

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

ВСТУП ДО ІНТЕРНЕТУ РЕЧЕЙ

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за освітньою програмою "Електронні системи мультимедіа та засоби Інтернету речей"
спеціальності 171 Електроніка

Укладач: В. В. Макаренко

Електронне мережеве навчальне видання

Київ
КПІ ім. ІГОРЯ СІКОРСЬКОГО
2025

Укладач: *Макаренко Володимир Васильович*, канд. техн. наук, с.н.с.

Рецензент: *Сафронов П.С.*, канд. техн. наук, доц.,
доцент кафедри електронних пристроїв та систем

Відповідальний редактор: *Трапезон К.О.*, канд. техн. наук, доц.

*Гриф надано Методичною радою КПП ім. Ігоря Сікорського
(протокол № 8 від 29.05.2025 р.)
за поданням вченої ради факультету електроніки
протокол № 03/2025 від 24.03.2025 р.)*

П88 **Вступ до Інтернету речей.** [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою "Електронні системи мультимедіа та засоби Інтернету речей" спеціальності 171 Електроніка / КПП ім. Ігоря Сікорського ; уклад.: В. В. Макаренко. – Електрон. текст. дані (1 файл). – Київ : КПП ім. Ігоря Сікорського, 2025. – 536 с.

В навчальному посібнику з освітньої компоненти "Вступ до Інтернету речей" викладено теоретичні та практичні відомості, які розкривають принципи роботи та способи реалізації систем Інтернету речей. Розглянуті загальні поняття про системи Інтернету речей та промислового Інтернету речей, їх склад, сфери застосування та особливості побудови в залежності від призначення системи.

Розглянуті поняття "розумний будинок", "розумна будівля", "розумний офіс" та "розумне місто" та основні компоненти таких систем, а саме: датчики систем безпеки та контролю стану навколишнього середовища та пристроїв систем IoT. Наведено принцип дії датчиків та приклади їх виконання.

У посібнику наведено коротку інформацію про інтерфейси зв'язку, що використовуються в системах IoT. Детально висвітлено інформації про канали зв'язку в системах Інтернету речей, а саме, проводові та безпроводові. Наведено поняття і структура структурованих кабельних систем "розумних" будівель та основні технології безпроводових систем, що використовуються в IoT: LORA, Sigfox, NB-IoT, ZigBee, Wireless HART та інших.

Окремо розглянуто питання керування системами "розумного" будинку на базі програмованих логічних контролерів. Висвітлені питання захисту інформації в каналах зв'язку систем Інтернету речей.

УДК 621.121: 004.77.056:61

Реєстр. № НП 24/25-536. Обсяг 23,5 авт. арк.

Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
проспект Берестейський, 37, м. Київ, 03056
<https://kpi.ua>

Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

© КПП ім. Ігоря Сікорського, 2025

ЗМІСТ

Перелік термінів та визначень	13
Вступ.....	17
1 Як будується інтернет речей.....	21
1.1 IoT-платформи.....	21
1.1.1 Інтернет речей як "мережа мереж"	21
1.1.2 Відмінність від M2M.....	22
1.1.3 Розумний транспорт та послуги.....	23
1.1.4 Торгівля й фінансові послуги.....	24
1.1.5 Лісова промисловість.....	26
1.1.6 IoT у сільському господарстві	26
1.1.6 IoT у промисловості (IIoT)	27
1.2 Бізнес-моделі для впровадження IoT	29
1.3 Технології IoT.....	31
1.3.1 Технічна й комерційна платформа для IoT	31
1.3.2 Вбудовані системи IoT.....	32
1.3.3 Співробітництво виробників вбудованих систем і розроблювачів ПЗ ...	33
1.4 Технологічні проблеми розвитку	33
1.4.1 Дефіцит адрес і перехід до IPv6.....	33
1.4.2 Проблеми живлення сенсорів	34
1.4.3 Стандарти й еталонні архітектури.....	34
1.5 Світовий ринок технологій IoT	35
1.6 Аналітика і аналіз даних великого об'єму	38
Контрольні питання	39
Перелік посилань	40
2 Датчики для систем інтернету речей	42
2.1 Складові частини систем IoT.....	42
2.2 Датчики для систем IoT та їх призначення	43
2.2.1 Загальні зауваження.....	43

2.2.2 Основні характеристики датчиків	43
2.2.3 Структура датчиків	44
2.3 Датчики тиску.....	45
2.3.1 Загальні зауваження.....	45
2.3.2 Датчики тиску компанії Omron.....	47
2.3.3 Що таке п'єзореzystор.....	49
2.3.4 Датчик тиску компанії Honeywell.....	50
2.4 Датчики та енкодери на основі ефекту Холла	52
2.5 Датчики температури	55
2.5.1 Термістори.....	55
2.5.2 Термопари	56
2.5.3 Пірометри й тепловізори	58
2.5.4 Напівпровідникові сенсори температури на основі транзисторів	61
Контрольні питання	62
Перелік посилань	63
3 MEMC-датчики для систем Інтернету речей	65
3.1 Особливості технології MEMC	65
3.2 Пристрої побудовані за MEMC-технологією.....	65
3.3 Датчики тиску.....	67
3.4 Сенсори прискорень та кутових швидкостей	69
3.5 MEMC-мікрофони.....	72
Контрольні питання	76
Перелік посилань	77
4 Оптичні датчики для систем інтернету речей.....	79
4.1 Особливості технології ToF	79
4.2 Тривимірна технологія ToF	81
4.3 Лазерні далекоміри	86
4.3.1 Загальні зауваження.....	86
4.3.2 Джерела лазерного випромінювання	88
4.3.3 Типи лазерних далекомірів	91

4.3.4 Практичні застосування лазерних далекомірів	92
4.4 Оптичні датчики диму	97
4.5 Лазерні та інфрачервоні датчики охорони периметру	102
4.5.1 Загальні зауваження	102
4.5.2 Лазерні датчики охорони	103
4.5.3 Інфрачервоні датчики охорони периметра	106
Контрольні питання	109
Перелік посилань	109
5 Датчики пожежної сигналізації та систем безпеки	112
5.1 Класифікація датчиків систем пожежної сигналізації та охорони	112
5.2 Пожежні датчики	113
5.2.1 Що таке пожежний сповіщувач	113
5.2.2 Види датчиків пожежної сигналізації	114
5.2.3 Безпроводові датчики систем пожежної безпеки	122
5.2.4 Установка сповіщувачів пожежної сигналізації	125
5.2.5 Різновиди систем пожежної сигналізації	125
5.3 Датчики системи безпеки	128
5.3.1 Омічні сповіщувачі (датчики розбиття скла)	128
5.3.2 Контактні датчики систем охоронної сигналізації	130
5.3.3 Датчики руху та розбиття скла для систем охоронної сигналізації	132
5.4 Компоненти систем пожежної сигналізації	135
Контрольні питання	136
Перелік посилань	137
6 "Розумний" будинок та "розумна" будівля	140
6.1 Що таке "розумний" будинок?	140
6.2 Основні системи "розумного" будинку	144
6.2.1 Системи безпеки	144
6.2.2 Системи підтримки мікроклімату	145
6.2.3 Зв'язок через шини будівлі або безпроводовий зв'язок	147
6.2.4 Системи контролю якості повітря	148

6.2.5 Системи освітлення.....	149
6.2.6 Інші системи "розумного" будинку.....	150
6.3 Технології автоматизації.....	151
6.4 Вимоги до функціональності систем "розумного" будинку	153
6.5 Що необхідно автоматизувати в першу чергу у розумних будинках?.....	154
6.6 Системи управління освітленням.....	155
6.7 Драйвери управління світлодіодними світильниками	160
6.8 Світлодіодні лампи та світильники.....	165
6.8.1 Світлодіодні лампи.....	165
6.8.2 Світлодіодні світильники	167
Контрольні питання	172
Перелік посилань	172
7 Системи безпеки та пожежної охорони.....	175
7.1 Системи пожежної охорони.....	175
7.1.1 Загальні зауваження.....	175
7.1.2 Панелі контрольні пожежні.....	177
7.1.3 Підключення сповіщувачів	186
7.1.4 Підключення оповіщувачів	188
7.1.5 Підключення безпроводових сповіщувачів Ajax.....	189
7.1.6 Шлейфи сигналізації.....	190
7.2 Системи контролю доступу	195
7.3 Контролери систем доступу.....	198
7.4 Різновиди систем СКУД.....	201
7.5 Приклади побудови функціональної схеми системи безпеки та пожежної сигналізації	204
Контрольні питання	206
Перелік посилань	207
8 Технологія радіочастотної ідентифікації в системах інтернету речей.....	209
8.1 Технологія радіочастотної ідентифікації.....	209
8.1.1 Загальні зауваження.....	209

8.1.2	Класифікація радіочастотних міток	212
8.1.3	Склад системи радіочастотної ідентифікації	214
8.2	Основні переваги систем радіочастотної ідентифікації	216
8.3	Стандартизація систем радіочастотної ідентифікації	219
8.4	Області застосування систем радіочастотної ідентифікації.....	221
	Контрольні питання	235
	Перелік посилань	235
9	Технологія nfc в системах інтернету речей	237
9.1	Загальні зауваження.....	237
9.2	Режими роботи пристроїв NFC	241
9.2.1	Режим емуляції карти	241
9.2.2	Режим зчитування/запису.....	243
9.2.3	Режим взаємодії двох пристроїв.....	244
9.3	Приклади застосування технології NFC.....	245
9.3.1	Платіжні системи.....	245
9.3.2	"Розумні" плакати.....	246
9.3.3	Громадський транспорт	247
9.3.4	Обмін інформацією	247
9.3.5	Медицина	248
	Контрольні питання	248
	Перелік посилань	248
10	Системи відеоспостереження.....	250
10.1	Призначення систем охоронного відеоспостереження.....	250
10.2	Переваги систем охоронного телебачення.....	253
10.3	Особливості обробки сигналів в охоронному телебаченні	254
10.4	Класифікація цифрових систем відеоспостереження	256
10.4.1	Вступні зауваження.....	256
10.4.2	Огляд можливостей і сфер застосування існуючих систем.....	259
10.5	Склад систем відеоспостереження.....	264
10.6	Приклади найпростіших систем відеоспостереження	265

Контрольні питання	270
Перелік посилань	271
11 Компоненти систем охоронного відеоспостереження	273
11.1 Де потрібно використовувати відеоспостереження	273
11.2 Основні параметри відеокамер	273
11.2.1 Запис і зберігання відео	274
11.2.2 Дозвіл і кут огляду	275
11.2.3 Підсвічування для нічного бачення	277
11.2.4 Можливість запису звуку	277
11.2.5 Наявність можливості встановлення карток пам'яті	277
11.2.6 Формат стиснення інформації та чутливість камери	278
11.2.7 Живлення камер	282
11.3 Особливості обробки сигналів відеокамер	282
11.3.1 Відеокамери "День/Ніч"	282
11.3.2 Робота з ІЧ-підсвіченням	283
11.3.3 Адаптивне ІЧ-підсвічування	284
11.3.4 Компенсація яскравого засвічування	285
11.4 Особливості встановлення телевізійних камер для інтелектуальних	286
відеосистем	286
11.5 Особливості перетворення відеосигналів з поворотних камер у цифровий код	287
11.6 Конструкції відеокамер	290
Контрольні питання	294
Перелік посилань	295
12 Інтерфейси систем IoT	297
12.1 Призначення інтерфейсів	297
12.2 Типові реалізації цифрових інтерфейсів	299
12.2.1 Загальні зауваження	299
12.2.2 Паралельні інтерфейси	300
12.2.3 Послідовні інтерфейси	302

12.3 Комунікаційні інтерфейси RS-232, RS-485 і RS-422	304
12.3.1 Загальні відомості про стандарт RS-485.....	304
12.3.2 Топологія мережі RS-485.....	307
12.3.3 Трансивери RS-485 Texas Instruments	310
12.4 Однопроводовий інтерфейс CAN.....	311
12.5 Внутрішньомодульний інтерфейс I ² C.....	313
12.6 Однопроводовий інтерфейс 1-wire.....	318
12.6.1 Загальні зауваження.....	318
12.6.2 Ведені однопроводові компоненти	321
12.6.3 Лінія зв'язку й топологія	324
12.7 Оптичний інтерфейс із відкритим каналом Irda	325
12.8 Безпроводовий інтерфейс Bluetooth.....	328
Контрольні питання	332
Перелік посилань	332
13 Системи контролю та керування параметрами "розумного" будинку	335
13.1 Використання технологій Інтернету речей для побудови "розумних" будівель	335
13.2 Інсталяційна шина KNX.....	336
13.2 Пристрої для керування освітленням по шині KNX.....	350
13.2.1 Загальні зауваження.....	350
13.2.2 Керування внутрішнім освітленням.....	351
13.2.3 Компоненти MEAN WELL для керування внутрішнім освітленням ..	352
13.3 Централізована система керування "розумним будинком".....	364
13.3.1 Розподілена система керування	364
13.3.1 Централізована система керування	366
13.3.3 Функціональні можливості ПЛК	369
13.3.4 Керування системою на ПЛК.....	371
Контрольні питання	371
Перелік посилань	372
14 Структуровані кабельні системи	374

14.1 Структура СКС.....	374
14.1.1 Топологія СКС.....	374
14.1.2 Комутація в СКС	376
14.1.3 Технічні приміщення СКС	378
14.1.4 Підсистеми СКС	381
14.1.5 Принципи адміністрування СКС	383
14.2 Класи і категорії кабелів, та їх зв'язок з довжинами кабельних трас	384
14.2.1 Кабелі СКС.....	384
14.2.2 Класи додатків, категорії кабелів і роз'єднувачів СКС	386
14.2.3 Обмеження довжини кабелів СКС	389
14.3 Методи проектування СКС.....	390
14.4 Організація кабельних трас.....	393
14.5 Приклад побудови реальної системи СКС.....	399
14.5.1 Кабельні траси	401
14.5.2 Вибір типу кабеля.....	402
14.5.3 Технологічні нюанси прокладання кабеля	403
14.6 Система інтелектуального моніторингу кабельної мережі AMPTRAC.....	404
14.7 Принцип роботи системи AMPTRAC.....	406
Контрольні питання	407
Перелік посилань	408
15 Безпроводові системи зв'язку Інтернету речей	411
15.1 Загальні зауваження.....	411
15.2 Важливість стандартів.....	411
15.3 Технології, засновані на існуючих стандартах мобільного зв'язку	412
15.4 Характерні особливості безпроводових сенсорних мереж.....	417
15.5 Базова архітектура сенсорної мережі.....	420
15.6 Типові архітектури та топології БСМ.....	421
15.7 Безпека у безпроводових сенсорних мережах	423
15.7.1 Загальні зауваження.....	423
15.7.2 Структура протоколу безпеки.....	429

15.8 Безпека в мережах Wi-Fi	431
15.8.1 Загальні зауваження	431
15.8.2 Протокол безпеки WPA2	432
15.8.3 Протокол безпеки WPA3	433
Контрольні питання	434
Перелік посилань	435
16 Технології безпроводових сенсорних мереж	437
16.1 Технології мереж з низьким енергоспоживанням	437
16.1.1 Технологія LORA	437
16.1.2 Технологія SIGFOX.....	442
16.1.3 Технологія NB-IoT	446
16.1.4 Технологія Weightless P.....	448
16.2 Порівняння технологій мереж далекого радіусу дії LPWAN	450
16.3 Мережа на основі HART-протоколу	451
16.4 Безпроводова технологія WirelessHART™	453
16.5. Технологія безпроводового зв'язку ZigBee	455
Контрольні питання	464
Перелік посилань	464
17 Безпроводові натільні та двопротокольні сенсорні мережі.....	468
17.1 Загальні зауваження.....	468
17.2 Стандарт IEEE 802.15.6	469
17.2.1 Загальні зауваження.....	469
17.2.2 Причини стандартизації БНМ.....	470
17.2.3 Прийомопередавачі на основі хаотичних радіоімпульсів.....	473
17.2.4 Фізичний рівень БНМ	474
17.2.5 Додатки БНМ.....	476
17.2.5.5 Штучна сітківка.....	482
17.3 Компоненти безпроводових натільних сенсорних мереж	489
17.3.1 Вимоги до функціональних можливостей БНС-систем.....	489
17.3.2 Фізичні рівні стандарту IEEE 802.15.6 і технології зв'язку.....	490

17.4 Оцінка вимог безпеки БСН	497
17.5 Двопротокольні сенсорні мережі	500
17.5.1 Загальні зауваження	500
17.5.2 Структура сенсорної смарт-мережі	501
17.5.3 Алгоритмічне й програмне забезпечення смарт-мережі	503
Контрольні питання	506
Перелік посилань	507
18 Смарт-технології в IoT	510
18.1 Інтелектуальний будинок	510
18.1.1 Загальні зауваження	510
18.1.2 Комплекс систем безпеки, життєзабезпечення та інформатизації	512
18.1.3 Інтеграція й керування	513
18.1.4 Об'єднана кабельна система (СКС + силова мережа)	515
18.1.5 Стандарти об'єднання систем інтелектуального будинку	516
18.1.6 Енергоефективні будинки	518
18.2 Розумний офіс	521
18.2.1 Особливості БЦ	521
18.2.2 Особливості інженерних систем БЦ	523
18.2.3 Система керування БЦ	526
18.3 Розумне місто	528
18.3.1 Поняття "розумного" міста	528
18.3.2 Система моніторингу вивозу сміття	529
18.3.3 Система виявлення витоків газу	530
18.3.4 Система виявлення аварій на транспорті	531
18.3.5 Інші системи "розумного" міста	533
Контрольні питання	534
Перелік посилань	534

ПЕРЕЛІК ТЕРМІНІВ ТА ВИЗНАЧЕНЬ

АМУ	–	активне мережне устаткування;
АС	–	автоматизована система;
АСУ	–	автоматизовані системи управління\$
АСУ ТП	–	автоматизовані системи управління технологічними процесами;
АЧХ	–	амплітудно-частотна характеристика;
БСМ	–	безпроводова сенсорна мережа;
ВОЛЗ	–	волоконно-оптична лінія зв'язку;
ВП	–	виділене приміщення;
ДТЗ	–	допоміжні технічні засоби;
ДТЗС	–	допоміжні технічні засоби і системи;
ЕМЗ	–	електромагнітна завада;
ЕМПШ	–	електромагнітне поле шуму;
ЕМС	–	електромагнітна сумісність;
ЕРС	–	електрорушійна сила;
ЗІ	–	захист інформації;
ЗОТ	–	засоби обчислювальної техніки;
ЗП	–	закладний пристрій;
ІБ	–	інформаційна безпека;
ІОД	–	інформація з обмеженим доступом;
ІС	–	інформативний сигнал;
ІСБ	–	інтегрована система безпеки;
ІТЗ	–	інженерно-технічний захист;
ІЧ	–	інфрачервоний;
КЗ	–	контрольована зона;
КЗЗ	–	комплексні засоби захисту;
МЕ	–	міжмережевий екран;
НД	–	нормативні документи;

НС	–	небезпечні сигнали;
НСД	–	несанкціонований доступ;
НСД	–	несанкціонований доступ;
НЧД	–	нормований частотний діапазон;
ПЗЗ	–	пристрій з зарядовим зв'язком;
ПКП	–	панель контрольна пожежна;
ПЛК	–	програмований логічний контролер;
РЗП	–	радіозакладний пристрій;
СКС	–	структурована кабельна система;
3GPP	–	The 3rd Generation Partnership Project (консорціум партнерство третього покоління);
B2C	–	Business-to-consumer – "би ту си" (бізнес для споживача);
BCI	–	BatiBUS Club International (європейських асоціація автоматизації будинків);
CAN	–	Control Area Network (послідовна однопроводова шина);
CSS	–	Chirp Spread Spectrum (варіації лінійної частотної модуляції);
DALI	–	Digital Addressable Lighting Interface (стандартний цифровий протокол керування освітленням);
DSR	–	Data Set Ready (готовність кінцевого пристрою до обміну даними);
DTR	–	Data Terminal Ready (готовність контролера до обміну даними);
EHSA	–	European Home Systems Association (європейських асоціація автоматизації будинків);
EIBA	–	European Installation Bus Association (європейських асоціація автоматизації будинків);
HDRi	–	High Dynamic Range imaging (широкий динамічний діапазон);
HLC	–	High Light Compensation (функція компенсації яскравого засвічування)
ICS	–	Industrial Control Systems (промислові системи управління);

IIC	–	Industrial Internet Consortium (промисловий інтернет-консорціум)
IIoT	–	Industrial Internet of Things (промисловий Інтернет речей);
IoT	–	Internet of Things (Інтернет речей)
IP	–	Internet Protocol (Інтернет протокол);
ISA	–	International Society for Automation (міжнародне товариство автоматизації);
IT	–	Information Technology (інформаційні технології);
ITU	–	International Telecommunication Union (міжнародний союз електрозв'язку);
LP-WAN	–	Low-Power, Wide-Area Networks (малопотужні глобальні мережі);
M2M	–	Machine-To-Machine (Від пристрою до пристрою);
MEMS	–	мікроелектромеханічні системи;
NB-IoT	–	Narrowband IoT (вузькосмуговий Інтернет речей);
NFC	–	Near Field Communication (зв'язок на невеликих відстанях);
OCF	–	Open Connectivity Foundation (галузева організація, метою якої є створення стандартної платформи для безпечної взаємодії пристроїв Інтернету речей);
OT	–	Operational Technology (операційні технології);
PTZC	–	Pan Tilt Zoom Camera (роботизована камера);
RFID	–	Radio Frequency IDentification (радіочастотна ідентифікація);
SCADA	–	Supervisory Control And Data Acquisition (диспетчерське управління та збір даних);
SIP	–	Stateful Inspection Protocol (технологія контролю стану протоколу);
SSH	–	протокол Secure Shell;
TLS	–	Transport Layer Security (захист транспортного рівня);
UDP	–	User Datagram Protocol (один із протоколів в стеку TCP/IP);
UNB	–	Ultra Narrow Band (ультра-вузька смуга частот);

VPN	–	Virtual Private Network (віртуальні приватні мереж);
W3C	–	World Wide Web Consortium (міжнародне співтовариство, яке працює спільно над довгостроковим розвитком Інтернету);
WBAN	–	Wireless Body Area Network (безпроводова мережа сенсорів, закріплених на тілі або в тілі пацієнта);
WDR	–	Wide Dynamic Range (широкий динамічний діапазон);
WEP	–	Wired Equivalent Privacy (провідний еквівалент конфіденційності);
WLAN	–	безпроводова локальна мережа;
WMAN	–	безпроводова міська мережа;
WoT	–	набір стандартів консорціуму World Wide Web Consortium Web of Things;
WPA	–	Wi-Fi Protected Access (Захищений доступ по Wi-Fi);
WPAN	–	безпроводова персональна мережа;
WSN	–	Wireless Sensor Networks (безпроводова сенсорна мережа).
WWAN	–	безпроводова глобальна мережа.

