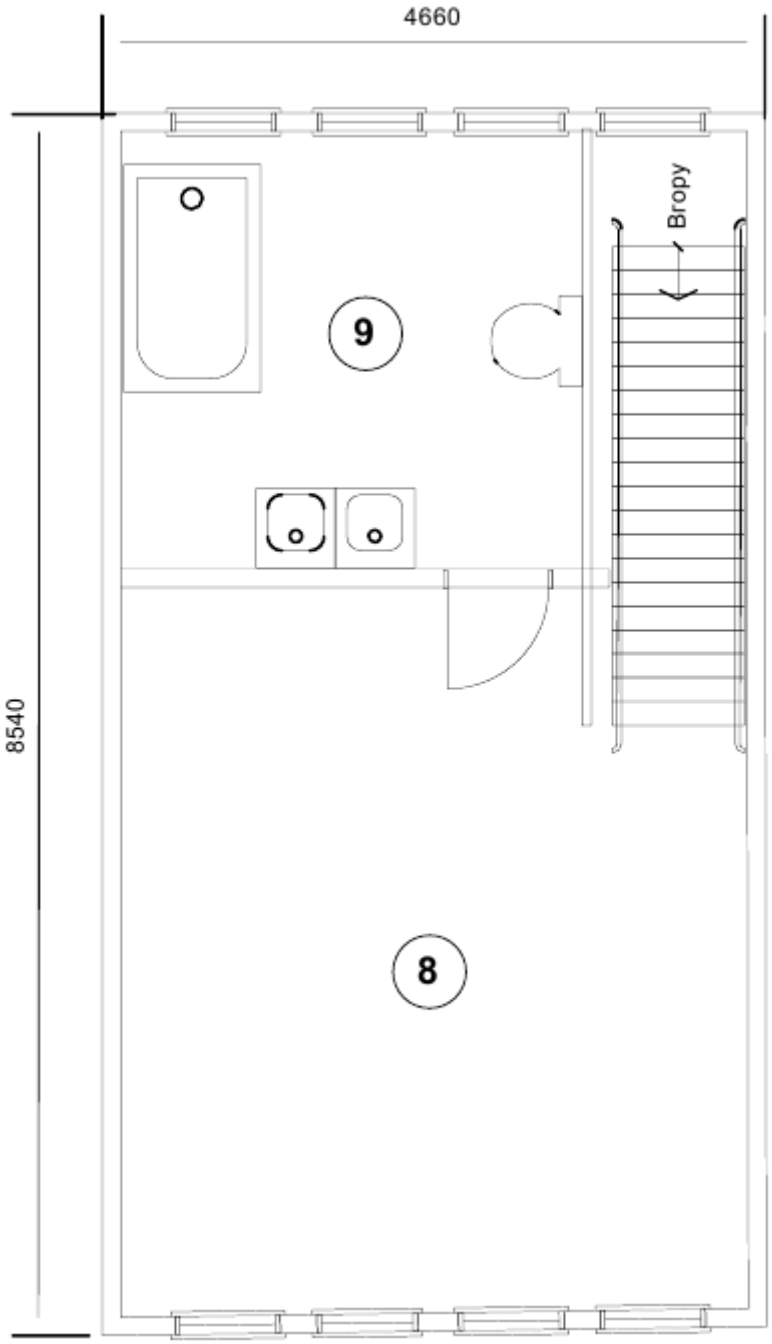
Рис. 3.1 Рівні інтеграції системи управління приміщенням з урахуванням технології Інтернет речей

Впровадженню системи комплексного моніторингу підлягає приміщення 2– х поверхового котеджу аграрного комплексу, що стоїть окремо.

Перекриття з монолітного залізобетону, зовнішні та міжкімнатні стіни з цегли. Всі приміщення, що захищаються опалюються автономно. Температура повітря в приміщеннях 15– 22^0C. Відносна вологість повітря до 90%. Вентиляція природна. Висота стелі в приміщеннях 2,8 метра.



План першого поверху



План другого поверху

Рис. 3.2 План будівлі, яка підлягає встановленню системи управління приміщенням з урахуванням технології Інтернет речей

Таблиця 3.1 – Експлікація приміщень

№ п.п	Найменування	Площа, м^2
	Перший поверх	
1	Тераса	4,3
2	Господарське приміщення	1,67
3	Тамбур	4,2
4	Приймальня	25,65
5	Санвузол	4,42
6	Склад	14,4
7	Виробниче приміщення	19,3
	Другий поверх	
8	Бухгалтерія	20,95
9	Санвузол	9,79

Система управління приміщенням з урахуванням технології Інтернет речей призначена для забезпечення комфортних умов, захисту матеріальних цінностей, людей, що знаходяться в приміщенні, що захищається, забезпечує виконання наступних функцій:

– виявлення тривожних / аварійних ситуацій (несанкціоноване проникнення, пожежа, витік води), формування сигналів тривог;

– підтримку заданої температури;

– видачу інформації про наявність і місце виникнення тривожної / аварійних ситуацій на пульт сигналізації і зовнішній світлозвуковий оповіщувач;

– аварійне перекриття кульових кранів подачі гарячої та холодної води;

– автоматичний контроль стану елементів системи і її складових частин;

– доставку повідомлення про тривожну / аварійну ситуацію в охоронні структури через термінал;

– доставку повідомлення про тривожну / аварійну ситуацію, інших подій дзвоном і за допомогою SMS власнику і / або в охоронні структури [25].

Алгоритм роботи системи представлений на рис. 3.3. Він дозволяє встановлювати критичні параметри відповідно до обраного режиму, регулює температуру і вологість в приміщенні, враховуючи особливості приміщення.

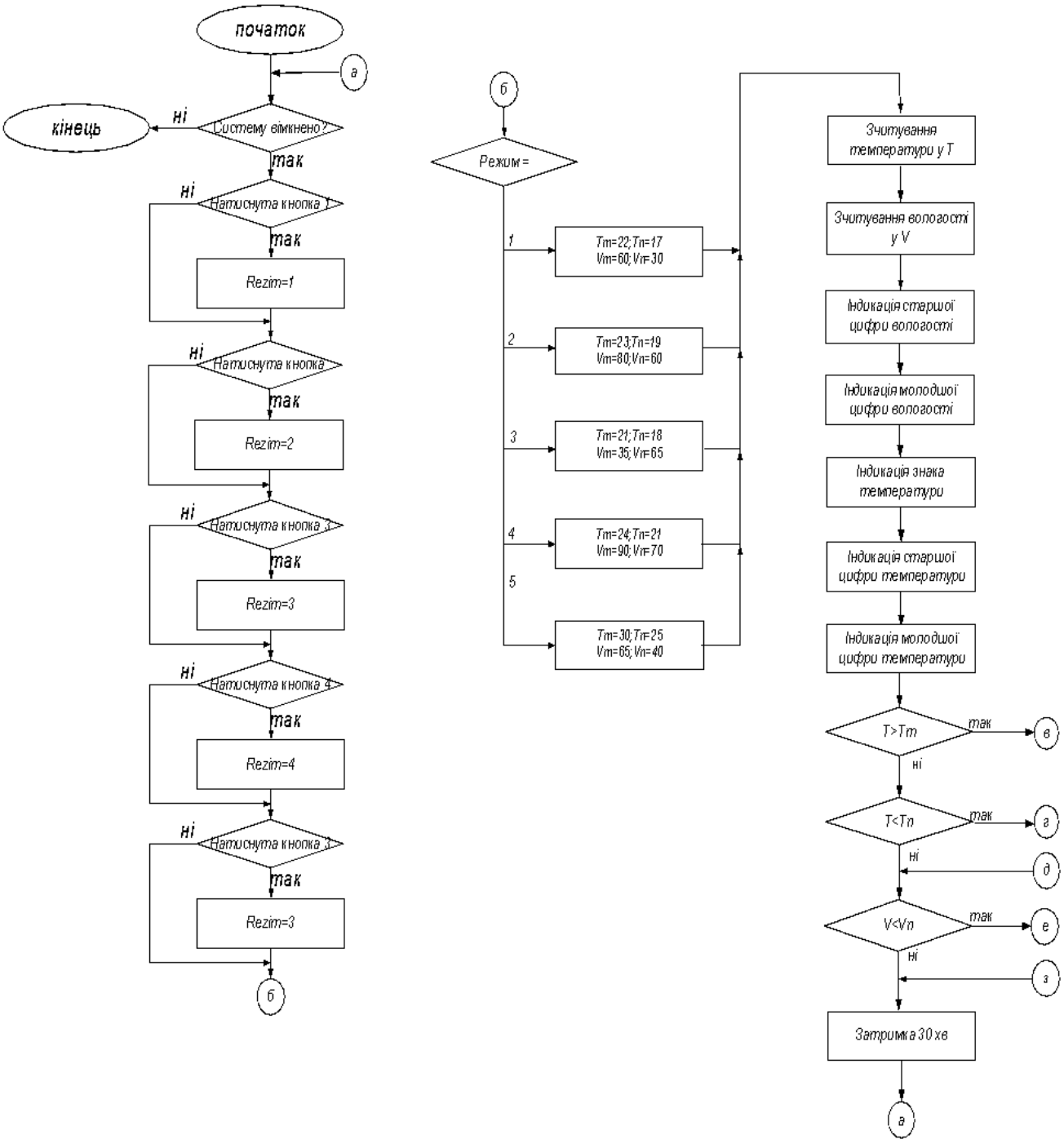
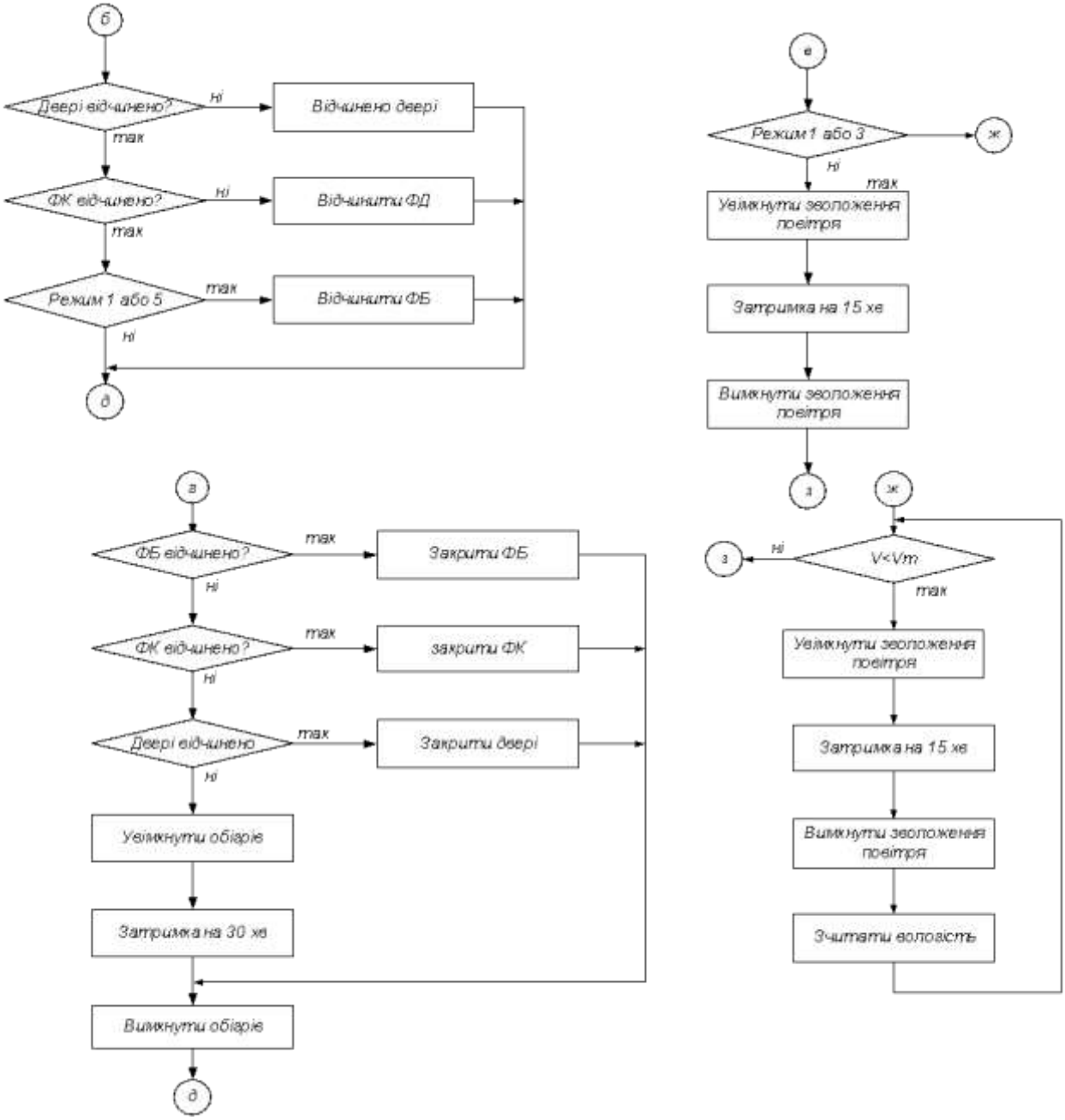


Рис. 3.3 Алгоритм роботи системи управління приміщенням



Продовження рисунку 3.3

Система, що розробляється є багаторівневою. Це позначає , що дані з певної групи датчиків і команди для виконавчих пристроїв концентруються на окремих модулях, які по загальній мережі пов'язані з центральним (керуючим) контролером. Як інтерфейс зв'язку пропонується використовувати надійний і перевірений інтерфейс RS– 485, який дуже широко застосовується в промисловій автоматиці, а так само мережу Ethernet. Загальна структурна схема системи, що розробляється показана на рис. 3.4.

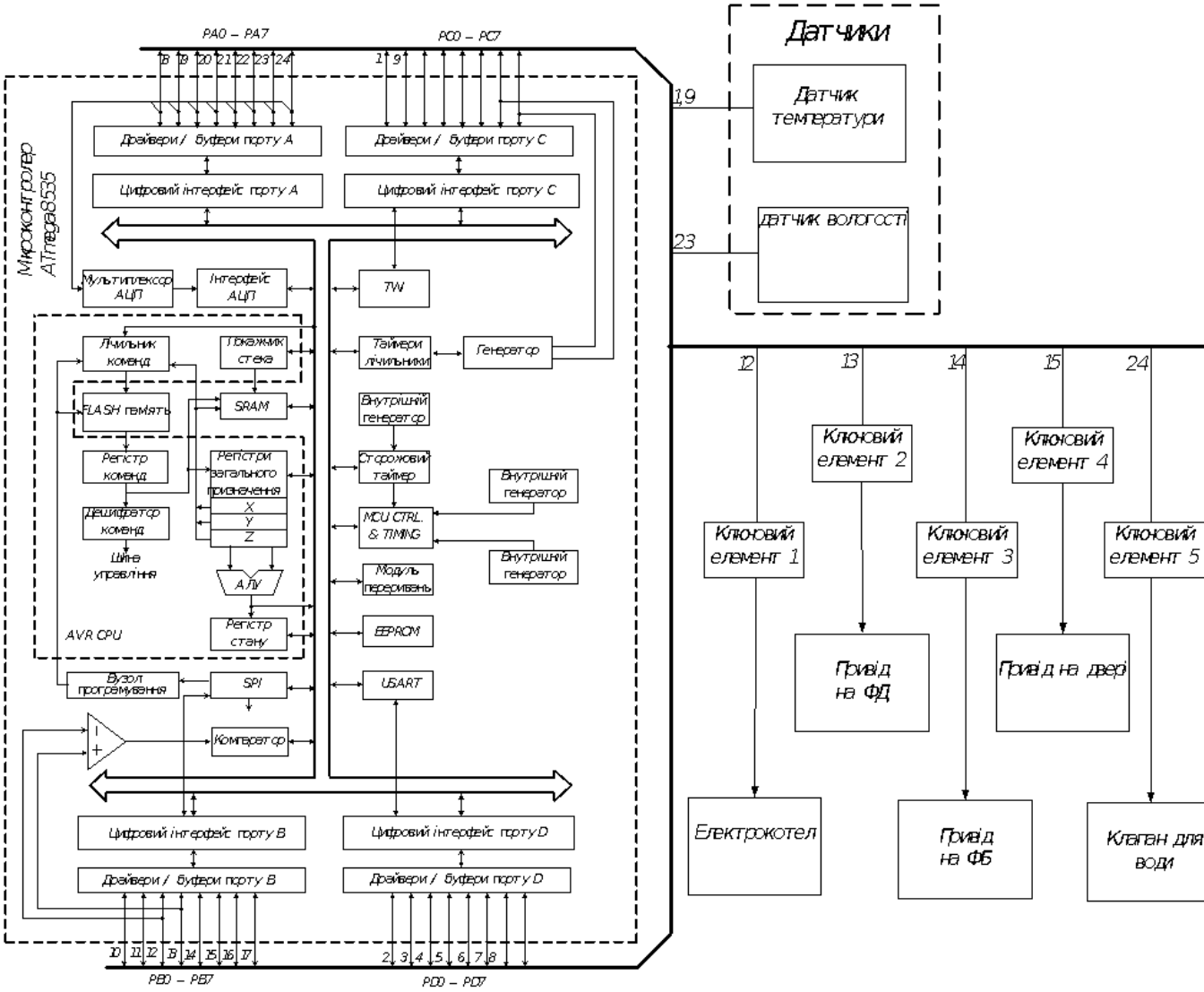


Рис. 3.4 Функціональна схема системи управління приміщенням

Температурний датчик працює по інтерфейсу I2C, який підтримує мікроконтролер, тому додаткових засобів узгодження та управління не потрібно. Обмін інформацією підтримується програмно через виходи PC0, PC1, а при підключенні датчика необхідно тільки поставити 2 резистора по 1кОм (типове підключення по datasheet). У датчика вологості вихід аналоговий, тому потрібно використовувати АЦП, який вбудований в Atmega 8535, використовуючи PA2. Передача підтримується програмно. Кнопки управління і ключові елементи підключаються до порту B, а порт D використовується для семисегментної індикації.

Електрична принципова схема наведена на рис. 3.5.

Живлення системи буде від стандартної мережі 220В, 50 Гц. Для живлення мікропроцесора та інших елементів схеми необхідна постійна напруга 5 В.

Будемо використовувати наступну схему: трансформатор знижує змінну мережеву напругу до 12 В. Діодний міст VD1 ... 4 випрямляє напругу в електромережі. Інтегральний діодний міст обраного типу DB157 комутує струми до 1 А. В якості стабілізатора напруги включена мікросхема інтегрального стабілізатора U1 – LM340K– 5, схема включення – стандартна, рекомендована виробником.

Дані з датчика температури зчитуються мікропроцесором по інтерфейсу I2C, а дані з датчика вологості – через АЦП. Перемикання каналів АЦП, обробка даних з датчиків температури, вироблення сигналів на виконавчі пристрої, вивід інформації на пристрій індикації здійснюється програмно за допомогою відповідних засобів мікроконтролера.

Для виведення візуальної інформації про встановлену вологість і температуру у приміщені використовуємо трирозрядний і дворозрядний семисегментні світлодіодні індикатори.