ВСТУП

Починаючи з сімдесятих років минулого століття, відтоді, коли широкого застосування знайшли комп'ютери (почався масовий випуск персональних та управляючих комп'ютерів), почалася масова автоматизація по двом практично незалежним напрямкам. Перший – **автоматизація бізнес-процесів**, який отримав назву інформаційні технології (ІТ – **Information Technology**). Другий – **автоматизація технологічних процесів**. Цей напрямок на протигагу ІТ стали називати операційними технологіями (ОТ – **Operational Technology**).

Варто уточнити, ІТ мають справу не з інформацією, а з даними, тому їх було б точніше називати "технології даних". ІТ поєднують у собі комп'ютери, системи зберігання даних і мережі із процесами створення, обробки, зберігання, забезпечення безпеки й обміну будь-якими формами електронних даних. ОТ – це теж комплекс апаратного й програмного забезпечення, але призначеного для контролю й управління фізичними процесами.

Раніше були популярні терміни АСУ (Автоматизовані Системи Управління) і АСУ ТП (Автоматизовані Системи Управління Технологічними Процесами).

Більш сорока років ІТ і ОТ розвивалися незалежно, і за цей час придбали характеристики, що суттєво розрізняють їх. Але в другому десятилітті ХХІ століття під впливом ряду факторів, у тому числі "сенсорної революції", розвитку мережних та хмарних технологій, аналітики великого обсягу даних і інших сучасних трендів почався процес конвергенції (ІТ/ОТ convergence), що поєднує два підходи – орієнтацію на дані й орієнтацію на події у фізичному світі [1].

У віддаленій перспективі варто очікувати появи єдиного цілого, що складається із традиційних технологій для роботи з даними й промисловими системами управління (ICS) і систем диспетчерського управління й збору даних (SCADA).

Процес об'єднання ІТ і ОТ надзвичайно складний, він обговорюється на різних рівнях, у першу чергу в діалозі між двома найбільшими комітетами зі

стандартизації International Society for Automation (ISA) і Industrial Internet Consortium (IIC).

Інтернет – це власне ім'я. Так багато років називається глобальна мережа, побудована на відомих стандартах. Сама популярна Інтернет-платформа WWW (World Wide Web) забезпечує доступ до документів, але дозволяє підключення до цієї мережі різного обладнання. Тобто, для створення технології мереж, що поєднує різноманітне обладнання з використанням Інтернет. Але таке об'єднання й назвати треба якось інакше: не Інтернет, а іншим іменем.

Сумніви відносно назви IoT залишаються хоча б тому, що відомі визначення IoT, запропоновані провідними галузевими аналітиками, ясності не додають. Ось декі з них:

- Gartner – Internet of Things – це мережа фізичних об'єктів, які використовують вбудовані технології, що дозволяють здійснювати взаємодію із зовнішнім середовищем, передавати інформацію про свій стан і отримувати зовнішні дані;
- McKinsey – Internet of Things – це сенсори (датчики) й приводи (виконавче обладнання), вбудовані у фізичні об'єкти й зв'язані через проводові або безпроводові мережі з використанням протоколу Internet Protocol (IP), який зв'язує Інтернет.

Треба пам'ятати, що Інтернет або просто мережа – це всесвітня система об'єднаних комп'ютерних мереж, що служить для зберігання й передавання даних. Вона побудована на базі стеку протоколів TCP/IP. Функція мережі зводиться до передачі пакетів даних. Для більшої частини людства мережа відома тим, що на ній працює всесвітня павутина WWW.

Але існує маса інших систем передавання даних, у тому числі обміну файлами, телефонії та багато інших. Інтернет можна використовувати для організації обміну даними між пристроями (речами). З боку мережі обмежень немає. Чому ж говорять про мережу речей, як про щось окреме й особливе? Ніхто ж не називає WWW "Інтернетом текстів".

Частіше, говорячи про IoT, звичайно мають на увазі не просто комунікації, у щось аналогічне WWW, щось начебто павутини речей, ця обставина була усвідомлена відносно недавно й з'явився відповідний термін **Web of Things** (WoT – описує набір стандартів консорціуму World Wide Web Consortium (W3C) для взаємодії різних платформ Інтернету речей (IoT) і доменів додатків), який точніше підходить ніж IoT.

Підміна понять виникла й зміцнилося через відсутність розуміння відмінностей між Інтернетом і WWW. Всесвітня павутина – це розподілена система, що надає доступ до зв'язаних між собою документам, розташованим на різних комп'ютерах, підключених до Інтернету. Можливість доступу до документів забезпечується мовою розмітки HTML (Hypertext Markup Language). Стандартним чином розмічені HTML-файли (веб-сторінки) є основним типом ресурсів всесвітньої павутини.

Самі по собі текстові документи не складні, а трьох складових – унікальної системи адресації документів URL/URI, мови HTML і протоколу HTTP – виявилось досить для того, щоб забезпечити людству можливість комунікації.

Швидше за все, у термінологічній плутанині "винуватий" Кевін Ештон. Це він запропонував термін Internet of Things, хоча в 1999 році він думав не про мережу речей, а про павутину речей. От, що він написав пізніше в 2009 році: *"Якби в нас були комп'ютери, які знали все те, що ми знаємо про речі, збираючи дані про них без нашої допомоги, то ми змогли б більш ефективно контролювати все навколишнє середовище. Нам потрібно модернізувати комп'ютери настільки, що вони змогли чути й бачити світ у всьому його розмаїтті"*.

Зовсім очевидно, він визнає, що не ідеться про мережі передавання даних, а про деяку інформаційну павутину, що полягає з образів речей.

Зараз у консорціумі W3C створена робоча група Web of Things Interest Group, ведуться роботи, націлені на розробку стандартів, але ця справа надзвичайна довга, оскільки обладнання (речі) не порівнянні по складності й різноманітності з текстами. Відповідно стандартизація взаємодії між пристроями на декілька

порядків складніша від того, що було зроблено для текстів. Ці роботи займуть не один рік. А доти буде вживатись неточний термін IoT.

На сьогоднішній день Інтернет речей (IoT) визначається ITU (International Telecommunication Union – Міжнародний союз електрозв'язку) як динамічна глобальна Мережева інфраструктура з можливостями самоконтактування на основі стандарту і взаємодіючих комунікаційних протоколів, де фізичні та віртуальні "Речі" мають ідентичність, фізичні атрибути та віртуальні особистості, використовують інтелектуальний Інтерфейси та інтегровані в інформаційну мережу.

1 ЯК БУДУЄТЬСЯ ІНТЕРНЕТ РЕЧЕЙ

1.1 IoT-платформи

1.1.1 Інтернет речей як "мережа мереж"

Інтернет речей складається зі слабо зв'язаних між собою розрізнених мереж, кожна з яких була розгорнута для розв'язку своїх специфічних завдань. Приміром, у сучасних автомобілях працюють відразу кілька мереж: одна управляє роботою двигуна, інша – системами безпеки, третя підтримує зв'язок і т.д. В офісних і житлових будинках також установлюється безліч мереж для управління опаленням, вентиляцією, кондиціонуванням, телефонним зв'язком, безпекою, освітленням. У міру розвитку Інтернету речей ці й багато інших мереж будуть підключатися одна до одної й формувати більш широкі можливості в сфері безпеки, аналітики й управління (рис. 1.1). У результаті Інтернет речей придбає ще більше можливостей відкрити людству нові, більш широкі перспективи [1, 2].

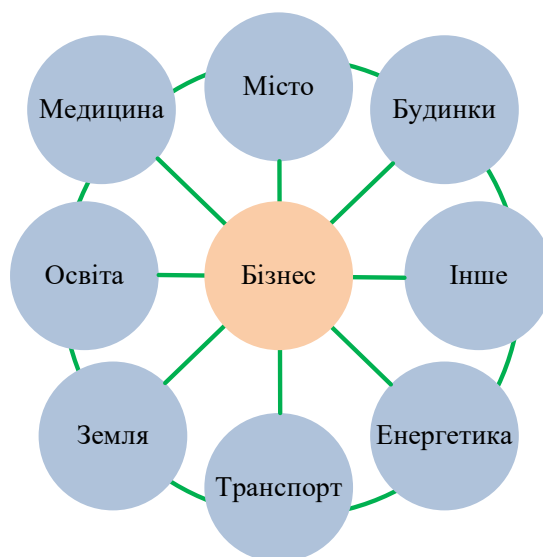


Рисунок 1.1 – Приклад об'єднання різних мереж у єдину мережу

Ця тенденція аналогічна тій, що спостерігалася на ранніх етапах розвитку мережних технологій. Наприкінці 1980-х – початку 1990-х років Cisco сформувалася як велика компанія саме завдяки своїм зусиллям по встановленню зв'язку між різнорідними мережами за допомогою багатопроTOCOLЬНОЇ маршрутизації, яка в остаточному підсумку зробила протокол IP

загальноприйнятим мережним стандартом. У тому, що стосується Інтернету речей, історія повторюється, але в значно більших масштабах.

1.1.2 Відмінність від M2M

Інтернет речей (Internet of Things, IoT) – концепція, яка припускає більш широке застосування технології M2M (Machine-To-Machine). Сегмент M2M багато в чому є основою концепції IoT (рис. 1.2), а на початковому етапі розвитку IoT був фактично синонімом M2M [3].



Рисунок 1.2 – Облaсті застосування технології M2M та IoT [4]

За даними світових аналітиків, у використанні технологій Інтернету провідні компанії орієнтуються в першу чергу на масові сегменти IoT, де є широкий попит, такі як:

- Інтернет речей в телекомунікаціях;
- розв'язки для створення інтелектуальних сервісів безпеки ("Розумний будинок");
- розв'язки для створення інтелектуальних сервісів оптимізації використання ресурсів домогосподарствами ("Розумний будинок").

1.1.3 Розумний транспорт та послуги

Нижче наведені приклади застосування технології IoT на транспорті (рис. 1.3 та 1.4). На рис. 1.4 показано яку інформацію можна отримати про переміщення товарів:

- вартість перевезення різними видами транспорту;
- час перевезення;
- місце та час перевантаження вантажів;
- необхідні механізми для завантаження/розвантаження;
- інформація про розміщені у контейнерах чи транспортних засобах вантажів та багато іншого.



Рисунок 1.3 – IoT-рішення про переміщення вантажів на транспорті [5]

Складна транспортна інфраструктура "розумного" міста може бути об'єднана в єдину систему (рис. 1.4), що дозволяє:

- контролювати завантаженість доріг та мостів;

- виклик таксі;
- рух міського транспорту;
- порушення швидкісного режиму;
- наявність і розташування закладів громадського харчування;
- міську мережу Wi-Fi;
- місця культурного відпочинку і багато чого іншого.

У переліку відсутні системи управління споживанням води, газу, тепла, електроенергії, освітлення вулиць та контролю стану цих та інших систем.



Рисунок 1.4 – Транспортні IoT-рішення для "розумного" міста [6]

Місто, у якому точно відомо, як пересуваються його жителі, можна побудувати найбільш ефективну транспортну систему.

1.1.4 Торгівля й фінансові послуги

У торгівлі та фінансах технології IoT можуть бути використані для:

- для автоматичної передачі й аналізу даних з POS-терміналів, включаючи віртуальні;
- контролю наявності товарів на складах;
- контроль місця розташування товару на складах;
- контроль перевезень товарів від виробників до магазинів;
- управління запасами домогосподарств (як сервіс).

Завдяки Інтернету речей класичні магазини вже можуть скласти конкуренцію онлайн-магазинам, запропонувавши унікальний, персоналізований і привабливий сервіс своїм клієнтам (рис. 1.5). Застосування IoT-технологій залежить від конкретної сфери. Самими популярними категоріями підключеного обладнання у сфері роздрібної торгівлі й дистрибуції виявилися: сканери штрих-кодів, особисті мобільні пристрої, а також "розумні" гучномовці, телевізори, акустичні системи [4].

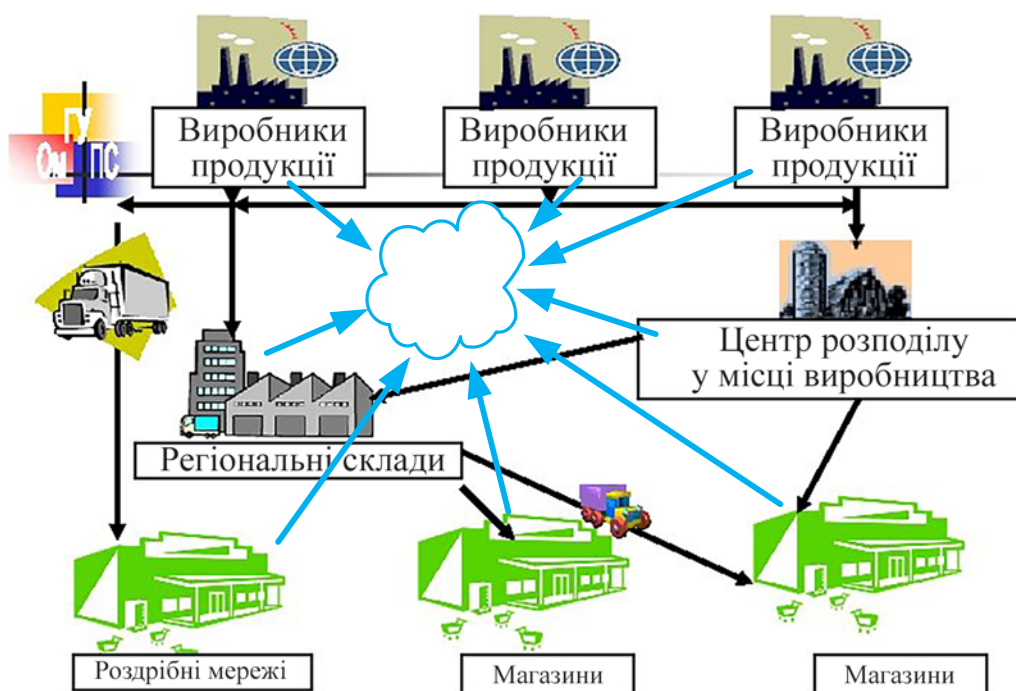


Рисунок 1.5 – Рішення IoT про переміщення та наявність товарів [7]

Переваги Інтернету речей говорять самі за себе, однак його використання не позбавлене погроз в області безпеки. Серед опитаних представників компаній, які

вже застосовують IoT-розв'язки, 84% зіштовхнулися з порушеннями безпеки. Більше половини респондентів вважають зовнішні кібератаки головним бар'єром на шляху впровадження цієї технології.

1.1.5 Лісова промисловість

Усі країни-експортери лісу говорять про зростаючий світовий попит на деревину. Однак успіх прийде до тих, хто буде управляти зеленими ресурсами розумно, тобто із застосуванням високих технологій. Сьогодні в смартфоні можна так само просто, як у мобільній грі, подивитися на дані аерофотознімання лісового масиву, оцінити запаси, проконсультуватися з експертом. Так само просто продати ліс і замовити послуги з висаджування або рубанню рослин.

1.1.6 IoT у сільському господарстві

Широкі можливості надає використання систем IoT у сільському господарстві. Перелічимо деякі з них (рис. 1.6):

- аналіз стану ґрунту;
- моніторинг стану сільгоспугідь;
- збір кліматичних даних;
- точний посів (точне землеробство);
- внесення добрив;
- захист рослин;
- моніторинг руху транспорту та витрат паливно-мастильних матеріалів;
- аналіз отриманих даних та прийняття рішень.

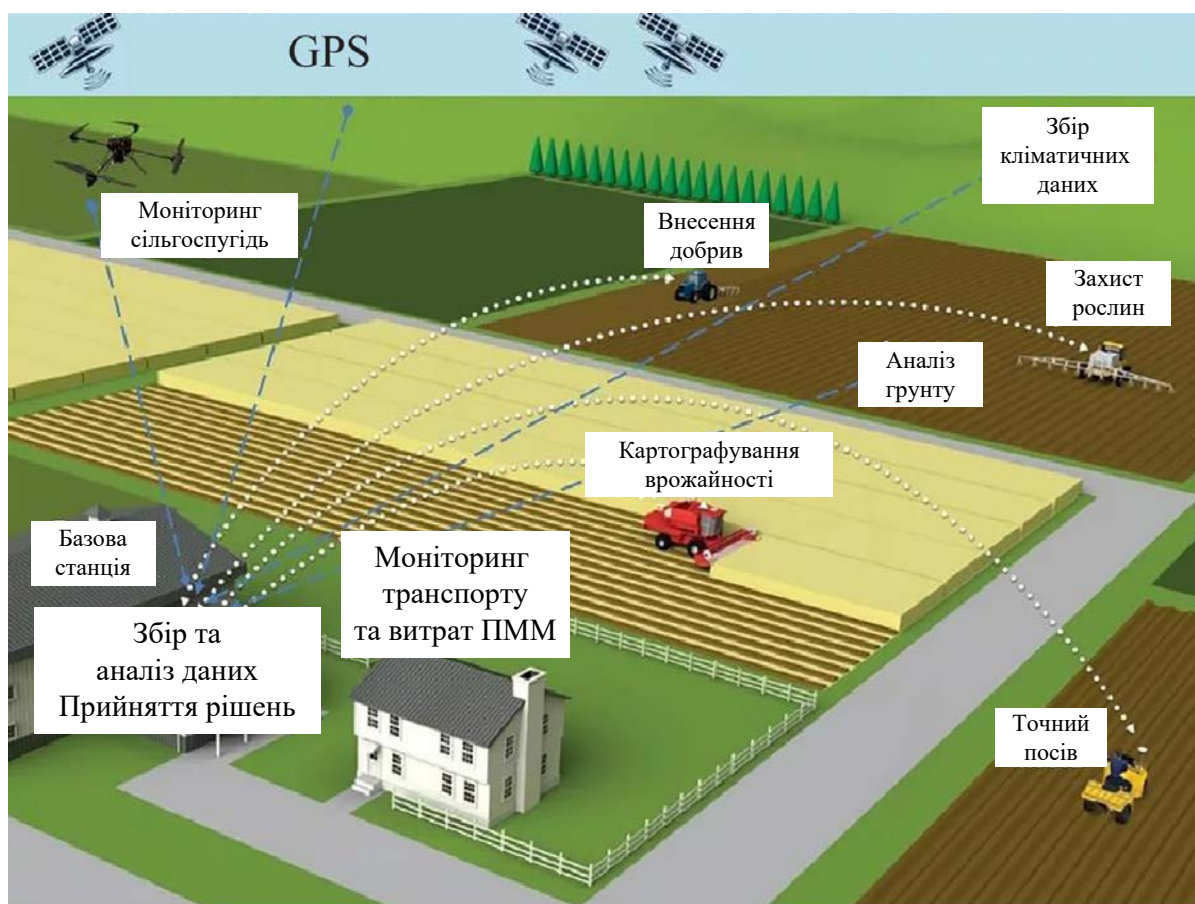


Рисунок 1.6 – IoT у сільському господарстві [8]

Всі перелічені (і ще багато інших) функції можна реалізувати використовуючи глобальні мережі позиціонування (наприклад, GPS, GLONASS, BAIDU та інші) та сенсорні мережі з низьким енергоспоживанням.

1.1.6 IoT у промисловості (IIoT)

Якщо будувати автоматизовані системи управління на принципах IoT, то всі виробничі процеси будуть докладно обмірювані й оптимізовані. Виробництво стане набагато більш надійним – системи моніторингу будуть повідомляти про проблемні ділянки до того, як вони вийдуть із ладу. Такі системи отримали назву IIoT – Industrial IoT. Інша назва що набула поширення – індустріальна революція 4 (Industry 4).

Центральне місце в концепції ІоТ займає промисловий Інтернет. Саме він забезпечує основну інфраструктуру, яка підтримує підключене устаткування й передавання даних. Цей термін означає інтеграцію машин з сенсорами, програмним забезпеченням і системами зв'язку, які разом утворюють Інтернет речей. Промисловий Інтернет поєднує технології й процеси з таких областей, як дані великого обсягу, самонавчання машин і комунікація між машинами (Machine to Machine – M2M).

Сьогодні промисловий Інтернет тісно пов'язаний з розумними лічильниками обліку споживання, відстеженням транспортних засобів і майна, а також оптимізацією роботи заводів, устаткування й машин. Однак у наступні кілька років існуючі цифрові пристрої будуть набагато більш тісно пов'язані з роботою устаткування. Крім того, промисловий Інтернет стане служити фундаментом для різноманітних споживчих пристроїв і систем (рис. 1.7).



Рисунок 1.7 – Ілюстрація деяких функцій промислового Інтернету речей [9]

Загалом архітектуру ІоТ у світовому масштабі можна представити як показано на рис. 1.8.

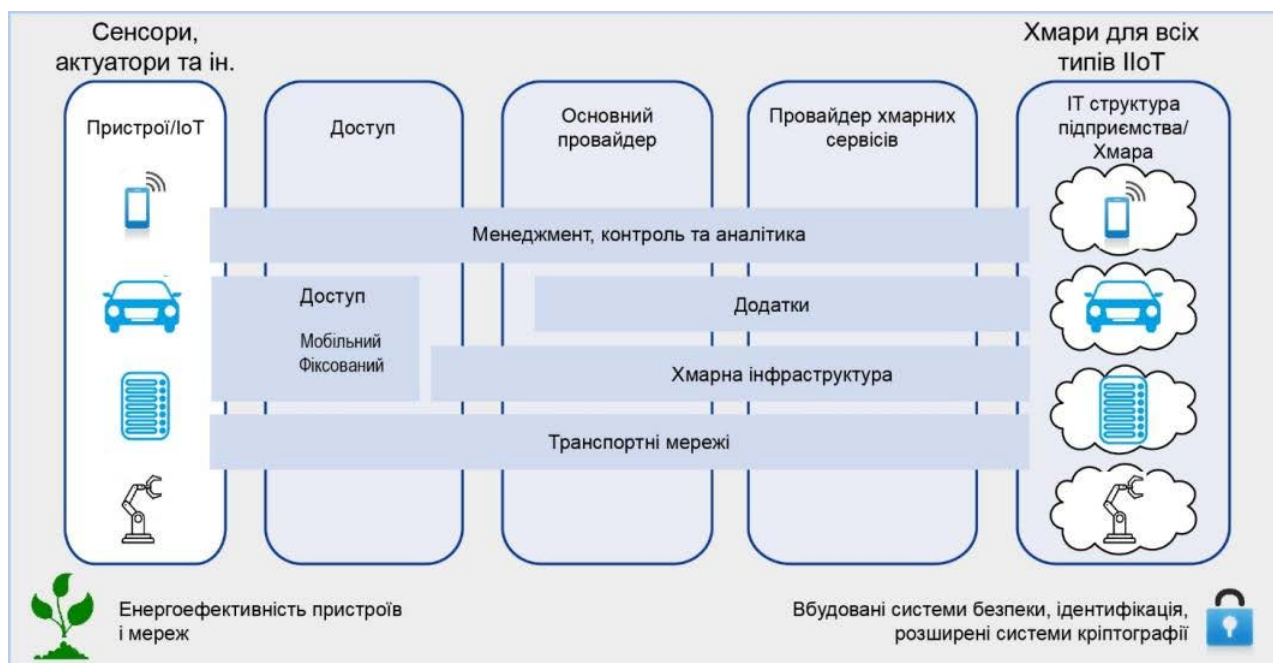


Рисунок 1.8 – Світова IoT-архітектура

1.2 Бізнес-моделі для впровадження IoT

На сьогоднішній день кількість підключених пристроїв, оснащених "розумними" сенсорами IoT, вже перевищує чисельність мобільних телефонів. Вендори (постачальники продукції) активно інвестують в розробку й впровадження IoT-розв'язків. Згідно з новим звітом IDC про світові витрати на Інтернет речей, у 2023 р. вони становили 805,7 млрд доларів. Очікується, що інвестиції в екосистему IoT перевищать 1 трлн дол. у 2026 році, а середньорічний темп зростання складе 10,4% протягом прогнозованого періоду 2023-2027 років.

Два варіанти використання Інтернету речей, які отримали найбільше інвестицій у 2023 році, тісно пов'язані з виробничими галузями [5]: виробничі операції (73,0 млрд дол.) та управління виробничими активами (68,2 млрд дол.). Наступні найбільші сфери використання – Інтелектуальна аналітика запасів (37,6 млрд дол.), розумні мережі в електроенергетиці (36,9 млрд дол.) та стійкість ланцюгів поставок (31,6 млрд дол.) отримали значні інвестиції з боку галузей роздрібної торгівлі та комунальних послуг. Найшвидше зростання витрат спостерігається в таких сферах застосування технологій Інтернету речей, як

зарядка електромобілів (30,9%), "нові" типи пристроїв мережевого захисту (14,5%), моніторинг сільськогосподарських земель (13,9%), а також підключені торгові автомати і камери схову (13,8%).

Основні бізнес-моделі, по яких будуть впроваджується IoT:

1. "Нормативний контроль". Дотримання вимог контролюючих організацій є необхідною умовою для ведення бізнесу, але прямій економічної вигоди вони компаніям не приносять, незважаючи на значні витрати. У контексті даної ситуації IoT має величезний потенціал по скороченню витрат у цій області.

2. "Превентивний контроль": IoT дозволяють вчасно виявляти передумови для аварійних ситуацій і зниження ефективності роботи устаткування. Завдяки IoT можна запустити дистанційний моніторинг і стежити за роботою устаткування онлайн у реальному часі.

3. "Дистанційна діагностика". Сенсори IoT можуть використовуватися для діагностики обладнання, на якому вони встановлені, і автоматично реагувати на зміни їх стану.

4. "Контроль операцій". За допомогою IoT можна контролювати ланцюжок технологічних операцій, здійснювати контроль переміщення будь-якого обладнання чи продукції і автоматично відслідковувати їхні характеристики в реальному часі. Це дозволяє позбутися злочинства й неконтрольованих втрат, підвищити ефективність роботи підконтрольних об'єктів, де встановлені "розумні" сенсори, добитися передбачуваності їх експлуатації.

5. "Автоматизація операцій". Прихід IoT дозволяє автоматизувати часто повторювані операції, підвищуючи ефективність роботи, якість дозвілля, ступінь задоволеності клієнтів. Переваги таких IoT-гаджетів виражається не тільки в спрощенні рутинних операцій. Вони стимулюють продажі, дозволяючи автоматизувати звички.

1.3 Технології IoT

1.3.1 Технічна й комерційна платформа для IoT

Успішна реалізація розв'язків на базі Інтернету – не ізольований і незалежний процес. В Cisco вважають, що для цього потрібні технічна й комерційна платформи, на яких можна буде легко вишиковувати різні розв'язки для раціонального й ефективного досягнення обіцяних комерційних переваг. В основі такої платформи Інтернету лежать надійний зв'язок і технологічна інфраструктура, операційні й управлінські сервіси, а також ряд вертикальних і горизонтальних розв'язків.

Досвід Cisco показує, що для реалізації розв'язків на базі Інтернету всі технічні й комерційні елементи повинні забезпечувати потрібний результат. Ефективне розгортання систем Інтернету забезпечить таку платформу для всього бізнесу або навіть для всіх галузей, яка дозволить реалізовувати цілий ряд унікальних прибуткових розв'язків на базі IoT.

Рівні, починаючи з нижнього:

1. Мережеві підключення – з'єднання всіх розв'язків, даних і додатків за допомогою оптоволоконної транзитної або ліцензованої стільникової мережі.

2. Мережний доступ – керована мережа Wi-Fi або інша неліцензована безпроводова мережа для підключення всіх сенсорів і додатків.

3. Технологічна платформа – платформа, що забезпечує швидке й надійне підключення нових пристроїв до архітектури за принципом "підключи й працюй", а також з'єднання із хмарними сервісами зберігання й обробки даних.

4. Вертикальні й горизонтальні розв'язки – сукупність пристроїв і додатків, що забезпечує унікальні розв'язки для різних вертикальних і горизонтальних галузевих сегментів.

5. Платформа монетизації – у деяких вертикалях, таких як "розумні" міста й сегмент B2C, існують можливості ефективного використання платформи для створення нових джерел прибутку.

B2C (*Business-to-consumer* – "би ту си", Бізнес для Споживача,) – термін, що означає комерційні взаємовідносини між організацією (*Business*) і

споживачем, так званім "кінцевим споживачем" (consumer). Також це форма електронної торгівлі, мета якої – прямі продажі для споживача.

6. Загальна платформа управління – загальна платформа, що забезпечує управління, обслуговування клієнтів і сервіси для всіх розв'язків.

7. Професійні послуги – спеціальні сервіси, такі як інтеграція систем, планування й проектування.

8. Керівництво проектом – сервіси по керуванню проектом, операціями й екосистемою партнерів.

1.3.2 Вбудовані системи IoT

Світовий ринок систем, що вбудовуються, росте, що обумовлене збільшенням попиту на портативне комп'ютерне обладнання, в яке вбудовуються розв'язки M2M. Іншими ключовими драйверами росту в останні роки стали тенденція до автоматизації обробної промисловості, безперервна еволюція комп'ютеризації, а також широке поширення Інтернету речей.

Сучасна концепція Інтернету речей передбачає, що все сучасне обладнання незалежно від платформи повинно мати можливість спільно функціонувати з іншим обладнанням й сервісами, утворюючи єдину взаємозалежну систему, а не існувати ізольовано.

Саме ця передумова є однією з основних причин трансформації ринку вбудованих систем. Сьогодні він рухається в напрямку розробки інтелектуальних систем (сенсорів, машин, механізмів, приладів і т.д.), об'єднаних у єдину глобальну обчислювальну мережу з метою одержання й обробки даних для підвищення ефективності виробництва (у промисловій сфері) або комфорту й зручності користувача (на рівні споживача).

1.3.3 Співробітництво виробників вбудованих систем і розроблювачів ПЗ

При такому значному зростанні ринку систем, що вбудовуються, і кількості кінцевих підключених до мережі й один до одного пристроїв уже зараз відчувається серйозна потреба в розроблювачах програмного забезпечення, що розуміють усю складність таких систем.

Це викликано тим, що потрібно забезпечити збір необхідної інформації, її аналіз, відображення й взаємодію з іншими системами виробника. Окремі деталі цього ПЗ можуть відрізнятися залежно від завдань конкретного виробника (ОЕМ), а для налаштування під окремих замовників у виробників сенсорів (контролерів, мікропроцесорів і т.д.) не завжди є достатні ресурси й можливості. Саме на цьому етапі потрібна підтримка досвідченої компанії-розроблювача розв'язків, що вбудовуються.

1.4 Технологічні проблеми розвитку

1.4.1 Дефіцит адрес і перехід до IPv6

Є фактори, здатні сповільнити розвиток Інтернету речей. З них найважливішими вважаються три:

- перехід до протоколу IPv6;
- енергоживлення сенсорів;
- прийняття загальних стандартів.

У лютому 2010 року у світі не залишилося вільних адрес IPv4. Хоча рядові користувачі не знайшли в цьому нічого страшного, даний факт може суттєво сповільнити розвиток Інтернету речей, оскільки мільярдам нових сенсорів знадобляться нові унікальні IP-адреси. Крім того, IPv6 спрощує управління мережами за допомогою автоматичного налаштування конфігурації й нових, більш ефективних функцій інформаційної безпеки.

1.4.2 Проблеми живлення сенсорів

Щоб Інтернет речей повністю реалізував свої можливості, його сенсори повинні працювати автономно. Зараз автономні пристрої живляться від батареї чи акумулятора. Але оскільки їх ємність обмежена, то виникає проблема їх заміни або пошуку альтернативних джерел живлення. Перспективним є використання сенсорів з живленням від сонячних батарей та збирачів енергії.

Ще один напрямок – перетворення в електроенергію людських рухів (навіть руху одного пальця) за допомогою мініатюрних генераторів. Про такі генератори було оголошено в березні 2011 року на 241-х зборах Американського хімічного суспільства. Але поки такі пристрої не знайшли широкого застосування.

1.4.3 Стандарти й еталонні архітектури

Хоча в області стандартів був досягнутий значний прогрес, попереду ще чекає велика робота, особливо в таких областях, як безпека, захист особистої інформації, архітектура й комунікації. IEEE – одна з організацій, що намагається розв’язати зазначені проблеми за рахунок стандартизації методів передачі пакетів IPv6 по мережах різних типів.

Розробкою універсальних специфікацій для "розумної" електроніки й відповідної програми сертифікації займаються кілька організацій, серед яких альянс Open Connectivity Foundation (OCF), у який входять Dell, Intel і Samsung Electronics.

До системотворчих рівнів IoT можна віднести чотири рівні: обладнання, зв’язок, обробка й управління даними. Свої еталонні моделі пропонують США, Німеччина і ЄС, а також Китай (рис. 1.9).

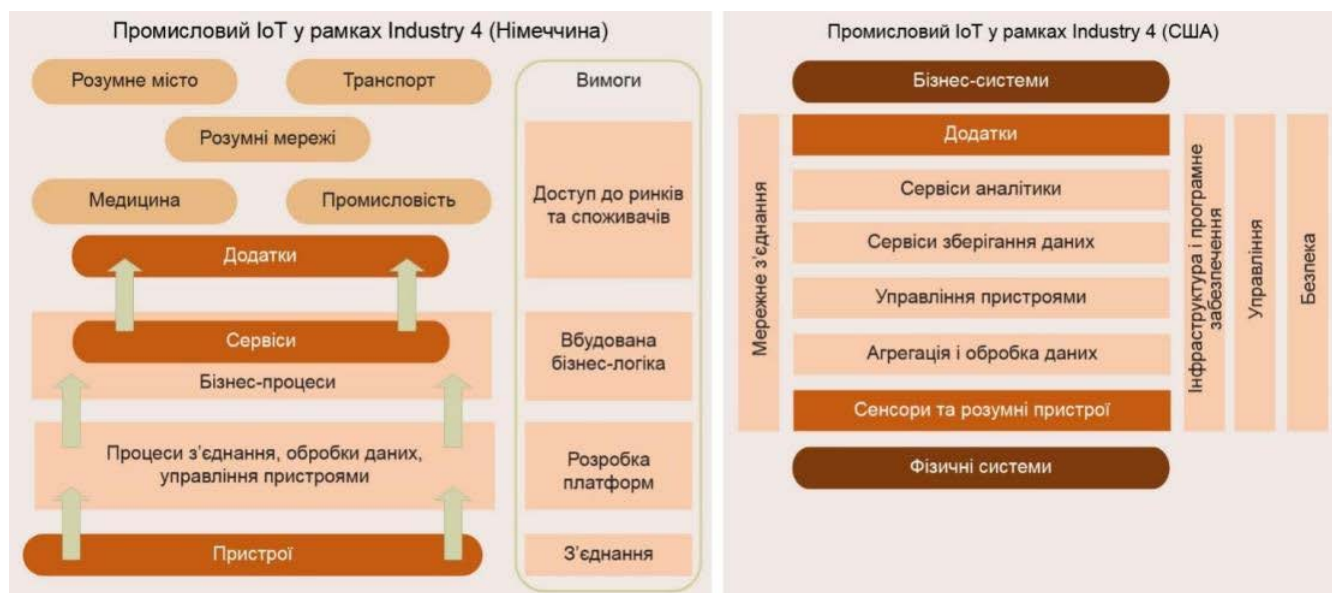


Рисунок 1.9 – Деякі архітектури промислового Інтернету речей

Найбільш активна робота на всіх рівнях IoT-платформ іде в області стандартизації. Ведеться робота в області стандартів, що покривають усі рівні архітектури IoT. Координатори: Міжнародний союз електрозв'язку (ITU), Асоціація по стандартизації Інституту інженерів з електротехніки й електроніки (IEEE Standards Association), консорціуми Open Interconnect, W3C і ін.

1.5 Світовий ринок технологій IoT

Як він з'явився [10]:

- 1926 р. – передбачення Ніколи Тесли *;
- 1990 р. – Джон Ромки створив першу у світі Інтернет-річ – підключений до мережі тостер і зміг віддалено включити й виключити його;
- 1999 р. – Кевін Ештон (Auto-Id Center) на презентації для керівництва Procter&Gamble сформулював концепцію IoT.

** В 1926 Нікола Тесла в інтерв'ю для журналу "Collier's" сказав, що в майбутньому радіо буде перетворено в "великий мозок", усі речі стануть частиною єдиного цілого, а інструменти, завдяки яким це стане можливим, будуть легко міститися в кишені.*

Перша "Інтернет-річ" з'явилася в 1990 році. Це тостер, розроблений американцем Джоном Ромки, одним із творців протоколу TCP/IP. Приєднавши кухонного помічника до Всесвітньої павутини, інженер зумів включити й виключити його віддалено. Просто так, забави заради, не підозрюючи, що його експеримент стане спусковим механізмом, який викличе "ефект лавини" і почне формувати нову реальність.

Інтернет речей зародився в Масачусетському технологічному інституті. В 1999 році там був створений центр автоматичної ідентифікації (Auto-Id Center), що займався радіочастотною ідентифікацією (RFID) і новими сенсорними технологіями. Центр координував роботу семи університетів, розташованих на чотирьох континентах. Саме тут була розроблена архітектура Інтернету речей.