Принцип індикації наступний. Кожні 16 мс загоряється одна цифра індикаторів. Для визначення номера цифри в програмі мікроконтролера є лічильник (покажчик індикатора), який сприймає від 0 до 2. Восьмирозрядний

таймер лічильника запрограмований так, що через кожні 16 мілісекунд виникає переривання. Таким чином, кожні 16 мілісекунд горить одна цифра. У наступну міллісекунду загоряється наступна цифра, а ця гасне. Око ж людини сприймає це так, як ніби горять одночасно всі цифри.

При включенні живлення мікро приймає сигнал RESET, який визначає початкову синхронізацію вбудованого генератора.

Вузол програмування отримує сигнали синхронізації від синхронізатора і управляє роботою лічильника команд і FLASH– пам'яттю програм.

Регістр команд містить команду, яка вибирається з FLASH– пам'яті програм для виконання. Дешифратор команд за кодом операції визначає, яка команда повинна виконуватися. Далі відбувається послідовна вибірка і виконання команд відповідно до алгоритму роботи.

При натисканні на кнопки управління відбувається переривання і управління відповідного обробника переривання, де за алгоритмом відбувається установка потрібного режиму. Задані значення температур і вологості зберігаються у відповідних РВВ при виборі режиму роботи.

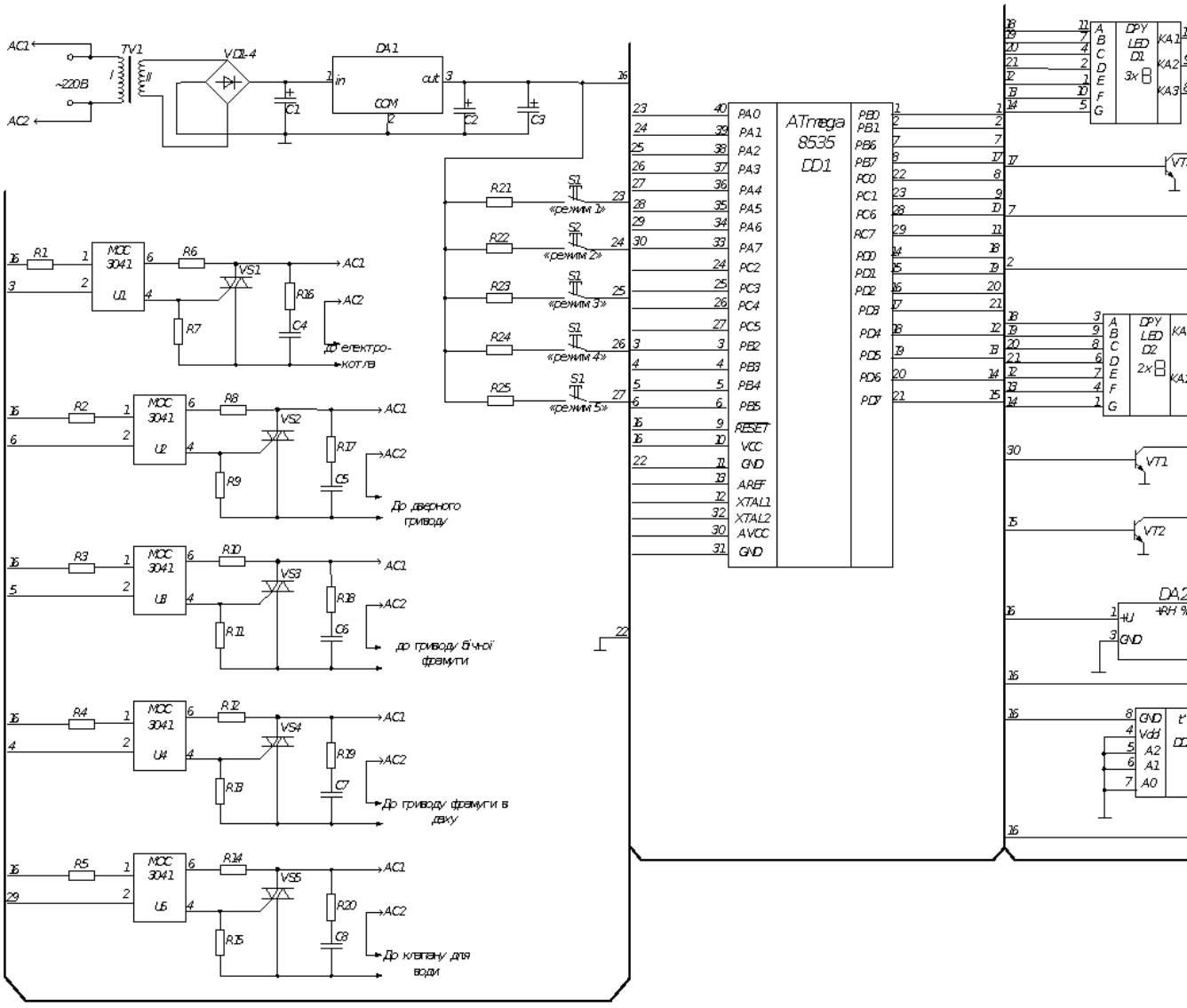


Рис. 3.5 Електрична принципова схема системи управління приміщенням

Підключення пристроїв до портів мікроконтролера Atmega8535 приведено в таблиці 3.2.

Таблиця 3.2 – Підключення пристроїв до портів мікроконтролера Atmega8535

№ виводу	Порт: розряд	Підключений пристрій
	Порт A	
40	0	Кнопка «режим 1»
39	1	Кнопка «режим 2»
38	2	Кнопка «режим 3»
37	3	Кнопка «режим 4»
36	4	Кнопка «режим 5»
35	5	Датчик вологості
34	6	Сімістор управління клапаном для води
	Порт B	
1	0	Молодша цифра дворозрядного індикатора
2	1	Перша цифра трирозрядного індикатора
3	2	Сімістор для обігріву приміщення
	Порт B	
4	3	Сімістор для управління ФД
5	4	Сімістор для управління ФБ
6	5	Сімістор для управління дверима
7	6	Друга цифра трирозрядного індикатора
8	7	Третя цифра трирозрядного індикатора
	Порт C	
22	0	Датчик температури
23	1	Датчик температури
	Порт D	
14	0	Сегмент індикатора (вихід)
15	1	Сегмент індикатора (вихід)
16	2	Сегмент індикатора (вихід)
17	3	Сегмент індикатора (вихід)
18	4	Сегмент індикатора (вихід)
19	5	Сегмент індикатора (вихід)
20	6	Сегмент індикатора (вихід)
21	7	Старша цифра дворозрядного індикатора

Впровадження системи управління приміщення 2– х поверхового котеджу, що стоїть окремо з урахуванням технології Інтернет речей передбачає:

− інтеграцію інженерних систем;

− створення системи моніторингу, контролю функціональності і управління інженерним обладнанням;

− інтеграцію системи управління інженерним обладнанням у систему управління приміщенням 2– х поверхового котеджу, що стоїть окремо.

Команди логічних операцій

Ці команди дозволяють виконувати стандартні логічні операції над байтами, такі як «логічне множення» (І), «роз'єднання» (АБО), операція «виключає АБО», а також обчислення зворотного і додаткового кодів числа. До цієї групи можна віднести також команди очищення / установки регістрів і команду перестановки тетрад. Всі операції проводяться над регістрами загального призначення, результат зберігається в одному з РВВ. Всі логічні операції виконуються за один машинний цикл.

Команди арифметичних операцій і команди зсуву

До даної групи належать команди, що виконують такі базові операції, як додавання, віднімання, зсув (вправо і вліво), інкремент і декремент. Всі операції проводяться тільки над регістрами загального призначення. При цьому мікроконтролери AVR дозволяють легко оперувати як знаковими, так і беззнаковими числами, а також працювати з числами, представленими в додатковому коді. Всі команди даної групи виконуються за один машинний цикл, за винятком команд, що оперують двобайтовими значеннями, які виконуються за два цикли.

Команди операцій з бітами

До даної групи належать команди, що виконують установку або скидання заданого розряду РОН або РВВ. Причому для зміни стану розрядів регістра стану SREG є також додаткові команди (точніше, еквівалентні

мнемонічні позначення загальних команд), тому що перевірка стану розрядів саме цього регістра проводиться найчастіше. Умовно до цієї групи можна віднести також дві команди передачі управління типу «перевірка / перепустку», які пропускають наступну команду в залежності від стану розряду РОН або РВВ.

Всі задіяні розряди РВВ мають свої символічні імена. Визначення цих імен описані в тому ж файлі, що і визначення символічних імен адрес регістрів. Таким чином, після включення в програму зазначеного файлу в командах замість числових значень номерів розрядів можна буде вказувати їх символічні імена.

Команди пересилання даних

Команди цієї групи призначені для пересилання вмісту комірок, що знаходяться в адресному просторі пам'яті даних. Поділ адресного простору на три частини (РОН, РВВ, ОЗП) зумовило різноманітність команд даної групи. Пересилання даних, виконувана командами групи, може проводитися в наступних напрямках:

РОН ⇔РОН;

РОН ⇔РВВ;

РОН ⇔пам'ять даних (3 види адресації).

Також до цієї групи можна віднести стекові команди PUSH і POP, що дозволяють зберігати в стеці і відновлювати зі стека вміст РОН.

На виконання команд даної групи потрібно від одного до трьох машинних циклів в залежності від команди.

Команди передачі управління

У цю групу входять команди переходу, виклику підпрограм і повернення з них і команди типу «перевірка / перепустка», пропускають наступну за ними команду при виконанні деякої умови. Також до цієї групи належать команди порівняння, формують прапори регістра SREG і призначені, як правило, для роботи спільно з командами умовного переходу.

В системі команд мікроконтролерів сімейства є команди як безумовного, так і умовного переходів. Команди непрямого (IJMP) і відносного (RJMP) безумовного переходу є найпростішими в цій групі. Їх функція полягає тільки в записі нової адреси в лічильник команд. Команди умовного переходу також змінюють вміст лічильника команд, проте ця зміна відбувається тільки при виконанні деякої умови або, точніше, при певному стані різних прапорів регістра SREG.

Команди управління системою

У цю групу входять всього 3 команди:

– NOP – порожня команда;

– SLEEP – переклад мікроконтролера в режим зниженого енергоспоживання;

– WDR – скидання сторожового таймера

Команди NOP і WDR виконуються за один машинний цикл, а команда SLEEP – за чотири машинних цикли. У таблиці 3.3 представлені коди для відображення цифр і знака «– »:

Таблиця 3.3 – Коди для відображення цифр і знака «– »

	d0	d1	d2	d3	d4	d5	d6	код
цифра 1	0	1	1	0	0	0	0	0x82
цифра 2	1	1	0	1	1	0	1	0x3e
цифра 3	1	1	1	1	0	0	1	0xae
цифра 4	0	1	1	0	0	1	1	0x87
цифра 5	1	0	1	1	0	1	1	0xad
цифра 6	1	0	1	1	1	1	1	0xbd
цифра 7	1	1	1	0	0	0	0	0x22
цифра 8	1	1	1	1	1	1	1	0xbf
цифра 9	1	1	1	1	0	1	1	0xaf
цифра 0	1	1	1	1	1	1	0	0xbb
знак	0	0	0	0	0	0	1	0x1
	A	B	C	D	E	F	G	

Чотири процедури є стандартними: main, read_adc, ds1621_temperature_10 (0), timer0_ovf_isr.

• read_adc – процедура для зчитування даних з датчика вологості, підтримує зв'язок з АЦП.

• ds1621_temperature_10 (0) – стандартна процедура для обміну з датчиком ds1621 по інтерфейсу i2c.

• timer0_ovf_isr – переривання таймера по переповненню. Дозволяє відображати режим і температуру на семисегментних індикаторах таким чином, щоб не виникало мерехтінь і зникнення цифр з індикатора.

• main – головна процедура, в неї входить призначені для користувача процедури:

• zapoln – процедура, що здійснює запам'ятовування критичних параметрів по обраному режиму.

• indik, otobr_chif – процедури для відображення даних на семисегментних індикаторах, подаючи на висновки A– G і транзисторні ключі відповідні сигнали.

3.2 Тестування системи моніторингу комплексом аграрного призначення

Для реалізації алгоритму застосування систем комплексного моніторингу приміщень за допомогою технології Інтернет речей, коротко опишемо функції, які повинна виконувати система, що розробляється:

1. Початковий запуск системи

2. Вибір необхідного для підтримки типу мікроклімату.

3. Прийом даних з датчиків і обробка цих даних відповідно до алгоритму.

4. Виведення поточних параметрів мікроклімату середовища.

5. Формування вихідних сигналів для запуску виконавчих пристроїв провітрювання / нагріву, зволоження.

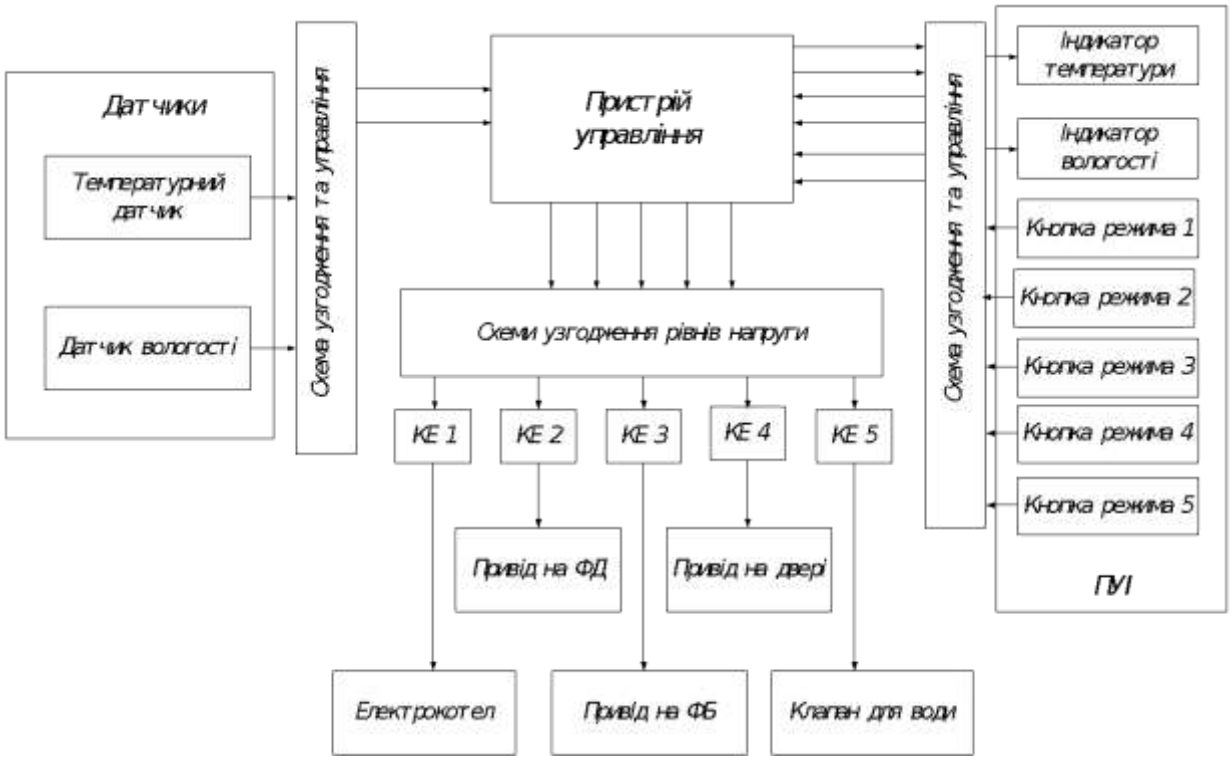
Виходячи з вимог технічного завдання та функцій, які повинна виконувати система, що розробляється, можна виділити основні модулі, з яких повинна складатися обчислювальна система.

Датчики – є невід'ємною частиною системи, вони використовуються для того, щоб система могла в реальному часі реагувати на зміни зовнішніх параметрів по заздалегідь розробленому алгоритму. В даний час на ринку представлена велика різноманітність різних типів датчиків, деякі з них є вузькоспеціалізованими.

Пристрій управління є головною частиною системи, він необхідний для збору і обробки інформації, що надходить з системи датчиків, вироблення керуючих сигналів для виконавчих пристроїв, а також виведення інформації на пристрій індикації.

Пульт управління та пристрій візуальної індикації необхідні для вибору типу мікроклімату, для візуального виведення поточної температури і вологості в приміщенні, моніторингу безпеки, витоку воду таке інше.

Відповідно до визначених вище функцій можна визначити загальну структуру системи. Структурна схема системи представлена на рис. 3.6.



КЕ – ключовий елемент; ФБ – фрамуга бокова; ФД – фрамуга в даху; ПУІ – пульт управління та індикації

Рис. 3.6 Структурна схема системи управління приміщення 2– х поверхового котеджу аграрного призначення, що стоїть окремо з урахуванням технології Інтернет речей

Пристрій управління отримує від датчиків і кнопок управління дані, перетворює їх відповідно до алгоритму роботи і видає дані на індикатори для відображення, а також при необхідності сигнали на ключові елементи. Ключові елементи дозволяють вмикати / вимикати виконавчі пристрої в тому порядку, в якому встановлено в алгоритмі.

Схема взаємодії всіх складових наведена на рис.. 3.7.

Рис. 3.7 Схема взаємодії всіх складових системи управління приміщення 2– х поверхового котеджу аграрного призначення, що стоїть окремо з урахуванням технології Інтернет речей

Інтерфейс системи управління наведено на рис. 3.8

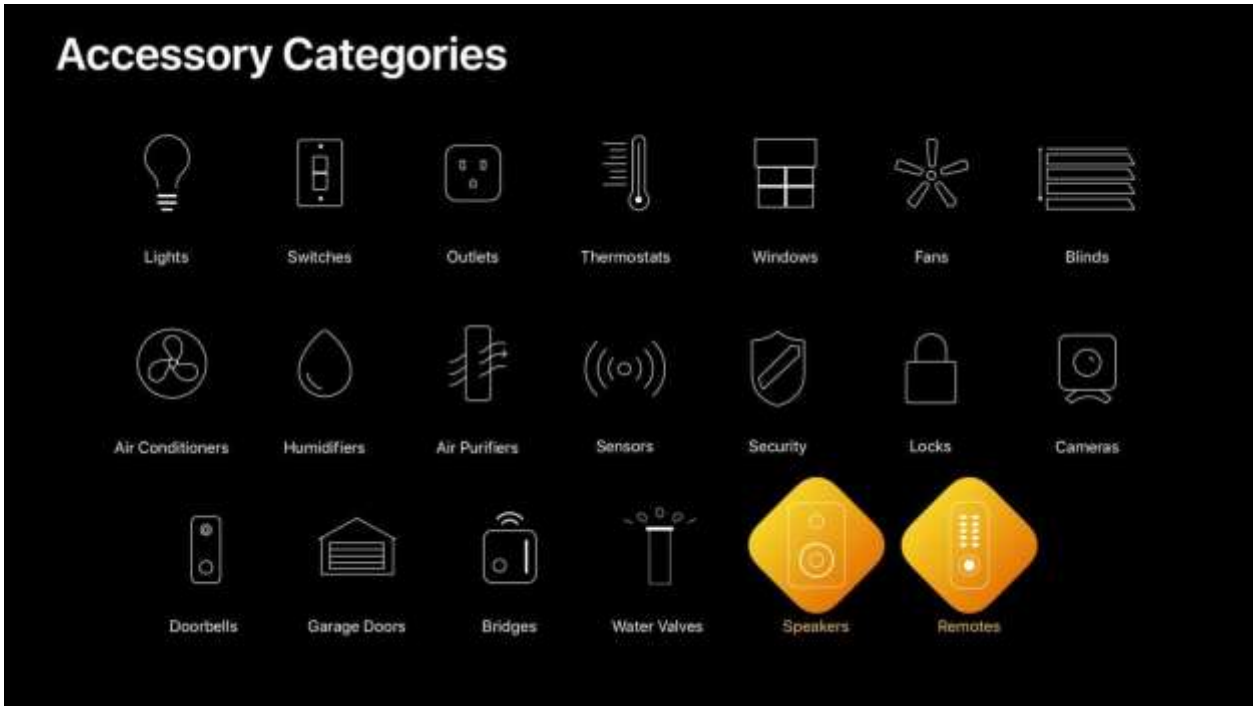


Рис. 3.8 Інтерфейс системи управління приміщення двоповерхової адміністративної будівлі, що стоїть окремо з урахуванням технології Інтернет речей

Налаштування системи відбувається наступним чином, варто додати будинок. За допомогою addHomeWithName: completionHandler: в HMHomeManager класі асинхронний метод. Ім'я будинку, передане як параметр для цього методу, має бути унікальним. Будинкові імена визнаються Siri.

```
[self.homeManager addHomeWithName:@"My Home" completionHandler:^(HMHome *home, NSError *error) {
    if (error != nil) {
        // Failed to add a home
    } else {
        // Successfully added a home
    }
}];
```

Потім варто додати кімнату до будинку, addRoomWithName:completionHandler: асинхронний метод. Назва приміщення, переданого як параметр для цього методу, має бути унікальним у будинку. Номери імен визнаються Siri.

```
    NSString *roomName = @"Living Room";
    [home addRoomWithName:roomName completionHandler:^(HMRoom *room, NSError *error) {
        if (error != nil) {
            // Failed to add a room to a home
        } else {
            // Successfully added a room to a home
        }
    }];
```

Наступний крок, це варто знайти аксесуари в будинку.