В 2003 році на нашій планеті проживало близько 6,3 млрд людей, а до Інтернету було підключено 500 млн пристроїв. Розділивши кількість підключених пристроїв на величину населення земної кулі, ми побачимо, що на кожну людину тоді доводилося по 0,08 такого пристрою (рис. 1.10) [11]. Таким чином, відповідно до визначення Cisco IBSG, в 2003 році Інтернету речей ще не було. Смартфони у той час тільки з'явилися на ринку. Наприклад, iPhone був анонсований 9 січня 2007 року.

В 2010 році в результаті стрімкого поширення смартфонів і планшетних комп'ютерів кількість підключених пристроїв значно зросла і уперше в історії на кожну людину стало доводитися більш одного підключеного пристрою (1,84 на душу населення).

Дослідники Cisco IBSG зробили висновок про те, що Інтернет речей "з'явився на світ" у проміжку між 2008 і 2009 роками. Сьогодні Інтернет речей існує, чому в чималому ступені сприяють такі ініціативи як Cisco Planetary Skin, Smart Grid і поява "розумних" автомобілів.

На рис. 1.12 наведено декілька напрямків розвитку Інтернету речей для споживачів.

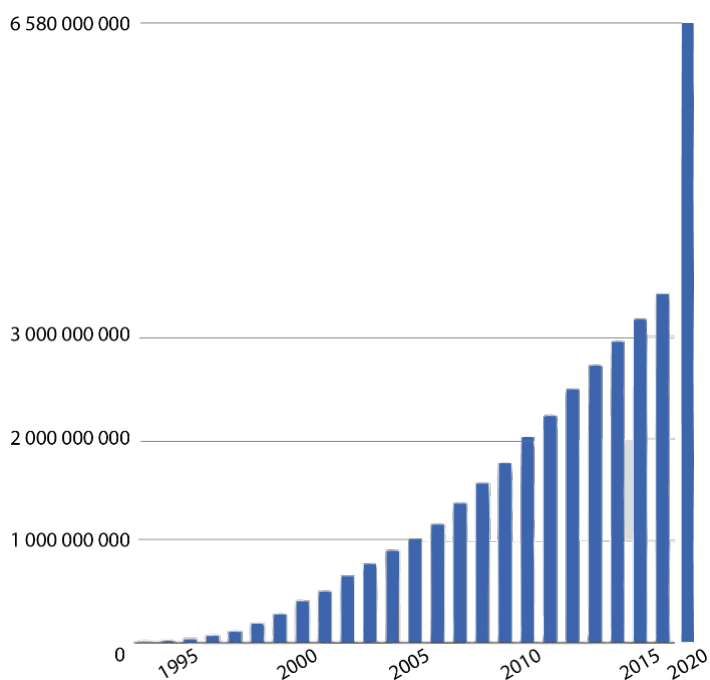


Рисунок 1.10 – Динаміка зміни кількості користувачів та пристроїв під'єднаних до Інтернету [12]



Рисунок 1.11 – Динаміка зміни кількості пристроїв під'єднаних і прогнозованих до Інтернету [12]

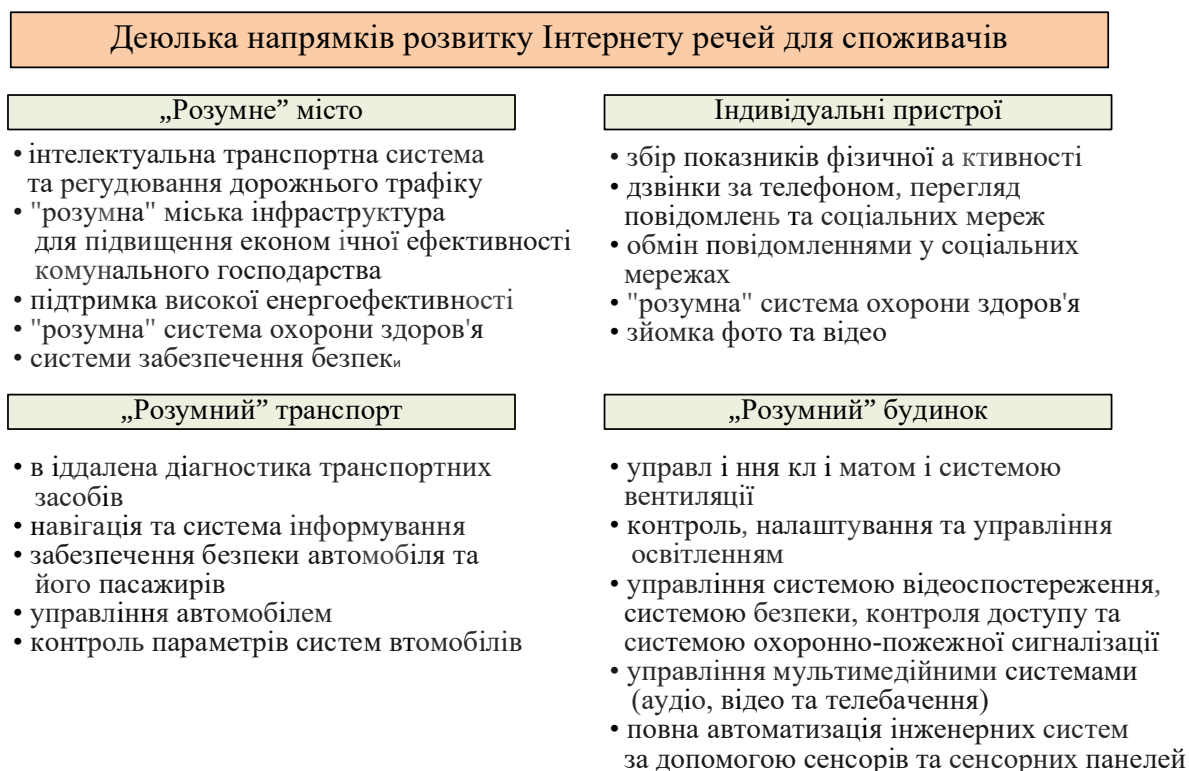


Рисунок 1.12 – Інтернет речей для споживачів

1.6 Аналітика і аналіз даних великого об'єму

Аналітика дозволяє збільшити ефективність бізнесу на основі прийняття більш ефективних розв'язків на базі зібраних за допомогою IoT-технології даних, у тому числі із застосуванням технології Big Data [12]. Надалі буде використовуватися термін великі дані. До даного сектору також відносяться аналітичні розв'язки, що з'являються, які дозволять забезпечувати інтеграцію даних, отриманих на базі моніторингу IoT і соціальних мереж.

Хмарні обчислення дозволяють створювати спрощені й більш дешеві кінцеві пристрої, оскільки інтелектуальну складову можна перенести з цих пристроїв у хмару. Інструменти великих даних, у тому числі програми з відкритим вихідним кодом дозволяють аналізувати величезні масиви даних, що генеруються IoT-пристроями.

Використання даних, одержуваних від сенсорів для аналізу й виявлення тенденцій і взаємозв'язків, можуть генерувати корисну бізнес-інформацію.

Потік даних від об'єктів що підключаються і устаткування розростається в геометричній прогресії. Згідно зі звітом компанії по керуванню даними Wipro за назвою "Великі дані: прискорення процесів виробництва", за час шестигодинного рейсу на Боїнгу-737 з Нью-Йорка в Лос-Анджелес генерується колосальна кількість інформації – 120 Тбайт. Уся вона збирається й зберігається на борту літака. Що ще більш важливо, ці дані можуть бути проаналізовані, щоб виявити всі аспекти роботи двигуна. Не дивно, що інформація стає цінним економічним активом.

По оцінці Mckinsey Global Institute, великі дані можуть знизити витрати на розробку продукції виробничих компаній на 50% і більше. Вивчення величезної кількості точок вводу даних аналітичними програмами приведе до виявлення недоліків як товарів так і послуг, знизить експлуатаційні витрати й у корені змінить підхід компаній до інвестування в людей і устаткування.

Картина дійсно міняється в міру того, як компанії вчаться одержувати доступ до великих даних і використовувати їх. Хоча бази даних, програмні додатки й неструктуровані потоки інформації вже приносять масу нових знань, ці джерела блякнуть на тлі великої й ще не дослідженої області даних, яка існує в межах фізичних границь нашої планети.

Контрольні питання

1. Яка різниця між технологіями M2M та IoT?
2. Що мається на увазі під терміном "розумний" транспорт?
3. Що мається на увазі під терміном "розумний" будинок?
4. Для чого можна використати IoT у сільському господарстві?
5. В чому полягають проблеми живлення сенсорів?
6. Чому використовують протокол IPv6?
7. Що означає скорочення IIoT?
8. Чи прогнозується подальший розвиток IoT і в яких областях найшвидше?
9. У чому полягають відмінності між IoT і IIoT?

10. Для чого використовуються хмарні сховища?

Перелік посилань

1. Dr. Ovidiu Vermesan Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. Published, sold and distributed by: River Publishers, 2013. pp. 363.
2. O. Vermesan, P. Friess Internet of Things – From Research and Innovation to Market Deployment. River publishers, 2014. pp. 374. (River publishers series in communications). Url: https://www.academia.edu/24701833/Internet_of_Things_From_Research_and_Innovation_to_Market_Deployment_River_Publishers_Series_in_Communication. (дата звернення: 29.06.2024).
3. Ad-hoc & sensor networking for M2M Communications. Threat Landscape and Good Practice Guide / European Union Agency for Network and Information Security. January 2017 Url: <http://www.enisa.europa.eu/>. (дата звернення: 29.06.2024).
4. M2M и IoT. Url: <https://shop-gsm.ua/ru/blog/m2m-i-iot/> (дата звернення: 29.06.2024).
5. Looking to transform your freight forwarding or shipping business digitally? Url: <https://logistaas.com/why-do-freight-forwarders-need-transportation-management-systems/> (дата звернення: 29.06.2024).
6. Generative AI Solutions for Smart Cities. Url: <https://xcognition.ai/generative-ai-solutions-for-smart-cities/> (дата звернення: 29.06.2024).
7. Сфери застосування логістики. Url: <https://ppt-online.org/256032> (дата звернення: 29.06.2024).
8. Agricultural guidance system geotrack explorer plus RTK. Url: <https://shop.gpsgeometer.com/en/products/sistema-parallelnogo-vozhdeniya-kursoukazatel-geotrek-eksplorer-plus-gm-smart-2-10-gts> (дата звернення: 29.06.2024).

9. Industrial Internet of Things & Industry 4.0. Url: <https://www.zen-networks.io/industrial-internet-of-things-industry-4-0/> (дата звернення:29.06.2024).
10. Marina Ruggieri, Homayoun Nikookar Internet of Things – From Research and Innovation to Market Deployment. River Publishers Series In Communications, 2014. pp. 374. Url: <http://riverpublishers.com/river-publisher/series.php?msg=Communications>. (дата звернення:29.06.2024).
11. Світові витрати на Інтернет речей. Url: https://ko.com.ua/svitovi_vitrati_na_internet_rechej_perevishhat_1_trln_dol_u_2026_roci_144424 (дата звернення:29.06.2024).
12. Доступ до Інтернету у світі. Url: <https://newreporter.org/2016/03/28/dostup-k-internetu-v-mire-statistika-trendy/> (дата звернення:29.06.2024).
13. Big Data. Url: <https://www.it.ua/knowledge-base/technology-innovation/big-data-bolshie-dannye> (дата звернення:29.06.2024).

2 ДАТЧИКИ ДЛЯ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Складові частини систем IoT

Розвиток технологій та систем, таких як нанoeлектроніка, комунікації, датчики, вбудовані системи, хмарні мережі, віртуалізація та програмне забезпечення буде важливим для розвитку систем IoT усюди. На базі існуючих та нових технологій вже створено велика кількість додатків та сервісів, які дозволяють охопити багато сфер діяльності людини. На рис. 2.1 умовно показано з яких рівнів та складових утворюються різноманітні системи IoT [1].

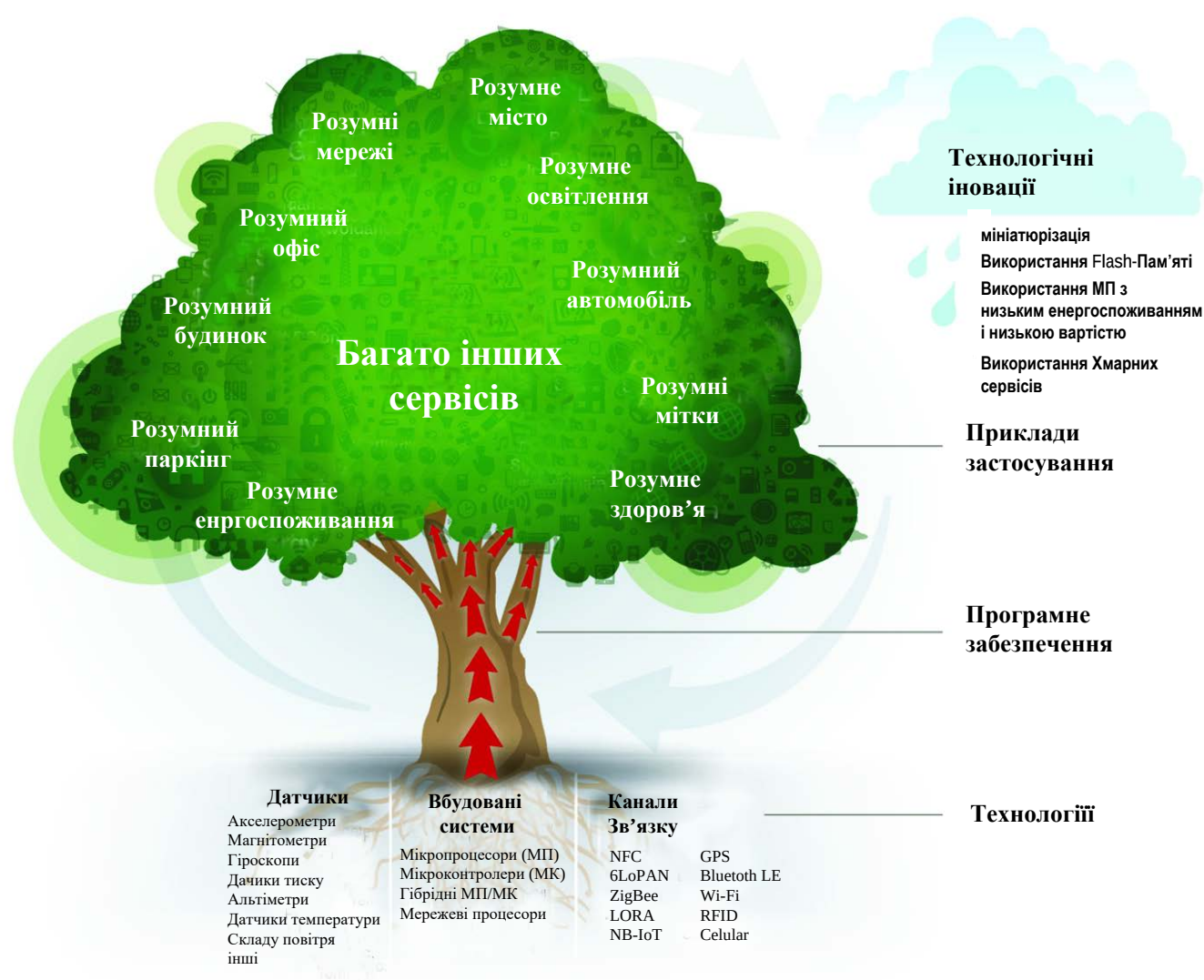


Рисунок 2.1 – Складові частини IoT

2.2 Датчики для систем IoT та їх призначення

2.2.1 Загальні зауваження

Датчиками називають пристрої, що вимірюють фізичні характеристики об'єктів або навколишнього середовища (наприклад, температуру, тиск, наявність домішок в повітрі, положення в просторі і т. д.) і перетворюють її в вид, зручний для подальшої обробки.

Першим датчиком, що з'явився на ринку, вважається термостат, винайдений в 1883 році Уорреном Джонсоном. З кінця 40-х років минулого століття почалося виробництво інфрачервоних датчиків, перший датчик руху з'явився на початку 50-х років минулого століття.

В кінці 20-го століття почали розроблятися датчики для визначення хімічного складу середовища і біосенсори. В даний час датчики є одними з основних компонент робототехніки, інтелектуальних систем та систем Інтернету речей.

2.2.2 Основні характеристики датчиків

Основні характеристики датчиків [2]:

- чутливість (поріг чутливості) – найменше значення вхідної величини, що приводить до зміни вимірюваної вихідної величини;
- похибка вихідного сигналу – визначається для нормальних умов експлуатації, при зміні умов навколишнього середовища, похибка збільшується;
- діапазон вимірів – мінімально і максимально можливі значення величин, які зможе зафіксувати датчик.

Датчики можна розділити на дві великі групи:

- активні (самі впливають на навколишнє середовище);
- пасивні (навколишнє середовище впливає на них).

За вимірювальними параметрами можна виділити такі датчики:

- вологості;
- світла;

- диму;
- руху;
- положення в просторі;
- газу;
- тиску;
- температури і багато інших.

За типом вихідного сигналу розрізняють аналогові та цифрові датчики.

За середовищем передавання інформації – проводові та безпроводові.

Датчики можуть бути частиною будь-якого приладу, а можуть бути виконані як незалежний пристрій.

За способом живлення датчики бувають автономні (працюють від батареї) і підключені до мережі електроживлення.

2.2.3 Структура датчиків

Датчик, в залежності від того аналоговий він чи цифровий, складається з декількох частин. На рис. 2.2 наведена типова структура датчика з цифровим виходом.

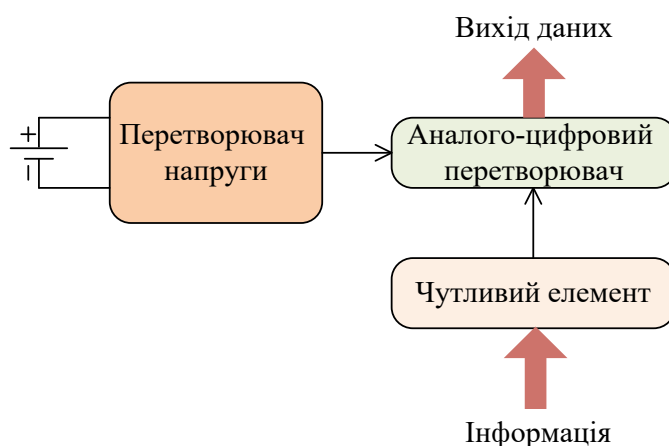


Рисунок 2.2 – Типова структура датчика з цифровим виходом

Чутливий елемент перетворює фізичну величину (наприклад швидкість) у електричний сигнал, що за допомогою аналого-цифрового перетворювача (АЦП)

трансформується у цифровий код. Живлення АЦП, а при необхідності і чутливого елемента, здійснюється за допомогою перетворювача напруги, що живиться від батареї. Використання перетворювача напруги викликане необхідністю підтримки напруги живлення АЦП при зміні напруги батареї.

Для використання в системах Інтернету речей частіше використовують не датчики, а модулі датчиків, як проводових, так і безпроводових. На рис. 2.3 наведена типова структура модуля безпроводового датчика.

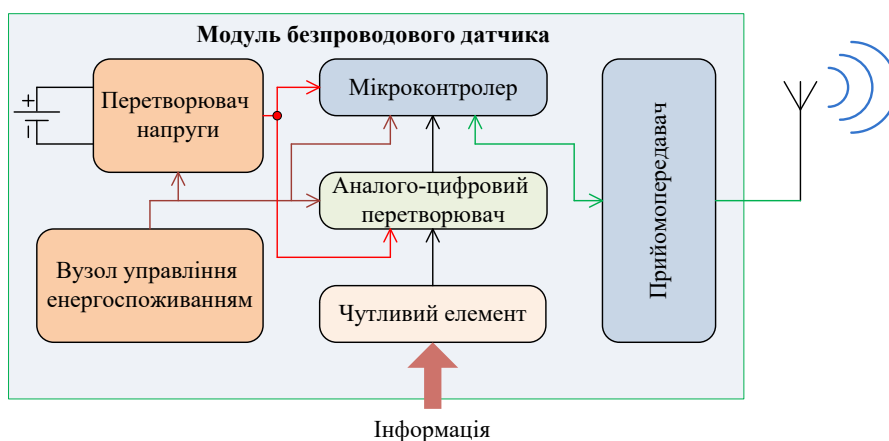


Рисунок 2.3 – Модуль безпроводового датчика

Як слідує з рис. 2.3 у модулі обов'язково присутній мікроконтролер, а також пристрій для обміну інформацією з зовнішнім середовищем. На рис. 2.3 це прийомопередавач, який дозволяє здійснювати двосторонній зв'язок між модулем та споживачем. При використанні модуля з проводовим зв'язком замість прийомопередавача використовується інтерфейсний пристрій – частіше називається просто інтерфейс.