Необхідно додати протокол делегатів додаткового браузера та додати властивості браузера до інтерфейсу класу.

```
@interface EditHomeViewController () <HMAccessoryBrowserDelegate>

@property HMAccessoryBrowser *accessoryBrowser;

@end
```

Варто замінити EditHomeViewController на ім'я свого класу.

Створити об'єкт браузера додатка та встановити його делегат.

```
self.accessoryBrowser = [[HMAccessoryBrowser alloc] init];
self.accessoryBrowser.delegate = self;
```

знайти аксесуари.

```
[self.accessoryBrowser startSearchingForNewAccessories];
```

Додати знайдені аксесуари до своєї колекції.

```
- (void)accessoryBrowser:(HMAccessoryBrowser *)browser didFindNewAccessory:(HMAccessory *)accessory {
    // Update the UI per the new accessory; for example, reload a picker view.
    [self.accessoryPicker reloadAllComponents];
}
```

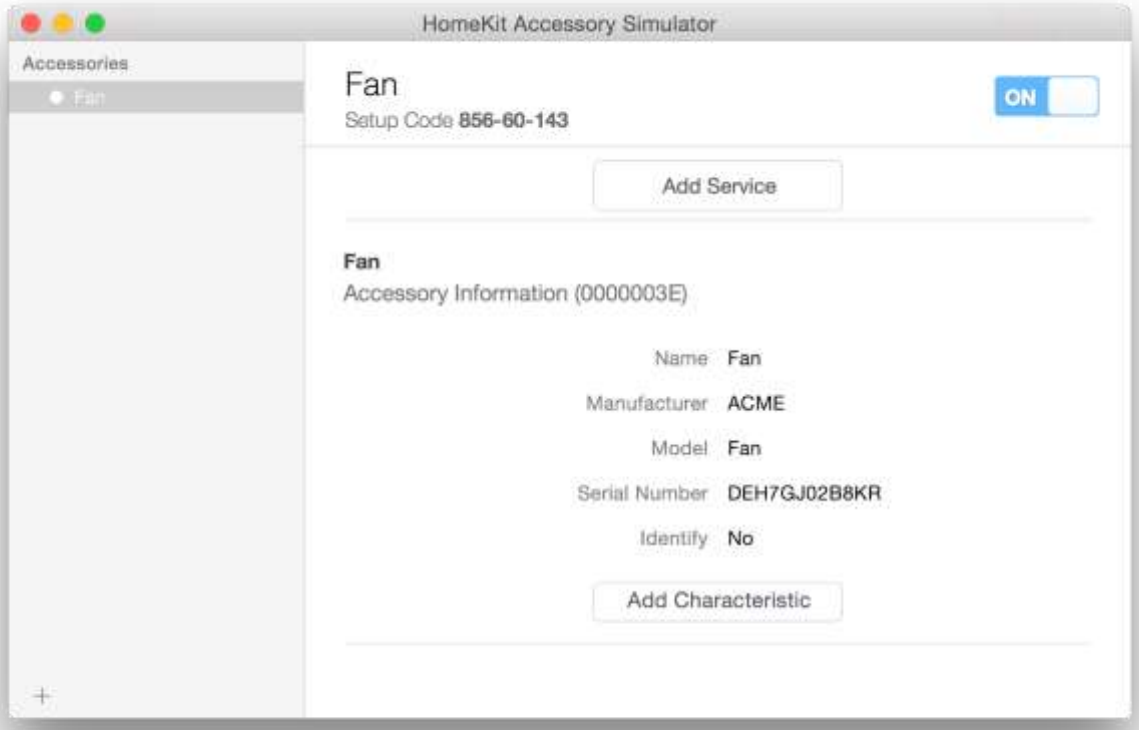


Рис. 3.9 Послуги для аксесуарів

Далі необхідно замінити наведену вище accessoryBrowser:didFindNewAccessory: реалізацію за допомогою коду. Крім того, застосувати accessoryBrowser:didRemoveNewAccessory: метод видалення аксесуара, який більше не є новим у колекції чи перегляді.

```
- (void)viewWillDisappear:(BOOL)animated {
    [self.accessoryBrowser stopSearchingForNewAccessories];
}
```

Зупинити пошук аксесуарів.

Якщо контролер перегляду починає шукати аксесуари, необхідно перевизначити, viewWillDisappear: щоб зупинити пошук аксесуарів.

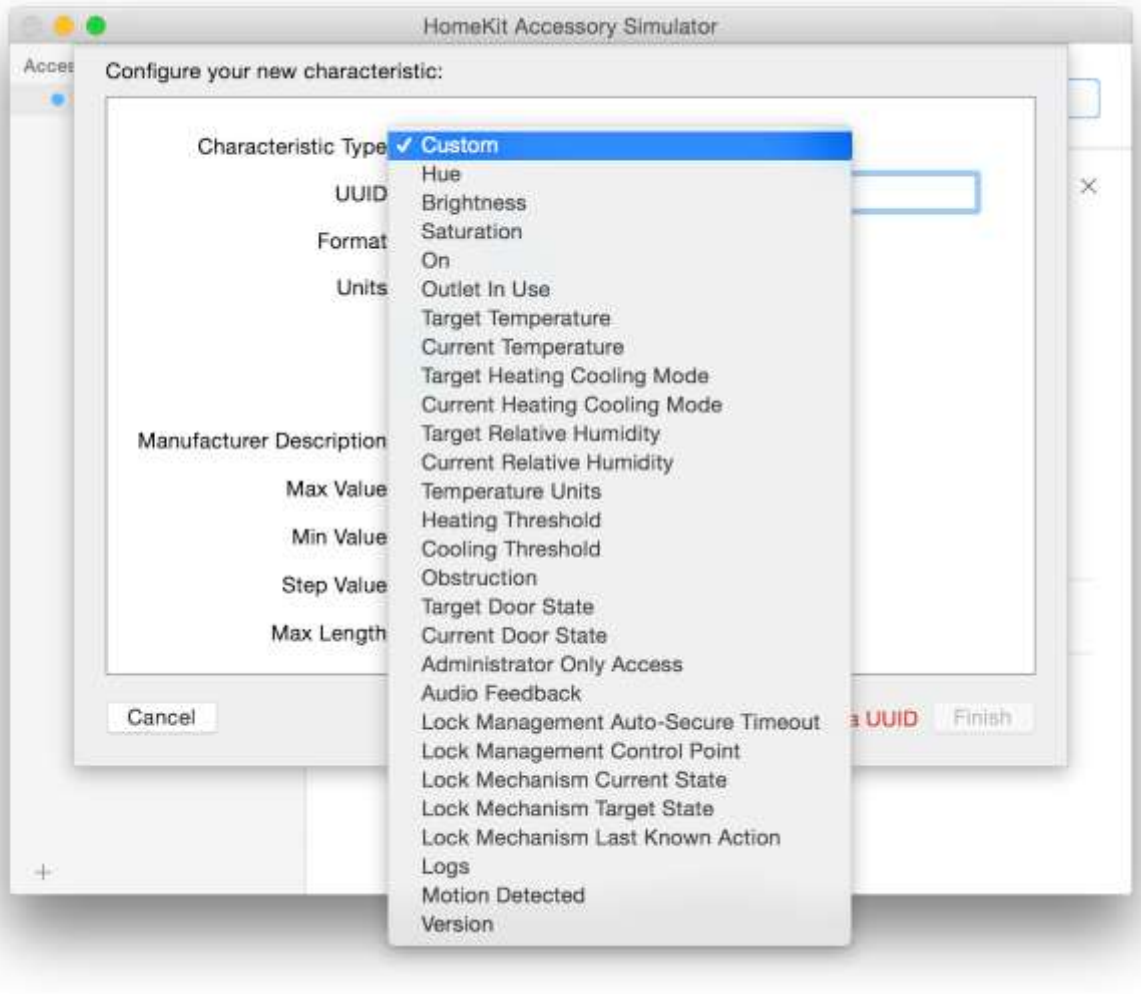


Рис. 3.10 Характеристики аксесуарів

Для управління аксесуарами

1. У Симуляторі аксесуарів Інтернет речей необхідно обрати аксесуар у стовпці "Аксесуари".

Послуги та їх характеристики відображаються на детальному екрані.

2. Необхідно маніпулювати елементом керування для характеристики, щоб змінити його значення.

Наприклад, щоб змінити тональність, насиченість та яскравість лампи, варто перемістити ручку відповідного слайдера. Щоб вимкнути лампочку, натиснути Ні на перемикачі On.

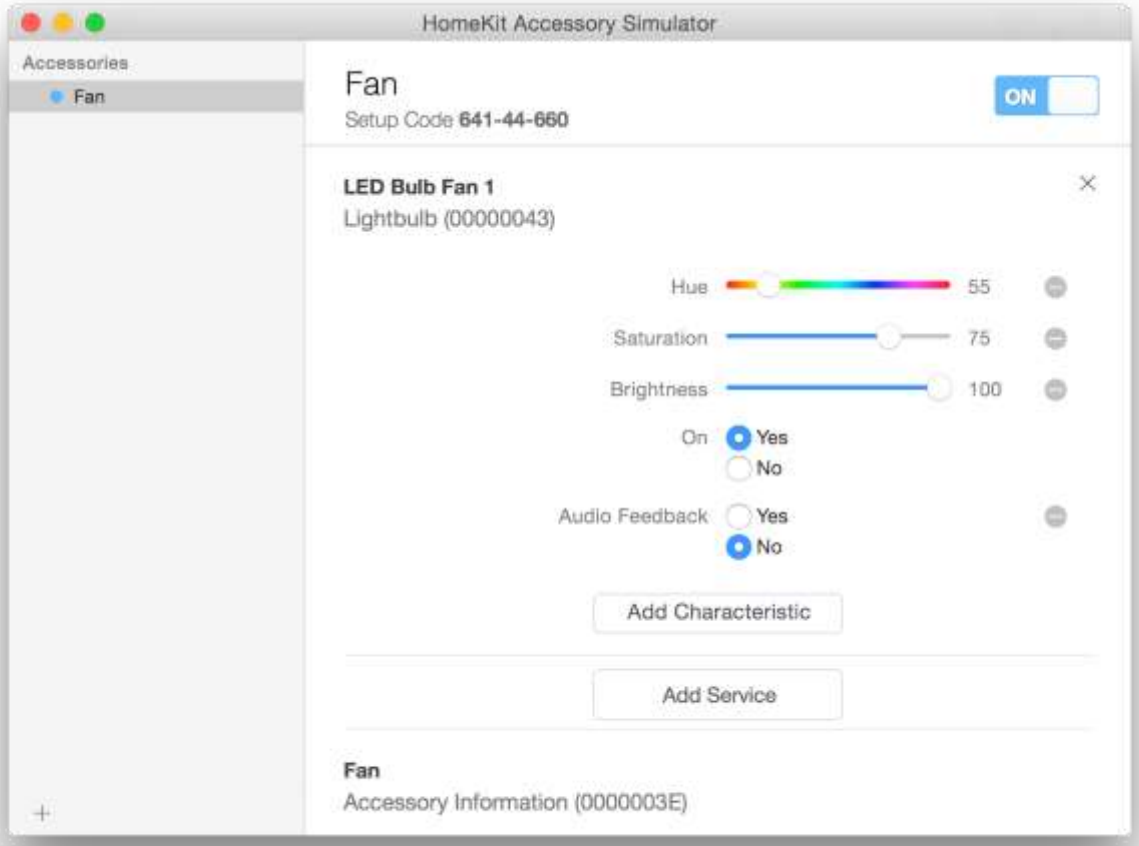


Рис. 3.11 Управління аксесуарами

Переваги створеної системи:

- охоплює всі процеси життєзабезпечення;
- відкрита гетерогенна архітектура;
- об'єднана розподілена база даних;
- інтерфейси між процесами;
- масштабовані рішення;
- модульна технологія, можливості для етапного впровадження;
- проста інтеграція існуючих і майбутніх систем і інтерфейсів;
- база управління, що настроюється;
- автоматизований аналіз подій;
- автоматичне управління аварійними ситуаціями.

3.3 Перспективи розвитку системи моніторингу комплексом аграрного призначення на базі інтернету речей

Здійснимо аналіз ефективності роботи системи комплексного моніторингу приміщень за допомогою технології Інтернет речей та порівняємо її з рівнем роботи системи комплексного моніторингу приміщень за допомогою технології Nest.

У якості параметрів досліджуються оцінки експертів щодо ефективності та параметри наведені у таблиці 3.4. Далі на основі отриманих даних проводиться математичний аналіз та здійснюється побудова діаграм та графіків для детального розуміння ефективності модернізації.

Таблиця 3.4 – Параметри звернень

Параметр	Опис	Можливі значення
$Е_ф$	Ефективність	5– надвисока,..., 0– низька
З	Зривання з'єднання	1– є з'єднання, 0– без з'єднання
$О_б$	обсяги даних на передачу	10– макс,..., 0– мінім.
$К_д$	категорії даних	1,2,3…n – категорія
$П_п$	пріоритет	1,2,3…n – пріоритет
$Р_{кін}$	кінцевий рівень вирішення	1,2,3,4 – рівні
П	продуктивність	0– відкритий, 1– закритий
К	коефіцієнт якості моніторингу	5– надвисокий, ..., 0– низький
$О_{клієн}$	оцінка клієнта	0,1,2,3,4,5

У табл. 3.4 показано параметри звернень, що надходять до системи комплексного моніторингу приміщень за допомогою технології Інтернет речей, їх опис та можливі значення.

Дані складемо таблицю значень отриманих при дослідженні системи комплексного моніторингу приміщень за допомогою технології Інтернет

речей та системи комплексного моніторингу приміщень за допомогою технології Nest, що прийняті до розгляду.

Таблиця 3.5 – Значення показників діяльності системи комплексного моніторингу приміщень за допомогою технології Інтернет речей

Параметр	Значення									
$Е_ф$	5	5	3	5	5	5	4	5	5	5
З	1	0	0	1	0	1	1	1	0	0
$О_б$	8	10	9	8	9	10	9	9	9	10
$К_д$	1	2	3	1	3	2	4	1	3	2
$П_п$	2	5	8	8	2	1	5	2	3	5
$Р_{кін}$	1	2	3	1	3	2	4	1	3	2
П	1	0	1	1	0	1	1	1	0	1
К	5	5	4	5	5	5	5	5	5	4
$О_{клієн}$	5	5	4	4	5	5	5	4	4	5

Таблиця 3.6 – Значення показників діяльності системи комплексного моніторингу приміщень за допомогою технології Nest

Параметр	Значення									
$Е_ф$	3	2	3	2	3	2	3	2	3	2
З	0	0	1	0	0	1	1	0	0	1
$О_б$	3	4	3	4	4	2	7	8	7	2
$К_д$	4	2	2	1	3	2	2	1	3	2
$П_п$	2	5	2	2	2	1	5	2	3	2
$Р_{кін}$	1	2	3	1	3	2	2	1	3	2
П	0	0	1	0	0	1	0	1	0	1
К	2	2	4	2	3	3	2	2	3	4
$О_{клієн}$	2	2	4	4	2	4	2	2	4	3

Відповідно до наведених даних здійснюємо аналіз отриманих даних. Розраховуємо середньоквадратичне відхилення та дисперсію, отримані результати наводимо у таблиці 3.7.

Таблиця 3.7 – Результати математичного аналізу

	Система комплексного моніторингу приміщень за допомогою технології Інтернет речей		Система комплексного моніторингу приміщень за допомогою технології Nest	
	Середне відхилення	Дисперсія	Середне відхилення	Дисперсія
$Е_ф$	0,48	0,41	0,5	0,25
З	0,5	0,25	0,48	0,24
$О_б$	0,54	0,49	1,4	3,16
$К_д$	0,84	0,96	0,68	0,76
$П_п$	2,1	5,69	1,04	1,64
$Р_{кін}$	0,84	0,96	0,6	0,6
П	0,42	0,21	0,48	0,24
К	0,32	0,16	0,7	0,61
$О_{клієн}$	0,48	0,24	0,9	0,89

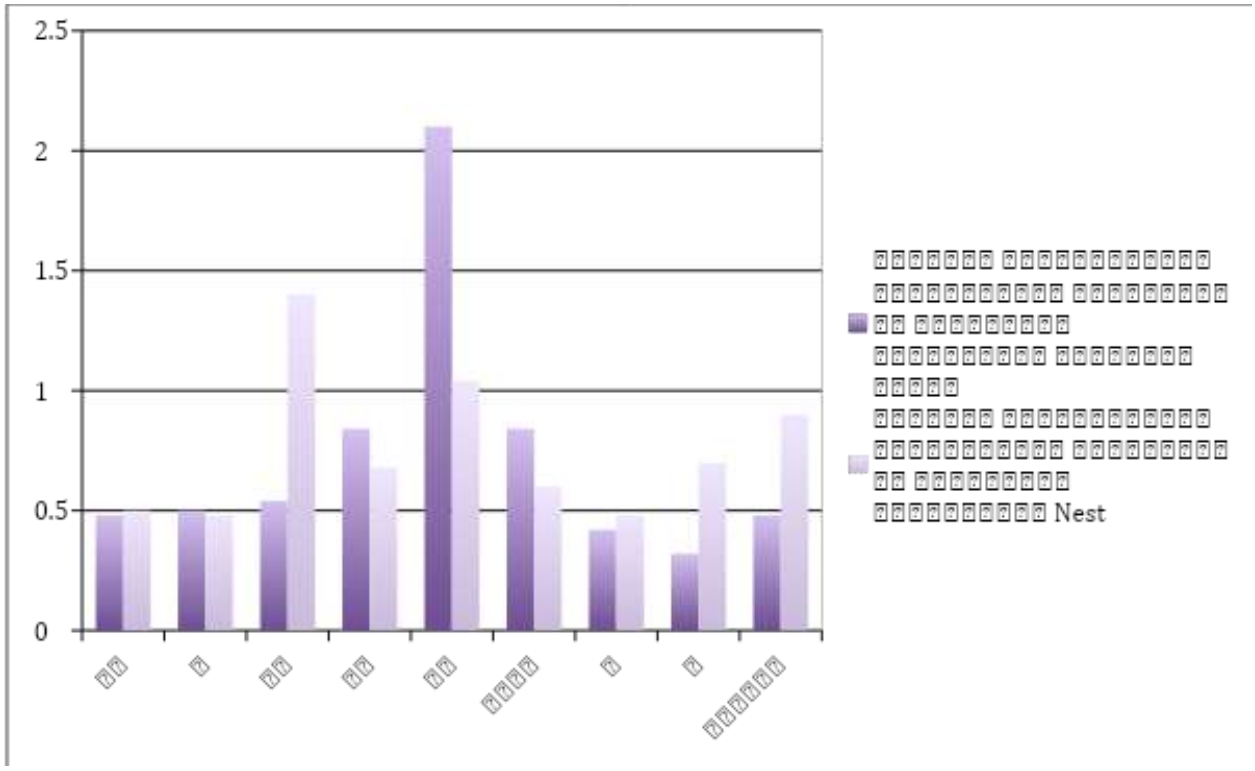


Рис. 3.12 Результати математичного аналізу

Наступним кроком є кореляційний аналіз. Результати у таблиці 3.8.

Таблиця 3.8 – Кореляційний аналіз отриманих результатів системи комплексного моніторингу приміщень за допомогою технології Інтернет речей

	1									
	0,910697	1								
	0,607393	0,868558	1							
	0,728198	0,881269	0,898442	1						
	0,832953	0,894452	0,728182	0,597219	1					
	0,962961	0,885368	0,582819	0,608258	0,911505	1				
	0,748442	0,921121	0,857917	0,766199	0,880287	0,751921	1			
	1	0,910697	0,607393	0,728198	0,832953	0,962961	0,748442	1		
	0,864767	0,937469	0,785538	0,693577	0,966478	0,906413	0,941068	0,864767	1	
н	0,902829	0,985091	0,867125	0,874907	0,891533	0,884572	0,861267	0,902829	0,902937	1
	$Е_ф$	З	$О_б$	$К_д$	$П_п$	$Р_{кін}$	П	К	$О_{клієн}$	

Таблиця 3.9 – Кореляційний аналіз отриманих результатів системи комплексного моніторингу приміщень за допомогою технології Nest

	1									
	0,805432	1								
	0,739299	0,372583	1							
	0,90632	0,638242	0,754777	1						
	0,805627	0,653376	0,704907	0,632027	1					
	0,575396	0,206284	0,810931	0,562544	0,83666	1				
	0,833108	0,887345	0,295395	0,689483	0,662037	0,235702	1			
	0,775107	0,597659	0,355539	0,736969	0,610845	0,359908	0,848311	1		
	0,768293	0,759345	0,670169	0,677048	0,864638	0,704203	0,618661	0,405517	1	
и	0,605302	0,324185	0,887125	0,565801	0,55814	0,628619	0,148167	0,168068	0,494416	
	$Е_ф$	З	$О_б$	$К_д$	$П_п$	$Р_{кін}$	П	К	$О_{клієн}$	

Таким чином, на основі проведеного математичного аналізу ефективності системи комплексного моніторингу приміщень за допомогою технології Інтернет речей та системи комплексного моніторингу приміщень за допомогою технології Nest, та використовуючи шкалу Чеддока [7– 9], можна зробити висновок, що найбільш впливають на ефективність такі чинники:

Для системи комплексного моніторингу приміщень за допомогою технології Інтернет речей:

- Ефективність ($Е_ф$),
- Пріоритет ($П_п$)
- Категорія даних ($К_д$)
- Коефіцієнт якості моніторингу (К)
- Оцінка клієнта ($О_{клієн}$)

Для системи комплексного моніторингу приміщень за допомогою технології Nest:

- Ефективність ($Е_ф$),
- Обсяги даних ($О_б$)
- Категорія даних ($К_д$)
- Кінцевий рівень вирішення ($Р_{кін}$)

Далі проведемо графічне порівняння двох систем комплексного моніторингу приміщень за основними показниками для виявлення найбільш ефективної та досконалої системи комплексного моніторингу приміщень.

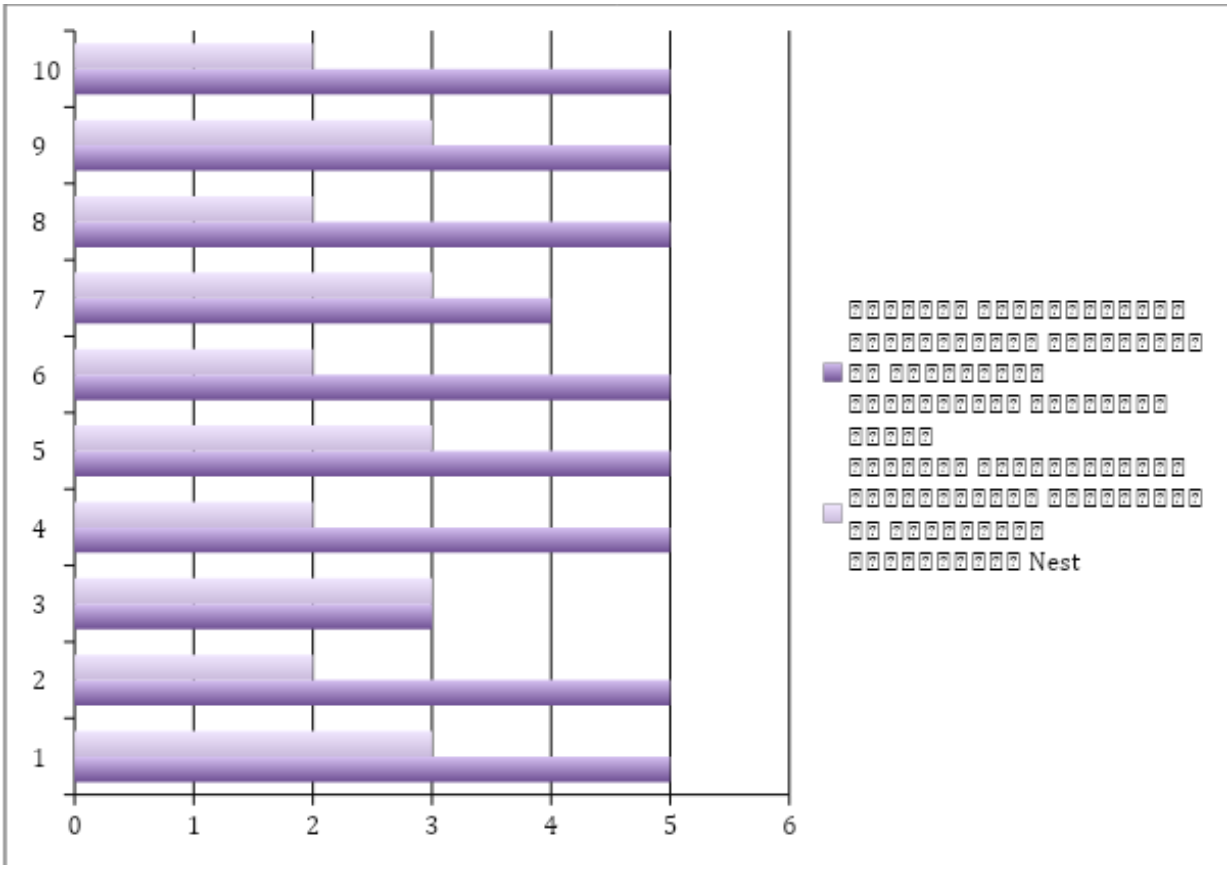


Рис. 3.13. Графік ефективності систем комплексного моніторингу приміщень

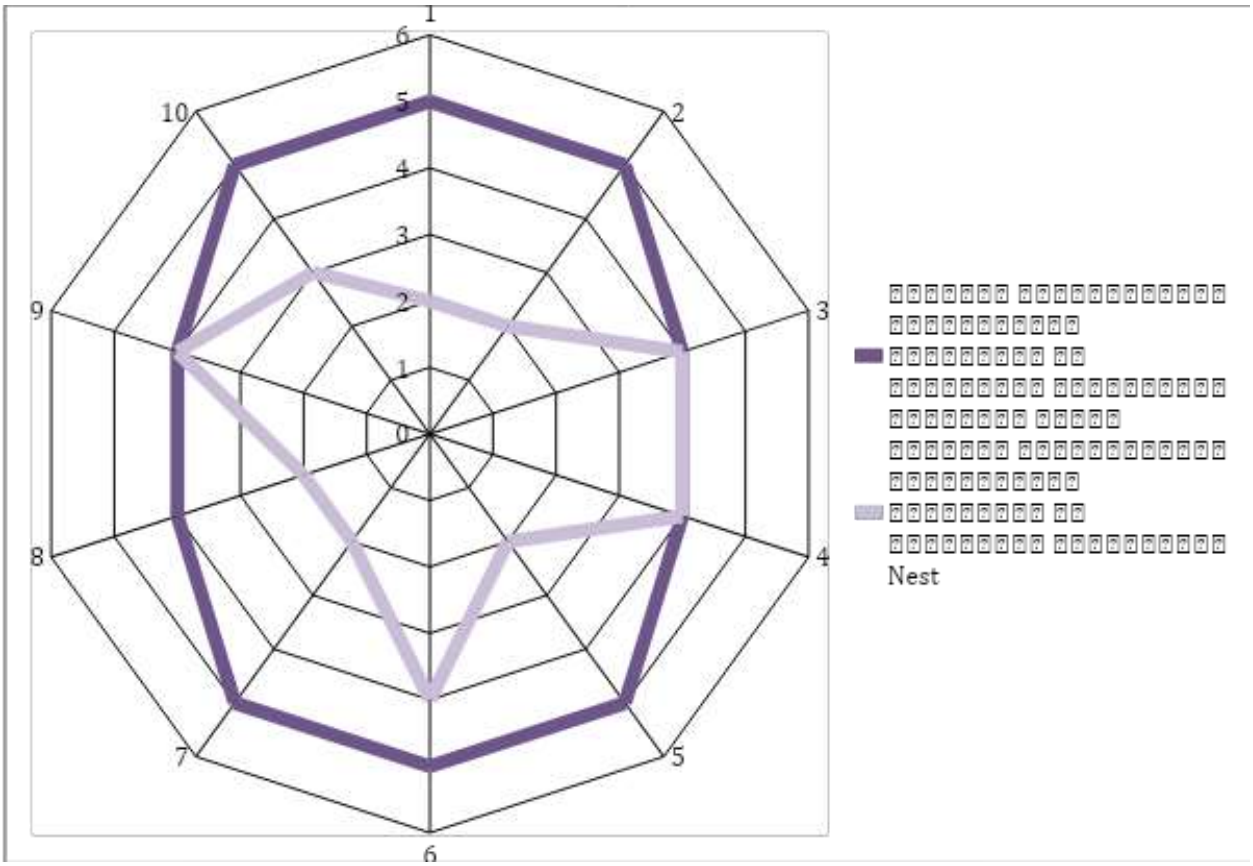


Рис. 3.14. Графік оцінки систем комплексного моніторингу приміщень

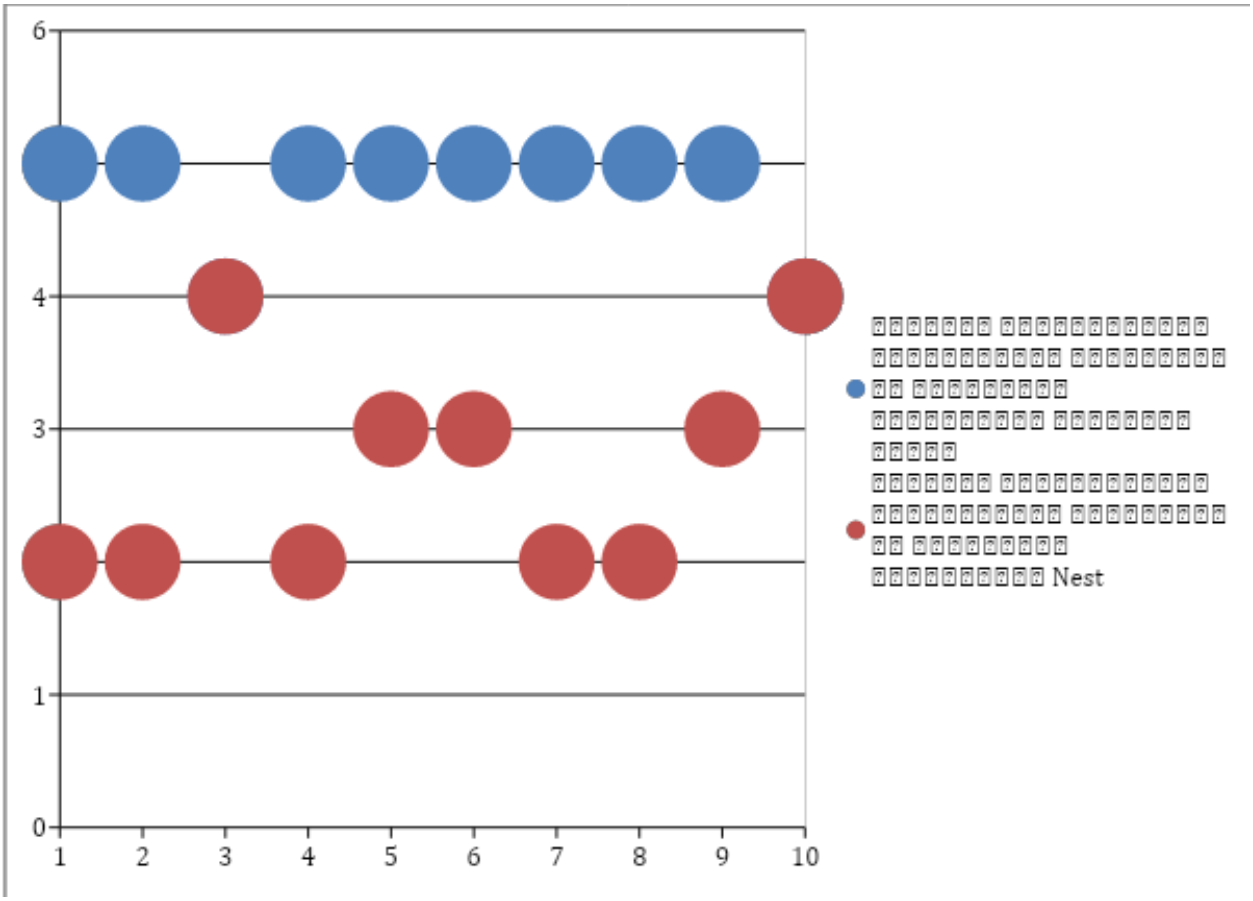


Рис. 3.15. Графік коефіцієнта якості систем комплексного моніторингу приміщень

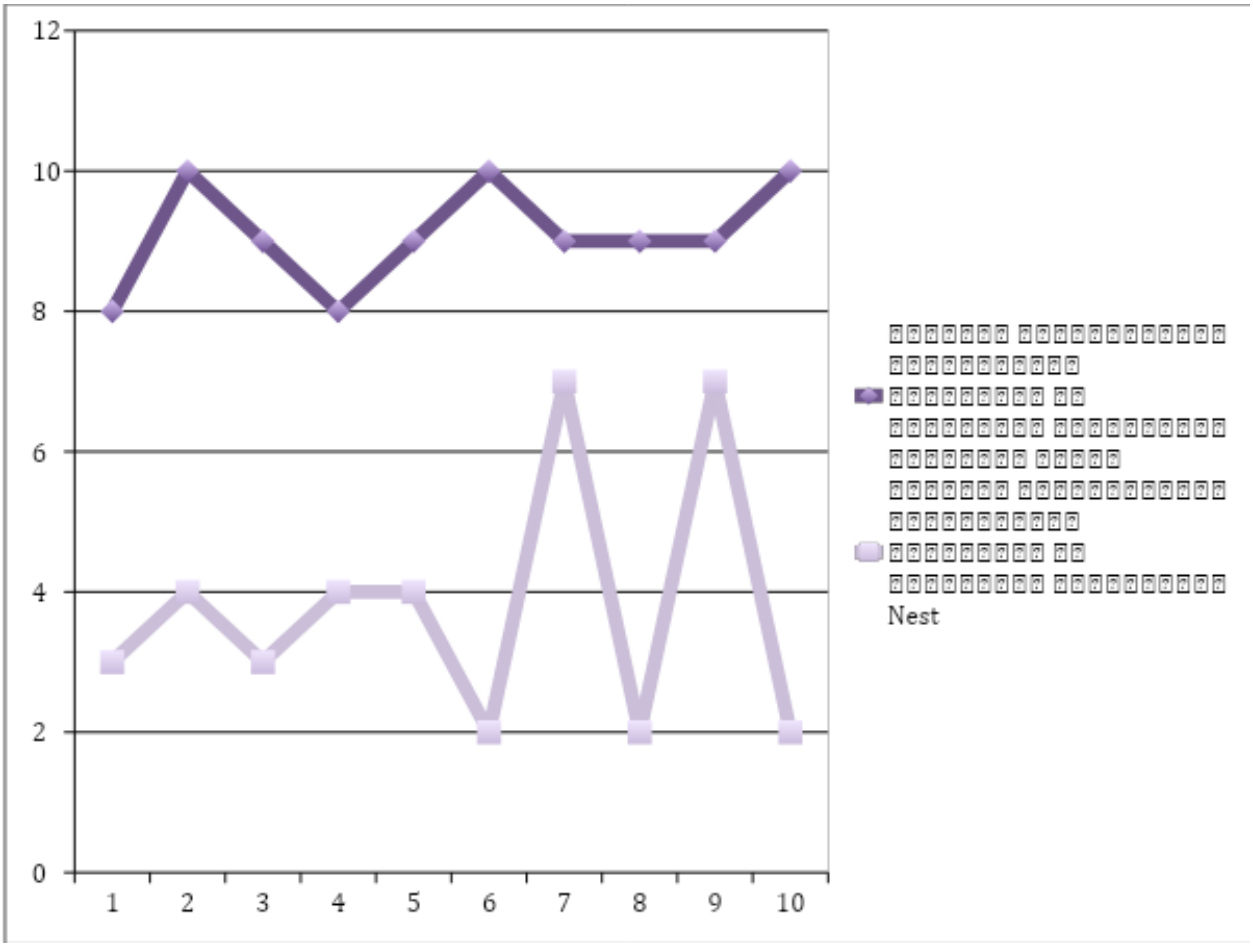


Рис. 3.16. Графік продуктивності систем комплексного моніторингу приміщень

Згідно до проведеного дослідження варто відзначити, що система комплексного моніторингу приміщень за допомогою технології Інтернет речей за всіма показниками перевершує систему комплексного моніторингу приміщень за допомогою технології Nest, що говорить про високу якість системи комплексного моніторингу приміщень та можливість впровадження її в реальну роботу за потребою.