2.3 Датчики тиску

2.3.1 Загальні зауваження

Датчики тиску призначені для вимірювання тиску газу в різних системах: трубопроводах, медичному обладнанні, в шинах автомобілів і в багатьох інших застосуваннях.

Залежно від призначення їх можна розділити на 3 типи:

1. Датчики абсолютного тиску, що вимірюють тиск щодо вакууму. Атмосферний тиск на рівні моря прийнято вважати рівним 101,325 кПа.
2. Датчики манометричного (надлишкового) тиску. Ці датчики призначені для виміру різниці між тиском, що діє на датчик, і атмосферним тиском.
3. Датчики диференціального тиску дозволяють вимірювати різницю двох або більше тисків, що діють на входи датчиків.

Для перетворення тиску в електричний сигнал у датчиках використовуються, переважно, чутливі елементи двох типів: ємнісні й п'єзорезистивні. У ємнісних датчиках – це діафрагма, що служить одночасно обкладкою конденсатора. Зовнішній тиск змінює положення діафрагми, у результаті чого змінюється ємність конденсатора (рис. 2.4,а). Основою п'єзорезистивних датчиків є гнучка кремнієва мембрана з тензочутливими елементами у вигляді чотирьох п'єзорезисторів, з'єднаних за мостовою схемою.

Зовнішній тиск викликає деформацію мембрани й, як наслідок, розбаланс мосту (рис. 2.4,б). При протіканні струму через датчик у діагоналі мосту виникає напруга неузгодженості, пропорційна прикладеному тиску.

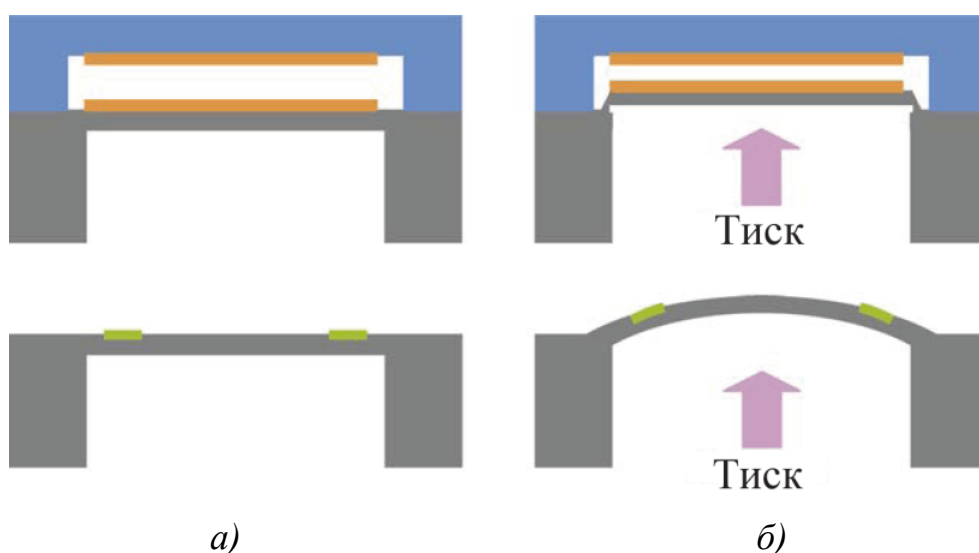


Рисунок 2.4 – Конструкція ємнісного (а) й п'єзоелектричного (б) датчиків

2.3.2 Датчики тиску компанії Omron

Датчики надлишкового тиску 2SMPP, що випускають японською компанією Omron, виконані в мініатюрному корпусі розмірами $6.1 \times 4.7 \times 8.2$ мм, споживана ними потужність не перевищує 0.2 мВт. Завдяки використанню п'єзорезистивного MEMS-елемента ці датчики по характеристиках перевершують ємнісні датчики тиску. Діапазон вимірів датчика 2SMPP-02 становить 0...37 кПа, а датчика 2SMPP-03 (рис. 2.5) – від -50 до 50 кПа [2]. Особливостями датчиків також є висока точність виміру й мала залежність вихідної напруги від температури навколишнього середовища. Датчики відповідають вимогам директиви RoHS.



Рисунок 2.5 – Датчик 2SMPP-03 компанії Omron [2]

Приклад схеми включення датчиків наведена на рис. 2.6, а залежності вихідної напруги від температури – на рис. 2.7.

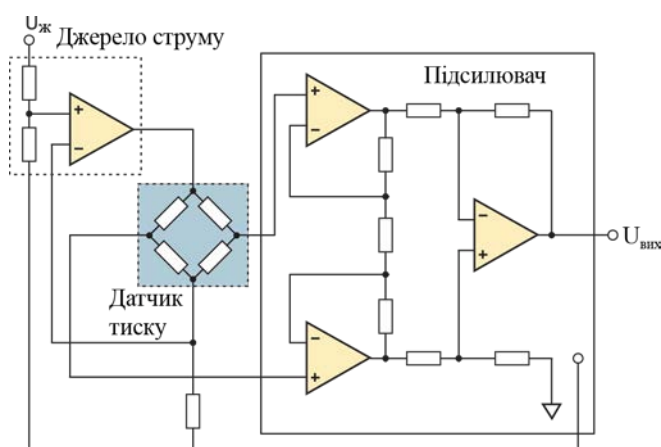


Рисунок 2.6 – Схема включення датчиків тиску

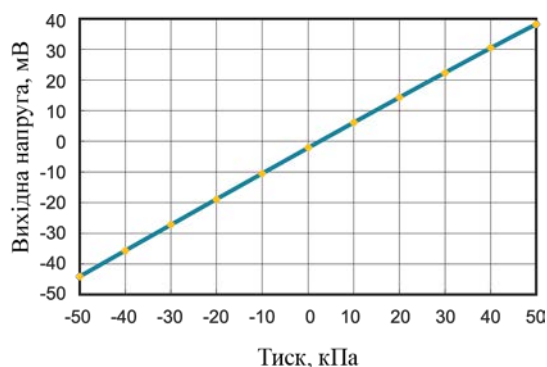


Рисунок 2.7 – Залежність вихідної напруги датчика 2SMPP-03 від тиску [2]

Характеристики датчиків 2SMPP (при струмі через датчик 100 мкА):

- опір п'єзорезисторів 20 ± 2 кОм;
- діапазон вихідної напруги датчиків:
 - 2SMPP-02 (0...37 кПа) $0...31 \pm 3.1$ мВ;
 - 2SMPP-03 (-50...50 кПа) $-43.0 \pm 5.5...42 \pm 5.5$ мВ;
- напруга зсуву -2.5 ± 4.0 мВ;
- нелінійність характеристики не більше 0.8% від повної шкали;
- гістерезис – не більше 0.5% від повної шкали;
- діапазон робочих температур датчиків:
 - 2SMPP-02 0...50 °C;
 - 2SMPP-03 0...85 °C.

Області застосування датчиків 2SMPP:

- медичне устаткування;
- побутова техніка;
- кондиціонування повітря;
- індикатори рівня;
- пристрої виявлення витoku повітря;
- регулятори тиску.

2.3.3 Що таке п'єзрезистор

П'єзо – з грецької стискання. У деяких матеріалів спостерігається п'єзоелектричний ефект. П'єзоелектричний ефект призводить до наявності електричного потенціалу з боків кристала, коли механічна напруга прикладається шляхом його стискання (рис. 2.8). У працюючій системі кристал діє як джерело напруги з позитивним зарядом на одній стороні й негативним зарядом на протилежній стороні. На базі таких кристалів будуються приймачі акустичних сигналів – мікрофони та гідрофони.

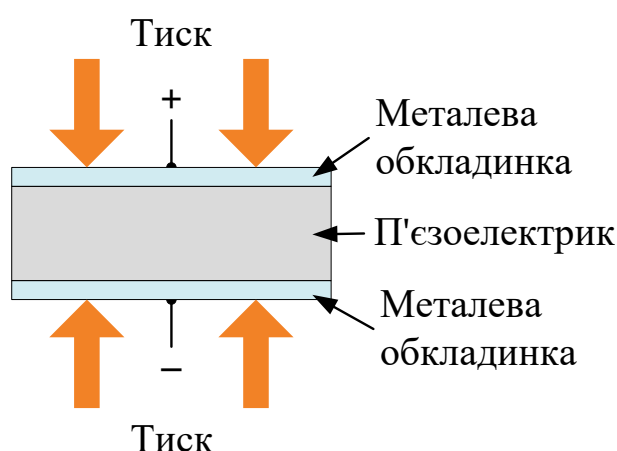


Рисунок 2.8 – Конструкція чутливого елемента на основі п'єзоелектричного матеріалу

П'єзоелектричний кристал має і зворотну дію. Під впливом напруги п'єзоелектричний кристал буде стискатися або розширюватися в залежності від знаку прикладеної напруги. На основі п'єзоелектричних кристалів будуються випромінювачі акустичних коливань – гучномовці, сирени, звукові сповіщувачі.

На рис. 2.9 наведено приклад сирени компанії Sonitron, що розвиває звуковий тиск 122 дБ. На рис. 2.10 наведено зовнішній вигляд п'єзокерамічного гучномовця SCS-17, що відтворює діапазон звукових частот 1500...8000 Гц [3].



Рисунок 2.9 – П'єзокерамічна сирена SAS-2835 [3]



Рисунок 2.10 – П'єзокерамічний гучномовець SCS-17 [3]

2.3.4 Датчик тиску компанії Honeywell

Розглянемо один з таких датчиків [4]. Зовнішній вигляд датчика тиску компанії Honeywell наведений на рис. 2.11.

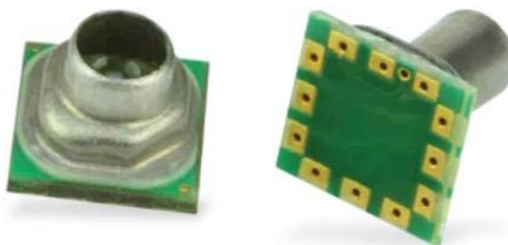


Рисунок 2.11 – Датчик тиску Honeywell MPR MicroPressure [4]

Датчик компанії Honeywell MPR MicroPressure – це п'єзорезистивний датчик з цифровим виходом для вимірювання тиску. Honeywell MPR калібрується і компенсується у певному температурному діапазоні для забезпечення чутливості, зменшення впливу температури та нелінійності. Датчики MPR відповідають вимогам до медичних (споживчих та не споживчих) пристроїв, комерційних та промислових приладів.

Датчик призначений для використання в медицині для неінвазивного моніторингу артеріального тиску, в терапії ран з негативним тиском, в мобільних концентраторах тиску, моніторах повітряного потоку, в амбулаторних вимірюваннях.

В промислових системах та споживчих пристроях кондиціонування повітря, лічильниках газу та води, кавових машинах, системах зволоження повітря.

Основні характеристики датчика MPR:

- габаритні розміри 5×5 мм;
- похибка вимірювання не більше 1,5%;
- напруга живлення 3,3 В;
- діапазон вимірювання тиску від 60 мбар до 2,5 бар (6 кПа до 250 кПа);
- 24-розрядний цифровий вихід, сумісний з I2C або SPI;
- низьке енергоспоживання <10 мВт, зазвичай;
- відкалібрований і компенсований;
- напірний отвір з нержавіючої сталі;
- сумісність з різними рідкими середовищами;
- вимірювання абсолютного і манометричного тиску;
- висока продуктивність;
- діапазон температур з компенсацією від 0 до 50 °C;
- відповідність вимогам REACH і RoHS;
- відповідає стандарту IPC / JEDEC J-STD-020D, 1 рівень чутливості до вологи.

2.4 Датчики та енкодери на основі ефекту Холла

В основу принципу дії датчика покладено ефект Холла, який отримав свою назву на честь американського фізика, який відкрив це явище в 1879 році. Якщо подати на краї прямокутної пластини (А і В на рис. 2.12) постійну напругу і помістивши її в магнітне поле, то на двох інших краях (С і D) формується різниця потенціалів [5].

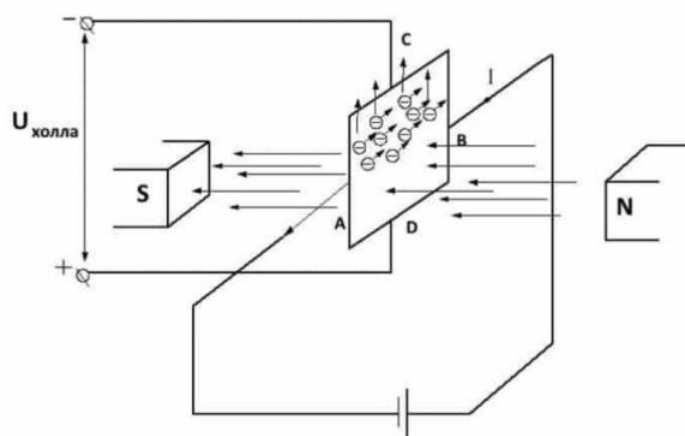


Рисунок 2.12 – Пояснення принципу дії датчика Холла [5]

Аналогові датчики використовують принцип перетворення магнітної індукції в напругу. Тобто, полярність, і величина напруги безпосередньо залежать від характеристик магнітного поля. На поточний момент цей тип датчиків, в основному, застосовується у вимірювальній техніці (наприклад, в якості, датчиків струму, вібрації, кута повороту).

Цифрові датчики, на відміну від аналогових мають всього два стійких положення, що сигналізують про наявність або відсутність магнітного поля. Тобто, спрацювання відбувається в тому випадку, коли інтенсивність магнітного поля досягла певної величини. Саме цей тип пристроїв застосовується в автомобільній техніці в якості датчика швидкості, фази, положення розподільного, а також колінчастого валу і т. д.

Наприклад на основі ефекту Холла побудований безконтактний датчик для вимірювання струму (рис. 2.13) [6].



Рисунок 2.13 – Датчик струму на основі ефекту Холла [6]

Провідник по якому протікає струм проходить через отвір датчика. Як відомо, навколо провідника зі струмом формується магнітне поле, яке і призводить до формування напруги на виході датчика.

Як правило, більшість датчиків являє собою компонент з трьома виводами, на два з яких подається дво- або однополярна напруга, а третій є сигнальним.



Рисунок 2.14 – Датчик Холла у корпусі [6]

Навіщо у смартфонах встановлюють датчик Холла?

Датчик Холла визначає, закритий або відкритий чохол на магнітній засувці, реагуючи на ослаблення або посилення магнітного поля. Коли магніт в обкладинці виявляється далеко, датчик дає команду включити дисплей, коли ж наближається, формує команду на відключення. На підставі цих даних смартфон може виконувати певні дії. Такі чохла часто отримують приставку Smart.

Наприклад, якщо ви використовуєте чохол без віконця на стороні дисплея, то датчик Холла допомагає автоматично відключати екран смартфона, коли чохол закритий. Коли ж чохол відкривається, екран активується.

А якщо чохол з віконцем, то датчик Холла дає команду на перемикання між різними видами вмісту екрану. У відкритій області виводяться тільки годинник, календар і повідомлення, на повному екрані – вся інформація. Наприклад, такий датчик встановлений у смартфоні Samsung Galaxy S10 (рис. 2.15).



Рисунок 2.15 – Смарт-чохол для смартфона Samsung Galaxy S10 [7]

Для вимірювання лінійних та кутових переміщень використовуються енкодери (датчики куту повороту або переміщення). Розглянемо основні параметри енкодерів компанії iC-Haus. Це досить складні пристрої, що виконані у вигляді інтегральних схем. На рис. 2.16 наведені структури деяких енкодерів [8].

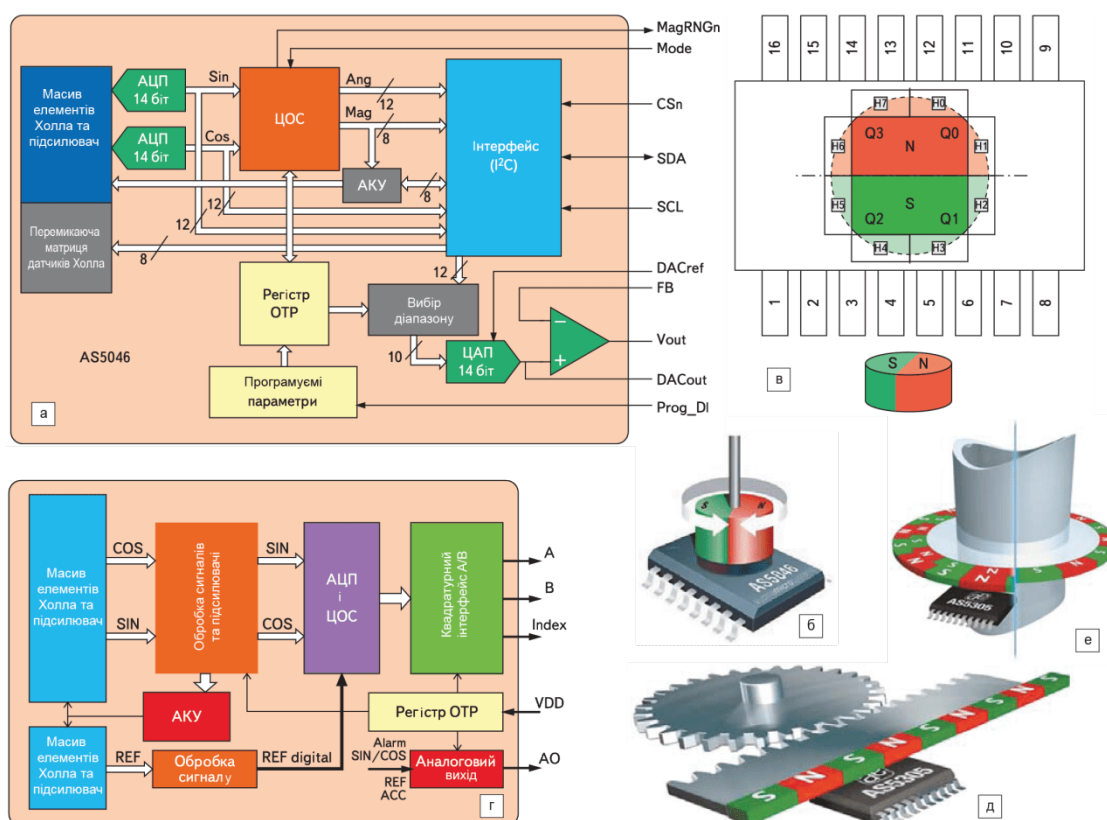


Рисунок 2.16 – Структури деяких енкодерів компанії iC-Haus [8]

2.5 Датчики температури

2.5.1 Термістори

Опір будь-якого провідника в загальному випадку залежить від температури. Опір металів з нагріванням збільшується. З погляду фізики це пояснюється збільшенням амплітуди теплових коливань елементів кристалічних ґрат і зростанням опору руху спрямованому потоку електронів. Опір електролітів і напівпровідників при нагріванні зменшується – це пояснюють іншими процесами.

Існують такі електронні компоненти, у яких залежність опору від температури яскраво виражена й нормована. Ці елементи називаються терморезисторами або термісторами.

Термістори (терморезистори) можна розділити на дві великі групи по реакції на зміну температури:

- якщо при нагріванні опір падає, такі терморезистори називаються NTC-термісторами (з негативним температурним коефіцієнтом опору);
- якщо при нагріванні опір збільшується, то термістор має позитивний ТКО (PTC-характеристику) – такі елементи називають ще позисторами.