Висновки до розділу

У рамках третього розділу розкрито інноваційні механізми застосування систем комплексного моніторингу приміщень за допомогою технології Інтернет речей.

Система управління приміщенням з урахуванням технології Інтернет речей призначена для забезпечення комфортних умов, захисту матеріальних цінностей, людей, що знаходяться в приміщенні, що захищається, забезпечує виконання наступних функцій:

- виявлення тривожних / аварійних ситуацій (несанкціоноване проникнення, пожежа, витік води), формування сигналів тривог;
- підтримку заданої температури;
- видачу інформації про наявність і місце виникнення тривожної / аварійних ситуацій на пульт сигналізації і зовнішній світлозвуковий оповіщувач;
- аварійне перекриття кульових кранів подачі гарячої та холодної води;
- автоматичний контроль стану елементів системи і її складових частин;
- доставку повідомлення про тривожну / аварійну ситуацію в охоронні структури через термінал;
- доставку повідомлення про тривожну / аварійну ситуацію, інших подій дзвоном і за допомогою SMS власнику і / або в охоронні структури.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

Дана дипломна робота передбачає розробку системи моніторингу комплексом аграрного призначення на базі Інтернету речей.

Відповідно до вимог Міждержавного стандарту ГОСТ 12.0.003-74 (1999) ССБП "Небезпечні й шкідливі виробничі фактори. Класифікація", небезпечні та шкідливі виробничі фактори поділяються по своїй природі дії на наступні групи: фізичні, хімічні, біологічні, психофізіологічні.

Метою частини даної дипломної роботи з охорони праці є визначення впливу мікроклімату і шумів в приміщенні на роботу персоналу працюючого у інформаційному центрі.

Поняття «Охорона праці» означає систему законодавчих актів, соціально-економічних, організаційних, технічних і лікувально-профілактичних заходів і засобів, що забезпечують безпеку, збереження здоров'я і працездатності людини в процесі праці.

Одним із законодавчих актів з охорони праці, є Конституція України, де вказано, що: «Кожен має право на належні, безпечні і здорові умови праці...».

Безпечна робота за комп'ютером передбачає виконання ряду правил, недотримання яких може призвести до небажаних наслідків, тому важливим є визначити порядок роботи за комп'ютером інженера-програміста.

Дана дипломна робота передбачає розробку системи моніторингу комплексом аграрного призначення на базі Інтернету речей.

Метою частини даної дипломної роботи з охорони праці є визначення впливу мікроклімату і шумів в приміщенні на роботу персоналу працюючого у інформаційному центрі.

4.1 Аналіз умов праці

4.1.1 Організація робочого місця

Зазначена розробка здійснюється в приміщеннях типу обчислювальних центрів, з використанням техніки, дані про яку зведені до табл. 4.1. До використовуваних приміщень висуваються певні вимоги по техніці безпеки та охороні праці на робочих місцях.

Безпечна робота за комп'ютером передбачає виконання ряду правил, недотримання яких може призвести до небажаних наслідків, тому важливим є визначити порядок роботи за комп'ютером інженера-програміста.

Площа приміщення інформаційного центру – S заг. = 20 м^2

Таблиця 4.1 – Характеристика офісної техніки застосованої в приміщеннях типу обчислювальних центрів

	Потужність	Напруга	Частота
Монітор з діагоналлю не менше 15”	130 Вт	220 В	не менше 85 Гц
Системний блок	300 Вт	220 В	50 Гц
Сканер (формат паперу А4)	20 Вт	220 В	50 Гц
Принтер (формат паперу А4)	60 Вт	220 В	50 Гц

Виходячи з того, що обчислювальний центр має відносно невелику площу робочих приміщень, систему кондиціювання повітря для відведення тепла від ЕОМ, розгалужену електромережу для живлення комп’ютерів і периферійної техніки, користувачі системи можуть під час роботи потрапляти під дію несприятливих виробничих факторів, перелік яких наведений у табл. 4.2, а шкідливі виробничі фактори зведені у таблицю 4.3.

Таблиця 4.2 – Небезпечні виробничі фактори

№ п/п	Небезпечний фактор	Джерело та причина появи небезпечного фактору	Характеристика
1	Ураження електричним струмом	Порушення електроізоляції обладнання(системний блок, монітор)	Y = 50 Гц V = 220 В I = 0,1 А P = 200-250 Вт
2	Виникнення пожежі	Несправність електромережі (ЕОМ, зовнішні пристрої)	Підвищення температури, ступінь

			вогнестійкості II, категорія В
3	Статична електрика (ЕОМ)	ЕОМ	$E \leq 5$ В/м $R \leq 10^6$ Ом

Таблиця 4.3 – Шкідливі виробничі фактори.

№ п/п	Шкідливі фактори	Джерело шкідливого фактору	Характеристика
1	2	3	4
1	Шум (для операторів ПК)	Принтер, системний блок	Рівень звуку $L \leq 65$ дБа
2	Несприятливий мікроклімат приміщення (категорія легка1)	Теплодіючі прилади: монітор	Оптимальні умови: В холодний і перехідний період: t = 22-24ºС, відносна вологість W = 40-60 %, швидкість руху повітря V = 0,1 м/с, в теплий період: 23-25ºС, t = 22-24ºС, відносна вологість W = 40-60 %, швидкість руху повітря V = 0,1 м/с
3	Електромагнітне випромінювання	Монітор	$E < 10$ В/м $H \leq 0.3$ А/м Припустимі рівні напруги 220 кВ протягом 1 години. Частота рівня магнітного поля 50 Гц
4	Недостатнє освітлення (клас високої точності)	Освітлювальні прилади	Рівень освітленості N=500Лк.Природне освітлення-4 пояс>1,68% Комб. освітлення-1,5%

На рисунку. 4.1. показана схема розташування робочих місць, джерел штучного та природного освітлення робочої зони.

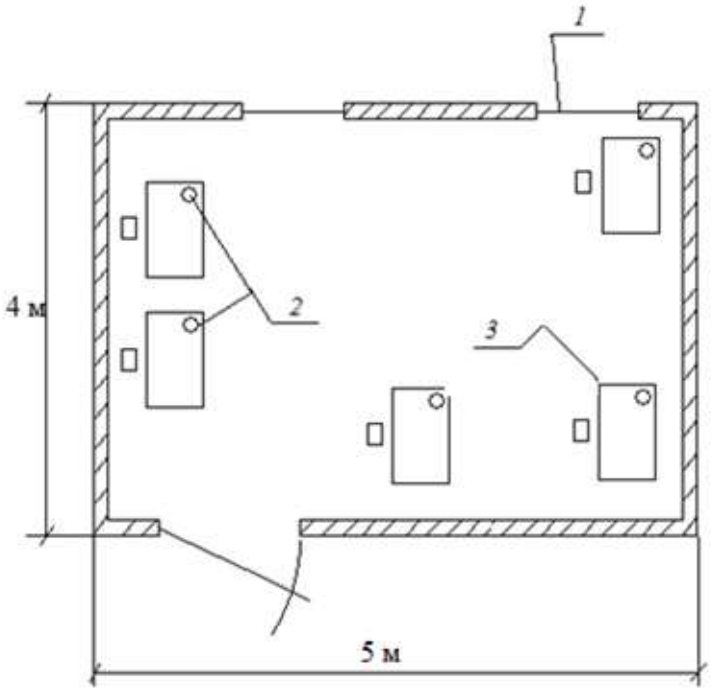


Рисунок 4.1 – Схема приміщення

1 – Вікно

2 – Лампа освітлення

3 – робоче місце

4.1.2 Мікроклімат приміщення

Організм людини постійно перебуває в стані теплового обміну з навколишнім середовищем. Основну роль у цьому процесі відіграє система терморегуляції людини, вона регулює теплообмін організму з навколишнім середовищем.

Значне коливання параметрів мікроклімату призводить до порушення терморегуляції організму, тобто здатності організму підтримувати постійну температуру тіла. Це призводить до порушення систем кровообігу, нервової та системи потовиділення, що може викликати підвищення або пониження температури тіла, слабкість, запаморочення [6].

На сьогоднішній день, для забезпечення оптимальних мікрокліматичних умов в будь-який період року приміщення, в яких розташовані комп’ютеризовані робочі місця обладнують кондиціонерами, які автоматично

підтримують задані параметри мікроклімату. Документ, який регулює це ДСН 3.3.6.42-99.

Обчислювальний центр в якому проводиться розробка має загальний розмір 5х4м., висота стелі 3 м., є три вікна розміром 1,2 х 1,5 м. В даному приміщенні знаходиться комп'ютер, сканер і 1 принтер. Температура повітря в кімнаті тримається рамок 23-24 °С, вологість не перевищує 50%, що задовольняє санітарним нормам мікроклімату виробничих приміщень.

Проведемо розрахунок сумарного надходження тепла до приміщення за для визначення кондиціонера необхідної потужності.

Обрана модель повинна давати таку саму, або навіть дещо вищу потужність.

Процедура розрахунків:

1) Розрахуємо надходження тепла в приміщення за формулою:

$$T_1 = S \cdot h \cdot k \qquad (4.1)$$

де S – площа приміщення S = 5*4=20 м^2;

h – висота приміщення, h = 3 м;

k – коефіцієнт, що дорівнює k = 35, оскільки сонце попадає до кімнати лише частину світлового дня.

$$T_1 = 20 \cdot 3 \cdot 35 = 2100\ Вт$$

2) Розрахуємо надходження тепла від оргтехніки.

Системний блок – 300 Вт;

Монітор – 130 Вт;

Принтер – 60 Вт;

Сканер – 60 Вт;

Лампа освітлення – 40 Вт.

$$T_2 = Q_1 + Q_2 + \cdots + Q_n \qquad (4.2)$$

де n – кількість приладів.

$$T_2 = 300 + 130 + 60 + 60 + 5 * 40 = 750\ Вт$$

3) Розрахуємо кількість тепла яке надходить від юдей, що постійно знаходяться в приміщенні:

$$T_3 = n_1 \cdot T_{сер} \quad (4.3)$$

де n_1 – кількість людей, $n_1 = 4$;

$T_{сер}$ – середнє виділення тепла людиною. В нашому випадку $T_{сер} = 100$ Вт, оскільки розрахунок проводиться для офісу.

$$T_3 = 4 \cdot 100 = 400\ Вт$$

4) Загальне надходження тепла:

$$T_{заг} = T_1 + T_2 + T_3 \quad (4.4)$$

$$T_{заг} = 2100 + 750 + 400 = 3250\ Вт$$

Прийнято встановлювати кондиціонер потужність якого або дорівнює, або перевищує отриману шляхом розрахунків величину.

Загальна площа приміщення складає 20 м^2, обираємо настінний кондиціонер Daikin FTY35, який має потужність 3,5 кВт, що дозволяє прохолоджувати приміщення площею до 35 м^2.

4.1.3 Шкідливі речовини в повітрі робочої зони

Шкідливі речовини - це речовини, що при контакті з організмом людини за умов порушення вимог безпеки можуть повести виробничої травми, професійного захворювання або розладів у стані здоров'я, які визначається сучасними методами як у процесі праці, так і у віддалені строки життя теперішнього і наступних поколінь. Шкідливі речовини у повітря робочої зони поступають у вигляді пару, газів та пилу. Вплив на організм людини залежить від хімічного складу, розміру (дисперсності), форми часток та їх кількості у одиниці об’єму.

Згідно ГОСТ 12.1.005-88 більшість шкідливих речовин має гостро направлений механізм дії. За концентрацією таких речовин повинен бути забезпечений безперечний контроль із сигналізацією на перевищення ГДК. До їх числа серед інших відносяться оксиди азоту, бром, хлор, ртуть та інші. В рядку "Особливості дії на організм" списків ГДК поряд з величиною нормативу стоїть літера "Г".

В залежності від ступеня небезпеки шкідливі речовини поділяються на 4 класи:

1 - надзвичайно небезпечні(ртуть, свинець, озон, фосген)

2 – високо небезпечні (оксид азоту, бензол, йод, хлор та інші)

3 - помірно небезпечні (метиловий спирт, ацетон, ксилол та інші) 4- мало небезпечні (аміак, бензин, етиловий спирт, окис вуглецю та інші)

Слід мати на увазі, що малонебезпечні речовини через тривалу д по і великі концентрації можуть призвести до таких отруєнь.

4.1.4 Виробниче освітлення

Відповідно до ДБН В.2.5-28:2018 “Природне і штучне освітлення” [3], характеристика зорової роботи на даних робочих місцях дуже високої точності (найменший розмір об’єкта розпізнавання – 0,15-0,3 мм). Освітлення в лабораторії природне і штучне загальне. Рівень освітленості на робочому

столі має бути 300-500 лк. Стіни і стеля – світлі, білого кольору з високим коефіцієнтом відбиття.

Природне освітлення бокове однобічне, здійснюється за допомогою вікон. Площа вікон у приміщенні складає $S_ф = 10{,}44\ м^2$, тоді як розрахована необхідна площа складає $S_B = 12{,}6\ м^2$. Отже, в приміщенні не вистачає природнього світла для забезпечення вимог згідно [3], і необхідне використання комбінованого освітлення.

Аналіз штучного освітлення

Для освітлення приміщень з ПК необхідно використовувати люмінесцентні світильники. Освітленість робочого місця у горизонтальній площині на висоті 0,8 м від підлоги повинна бути не менше 400 лк. Вертикальна освітленість у площині екрану не більше 300 лк. Робоче місце з дисплеєм необхідно розташовувати таким чином, щоб до поля зору не потрапляли вікна та освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90 - 105 градусів до вікон та на відстані, не меншій 2,5 - 3 м від стіни з вікнами.

Приміщення обладнано 16 світильниками типу ЛПО-71 4х18. Фактична освітленість складає $E_ф = 452\ лк$. Нормована складає $E_H = 300 - 500\ лк$. Отже, штучне освітлення задовольняє вимогам нормативної документації.

Проводиться очистка скла вікон та світильників не рідше одного разу на рік, а також замінюються перегорілі лампи у міру їх виходу з ладу.

Для збереження зору працівників необхідно робити невеликі перерви, щоб дати очам відпочити.

4.1.5 Шум, вібрація ультразвук, інфразвук

Згідно ДСН 3.3.6.037-99, шум – це будь-який небажаний звук, якій наносить шкоду здоров'ю людини, знижує його працездатність, а також може сприяти отриманню травми в наслідок зниження сприйняття попереджувальних сигналів.

Інфразвук - є невідчутна для людини ділянкою коливань. Верхньою його межею вважають частоти 16-25Гц. Нижня межа не визначена. Коливання інфразвукових частот виникають у деякому виробництві й на транспорті. Вони утворюються під час роботи компресорів, двигунів внутрішнього згоряння, великих вентиляторів, руху локомотивів та автомобілів.

Ультразвук - високочастотні коливання. Ультразвуковий діапазон частот поділяється на низькочастотний (1000 – 10000Гц), коли хвилі поширюються повітряними і контактними шляхами та високочастотний (10000 – 1´109Гц), коли хвилі передаються тільки контактними шляхами.

Ультразвук широко застосовують в техніці для диспергування рідин, очищення частин, зварювання пластмас, дефектоскопії металів, очищення газів від шкідливих домішок тощо.

Вібрація - це механічні коливання пружних тіл або коливальні рухи механічних систем. Для людини вібрація є видом механічного впливу, який має негативні наслідки для організму. Причиною появи вібрації є неврівноважені сили та ударні процеси в діючих механізмах.

На робочому місці використовуються прилади в яких рівень шуму та вібрації не перевищують гранично допустимих норм.

4.1.6 Захист від електромагнітних полів, іонізуючих і лазерних випромінювань

Потенційно, джерелами слабкого іонізуючого випромінювання є ЕПТ-монітори. Але дані робочі місця обладнані сучасним LCD-моніторами, що не генерують іонізуючого випромінювання.

Рівень електромагнітних полів, що виникають при роботі ЕОМ є достатньо малим, отже ним можна знехтувати.

Джерела лазерного випромінювання, доступні для робітників – відсутні.

4.1.7 Небезпека ураження електричним струмом

Відповідно до [7], за ступенем небезпеки враження електрострумом приміщення відноситься до приміщення без підвищеної небезпеки. У приміщення проведено однофазне електроживлення напругою 220 В, частотою 50 Гц та з максимальним струмом у 32 А.

Електропроводка як відкрита, так і схована. Використовується розміщений в приміщенні груповий щиток. До щитка підключаються електроустановки, кабелі та проводи з мідними жилами з діаметром розрізу не менше 2,5 мм^2.

Використовуються наступні технічні заходи забезпечення електробезпеки:

- для закритої проводки – недоступність струмопровідних частин;
- для відкритої проводки – пластмасові короби з важкогорючих матеріалів з помірною димоутворювальною здатністю;
- робоча ізоляція струмопровідних частин;
- при підключенні електричного роз’єму до електричної мережі гарантується з’єднання корпусу з заземленням.

4.1.8 Статична електрика

Згідно ДСТУ 7302:2013 “Статична електрика. Терміни та визначення основних понять”:

Статична електрика – особливий вид зарядів, що виникають при терті двох діелектриків або діелектрика і провідника.

Систематичний вплив статичної електрики на тіло людини викликає порушення фізіологічних процесів, функціональні розлади центральної нервової системи, органів кровообігу.

4.2 Розробка заходів з охорони праці

4.2.1 Захист від виробничого шуму та вібрацій

Шум - сукупність звуків різної інтенсивності і частоти. Під шумом розуміють усі неприємні та небажані звуки чи їх сукупність, які заважають нормально працювати, сприймати потрібні звукові сигнали, відпочивати. Шум підвищує втомленість робітника, знижує його працездатність і увагу до небезпеки. Шум як стрес-чинник є загально біологічним подразником, негативно впливає на всі органи і системи організму. В разі тривалого систематичного впливу шуму може виникнути патологія з переважним ураженням слуху, центральної нервової і серцевосудинної систем. Вплив шуму на організм умовно поділяють на специфічний, що спричиняє зміни в органі слуху, і не специфічний - з боку інших органів і систем. Шум є однією з найбільш частих причин зниження слуху.

Основними методами боротьби з виробничим шумом і вібрацією є:

– зменшення шуму в джерелі;

– звукопоглинання і вібропоглинання;

– звукоізоляція і віброізоляція;

– акустична обробка приміщень;

– зменшення шуму на шляху його поширення;

– раціональне планування підприємства і цехів;

– установка глушників шуму;

– вживання засобів індивідуального захисту.

Гранично припустимі значення вібрацій (11-2800 Гц) при роботі з інструментами, механізмами та й устаткуванням, що безупинно впливають на працюючих протягом робочого дня (8 годин).

4.2.2 Електробезпека

Електробезпека — це система організаційних та технічних заходів і засобів, що забезпечують захист людей від шкідливого та небезпечного

впливу електричного струму, електричної дуги, електромагнітного поля і статичної електрики.