Тип термістора визначається властивостями матеріалів, з яких виготовлені терморезистори. Метали при нагріванні збільшують опір, тому на їхній основі (точніше, на базі оксидів металів) випускають термоопори з позитивним ТКС. У напівпровідників залежність зворотна, тому з них роблять NTC-елементи.

Конструкція термісторів може бути різною. Їх випускають у вигляді циліндрів, бусин, шайб і т.п. із двома виводами (як у звичайного резистора). Можна підібрати найбільш зручну форму для установки у пристрій.

Сама головна характеристика будь-якого терморезистора – його температурний коефіцієнт опору (ТКО). Він показує, наскільки змінюється опір при нагріванні або охолодженні на 1 градус Кельвіна.

Інша важлива характеристика – номінальний опір. Це значення опору при 25 °С. Знаючи ці параметри, легко визначити придатність термістора для конкретної схеми.

Також для використання термісторів важливі такі характеристики, як номінальна й максимальна робоча напруга. Перший параметр визначає напругу, при якій елемент може працювати тривалий час, а другий – напругу, вище якої працездатність термістора не гарантується.

Умовне позначення термістора показано на рис. 2.17, а зовнішній вигляд деяких термісторів – на рис. 2.18 [9].

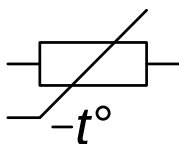


Рисунок 2.17 – Умовне позначення термістора



Рисунок 2.18 – Зовнішній вигляд термісторів [9]

Саме очевидне застосування терморезисторів – датчики для виміру температури. Для цієї мети придатні як термістори з характеристикою NTC, так і РТС. Треба лише вибрати елемент по робочій ділянці й урахувати характеристику термістора у вимірювальному приладі.

2.5.2 Термопары

Робота термопары обумовлена виникненням термоелектричного ефекту, відкритим німецьким фізиком Томасом Зеебеком (Tomas Seebeck) в 1821 р.

Явище засноване на виникненні струму в замкнутому електричному контурі при впливі певної температури навколишнього середовища (рис. 2.19) [10]. Електричний струм виникає при наявності різниці температур між двома провідниками (термоэлектродами) різного состава (різнорідних металів або сплавів) і підтримується збереженням місця їхніх контактів (спаїв).

Вихідна напруга термопары й температура перебувають у лінійній залежності. Це означає, що збільшення вимірюваної температури приводить до збільшення напруги на вільних кінцях термопары.

Спай, що перебуває в точці виміру температури, називається "гарячим", а місце підключення проводів до вимірювача (перетворювача) – "холодним".

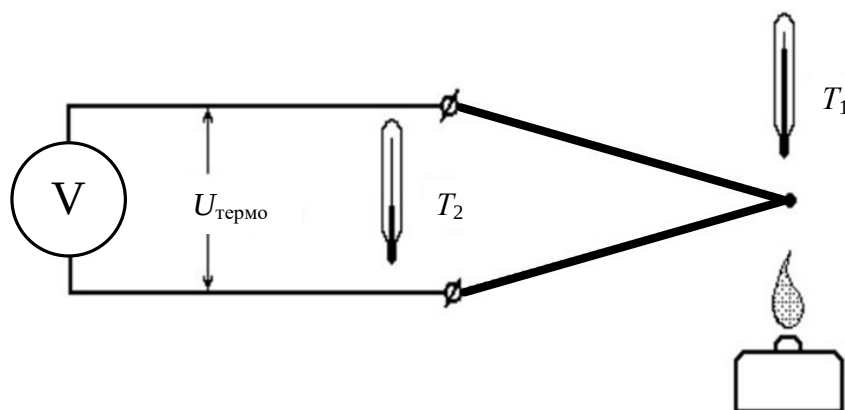


Рисунок 2.19 – Виникнення ЕРС у термопарі при наявності різниці температур "гарячого" і "холодного" спаїв [10]

Для використання в промисловості термопары містять у корпуси (рис. 2.20) [11].



Рисунок 2.20 – Зовнішній вигляд термопар у корпусах [11]

Спосіб ізоляції проводів у корпусі термопар підбирається з урахуванням верхньої температурної межі:

- 100...120 °C – будь-яка ізоляція;
- до 1300 °C – керамічні трубки або намисто;
- до 1950 °C – трубки з Al_2O_3 ;
- понад 2000 °C – трубки з Mg, Be, Th₂, Zr₂.

Термопари забезпечують високу точність вимірів, але мають низьку чутливість, що ускладнює їх використання. Основне призначення термопар – вимірювання високих температур (до декількох сотень градусів).

2.5.3 Пірометри й тепловізори

Пірометр (безконтактний термометр) – пристрій для дистанційного вимірювання температури. Він дозволяє дистанційно довідатися тепловтрати в приміщенні, визначити температуру деталей автомобіля й електронних пристроїв, проводів і інших об'єктів [12].

Тепловізор – це пристрій, який допомагає побачити невидимі для людського ока теплові випромінювання від різних предметів, істот та людей з точністю 0,1 °C

і вище у вигляді спеціальної теплової мапи. Палітра теплової мапи може бути різною, що дозволяє підібрати зображення, яке найкраще підходить до конкретної ситуації [13].

Відповідаючи на запитання, що таке тепловізор, варто зазначити, що його основним завданням є безконтактне вимірювання температури об'єктів неживої і живої природи, пошук людей тощо.

Сучасні пірометри й тепловізори, як правило, будуються на основі спеціальних матричних датчиків температури – болометрів [14]. Вони являють собою матрицю мініатюрних тонкоплівкових терморезисторів. Інфрачервоне випромінювання, зібране й сфокусоване на матриці об'єктивом тепловізора, нагріває елементи матриці відповідно до розподілу температури спостережуваного об'єкта. Просторовий дозвіл болометричних матриць досягає 1280×720 пікселів. Комерційні болометри звичайно роблять неохолоджуваними для зменшення вартості й розмірів устаткування.

Температурний дозвіл сучасних тепловізорів досягає сотих часток градуса Цельсія.

Розрізняють спостережливі й вимірювальні тепловізори. Спостережливі тепловізори показують тільки градієнти температур об'єкта. Вимірювальні тепловізори дозволяють виміряти значення температури заданої точки об'єкта з точністю до коефіцієнта випромінювання матеріалу об'єкта.

Вимірювальні тепловізори вимагають періодичного калібрування, для чого найчастіше постачаються з вбудованим пристроєм для калібрування матриці, звичайно у вигляді шторки, температура якої точно вимірюється. Шторка періодично насувається на матрицю, даючи можливість відкалібрувати матрицю по температурі шторки.

Оскільки звичайне оптичне скло непрозоре в інфрачервоному діапазоні, оптику тепловізорів роблять зі спеціальних матеріалів. Найчастіше використовують германій, але він дорогий, тому іноді використовують селенид цинку. Можна використовувати кварцове скло.

Розглянемо характеристики пірометра на прикладі DEKO CWQ02 [12].

Інфрачервоний пірометр DEKO CWQ02 призначений для виміру температури безконтактним шляхом за допомогою наведення за допомогою лазера на об'єкт.

Пістолетна форма інструмента забезпечує зручність використання (рис. 2.21). Прилад оснащений функціями збереження даних, автоматичного відключення живлення й відключення підсвічування дисплея. Діапазон вимірюваних температур від -50 до $+600$ $^{\circ}\text{C}$, точність вимірів – ± 1.5 $^{\circ}\text{C}$. Живлення здійснюється від 2 батарейок типу ААА.

Професійні пірометри та тепловізори оснащені проводовими та безпроводовими інтерфейсами зв'язку.



Рисунок 2.21 – Інфрачервоний пірометр DEKO CWQ02 [12]

Основні параметри пірометра:

- діапазон вимірюваних температур від -50 до $+600$ $^{\circ}\text{C}$;
- точність вимірів $\pm 0,5\%/^{\circ}\text{C}$;
- дозвіл дисплея $\pm 0,1$ $^{\circ}\text{C}$;
- погрішність виміру $1,5\%$;
- живлення 2 батарейки ААА;
- маса $0,17$ кг.

На рис. 2.22 наведено зовнішній вигляд тепловізора при вимірюванні температури у приміщенні [15].



Рисунок 2.22 – Вимірювання температури в приміщенні тепловізором [15]

2.5.4 Напівпровідникові сенсори температури на основі транзисторів

Напівпровідникові сенсори температури найбільш поширені й мають широке коло застосувань [16]. Багато компаній випускають такі сенсори, як аналогові, так і цифрові.

У напівпровідникових датчиках температури як чутливий елемент використовується емітерний перехід транзистора. Напруга на переході описується приблизним рівнянням:

$$U \approx \varphi_T \ln(I/I_S).$$

де φ_T – температурний потенціал переходу, пропорційний абсолютній температурі T , I_S – тепловий струм через перехід.

Для реалізації кола, що має властивості електронно-діркового переходу, використовують біполярні транзистори, базу яких з'єднують із колектором. При такому включенні напруга на транзисторі визначається сумою спадань напруги на емітерному переході й опорі бази, через які протікають струми емітера й бази. Струм бази невеликий, він майже в h_{21E} раз менше струму емітера (h_{21E} – коефіцієнт

підсилення транзистора по струму в схемі із загальним емітером), у зв'язку із чим спаданням напруги на опорі бази можна знехтувати (при $h_{21E} \gg 1$).

На рис. 2.23 наведені варіанти підключення транзисторів до підсилювача для побудови датчиків температури.

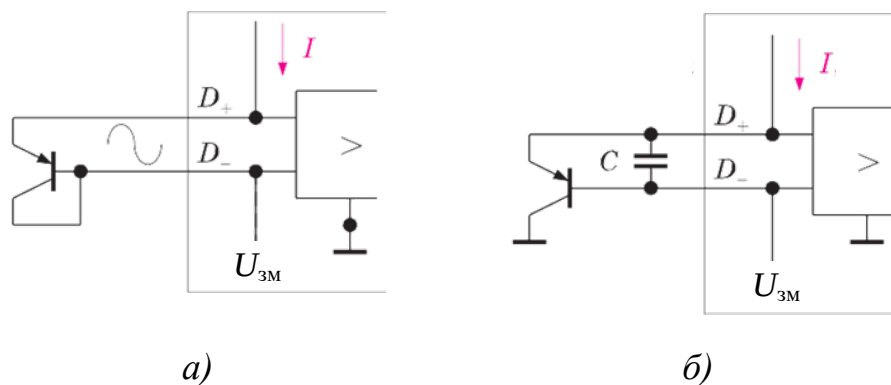


Рисунок 2.23 – Підключення транзистора в якості датчика температури при з'єднанні колектора та бази (а) та з заземленим колектором (б)

На рис. 2.24 наведені найпростіші датчики температури на транзисторах. Джерело струму зумовлює напругу на емітерному переході.

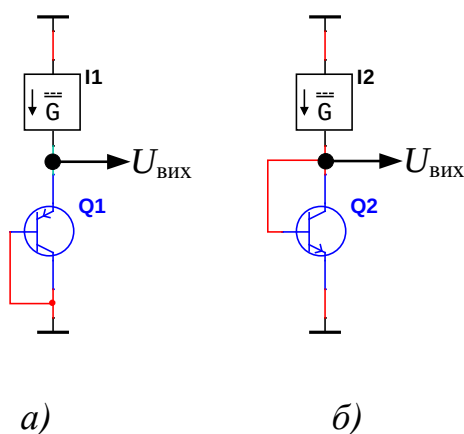


Рисунок 2. 24 – Найпростіші датчики температури на транзисторі *pnp* (а) та *nnp* (б)

Контрольні питання

1. Які основні характеристики датчиків вам відомі?
2. Для чого використовуються п'єзорезистори?
3. З використанням яких елементів можна побудувати датчики тиску?

4. Які елементи можна використати для вимірювання маси?
5. В чому полягає ефект Холла?
6. В яких датчиках можна використовувати ефект Холла?
7. Яка залежність напруги від температури на термісторі?
8. Що таке термопара?
9. Для яких діапазонів температур призначені термопари?
10. Які функції виконує тепловізор?
11. Для чого використовуються пірометри?
12. В яких діапазонах температур працюють напівпровідникові датчики температури?

Перелік посилань

1. O. Vermesan, P. Friess Internet of Things – From Research and Innovation to Market Deployment. River publishers, 2014. pp. 374. (River publishers series in communications). / Url: https://www.academia.edu/24701833/Internet_of_Things_From_Research_and_Innovation_to_Market_Deployment_River_Publishers_Series_in_Communication. (дата звернення: 29.06.2024).
2. 2SMPP-03 MEMS Gauge Pressure Sensor. Url: <https://components.omron.com/en-en/products/sensors/2SMPP-03> (дата звернення: 29.06.2024).
3. SCS-17-S | SONITRON. Url: <https://www.soselectronic.com/en-nl/products/sonitron/scs-17-s-64050> (дата звернення: 29.06.2024).
4. Honeywell MPR MicroPressure Sensors. / Url: https://eu.mouser.com/new/honeywell/honeywell-mpr-sensors?utm_source=aac&utm_medium=email&utm_campaign=3p-honeywell-newest-supplier4-emea-en (дата звернення: 29.06.2024).
5. Датчик Холла. Url: https://corelamps.com/elektronika/datchyk-kholla/#google_vignette (дата звернення: 29.06.2024).

6. ПИМ-40-У-Б30. Url: https://saltako.by/catalog/energetika_-teplotekhnika_-davlenie/datchiki-_izmeritelnye-preobrazovateli_-aktivnoy-moshchnosti/7238/ (дата звернення: 29.06.2024).
7. Чохол LUX. Url: <https://rozetka.com.ua/ua/133952004/p133952004/> (дата звернення: 29.06.2024).
8. iC-МНМ 14-bit absolute angle hall encoder. Url: <https://www.ichaus.de/product/ic-mhm/> (дата звернення: 29.06.2024).
9. Термістор NTC MF52A1. Url: <https://prom.ua/ua/p2112737203-termistor-ntc-mf52a1.html> (дата звернення: 29.06.2024).
10. Термoeлектричні явища у напівпровідниках. Url: <https://extxe.com/33041/poluprovodniki-fizicheskie-processy-v-poluprovodnikah/> (дата звернення: 29.06.2024).
11. Temperature Transducer TMI400. Url: https://www.flickr.com/photos/alarm_and_control/13443281524/ (дата звернення: 29.06.2024).
12. Пірометр інфрачервоний DEKO CWQ02. / Url: <https://profinstrument.su/good/pirometr-infrakrasnyy-deko-cwq02/> (дата звернення: 29.06.2024).
13. Тепловізор: що це таке. Url: <https://tsn.ua/ato/scho-take-teplovizor-princip-roboticina-harakteristiki-de-vikoristovuyetsya-2079811.html> (дата звернення: 6.12.2024).
14. Болومتر. Url: <https://vue.gov.ua/%D0%91%D0%BE%D0%BB%D0%BE%D0%BC%D0%B5%D1%82%D1%80> (дата звернення: 6.12.2024).
15. Для чого потрібен тепловізор. Url: <https://ek.ua/ua/post/1365/260-dlya-chego-nuzhen-teplovizor/> (дата звернення: 29.06.2024).
16. Датчики температури. Url: <http://www.maksvel.com.ua/index.php/statti/79-datchyky-temperatury> (дата звернення: 29.06.2024).

3 MEMC-датчики для систем Інтернету речей

3.1 Особливості технології MEMC

Мікроелектромеханічні системи (MEMC) – поєднують в собі мікроелектронні і мікромеханічні компоненти [1]. MEMC-пристрої найчастіше виготовляють на кремнієвій підкладці за допомогою технології мікрообробки, аналогічно технології виготовлення однокристальних інтегральних мікросхем. Типові розміри мікромеханічних елементів лежать в діапазоні від 1 до 100 мікрометрів, а розміри кристалів пристроїв MEMC мають розміри від 20 мкм до одного міліметра.

Пристрої MEMC можуть бути реалізованими з використанням цілого ряду різних матеріалів і технологій виробництва. Найбільш поширеним для використання є кремній.

MEMC-пристрої можуть бути зроблені з полімерів за допомогою таких процесів, як формування литтям, штампування або стереолітографія.

3.2 Пристрої побудовані за MEMC-технологією

MEMS-пристрої діляться на дві великі групи:

- датчики, які здійснюють перетворення фізичної величини в електричний сигнал;
- актуатори (виконавчі пристрої), які здійснюють перетворення електричного сигналу в різні дії.

Самими відомими є MEMC-сенсори руху та гіроскопи (рис. 3.1) [2-4]. Вони використовуються у смартфонах, комунікаторах, ігрових приставках, фотокамерах й ноутбуках. Такі пристрої оснащуються акселерометрами (сенсорами прискорення) і гіроскопами (сенсорами повороту).

У мобільних телефонах і відеоприставках чутливість до рухів користувача використовується в основному для підвищення зручності користування. У ноутбуках акселерометри уловлюють момент коли жорсткий диск може піддатися

ушкодженню через удар і паркують його магнітні головки. У фототехніці сенсори руху використовують в системах стабілізації зображення при зйомці.

Автовиробники уже кілька десятиліть використовують сенсори руху, наприклад, у подушках безпеки й антиблокувальних системах гальм.

В авіації, у пілотажних системах вони використовуються в основному як датчики кутових швидкостей у колах зворотного зв'язку автоматичних систем керування. У навігаційних системах – як датчики кутового положення літака або індикатора нульового положення гіростабілізованої платформи. Як датчики лінійних прискорень використовуються акселерометри.

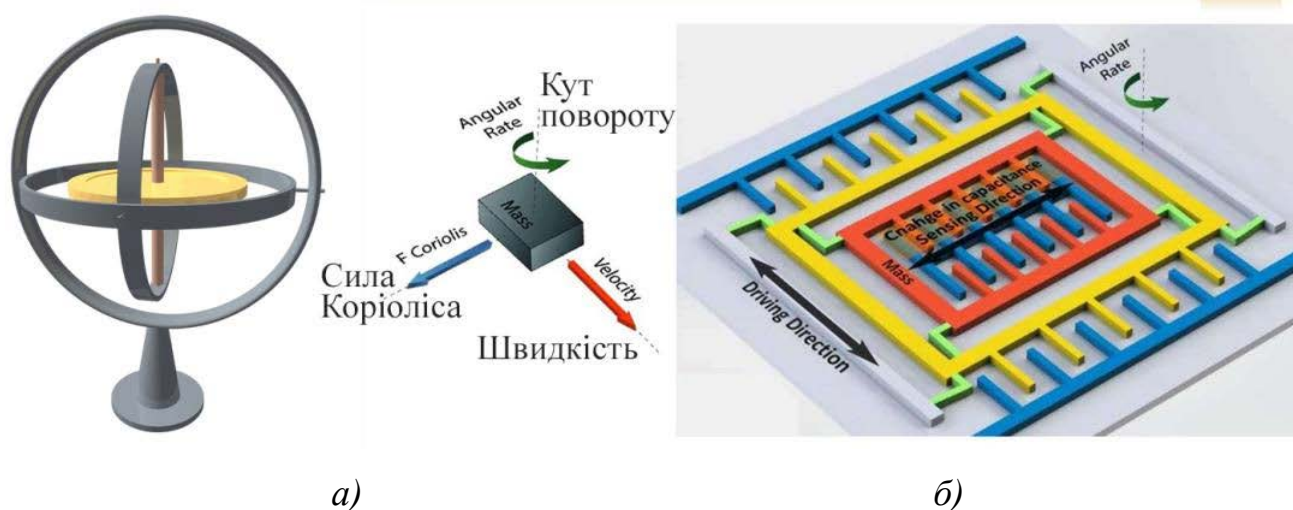


Рисунок 3.1 – Класичний гіроскоп зразка XIX століття (а)
та MEMС-гіроскоп (б) [2]

При польоті літака пілотам або автопілоту необхідно мати точні дані про географічні координати тих пунктів земної поверхні, над якими він у цей момент часу пролітає. Тільки при цій умові можна здійснювати політ по заздалегідь заданому маршруту. На зорі авіації, коли польоти літаків здійснювались тільки в гарну, так названу літну погоду, виконання зазначених умов не викликало утруднень.