Аналіз виробничого травматизму показує, що кількість травм, які спричинені дією електричного струму є незначною і складає близько 1%, однак із загальної кількості смертельних нещасних випадків частка електротравм вже складає 20—40% і займає одне з перших місць.

З метою зменшення небезпечного впливу електричного струму і ефективного виконання прямих службових обов'язків працівник ОВС повинен орієнтуватися, у яких місцях він може зустріти небезпечну напругу.

Величини напруги залежать від робочого устаткування:

- до 42 В — напруга використовується для індивідуального освітлення і ручних електроінструментів при роботі в небезпечних зонах;
- 127, 220 В — напруга використовується для освітлення і ручного інструмента на виробництві й у побуті;
- 380 В — напруга використовується при експлуатації промислових установок;
- понад 380 В — напруга використовується для передачі електроенергії на відстань (лініями електропередач — ЛЕП).

4.3 Пожежна безпека

Пожежі в обчислювальних центрах (ОЦ) становлять особливу небезпеку, тому що пов'язані з великими матеріальними втратами. Характерна риса ОЦ - невеликі площі приміщень. Як відомо пожежа може виникнути при взаємодії горючих речовин, окиснення й джерел запалювання. У приміщеннях ОЦ присутні всі три основні фактори, необхідні для виникнення пожежі.

Горючими компонентами на ОЦ є : персональна ЕОМ, принтер, дисплей, меблі, книги, документи, ізоляція кабелів і ін.

Джерелами запалювання в ОЦ можуть бути електронні схеми від ЕОМ, прилади, що застосовуються для технічного обслуговування,

обладнання електроживлення, кондиціювання повітря, де в результаті різних порушень утворюються перегріті елементи, електричні іскри й дуги, здатні спричинити загоряння горючих матеріалів.

Згідно НАПБ Б.03.002-2007. Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою [5] приміщення які містять ЕОМ належать до категорії «В».

Одним з найбільш важливих завдань протипожежного захисту є захист будівельних приміщень від руйнувань і забезпечення їх достатньої міцності в умовах впливу високих температур при пожежі. Враховуючи високу вартість електронного обладнання ОЦ, а також категорію його пожежної небезпеки, будівля для ОЦ і частини будівлі іншого призначення, у яких передбачено розміщення ЕОМ, повинні бути 1 і 2 ступеня вогнестійкості.

Для виявлення початкової стадії загоряння й оповіщення служби пожежної охорони використовують системи автоматичної пожежної сигналізації (АПС). Крім того, вони можуть самостійно пускати в хід установки пожежогасіння, коли пожежа ще не досягла великих розмірів. Системи АПС складаються з пожежних оповіщувачів, ліній зв'язку й приймальних пультів (станцій).

Ефективність застосування систем АПС визначається правильним вибором типу оповіщувачів і місць їх установки . При виборі пожежних оповіщувачів необхідно враховувати конкретні умови їх експлуатації: особливості приміщення й повітряного середовища, наявність пожежних матеріалів, характер можливого горіння, специфіку технологічного процесу й т.п.

До засобів гасіння пожежі, призначених для локалізації невеликих загорянь, належать пожежні стовбури, внутрішні пожежні водопроводи, вогнегасники, сухий пісок, азбестові ковдри й т.п..

Газові вогнегасники застосовуються для гасіння рідких і твердих речовин, а також електроустановок, що перебувають під напругою.

У виробничих приміщеннях ОЦ застосовуються головним чином вуглекислотні вогнегасники, достоїнством яких є висока ефективність гасіння пожежі, схоронність електронного встаткування, діелектричні властивості вуглекислого газу, що дозволяє використовувати ці вогнегасники навіть у тому випадку, коли не вдається знеструмити електроустановку відразу.

Якщо у інформаційному центрі не вдалося уникнути пожежі, необхідно слідувати твердо установленому порядку дій при пожежі.

Керівник установи, співробітники і обслуговуючий персонал у разі виникнення пожежі або її ознак (диму, запаху горіння або тління різних матеріалів і т. п.), а також кожен громадянин зобов'язані:

• негайно повідомити про пожежу за телефоном в пожежну охорону (при цьому необхідно назвати адресу об'єкта, місце виникнення пожежі, а також повідомити своє прізвище);

• прийняти по можливості заходів з евакуації людей, гасіння пожежі та збереження матеріальних цінностей.

Прибулі до місця пожежі зобов'язані:

• продублювати повідомлення про виникнення пожежі в пожежну охорону, чітко назвавши адресу установи, по можливості місце виникнення пожежі, що горить і чому пожежа загрожує (в першу чергу - яка загроза для людей), а також повідомити свою посаду і прізвище, номер телефону, дати сигнал тривоги місцевій добровільній пожежній дружині, повідомити черговому по установі або керівнику (у робочий час);

• вжити негайних заходів по організації евакуації людей, починаючи евакуацію з приміщення, де виникла пожежа, а також з приміщень, яким загрожує небезпека поширення вогню і продуктів горіння, використовуючи для цього наявні сили і засоби;

• перевірити включення в роботу (або привести в дію) автоматичні системи протипожежного захисту (оповіщення людей про пожежу, пожежогасіння, протидимного захисту);

• при необхідності відключити електро-і газопостачання (за винятком систем протипожежного захисту), зупинити роботу транспортувальних пристроїв, агрегатів, апаратів, перекрити сировинні, газові, парові і водяні комунікації, зупинити роботу систем вентиляції в аварійному та суміжному з ним приміщеннях, виконати інші заходи, що сприяють запобіганню поширення пожежі і задимлення приміщень будівлі;

• припинити всі роботи в будівлі (якщо це допустимо по технологічному процесу виробництва), крім робіт, пов'язаних із заходами щодо ліквідації пожежі;

• видалити за межі небезпечної зони всіх працівників, які беруть участі у гасінні пожежі;

• здійснити загальне керівництво з гасіння пожежі (з урахуванням специфічних особливостей об'єкта) до прибуття підрозділу пожежної охорони;

• забезпечити дотримання вимог безпеки працівниками, які беруть участь у гасінні пожежі;

• одночасно з гасінням пожежі організувати евакуацію і захист матеріальних цінностей;

• організувати зустріч підрозділів пожежної охорони і надати допомогу у виборі найкоротшого шляху для під'їзду до осередку пожежі.

Після прибуття пожежного підрозділу керівник об'єкта (або особа, яка його заміщає) зобов'язаний чітко проінформувати керівника гасіння пожежі про те, чи всі евакуйовані з палаючої чи задимленої будівлі і в яких приміщеннях ще залишилися люди; про конструктивні і технологічні особливості об'єкта, прилеглих будівель та споруд; про наявність та місцях зберігання отруйних і вибухових речовин, установок, що не підлягають відключенню за спеціальними вимогами, для чого він повинен мати списки із зазначенням кількості цих речовин і числа установок для кожного приміщення, і т.д., а також організувати залучення сил і засобів об'єкта до здійснення необхідних заходів, пов'язаних із ліквідацією пожежі та попередженням її поширення.

Згідно ДСТУ 2272:2006 “Пожежна безпека. Терміни та визначення основних понять.”, план евакуації – документ, в якому зазначені евакуаційні шляхи і виходи, встановлені правила поведінки людей, а також порядок і послідовність дій обслуговуючого персоналу на об'єкті при виникненні надзвичайної ситуації. План евакуації, знаки безпеки та покажчики напрямку дозволяють вжити необхідних заходів з евакуації людей з місць масового скупчення при виникненні надзвичайних ситуацій.

Призначення плану евакуації:

чітко позначити шляхи евакуації, евакуаційні виходи, що забезпечують безпеку процесу організованого самостійного руху людей назовні з приміщень, в яких є можливість впливу на них небезпечних факторів пожежі, без урахування вживаних в них засобів пожежогасіння та захисту від диму;

вказати розташування пожежного обладнання та засобів оповіщення про пожежу;

нагадати про першочергові дії, які необхідно вжити кожній людині, яка виявила пожежу, що почалася План евакуації інформаційного центру наведено на рис. 4.2.

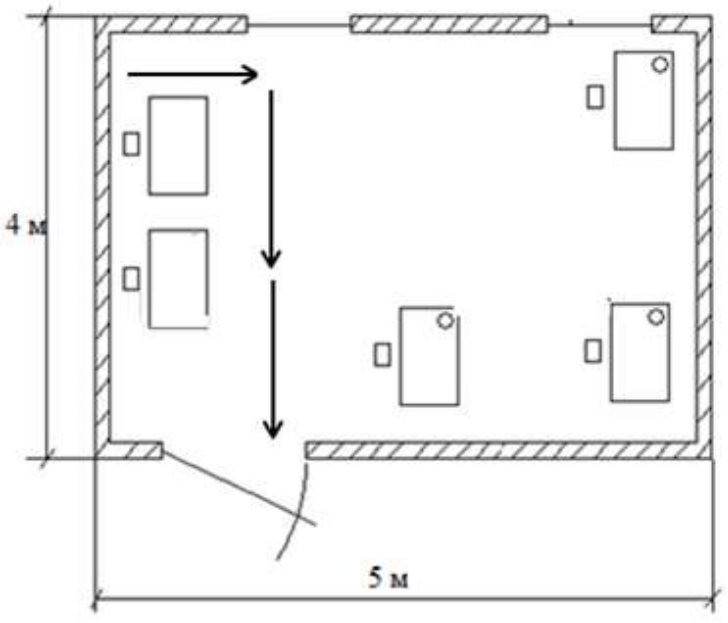


Рисунок 4.2 – Схема евакуації

4.4. Інструкція з охорони праці при обслуговуванні електричного обладнання

Згідно з вимогами НПАОП 0.00-4.15-98 «Положення про розробку інструкцій з охорони праці» (Наказ Держнаглядохоронпраці від 29.01.1998 р. №9) розробимо типову інструкцію.

ЗАГАЛЬНІ ВИМОГИ

1) До роботи з приладом допускається інженерно - технічний склад, що вивчив об’єкт, інструкцію з технічної експлуатації, діючу інструкцію, а також склав залік з технічної безпеки та пожежної безпеки;

2) Ремонт та наладку мають виконувати не менше, ніж два спеціаліста. При цьому інструмент має бути справним, джерело живлення відключеним;

3) Робоче місце або ділянка має бути устаткована засобами захисту від пожежі – вогнегасниками порошкового або іншого типу;

4) Готовий до роботи прилад має бути у надітому корпусі.

ВИМОГИ БЕЗПЕКИ ПЕРЕД ПОЧАТКОМ РОБОТИ

Перед початком роботи слід пересвідчитись, що:

– прилад правильно підключений і має заземлення;

– перед запуском не залишилось зайвих незакріплених предметів;

– всі прилади, що досліджуються, закріплені належним чином, що відповідає аналогічно кріпленню на амортизаційній рамі літака;

– усі з’єднувальні кабелі та місця рознімання справні.

ВИМОГИ БЕЗПЕКИ ПІД ЧАС РОБОТИ

Під час виконання роботи необхідно:

– використовувати тільки справний інструмент і за призначенням;

– слідкувати, щоб на робочому місці не було зайвих предметів, що відволікають увагу і можуть призвести до його травмування;

– при появі іскріння, короткого замикання, запаху гару, диму прилад негайно відключити та виявити причини можливого виникнення пожежі.

ВИМОГИ БЕЗПЕКИ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ

Після закінчення роботи необхідно:

– вимкнути прилад, коли спеціаліст залишає своє місце;

– прибрати своє робоче місце;

– перевірити наявність всього інструменту згідно опису;

– повідомити керівника робіт про виявлені недоліки в роботі приладу.

ВИМОГИ БЕЗПЕКИ В АВАРІЙНИХ СИТУАЦІЯХ:

– у випадку виникнення пожежі негайно викликати пожежну команду. До її приїзду приступити до тушіння пожежі підручними засобами, а також спасінню людей та надання їм допомоги;

– у випадку ураження електричним струмом відключити живлення, прийняти необхідні міри по наданню першої медичної допомоги;

– в робочому приміщенні працівники мають бути ознайомлені з планом та порядком евакуації з приміщення, що має бути повішеним на видному місці.

Висновки до розділу

У межах даного розділу подано характеристику робочого місця, де проводиться розробка алгоритму. Розглянуто та проаналізовано вплив шкідливих та небезпечних виробничих факторів, до яких відносяться показники мікроклімату, шум, освітлення та випромінювання. Приміщення відповідає встановленим нормам, що регламентовані законодавством, щодо вищезазначених факторів. Також було розглянуто пожежну безпеку та електробезпеку приміщення, в результаті чого було виявлено, що приміщення також відповідає необхідними вимогам безпеки. Розроблено план-схему евакуації. Аналіз усіх розрахованих у даному розділі факторів показав

результати, які дають всі підстави вважати, що розглянуте виробниче приміщення повністю відповідає всім нормативним документам і вимогам.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

5.1 Основні принципи охорони атмосферного повітря

Охорона атмосферного повітря здійснюється на основі дотримання таких основних принципів:

1) пріоритету охорони життя і здоров'я людини, теперішнього і майбутніх поколінь;

2) недопущення незворотних наслідків забруднення атмосферного повітря для навколишнього середовища;

3) державного регулювання викидів шкідливих (забруднюючих) речовин в атмосферне повітря і шкідливих фізичних впливів на нього;

4) гласності, повноти та достовірності інформації про стан атмосферного повітря, його забруднення;

5) наукової обґрунтованості, системності та комплексності підходу до охорони атмосферного повітря та охорони навколишнього середовища в цілому [2].

Юридичні особи, які мають джерела викидів шкідливих (забруднюючих) речовин у атмосферне повітря, а також шкідливого фізичного впливу на атмосферне повітря, які перевищують встановлені для них нормативи гранично допустимих викидів, здійснюють погоджені з територіальними підрозділами уповноваженого державного органу в галузі охорони атмосферного повітря заходи щодо його охорони з метою досягнення норм гранично допустимих викидів.

Заходи з охорони атмосферного повітря повинні проводитися відповідно до чинного законодавства України у галузі охорони атмосферного повітря.

Проекти програм охорони атмосферного повітря виносяться на обговорення громадян і громадських об'єднань з метою врахування їх

пропозицій при плануванні та здійсненні заходів щодо поліпшення якості атмосферного повітря.

Фінансування програм охорони атмосферного повітря та заходів по їх здійсненню проводиться відповідно до законодавства України.

З метою визначення критеріїв безпеки та (або) нешкідливості впливу хімічних, фізичних, біологічних та радіаційних факторів на людей, тварин і рослини, особливо охоронювані природні території та інші об'єкти, а також з метою оцінки стану атмосферного повітря встановлюються екологічні нормативи якості атмосферного повітря і гранично допустимі рівні фізичних впливів.

З метою державного регулювання викидів шкідливих (забруднюючих) речовин в атмосферне повітря встановлюються питомі нормативи викидів і нормативи гранично допустимих викидів.

Питомі нормативи викидів встановлюються уповноваженим державним органом у сфері охорони атмосферного повітря за погодженням з відповідним державним органом, до компетенції якого входить розробка технологічних нормативів охорони атмосферного повітря для окремих видів стаціонарних джерел викидів шкідливих (забруднюючих) речовин у атмосферне повітря, а також для джерел забруднення атмосферного повітря транспортних чи інших пересувних засобів.

З метою державного регулювання шкідливих фізичних впливів на атмосферне повітря встановлюються гранично допустимі нормативи шкідливих фізичних впливів на атмосферне повітря.

Нормативи викидів шкідливих (забруднюючих) речовин у атмосферне повітря і гранично допустимі нормативи шкідливих фізичних впливів на атмосферне повітря, методи їх визначення та види джерел, для яких вони встановлюються, розробляються і затверджуються в порядку, визначеному Законом України «Про охорону атмосферного повітря» [1].

Система економічного стимулювання та механізми зменшення викидів шкідливих (забруднюючих) речовин встановлюються Законом України «Про охорону атмосферного повітря» [1].

Державна реєстрація шкідливих (забруднюючих) речовин, реєстрація виданих дозволів на допустиму кількість викидів і реєстрація фактично вироблених викидів провадяться відповідно до правил, затверджених Верховною Радою України.

Викид шкідливих (забруднюючих) речовин у атмосферне повітря стаціонарним джерелом допускається на підставі дозволу, виданого уповноваженим державним органом у сфері охорони атмосферного повітря або його територіальними підрозділами у порядку, визначеному Законом України «Про охорону атмосферного повітря» [1].

Порядок видачі дозволів на викиди шкідливих (забруднюючих) речовин у атмосферне повітря при експлуатації транспортних та інших пересувних засобів встановлюється Законом України «Про охорону атмосферного повітря» [1].

Шкідливі фізичні дії на атмосферне повітря допускаються на підставі дозволів, виданих уповноваженим державним органом у сфері охорони атмосферного повітря за погодженням з органами Державної санітарно-епідеміологічної служби, у порядку, встановленому Законом України «Про охорону атмосферного повітря» [1].

При відсутності дозволів на викиди шкідливих (забруднюючих) речовин у атмосферне повітря і шкідливі фізичні впливи на атмосферне повітря, а також при порушенні умов, передбачених даними дозволами, діяльність фізичних та юридичних осіб, які здійснюють викиди шкідливих (забруднюючих) речовин у атмосферне повітря і шкідливі фізичні впливу на нього, може бути заборонена або припинена в порядку, визначеному чинними законодавчими актами України.

5.2 Аналіз впливу забруднення атмосфери на організм людини

Наша планета оточена повітряною оболонкою – атмосферою, яка поширюється над Землею на 1500 - 2000 км. Однак ця межа умовна, оскільки сліди атмосферного повітря виявлені і на висоті 20000 км.

Наявність атмосфери – необхідна умова існування життя на Землі, оскільки атмосфера регулює клімат Землі, а також згладжує добові коливання температур на планеті. В даний час середня температура поверхні Землі дорівнює $140C^0$. атмосфера пропускає випромінювання Сонця і пропускає тепло. У ній утворюються хмари, дощ, сніг, вітер. Вона є переносником вологи на Землі і середовищем, у якому поширюється звук.

Атмосфера служить джерелом кисневого дихання, вмістилищем газоподібних продуктів обміну речовин, впливає на теплообмін і інші функції живих організмів. Основне значення для життєдіяльності організму мають кисень і азот, вміст яких у атмосферному повітрі відповідно дорівнює 21 і 78% [3].

Кисень необхідний для дихання більшості живих істот (виняток становить лише невелика кількість анаеробних мікроорганізмів). Азот входить до складу білків і азотистих сполук. Вуглекислий газ –о джерело вуглецю органічних речовин – найважливішого компонента цих сполук.

За добу людина вдихає близько 12 - 15 $м^3$ кисню, а виділяє приблизно 580 л вуглекислого газу. Тому атмосферне повітря є одним з основних життєво важливих елементів навколишнього середовища. Необхідно відзначити, що у видаленні від джерел забруднення хімічний склад атмосфери досить стабільний. Проте в результаті господарської діяльності людини з'явилися осередки вираженого забруднення повітряного басейну в тих районах, де розміщені великі промислові центри. Тут у атмосфері відзначається наявність твердих і газоподібних речовин, що роблять несприятливий вплив на умови життя і здоров'я населення.

До теперішнього часу накопичилося багато наукових даних про те, що забрудненість атмосфери, особливо у великих містах, досягла небезпечних для здоров'я людей розмірів. Відомо чимало випадків захворювань і навіть смерті жителів міст індустріальних центрів в результаті викидів токсичних речовин промисловими підприємствами та транспортом за певних метеорологічних умовах.