Характерна риса сучасної авіації – здійснення польотів при відсутності видимості земної поверхні. Пасажирські й поштові літаки повинні робити регулярні рейси в будь-який час дня й ночі, при будь-якій погоді, тому що в

протилежному випадку, при очікуванні літної погоди буде губитися одне з основних переваг повітряного сполучення – швидкість.

Для виконання сліпого польоту по заздалегідь наміченому маршруті літак повинен бути обладнаний приладами, які протягом усього часу вказували б напрямок лінії північ-південь. На перший погляд такі вимоги можуть бути забезпечені досить простими засобами. Досить, здавалося б, обладнати літак маятником і магнітною стрілкою, щоб дати можливість льотчикові визначити положення літака щодо площини обрію й меридіана.

Все це, з огляду на безперервні коливання літака, породжує й коливання, що не припиняються, маятника й магнітної стрілки біля напрямків вертикалі й полуденної лінії. Зазначені обставини утрудняють користування розглянутими приладами для визначення кутів крену літака стосовно площини обрію і його курсових кутів щодо площини меридіана.

Таким чином, ні магнітна стрілка, ні маятниковий креномір не могли з'явитися надійними показниками положень площини меридіана й обрію. От чому виникла насущна потреба в створенні принципово нових приладів, які б у специфічних умовах польоту зберігали незмінним своє положення щодо площини обрію або меридіана.

І тільки застосування гіроскопа дозволило створити навігаційні прилади, що задовольняють все зростаючим вимогам авіації.

3.3 Датчики тиску

У тензорезистивних датчиках на кремнієву діафрагму поміщені п'єзорезистори. Після механічного впливу опір резисторів внаслідок п'єзорезисторного ефекту змінюється на величину ΔR , що приводить до зміни вихідної напруги датчика [5].

Основною перевагою монокристалічного кремнію в датчиках є його гарні характеристики пружності, високий коефіцієнт тензочутливості, а так само, у

такому датчику відсутній гістерезис і деформація, викликана безперервним впливом, навіть при високому тиску.

Важливо враховувати, що кремнієві тензорезистори мають досить сильну температурну чутливість, тому завжди при розробці датчиків на їхній основі передбачають наявність пристроїв температурної компенсації.

На рис. 3.2 наведена схема підключення тензорезисторів, а на рис. 3.3 – конструкція датчика тиску.

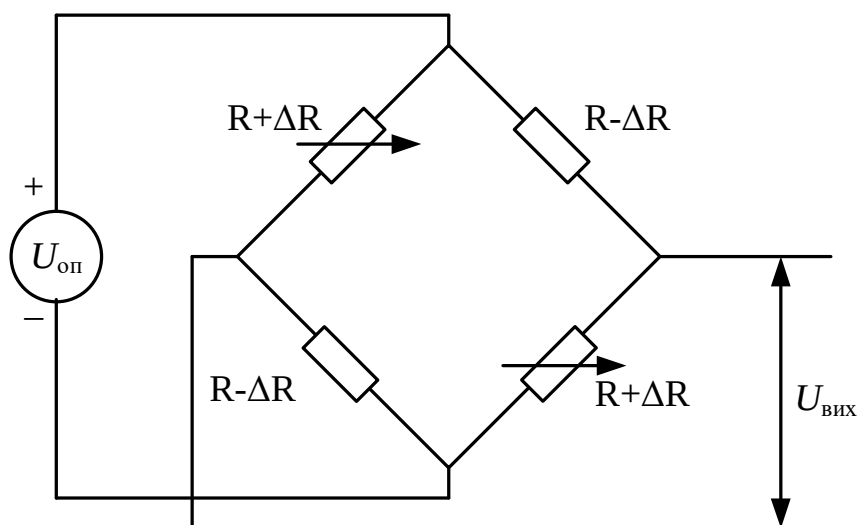


Рисунок 3.2 – Мостова схема підключення тензорезисторів

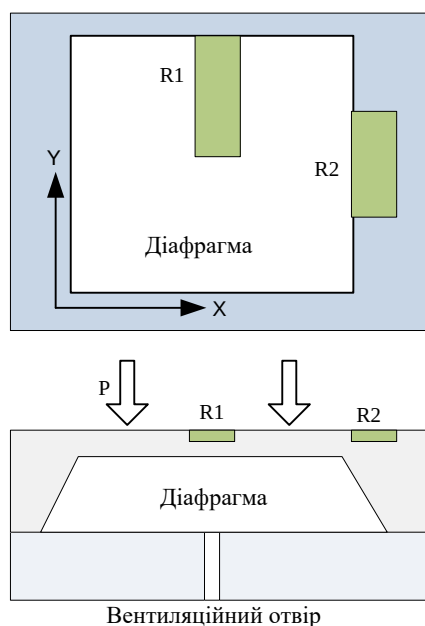


Рисунок 3.3 – Конструкція датчика тиску

3.4 Сенсори прискорень та кутових швидкостей

Інклінометр, реагує на складову сили тяжіння (вагу) і дозволяє визначати нахил, наприклад, транспортного засобу й, відповідно, дорожнього полотна. Акселерометр реагує на силу інерції і дозволяє визначати прискорення руху. Інклінометр і акселерометр виконуються однаково, а вимірюваний параметр зумовлений відповідною установкою сенсора й способом виміру [4].

Сказане ілюструє рис. 3.4. Ліворуч, на похилій площині (рис. 3.4,а) показана дія складової сили тяжіння $\mathbf{P}_\alpha$. Сила тяжіння, пропорційна масі транспортного засобу M , передається до джерела гальмуючої сили $\Delta\mathbf{F}_{\text{тя1}} = -\mathbf{P}_\alpha$. Якщо на транспортному засобі встановлений сенсор (у цьому випадку, інклінометр), він вимірює складову прискорення тяжіння $g\sin\alpha$ і, відповідно, при відомому модулі g дозволить визначити кут нахилу. У наведеному прикладі первинної є сила $\mathbf{P}_\alpha$, а вторинної $\Delta\mathbf{F}_{\text{тя1}}$, яка, будучи зовнішньою, незалежною від $\mathbf{P}_\alpha$, установлюється їй рівній. Первинною є сила тяжіння (показана червоним кольором), вторинною – сила $\Delta\mathbf{F}_{\text{тя1}}$ (показана синім кольором).

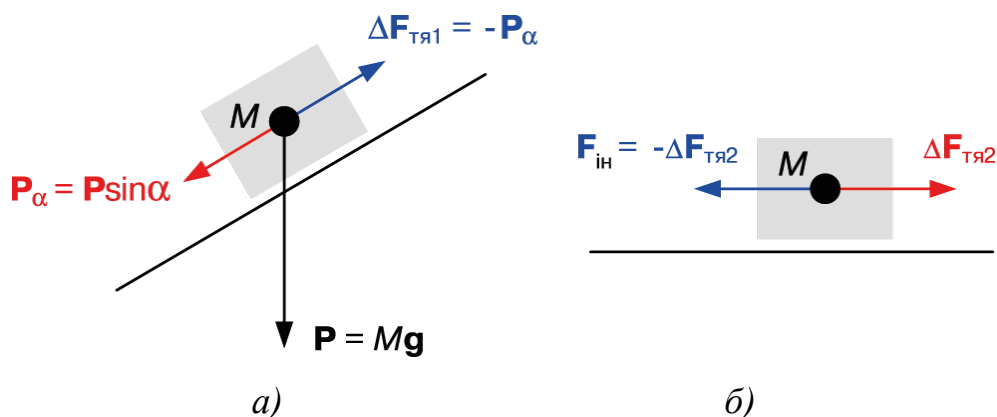


Рисунок 3.4 – Дія сили тяжіння (ваги) $\mathbf{P}_\alpha$ і утримуючої сили тяги $\Delta\mathbf{F}_{\text{тя1}}$ (а), дія гальмуючої сили тяги $\Delta\mathbf{F}_{\text{тя2}}$ (рух ліворуч) і сили інерції $\mathbf{F}_{\text{ін}}$ (б)

Другий приклад – праворуч на рис. 3.4,б. Транспортний засіб рухається з рівномірною швидкістю ліворуч. До нього прикладається сила $\Delta\mathbf{F}_{\text{тя2}}$, що є гальмуючою. У результаті, виникає сила інерції, їй рівна (тертям зневажаємо).

Якщо на транспортному засобі встановлений сенсор (у цьому випадку, акселерометр), він вимірює прискорення інерції, якому дорівнює прискорення руху (у цьому випадку, що сповільнює) зі зворотним знаком. Первинною є гальмуюча сила тяги (показана червоним кольором), вторинною – сила інерції F_{iH} (показана синім кольором).

Найчастіше сенсори руху будуються на принципі зміни ємності конденсатора. Рухлива частина системи це грузик на підвісах (рис. 3.5). При наявності прискорення грузик зміщується щодо нерухомої частини датчика. Обкладинка конденсатора, що прикріплена до грузика, зміщується щодо обкладинки на нерухливій частині. Ємність конденсатора змінюється, при незмінному заряді на конденсаторі змінюється напруга. Вимірюючи цю напругу можна розрахувати зсув грузика. Знаючи масу грузика й параметри підвісу, можна знайти прискорення.

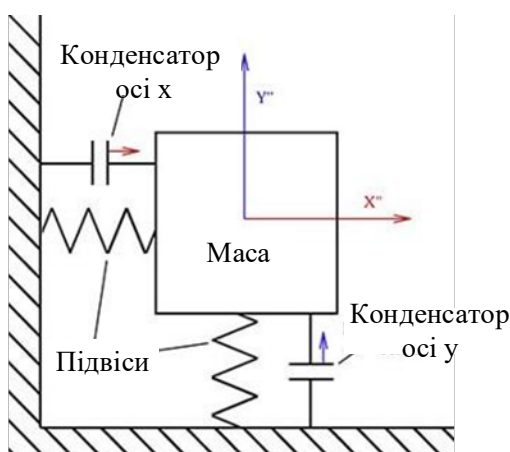


Рисунок 3.5 – Пояснення принципу роботи конденсаторних акселерометрів

На практиці у MEMS-акселерометрах відокремити одну від одної складові частини – грузик, підвіс, корпус і обкладки конденсатора не просто. У більшості випадків в одній деталі тут комбінуються відразу декілька різних елементів як показано на рис. 3.6 [6].

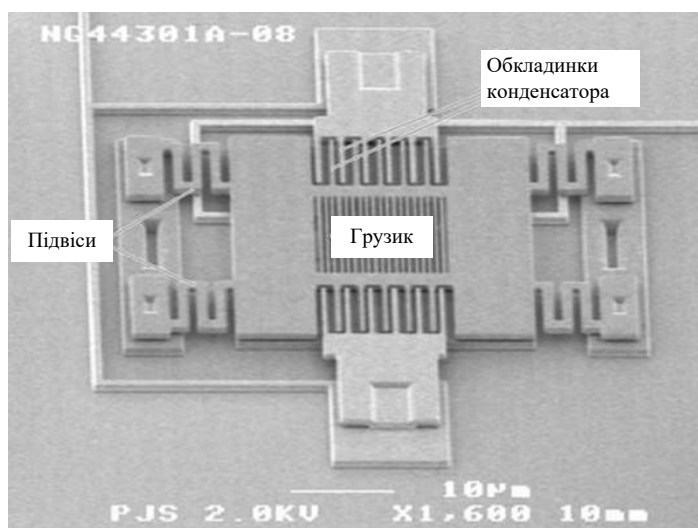


Рисунок 3.6 – MEMS-акселерометр компанії Sandia Labs [6]

На рис. 3.7 наведено декілька MEMS-акселерометрів для порівняння їх розмірів. Мініатюрні акселерометри знаходять широке застосування в медицині.

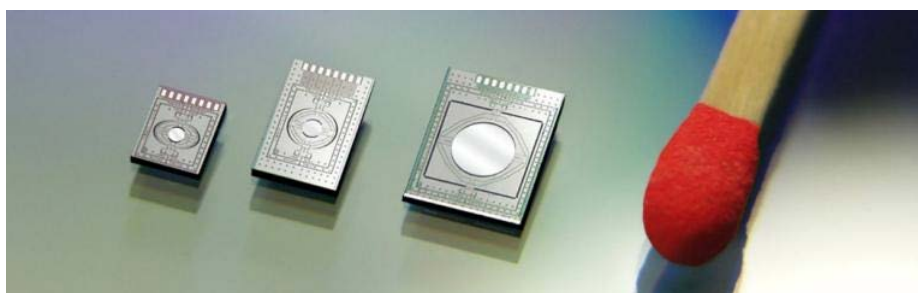


Рисунок 3.7 – MEMS-акселерометри [7]

Наприклад, компанія STMicroelectronics випускає спеціалізовану мікросхему 3-осьового акселерометра MIS2DH з наднизьким енергоспоживанням для застосування в медичних додатках і пристроях що імплантуються (рис. 3.8) [8].



Рисунок 3.8 – MEMS-акселерометр MIS2DH у кардіостимуляторі [8]

Медичні пристрої що імплантуються, такі як кардіостимулятори, кардіодефібрилятори й нейростимулятори, уже успішно використовуються протягом багатьох років, щоб продовжити життя пацієнтам із серцевими захворюваннями або полегшити життя людям із хронічними захворюваннями. На сьогоднішній день перед ученими стоїть завдання вивчити, як інноваційні імплантовані пристрої можуть допомогти в лікуванні інших хронічних захворювань, таких як високий кров'яний тиск, епілепсія, тремор. Для багатьох із цих додатків вбудований акселерометр, здатний надати електронному імпланту або приладу інформацію про активність і позу пацієнта, може підвищити ефективність лікування й поліпшити стан пацієнта [9].

Основні характеристики MIS2DH [10]:

- габаритні розміри $2 \times 2 \times 1$ мм;
- наднизьке енергоспоживання (менш 2 мкА в енергозберігаючому режимі роботи);
- обраний користувачем діапазон вимірів прискорень: $\pm 2g/\pm 4g/\pm 8g/\pm 16g$;
- вбудовані механізми визначення руху й умов вільного падіння;
- вбудований датчик температури;
- напруга живлення 1,71...3,6 В.

3.5 МЕМС-мікрофони

Швидке зростання числа різноманітних переносних (малогабаритних) електронних пристроїв, призначених для передавання, приймання й відтворення голосу, вимагає розробки нових мініатюрних високоякісних мікрофонів [11].

Два або більш одночасно використовуваних мікрофона дозволяють побудувати систему придушення шуму навколишнього середовища й підвищення якості переданого звуку в телефонах і смартфонах. Наприклад, в iPhone застосовується два пристрої з MEMS-мікрофонами для ефективного шумозниження. Такий же підхід практикують компанії HTC і Motorola. Ринок мобільних телефонів сьогодні величезний і постійно збільшується. Для

ефективного просування своєї продукції багато виробників вводять нові функції, у тому числі, за рахунок використання пристроїв поліпшення якості звуку, що вводиться з мікрофону.

Удосконалювання процесу MEMS привело до створення мініатюрних дешевих мікрофонів з високими параметрами. У деяких додатках такий прилад забезпечує певні переваги над традиційними електретними мікрофонами (ЕСМ). Шляхом нанесення й травлення напівпровідникового матеріалу на кремнієвій підкладці формується конденсатор, що є основою мікрофона. Як і звичайний електретний мікрофон, MEMS-мікрофон складається із гнучкої діафрагми, твердої підкладки й отвору, що демпфірує, з електричним зарядом на підкладці. Діафрагма перебуває в безпосередній близькості від підкладки, утворюючи з нею конденсатор [11]. Під впливом звукового тиску діафрагма рухається, при цьому змінюється ємність між нею й підкладкою. Ці зміни вимірюються й виводяться у вигляді електричного сигналу. На рис. 3.9 наведена конструкція MEMC-мікрофона.

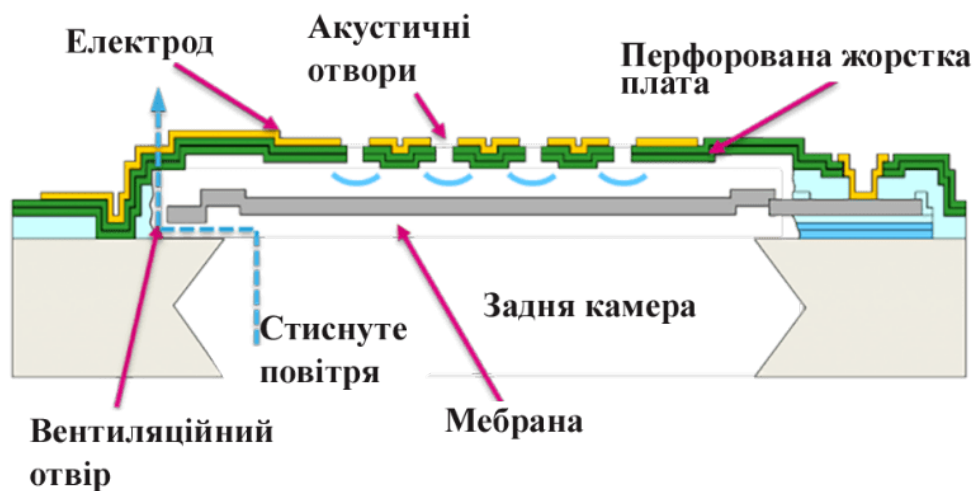


Рисунок 3.9 – Конструкція MEMC-мікрофона [11]

В друкованій платі необхідно просвердлити отвір більшого діаметра, чим діаметр отвору мікрофона тому що всі MEMS-мікрофони конструктивно виконані в корпусах для поверхневого монтажу й отвір, через який у мікрофон попадає повітря, розташовується на його дні (рис. 3.10). Для захисту мікрофона від попадання в нього вологи, пилу й бруду, на плату кріпиться мембрана з

еластичного матеріалу. Для зменшення нерівномірності АЧХ мікрофона між платою й мембраною слід закріпити круглу шайбу, діаметр отвору якої більше діаметра отвору в платі. порожнина, що утворюється за рахунок цього (рис. 3.10) [11] утворює акустичну камеру, яка й вирівнює частотну характеристику мікрофона на верхніх частотах. На рис. 3.11 наведені залежності АЧХ чутливості мікрофона без шайби (суцільна лінія) і із шайбою (пунктирні лінії).

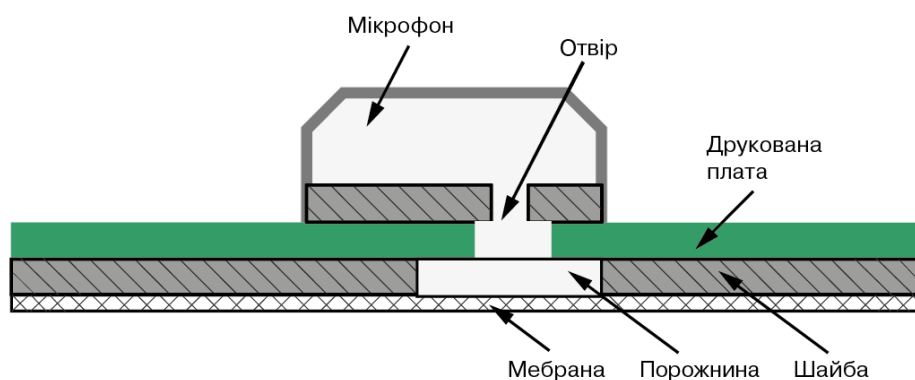


Рисунок 3.10 – Рекомендована конструкція кріплення MEMS-мікрофона

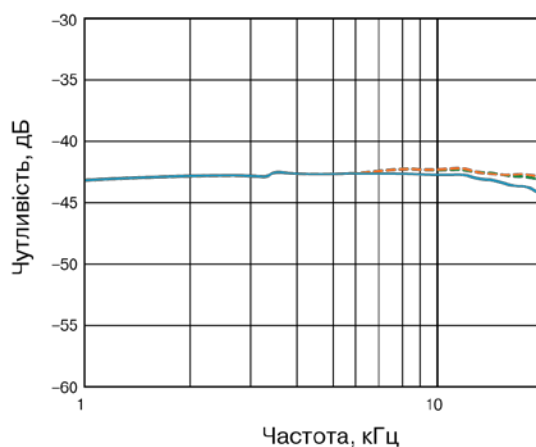


Рисунок 3.11 – Частотні характеристики чутливості MEMS-мікрофона при кріпленні мембрани без шайби (синя) та з шайбою [11]

Нерівномірність АЧХ в області верхніх частот залежить не тільки від наявності шайби, але й від діаметра отвору в ній і від матеріалу мембрани. Експериментально виміряні характеристики чутливості мікрофона залежно від матеріалу мембрани й від діаметра отвору в шайбі наведені на рис. 3.12. Звичайно,

нерівномірність АЧХ повинна залежати й від товщини шайби, тобто від обсягу акустичної камери, але інформація про це відсутня.