Двоокис кремнію і вільний кремній, що міститься в летючій золі, є причиною важкого захворювання легень - силікозу, розвиваючогося у робітників «курних» професій, наприклад у гірників, працівників коксохімічних, вугільних, цементних і ряду інших підприємств. Тканина легенів покривається сполучною тканиною, і ці ділянки перестають функціонувати. У дітей, що проживають поблизу потужних електростанцій, не обладнаних пиловловлювачами, виявляють зміни в легенях, подібні з формами силікозу [4]. Велика забрудненість повітря димом і кіптявою, що триває протягом декількох днів, може викликати отруєння людей зі смертельними наслідками.

Особливо згубно діє на людину забруднення атмосфери в тих випадках, коли метеорологічні умови сприяють застою повітря над містом. Шкідливі речовини, що містяться в атмосфері впливають на людський організм при контакті з поверхнею шкіри або слизовими оболонками. Поряд з органами дихання забруднювачі вражають органи зору і нюху, а також впливаючи на слизову оболонку гортані, можуть викликати спазми голосових зв'язок. Вдихувані тверді і рідкі частки розмірами 0,6 - 1,0 мкм досягають альвеол і абсорбуються у крові, деякі накопичуються в лімфатичних вузлах.

Забруднене повітря дратує здебільшого дихальні шляхи, викликаючи бронхіт, емфізему, астму. До подразників, що викликають ці хвороби, відносяться сірчистий (SO_2) і сірчаний (SO_3) ангідриди, оксиди азоту, хлороводень (HCl), сірководень (H_2S), фосфор та його сполуки [2].

Ознаки та наслідки дій забруднювачів повітря на організм людини проявляються здебільшого у погіршенні загального стану здоров'я:

з'являються головні болі, нудота, відчуття слабкості, знижується або втрачається працездатність. Окремі забруднюючі речовини викликають специфічні симптоми отруєння. Наприклад, хронічне отруєння фосфором супроводжується болями у шлунково-кишковому тракті і пожовтінням шкірного покриву. Ці симптоми пов'язані з втратою апетиту і уповільненням обміну речовин. Надалі отруєння фосфором призводить до деформації кісток, які стають все більш крихкими. Знижується опірність організму в цілому.

Оксид вуглецю (II), (CO) – це безбарвний і не маючий запаху газ, який впливає на нервову і серцево-судинну системи, викликаючи задуху. Первинні симптоми отруєння чадним газом (поява головного болю) виникають у людини через 2 - 3 години його перебування в атмосфері, що містить 200 - 220 мг / $м^3$ CO. При більш високих концентраціях чадного газу з'являються відчуття пульсації крові в скронях, запаморочення. Токсичність чадного газу зростає при наявності у повітрі азоту, в цьому випадку концентрацію CO в повітрі необхідно знижувати в 1,5 рази.

Оксидиазоту (NO, N_2O_3, NO_2, N_2O). У атмосферу викидаються в основному діоксид азоту NO_2 - безбарвний, такий, що не має запаху отруйний газ, дратівливо діючий на органи дихання. Особливо небезпечні оксиди азоту в містах, де вони взаємодіють з вуглеводнями вихлопних газів і утворюють фотохімічний туман – зміг. Перші симптом отруєння оксидами азоту – легкий кашель. При підвищенні концентрації NO_2 виникає сильний кашель, блювота, іноді головний біль. При контакті з вологою поверхнею слизових оболонок оксиди азоту утворюють азотну та азотисту кислоти (HNO_3 і HNO_2), що призводить до набряку легенів [3].

Сірчистий ангідрид (SO_2) - безбарвний газ з гострим запахом – вже в малих концентраціях (20 - 30 мг / $м^3$) створює неприємний смак у роті, подразнює слизові оболонки очей і дихальні шляхи. Вдихання SO_2 викликає хворобливі явища в легенях і дихальних шляхах, іноді призводять до набряку легенів, глотки і паралічу дихання.

Вуглеводні (пари бензину, метану і т. д.) мають наркотичну дію, у малих концентраціях викликають головний біль, запаморочення і т. д. Так, при вдиханні протягом 8 годин парів бензину в концентрації 600 мг / м^3 виникають головні болі, кашель, неприємні відчуття в горлі. Особливо небезпечні поліциклічні ароматичні вуглеводні типу 3, 4 - бензопірену ($C_{20}H_{12}$), що утворюються при неповному згорянні палива. За даними ряду вчених, вони мають канцерогенні властивості.

Альдегіди. При тривалому впливі альдегіди викликають подразнення слизових оболонок очей і дихальних шляхів, а при підвищенні концентрації – головний біль, слабкість, втрату апетиту, безсоння.

З'єднання свинцю. В організм через органи дихання надходить приблизно 50% сполук свинцю. Вплив свинцю порушує синтез гемоглобіну, призводить до захворювання дихальних шляхів, сечостатевих органів, нервової системи. Особливо небезпечні сполуки свинцю для дітей молодшого віку. У великих містах вміст свинцю в атмосфері досягає 5 - 38 мг / м^3, що перевищує природний фон в 10000 разів.

Дисперсний склад пилу і туманів визначає загальну проникаючу здатність в організм людини шкідливих речовин. Особливу небезпеку становлять токсичні тонкодисперсні пилинки з розміром частинок 0,5 - 1,0 мкм, які легко проникають в органи дихання.

Нарешті, різні прояви дискомфорту у зв'язку із забрудненням повітря – лнеприємні запахи, зниження освітленості та ін. – психологічно діють на людей.

Шкідливі речовини, що знаходяться в атмосфері і випадають вражають і тварин. Вони накопичуються в тканинах тварин і можуть стати джерелом отруєнь, якщо м'ясо цих тварин використовується в якості харчових продуктів.

5.3 Вплив центрів обробки даних

Центри обробки даних – це другий за енергоємністю елемент Інтернету після пристроїв. Центр обробки даних Facebook в Приневіллі, штат Орегон, споживає близько 78 мегават електроенергії, що дорівнює приблизно 64 000 будинкам.

Проте центри обробки даних є найефективнішим способом підтримання роботи Інтернету, враховуючи, що централізація серверів в одному місці дозволяє використовувати енергію та мінімізувати використання електроенергії. Однією з переваг хмари є те, що вона забезпечує набагато більшу концентрацію обчислювальної та обробної потужності при меншій кількості серверів, що завжди означає енергозбереження. Але єдиним способом зменшити забруднення є використання відновлюваних джерел енергії, а також підвищення енергоефективності [33-35].

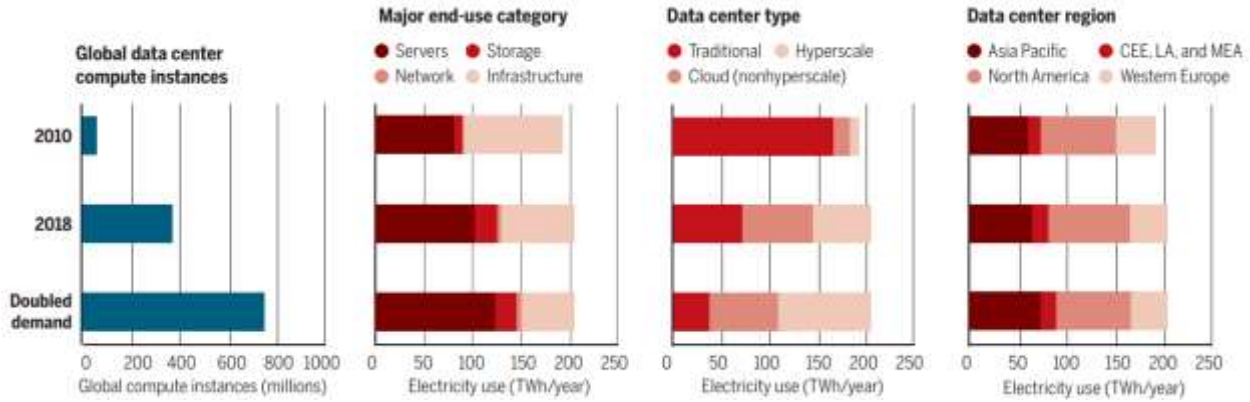


Рис.4.2. Історичне споживання енергії ЦОД в 2010-2018 рр і прогноз на найближчі роки, коли відбудеться чергове подвоєння кількості обчислювальних інстанси (ядер) в дата-центрах

Проблема пов'язана з джерелами енергії, які підтримують роботу центрів обробки даних. В даний час більшість центрів обробки даних працюють з енергетичними компаніями, які покладаються на вугілля або атомні електростанції для виробництва електроенергії.

В звіті «Наскільки чистою є ваша хмара?» встановлено, що 55,1% електроенергії, що використовується серверами Apple, виробляється

вугільними заводами, 49,7% енергії, яку використовують сервери IBM, і 39,4% сервери Facebook. Ці значні цифри спричиняють тисячі тонн вуглекислого газу, що викидається в атмосферу та брудне повітря, яке з нею йде.

З 2000 по 2006 рік загальний інтернет-трафік зріс на 32 000 000%, тоді як загальне споживання енергії зросло лише на 200% за той самий період.

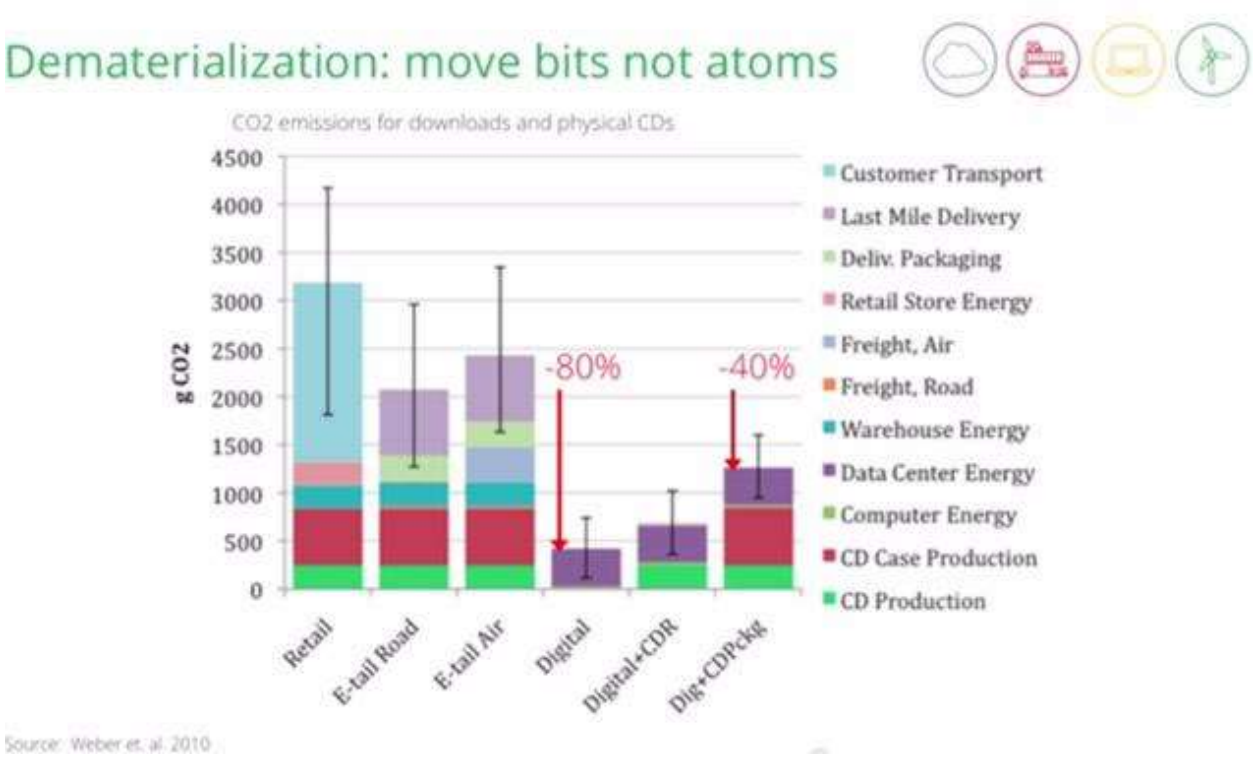


Рис.4.3. Чинники що впливають на викиди вуглекислого газу

В [36] автори інтегрували дані з різних джерел, які з'явилися останнім часом. Стаття написана декількома провідними експертами по використанню енергії в центрів обробки даних з Північно-Західного університету, Національної лабораторії Лоуренса Берклі і дослідницької компанії Koomey Analytics (США).

Новий аналіз показує досить скромне зростання енергоспоживання в останні роки. Зокрема, до 2018 року робочі навантаження і кількість обчислювальних інстансів збільшилася більш ніж в шість разів, IP-трафік збільшився більш ніж в 10 разів. Ємність сховищ ЦОД за цей термін виросла в 25 разів. Але з 2010 року споживання електроенергії в розрахунку на один сервер знизилося в чотири рази, в основному, завдяки технологічним поліпшеням і скороченню часу холостої роботи.

Показник ват на терабайт встановленої пам'яті знизився приблизно в дев'ять разів через збільшення щільності та ефективності накопичувачів.

Крім того, зростання числа серверів значно сповільнилося внаслідок п'ятикратного збільшення середнього числа інстанси на одному сервері (внаслідок віртуалізації).

При цьому протягом 2010-2019 років спостерігалося стійке поліпшення якості енерговитрат PUE (power usage effectiveness), яке обчислюється як частка від ділення загального енергоспоживання дата-центру на енергоспоживання його IT-обладнання. Внесок різних складових в змінах PUE показаний на діаграмі нижче.

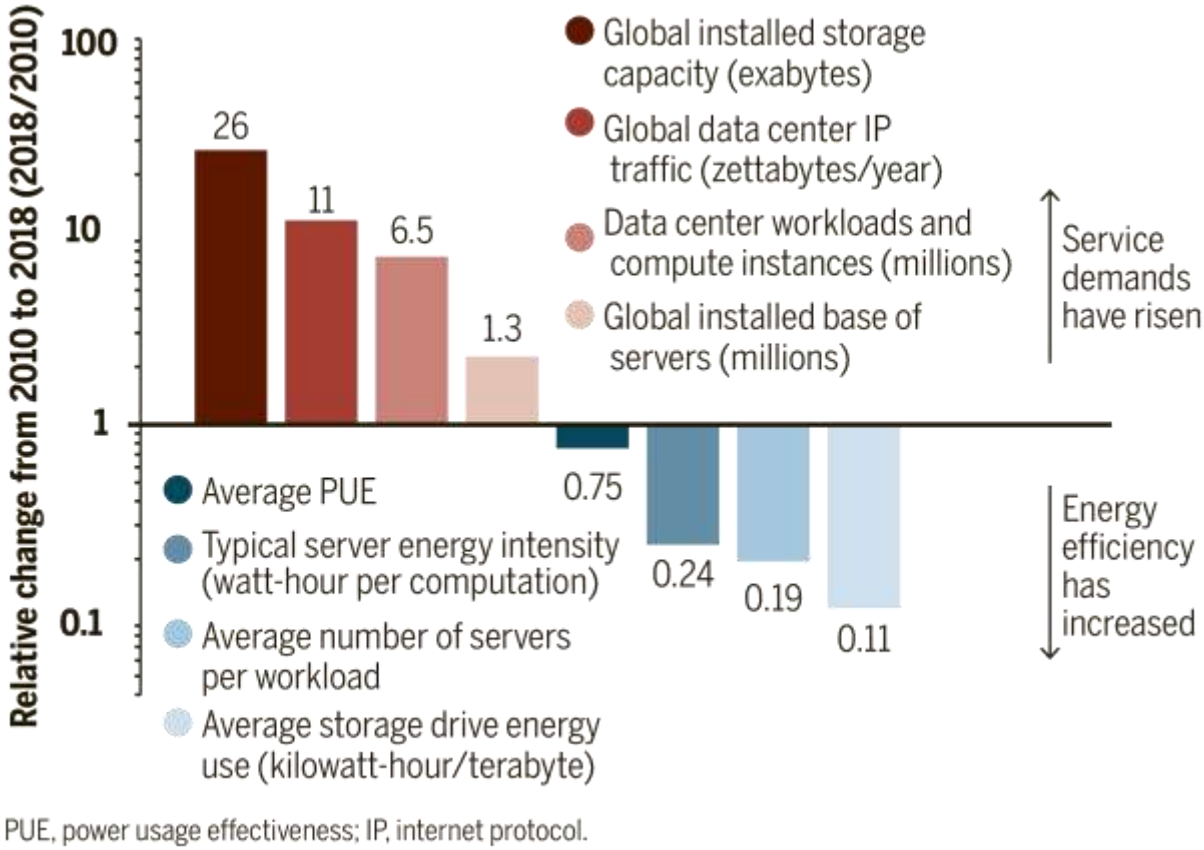


Рис.4.4. Тенденції в енергоспоживанні дата-центрів

У 2018 році глобальне споживання енергії дата-центрів зросло до 205 ТВт/год, що представляє собою збільшення всього на 6% в порівнянні з 2010 роком, тоді як загальна кількість «обчислювальних інстансів» збільшилася на

550% за той же період часу (під обчислювальними інстнасами маються на увазі обчислювальні ядра CPU, в першу чергу).

Якщо обчислити використання енергії на обчислювальний інстанси, то енергоємність кількість глобальних центрів обробки даних з 2010 року щорічно зменшувалася на 20%.

Загальне енергоспоживання дата-центрів у 2010-2018 роки практично не змінилося, зате енергоспоживання IT-пристроїв (серверів, систем зберігання та мережевого обладнання) зросла з 92 до 130 ТВт/ год, що вказує на збільшення ефективності ЦОД. Іншими словами, тепер більше енергії йде безпосередньо на роботу серверів, а менше - на допоміжні системи на зразок системи охолодження. У той же час це говорить про підвищення технологічної та експлуатаційної ефективності інфраструктури: «Це зниження пояснюється продовженням переходу від невеликих традиційних центрів обробки даних (79% обчислювальних інстанси в 2010) до великих і більш енергоефективним хмарним (включаючи гіпермасштабуємі) дата-центри (89% обчислювальних операцій в 2018 році)».

В найближчій перспективі ринкові аналітики прогнозують ще більшу віртуалізацію серверів, а технологічні дослідження вказують, що у IT-пристроїв зберігся потенціал для підвищення енергоефективності, в тому числі більше переходів на малопотужні пристрої.

З точки зору інфраструктури, надвеликі ЦОД світового класу вже працюють на PUE = 1,1 або нижче, що близько до мінімального можливого значення.

Дослідники прогнозують, що в короткостроковій перспективі продовжиться перехід від менших традиційних дата-центрів на більш ефективні гіпермасштабуємі ЦОД. При цьому є достатній ресурс енергоефективності для поглинання наступного подвоєння обчислювальних операцій в дата-центрах паралельно з не значним збільшенням обсягу глобального використання енергії.

Як приклад: PUE 1,95 означає, що на системи кондиціонування, охолодження та інші «комунальні» потреби Цода використовується 95% енергії щодо потреби серверів в ЦОД.

У більшості дата-центрів Китаю PUE дорівнює 2,2. Це набагато вище, ніж в ряді європейських країн. А в США середній PUE дорівнює 1,9. Компанії-лідери за показником демонструють цифру не більше 1,2.

5.4 Рекомендації щодо зниження негативного вливу ЦОД

У 2016 році The Green Grid розробила й опублікувала глобальний стандарт коефіцієнта PUE для оцінки енергоефективності дата-центрів. Хоча PUE використовували і раніше, галузевим стандартом він став недавно.

PUE (Power Usage Effectiveness) – показує, наскільки ефективно ЦОД використовує енергію, яку отримують його споживачі. Коефіцієнт PUE регулярно включають в свої розрахунки найбільші власники центрів обробки даних, такі як Microsoft і Google.

PUE показує відношення сумарної потужності ЦОД до сумарної потужності повного набору IT-обладнання: серверів, систем зберігання даних, комутаторів та інших мережевих пристроїв.

$$POE = \frac{\text{сумарна потужність ЦОД}}{\text{сумарна потужність повного набору IT обладнання}}$$

При ідеальній організації ЦОД PUE не перевищує значення 1.25, а в оптимальному випадку знаходиться в межах 1.25-1.43 одиниць. Компанії, які не вживають заходів для підвищення енергоефективності, в розрахунках отримують більше 2.5 одиниць.

Приклади розрахунку PUE для центру обробки даних

1) ЦОД купує всю електроенергію

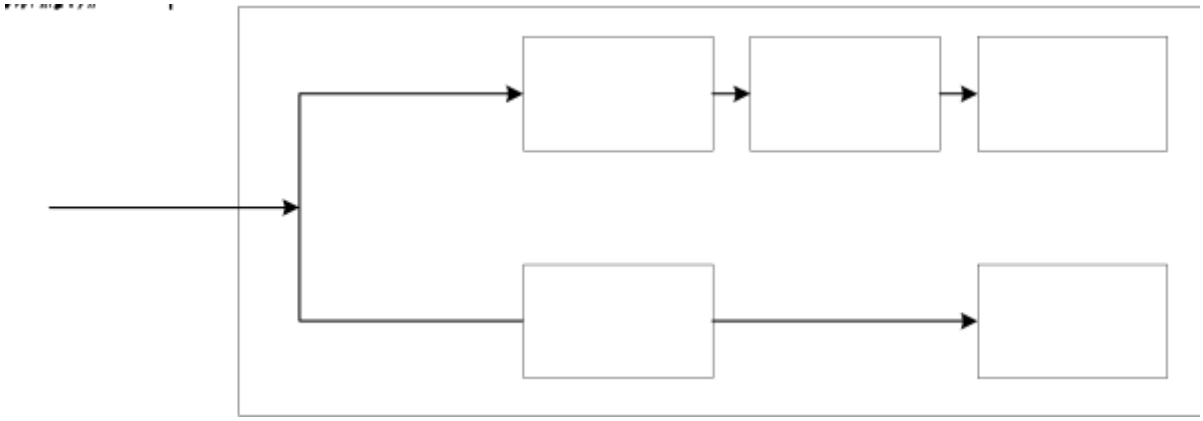


Рис.4.6. ЦОД купує всю електроенергію

$$PUE = \frac{1{,}633{,}333 * 1}{1{,}000{,}000 * 1} = 1.63$$

2) ЦОД купує електроенергію та охолоджувальну рідину

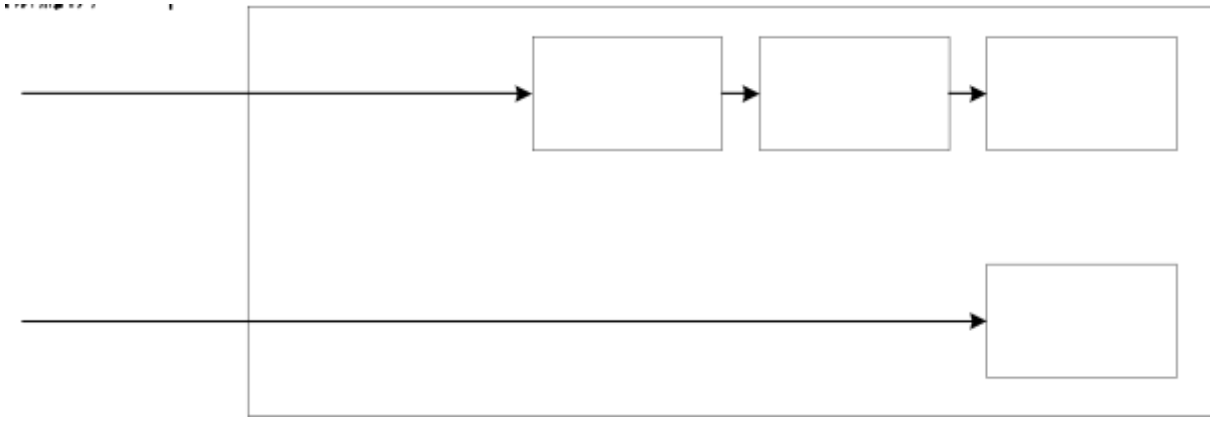


Рис.4.7. ЦОД купує електроенергію та охолоджувальну рідину

$$PUE = \frac{1{,}100{,}000 * 1 + 1{,}600{,}000 * 0.4}{1{,}000{,}000 * 1} = 1.58$$

Наступне рівняння ілюструє, як кількісно визначити використання енергії системи охолодження для центру обробки даних, яка має загальну установку охолоджувальної рідини.

$$Q = \frac{VHC * \text{швидкість потоку} * \Delta\text{T} * \text{час}}{\text{Перетворення енергії}}$$

де Q – енергія від тепла, захопленого охолодженою рідиною, в мегават-часах (МВтч)

VHC – об'ємна теплоємність, властивість текучого середовища, яке зазвичай використовується на установках з охолодженою водою.

$$VHC = \text{Щільність рідини} * \text{Специфічна теплота рідини}$$

Швидкість потоку – витрата охолодженої води (наприклад, кубічні метри на секунду (м3/с)

ΔT – різниця температур між подачею та поверненням охолодженої води (Кельвін)

Час – проміжок часу для вимірювання енергії (використовуючи ту саму часову базу, що і знаменник витрати)

Перетворення енергії – стандартне перетворення, необхідне для зміни одиниць вимірювання енергії з Джоулів на МВтч.

Приклад розрахунку:

$$VHC = 1{,}000\frac{kg}{m^3 * 4.184\frac{J}{(kg * °K)} = 4.184.000\frac{J}{(m^3 * °K)}}$$

$$\text{Швидкість потоку} = 0{,}003\frac{m^3}{s}$$

$$\Delta\text{T} = 5℃ = 5°K$$

$$\text{Час} = 1\text{ рік} = 31{,}536{,}000\ s$$

$$\text{Перетворення енергії} = 3{,}600{,}000{,}000\ \frac{J}{MWh}$$

$$Q = \frac{4.184.000\frac{J}{(m^3 * °K)} * 0{,}003\frac{m^3}{s * 5°K * 31{,}536{,}000\ s}}{3{,}600{,}000{,}000\ \frac{J}{MWh}} = 549{,}78MWh$$

Щоб знизити PUE можна імплементувати природнє охолодження, моніторинг і прогнозоване обслуговування, зменшувати фізичні сервери та збельшувати кількість віртуальних машин.

Близько 40% всієї енергії, яку споживають дата-центри, йде на роботу штучних систем охолодження. Істотно знизити витрати допомагає реалізація природного охолодження (фрікулінга). При такій системі зовнішнє повітря фільтрується, підігрівається або охолоджується, після чого подається в

серверні приміщення. «Відпрацьоване» гаряче повітря викидається назовні або частково підмішується при необхідності до вхідного потоку.

Крім того, дата-центр може розміщуватися у водоймах, в такому випадку вода з нього може використовувати для охолодження ЦОД. За прогнозами Stratistics MRC, до 2023 року вартість ринку технологій рідинного охолодження досягне $4.55 млрд. Серед його видів виділяють іммерсійне охолодження (занурення обладнання в іммерсійне масло), адіабатичне охолодження (в основі - технологія випаровування, використовується в ЦОД Facebook) , теплообмінне (теплоносій потрібної температури надходить безпосередньо до стійки з обладнанням, видаляючи надлишки тепла).

Підвищити енергоефективність також допоможе правильне використання потужностей, якими володіє дата-центр. Вже придбані сервери повинні або працювати на завдання клієнтів, або не споживати енергію під час простою. Один із способів контролювати ситуацію - використовувати ПЗ для керування інфраструктурою. Наприклад, систему Data Center Infrastructure Management (DCIM). Таке ПЗ автоматично перерозподіляє навантаження на сервери, відключає незадіяні пристрої і дає рекомендації по швидкості роботи вентиляторів холодильних установок (знову ж таки, для економії енергії на зайвому охолодженні).

Важлива частина підвищення енергоефективності ЦОД - своєчасне оновлення обладнання. Застарілий сервер найчастіше поступається по продуктивності і ресурсоємності новому поколінню. Тому для зниження PUE рекомендовано оновлювати обладнання якомога частіше - деякі компанії роблять це щороку. З дослідження Supermicro: оптимізовані цикли оновлення обладнання дозволять скоротити обсяг електронних відходів більш ніж на 80% і підвищити продуктивність ЦОД на 15%.

Існують також способи оптимізації екосистеми дата-центрів без істотних витрат. Так, можна закрити щілини в серверних шафах, щоб запобігти витоку холодного повітря, ізолювати гарячий або холодний коридори, перенести високонавантажених сервер в більш холодну частину ЦОД і так далі.

Компанія VMware підрахувала, що перехід на віртуальні сервери в ряді випадків знижує електроспоживання на 80%. Це пояснюється тим, що розміщення більшої кількості віртуальних серверів на меншій кількості фізичних машин логічно скорочує витрати на обслуговування «заліза», охолодження і харчування.

Експеримент компаній NRDC і Anthesis показав, що заміна 3 000 серверів на 150 віртуальних машин економить $ 2 млн на електриці.

Крім іншого, віртуалізація дає можливість перерозподіляти і нарощувати віртуальні ресурси (процесори, пам'ять, обсяг сховища) в процесі. Тому електроенергія витрачається тільки на забезпечення роботи, виключаючи витрати на обладнання, що простоює.

Безумовно, для підвищення енергоефективності можна також вибирати альтернативні джерела енергії. Для цього деякі ЦОД використовують сонячні батареї і вітряні генератори. Це, однак, досить дорогі проекти, які можуть собі дозволити тільки великі компанії.

Висновки до розділу

У межах даного розділу описано порядок проведення заходів, в разі якщо юридична особа має джерела викидів шкідливих (забруднюючих) речовин у атмосферне повітря, а також шкідливого фізичного впливу на атмосферне повітря, які перевищують встановлені для них нормативи гранично допустимих викидів. Описано як держава регулює питання, щодо нормалізації шкідливих фізичних впливів на атмосферне повітря.

Проведено аналіз впливу забруднення атмосфери на організм людей. Описано як мешканці індустріальних міст, розташованих поруч з підприємствами які мають джерела шкідливих викидів, страждають від хронічних хвороб легенів, дихальних шляхів.

Проведено аналіз впливу інформаційних технологій, зокрема центрів обробки даних, на навколишнє середовище. В результаті встановлено, що

найближчим часом швидкого зростання споживання електроенергії центрами обробки даних не передбачається. Наведено стандарти сертифікації, для того щоб регулювати споживання енергії в ЦОД.

ВИСНОВКИ

В магістерській дипломній роботі проведено дослідження системи моніторингу комплексом аграрного призначення на базі інтернету речей. При вивченні концепції інтелектуальної системи управління будівлею були сформульовані основні вимоги і характеристики її реалізації. Серед існуючих в світі на сьогоднішній день реалізацій ті, які найбільш повно задовольняють вимогам концепції інтелектуального комплексного моніторингу приміщень інтегровані до системи управління будівлею. В рамках своїх стандартів вони забезпечують виконання всіх вимог системи, володіючи при цьому безсумнівними перевагами:

- тривале і глибоке опрацювання таких систем безліччю розробників;
- наявність відкритих стандартів, підтримуваних широким колом розробників;
- економічні вигоди як для творців систем, так і для їх користувачів;

Тому, дана реалізація була обрана в якості об'єкта для створення макета. Таким чином, у межах дипломного проекту було створено модель системи комплексного моніторингу приміщень за допомогою технології Інтернет речей. Модель зроблена щоб максимально знизити витрати на монтаж системи. Щодо моделі сучасної інтелектуальної системи комплексного моніторингу приміщень за допомогою технології Інтернет речей, то вона зроблена так, щоб за потребою у неї можна було вносити необхідні зміни не перериваючи її роботу та не припиняючи її.

Переваги створеної системи:

- охоплює всі процеси життєзабезпечення;
- відкрита гетерогенна архітектура;

- об'єднана розподілена база даних;
- інтерфейси між процесами;
- масштабовані рішення;
- модульна технологія, можливості для етапного впровадження;
- проста інтеграція існуючих і майбутніх систем і інтерфейсів;
- база управління, що настроюється;
- автоматизований аналіз подій;
- автоматичне управління аварійними ситуаціями.

Недоліки створеної системи:

- висока вартість;
- обов’язкове навчання персоналу призначеного для роботи з системою.

Згідно до проведеного дослідження варто відзначити, що система комплексного моніторингу приміщень за допомогою технології Інтернет речей за всіма показниками перевершує систему комплексного моніторингу приміщень за допомогою технології Nest, що говорить про високу якість системи комплексного моніторингу приміщень та можливість впровадження її в реальну роботу за потребою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. «Интернет вещей» в промышленности: обзор ключевых технологий и трендов // Ли Да Сюй (Li Da Xu), By Xe (Wu He) - whe@odu.edu, Сянчан Ли (Shancang Li) - shanchang.li@bristol.ac.uk, перевод Алексей Осотов. – http://www.controlengrussia.com/internet-veshhej/klyuchevy-h-tehnologij/ (Станом на 26.09.2020)

2. Семенченко П.И. Обзор и анализ функциональных возможностей платформ для устройств интернета вещей / П.И. Семенченко // Российский экономический университет им. Г.В. Плеханова, 2017. – № 5. – С. 156-168.

3. Шварц Марко Интернет вещей с ESP8266: Пер. с англ. – СПб.: БХВ-Петербург, 2018. – 192 с.

4. Li S., Xu L., Wang X. Compressed sensing signal and data acquisition in wireless sensor networks and internet of things // IEEE Trans. Ind. Informat. 2013. – Vol. 9. – No. 4.

5. He W., Xu L. Integration of distributed enterprise applications: A survey // IEEE Trans. Ind. Informat. 2014. – Vol. 10. – No. 1.

6. Uckelmann D., Harrison M., Michahelles F. An architectural approach towards the future internet of things // Uckelmann D., Harrison M., Michahelles F. Architecting the Internet of Things. USA, NY: Springer, 2011.

7. Wang L., Xu L., Bi Z., Xu Y. Data filtering for RFID and WSN integration // IEEE Trans. Ind. Informat. 2014. – Vol. 10. – No. 1.

8. 1. Internet of Things Global Standards Initiative [Электронный ресурс]. – Режим доступа : http://www.itu.int/en/ITU-T/gsi/ iot/Pages/default.aspx (дата обращения: 25.09.2020).

9. Алгулиев, Р. Ш. Интернет вещей / Р. Ш. Алгулиев, Р. Ш. Махмудов // Информационное общество. – 2013. – № 3. – С. 42–48.

10. L. A. Grieco, M. B. Alaya, T. Monteil, K. K. Drira, Architecting information centric ETSI-M2M systems, in: IEEE PerCom, 2014.

11. R. H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev, Jan. 2010, Vol. 26, № 1, pp. 23–30.

12. H. Feng, W. Fu, Study of recent development about privacy and security of the internet of things, in: 2010 : International Conference on Web Information Systems and Mining (WISM), Sanya, 2010, pp. 91–95

13. R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Networks, 2013, Vol. 57, № 10, pp. 2266–2279.

14. S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for internet of things (iot), in: 2011 : 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (VITAE), Chennai, India, 2011, pp. 1–5.

15. Y. Zhao, Research on data security technology in internet of things, in: 2013 : 2nd International Conference on Mechatronics and Control Engineering (ICMCE), Dalian, China, 2013, pp. 1752– 1755.

16. T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the internet of things, Ad Hoc Networks, 2013, Vol. 11. № 8, pp. 2710–2723.

17. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials, 2013, Vol. 15, № 3, pp. 1389–1406.

18. R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electrical Eng., 2011, Vol. 37, № 2, pp. 147–159.

19. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur. (TISSEC), 2005, Vol. 8, № 2, pp. 228–258.

20. Z.-Q. Wu, Y.-W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chin. J. Comput., 2011, Vol. 34, № 8, pp. 1351–1364.

21. Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini, Security, Privacy & Trust in Internet of Things: the road ahead, Computer Networks (Elsevier), 2015, Vol. 76, pp. 146–164.

22. J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 : International Symposium on Next-Generation Electronics (ISNE), Kwei-Shan, 2014, pp. 1–2.

23. M. Turkanovi, B. Brumen, M. Holbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Networks, 2014, Vol. 20, pp. 96–112.

24. N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci., 2014, Vol. 8, № 4, pp. 1617–1624.

25. A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving iot targetdriven applications, Comput. Secur., 2013, Vol. 37, pp. 111–123.

26. J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of iot, Jisuanji Yanjiu yu Fazhan, Comput. Res. Dev., 2013, Vol. 50, № 6, pp. 1267– 1275.

27. M. Ali, M. ElTabakh, C. Nita-Rotaru, FT-RC4: A Robust Security Mechanism for Data Stream Systems, Tech. Rep. TR-05- 024, Purdue University, Nov. 2005, pp. 1–10.

28. M. A. Hammad, M. J. Franklin, W. Aref, A. K. Elmagarmid, Scheduling for shared window joins over data streams, in : Proceedings of the 29th International Conference on Very Large Data Bases (VLDB), Berlin, Germany, 2003, pp. 297–308.

29. S. Papadopoulos, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB Journal, 2010, Vol. 19, № 1, pp. 161–180.

30. S. Papadopoulos, G. Cormode, A. Deligiannakis, M. Garofalakis, Lightweight authentication of linear algebraic queries on data streams, in : Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data (SIGMOD), New York, USA, 2013, pp. 881–892.

31. A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, R. Borgaonkar, New paradigms for access control in constrained environments, in: 2014 : 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), Montpellier, 2014, pp. 1–4.

32. L. Veltri, S. Cirani, S. Busanelli, G. Ferrari, A novel batchbased group key management protocol applied to the internet of things, Ad Hoc Networks, 2013, Vol. 11, № 8, pp. 2724–2737.

33. Джигирей В.С. "Охорона навколишнього середовища" Навчальний посібник / К.: Знання, 2006.- 319 с.

34. Бойчук Л Д., Соломенно Е.М., Бугай О.В. Екологія і охорона навколишнього середовища: Навч. посіб. — Суми: Університетська книга, 2003. — 284 с.

35. Сухарев С М., Чудак С О., Сухарева О.Ю. Технологія та охорона навколишнього середовища: Навч. посіб. — Львів: Новий Світ — 2000, 2004. — 256 с.

36. Eric Masanet, Arman Shehabi, Nuoa Lei, Sarah Smith and Jonathan Koomey, “Recalibrating global data center energy-use estimates,” Science, vol 367, 2020, pp. 984-986