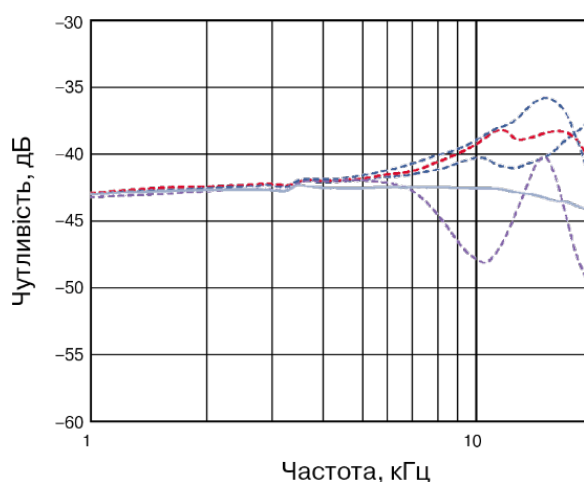


Рисунок 3.12 – Частотні характеристики чутливості MEMS-мікрофона при різних діаметрах отвору в шайбі и різних матеріалах мембрани [11]

Основні параметри MEMS-мікрофонів компанії Analog Devices наведені в табл. 3.1.

Таблиця 3.1 – Основні параметри MEMS-мікрофонів компанії Analog Devices

Тип мікрофона	Вихідний сигнал	Відношення сигнал/шум, дБ	Чутливість на частоті 1 кГц, дБ	PSRR *, дБ	АЧХ, кГц	U _{живл.} , В	Струм спожив., мкА	Габаритні розміри, мм
ADMP401	аналоговий	62	-42	70	0.1...15	1.5...3.3	250	4.72×3.76×1.0
ADMP504	аналоговий	65	-38	70	0.1...20	1.6...3.3	180	3.4×2.6×1.0
ADMP521	цифровий	65	-26	80	0.1...16	1.8...3.3	900	4.1×3.1×1.0
ADMP421	цифровий	61	-26	80	0.1...15	1.8...3.3	650	4.1×3.1×1.0
ADMP441	цифровий	61	-26	75	0.06...15	1.8...3.3	1400	4.72×3.76×1.0

* PSRR – Power supply rejection ratio (коефіцієнт послаблення шумів джерела живлення)

На рис. 3.13 наведено зображення декількох MEMS-мікрофонів на пальці людини, що дозволяє порівняти їх розміри.

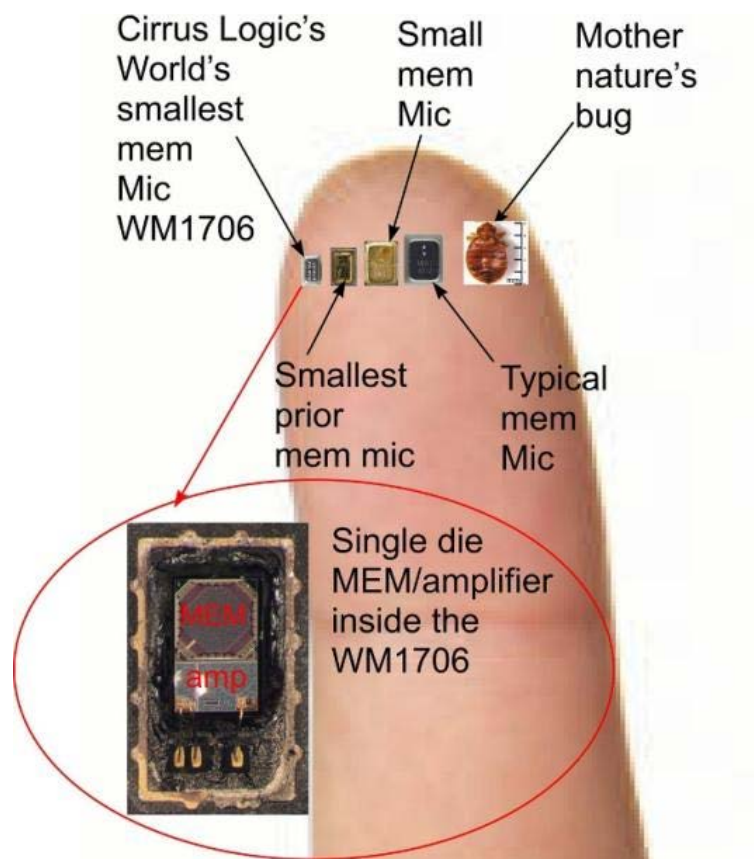


Рисунок 3.13 – Порівняння розмірів MEMS-мікрофонів різних виробників [12]

Контрольні питання

1. Що означає термін МЕМС?
2. В чому полягають особливості технології МЕМС?
3. За яким принципом можна побудувати датчики тиску?
4. Які параметри вимірює акселерометр?
5. Які параметри вимірює інклінометр?
6. Які параметри вимірюють трьохосеві акселерометри?
7. Який МЕМС-пристрій вимірює прискорення?
8. Який МЕМС-пристрій вимірює кут нахилу?
9. За яким принципом будуються МЕМС-мікрофони?
10. Які основні переваги МЕМС-мікрофонів перед електретними мікрофонами?

Перелік посилань

1. MEMS Technology Provides Tangible Benefits for Real-Time Clocks. Url: <https://www.analog.com/en/resources/technical-articles/mems-technology-provides-tangible-benefits-for-realtime-clocks.html> (дата звернення: 18.02.2024).
2. What is MEMS? Accelerometer, Gyroscope & Magnetometer. Url: <https://howtomechatronics.com/how-it-works/electrical-engineering/mems-accelerator-gyroscope-magnetometer-arduino/> (дата звернення: 18.02.2024).
3. Бондар П.М., Мелешко В.В Гіроскопи напрямку : монографія. Київ, 2016. 153 с.
4. Accelerometer Specifications - Quick Definitions. Url: <https://www.analog.com/en/lp/001/accelerometer-specifications-definitions.html>. (дата звернення: 18.02.2024).
5. Precision Pressure Sensor Measurements Using the MAX11254 Analog-to-Digital Converter. Url: <https://www.analog.com/en/resources/design-notes/precision-pressure-sensor-measurements-using-the-max11254-analogtodigital-converter.html> (дата звернення: 18.02.2024).
6. Laser Focus takes on the world. Url: <https://www.laserfocusworld.com/test-measurement/research/article/16556222/laser-focus-takes-on-the-world> (дата звернення: 18.02.2024).
7. High-precision microsensor technology for a wide application range. Url: <https://www.innovations-report.com/power-and-electrical-engineering/high-precision-microsensor-technology-for-a-wide-application-range/> (дата звернення: 18.02.2024).
8. High-precision microsensor technology for a wide application range. Url: <https://www.innovations-report.com/power-and-electrical-engineering/high-precision-microsensor-technology-for-a-wide-application-range/> (дата звернення: 18.02.2024).
9. Sensor de movimiento para productos médicos implantables. Url: <https://www.interempresas.net/Electronica/Articulos/176078-Sensor-de-movimiento-para-productos-medicos-implantables.html> (дата звернення: 18.02.2024).
10. 3-axis accelerometer for medical/healthcare applications. Url: <https://www.st.com/en/mems-and-sensors/mis2dh.html> (дата звернення: 18.02.2024).

11. Lewis J, Moss B. MEMS Microphones, the Future for Hearing Aids. Url: <https://www.analog.com/en/resources/analog-dialogue/articles/mems-microphones-future-for-hearing-aids.html> (дата звернення: 18.02.2024).
12. ABI Research Finds Cirrus Logic Outperforms Mother Nature and Introduces World's Smallest MEM Microphone. Url: <https://www.businesswire.com/news/home/20150910006385/en/ABI-Research-Finds-Cirrus-Logic-Outperforms-Mother-Nature-and-Introduces-World%E2%80%99s-Smallest-MEM-Microphone> (дата звернення: 18.02.2024).

4 ОПТИЧНІ ДАТЧИКИ ДЛЯ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

4.1 Особливості технології ToF

ToF-технології (ToF – Time of Flight) визначення відстані одержали поширення завдяки малим габаритам, широкому динамічному діапазону й можливості роботи в різних середовищах [1, 2]. Незважаючи на те, що ToF-технології використовуються давно в науковій сфері й обороні, тільки зараз у зв'язку з розвитком мікроелектронної елементної бази, у тому числі з появою нових мікросхем, вони почали широко застосовуватися в різних сферах людської діяльності. Особливості застосування цих технологій розглянуті в справжній публікації.

На рис. 4.1 показано принцип роботи ToF-систем визначення відстані між об'єктами. Логістика, контроль якості, навігація, робототехніка, розпізнавання осіб, охорона здоров'я й моніторинг руху транспортних коштів – це основні області використання ToF-систем з 3D-зондуванням відстані для розв'язку завдань, які практично неможливо було розв'язати за допомогою 2D-технології [3].

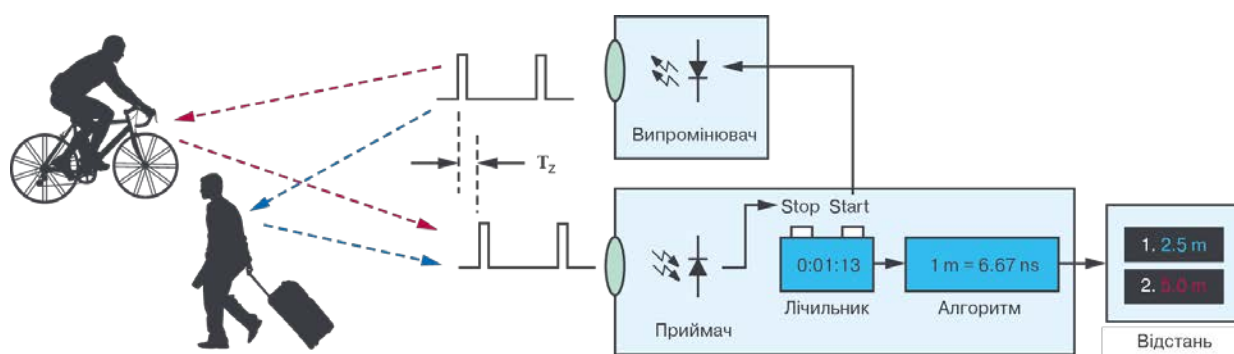


Рисунок 4.1 – Спрощена схема виміру відстані із застосуванням ToF-технології [3]

Затримка пропорційна подвоєній відстані між камерою й об'єктом опромінення, тому відстань може бути оцінена по формулі як: $d = c\Delta T/2$, де c – швидкість світла.

Завдання обладнання полягає у вимірі затримки Δt між випромінюваним і відбитим сигналом. Існують різні методи виміру інтервалу ΔT , два з яких одержали найбільше поширення. Це метод незатухаючих хвиль (CW-метод) і імпульсний метод.

У методі незатухаючих CW-хвиль періодичний модульований сигнал використовується для активного опромінення об'єкта, як показано на рис. 4.2, а зрушення фази відбитого світла вимірюється за допомогою демодуляції прийнятого фотоприймачем сигналу. Наприклад, можна використовувати синусоїдальну модуляцію, де випромінюваний сигнал має вигляд:

$$s(t) = A_s \cos(2\pi f_{\text{mod}} t) + B_s$$

де A_s – амплітуда сигналу, B_s – зміщення сигналу за рівнем, f_{mod} – частота модулюючого сигналу, $f_{\text{mod}} = 1/T_{\text{mod}}$, T_{mod} – період модулюючого сигналу.

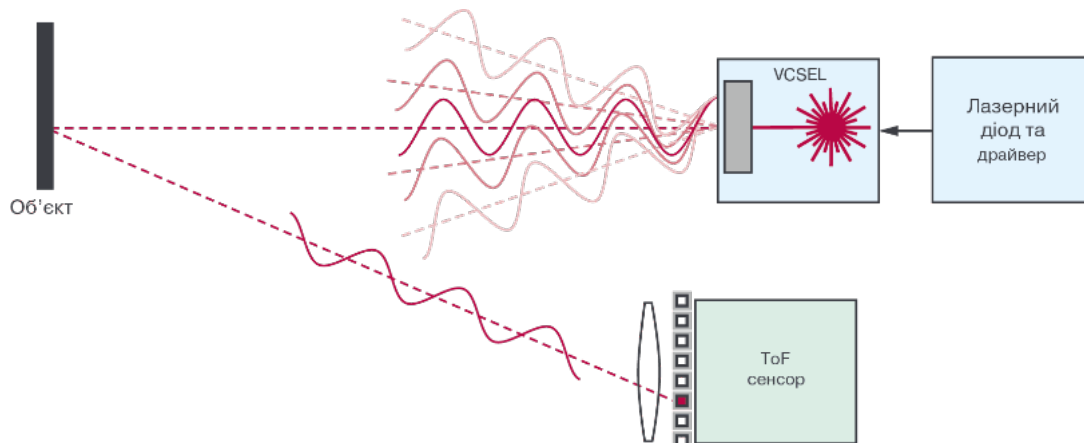


Рисунок 4.2 – Принцип дії ToF-системи на основі методу незатухаючих хвиль [1]

Прийнятий фотоприймачем сигнал $r(t)$ є відбитим від об'єкта сигналом, що приходить з затримкою і ослабленим по відношенню до сигналу опромінення:

$$r(t) = \alpha S(t - \Delta T),$$

де $0 \leq \alpha < 1$ – коефіцієнт ослаблення, який залежить від відстані й відбивної здатності об'єкта, а ΔT – затримка сигналу.

Час прольоту СВ-хвилі пропорційний відстані й вимірюється шляхом вибірки кореляційної функції між прийнятим відбитим сигналами $r(t)$ і демодульованим сигналом $g(t)$ з тою же частотою, що й $s(t)$. В ідеальному випадку демодульований сигнал також є синусоїдальною хвилею:

$$g(t) = A_g \cos(2\pi f_{mod} t) + B_g$$

Операція кореляції описується виразом:

$$c(\tau) = \int_0^{NT} r(t)g(t-\tau)dt.$$

4.2 Тривимірна технологія ToF

Тривимірна ToF-камера або 3D ToF це тип лідара, у якому використовуються потужні оптичні імпульси тривалістю декілька наносекунд для виміру відстані до об'єкта й визначення глибини його рельєфу (як правило, на коротких відстанях). Структура такої камери, що випускається компанією Analog Devices. наведена на рис. 4.3.

Існують кілька типів ToF-камер [2-4]. Для кожного з типів використовується своя технологія вимірювання дальності положення об'єкта. Найпростіша технологія – "Pulsed Modulation" або, по-іншому, "Direct Time-Of-Flight imagers" полягає в наступному (рис. 4.4).

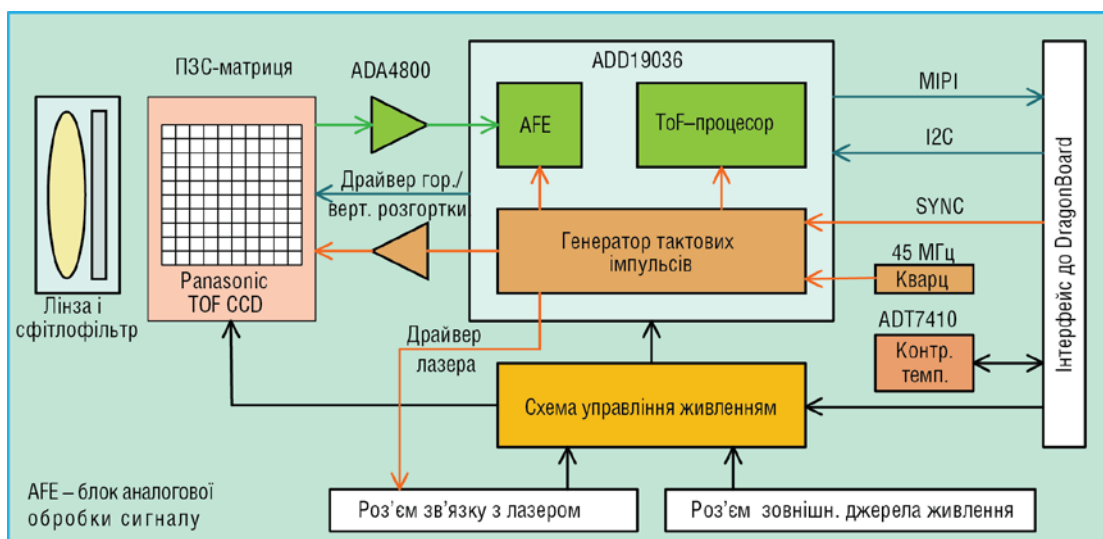


Рисунок 4.3 – Структура ToF-камери

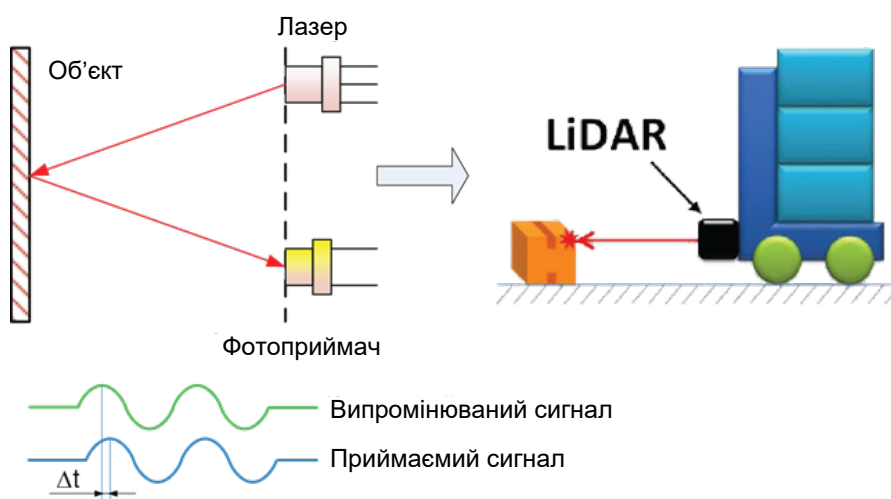


Рисунок 4.4 – Пояснення принципу дії ToF-камери [3]

Імпульс випромінюється джерелом світла, вбудованим у камеру, і відбивається від об'єкта. Відбите світло направляється на фотоприймач (фотодіод або ПЗС-матрицю) через вбудований об'єктив. Камерою вимірюється час, за яке світло покриває відстань до об'єкта й назад до фотоприймача. Знаючи швидкість світла, отримане значення можна використовувати для обчислення відстані до світловідбиваючої поверхні для кожного елемента фотоприймача.

Якщо в якості фотоприймача використовується ПЗС-матриця, то цей метод дозволяє одночасно одержувати велику кількість точок і побудувати карту

"глибин", тобто рельєф об'єкта, а також профіль інтенсивності відбитого світла в режимі реального часу.

Якщо основними вимогами до ToF-камери є велика робоча відстань, висока швидкість роботи й, при цьому, нескладна архітектура системи (за умови, що дотримання цих умов більш важливо, ніж точність вимірів), то доцільно використовувати ToF-камери, навіть у випадку порівняно невеликого бюджету. Через відносно низьку точність значень виміру "глибини" вони найкраще підходять для розв'язку завдань, що не вимагають високої точності, таких як автоматизація виробництва й переміщення великогабаритних об'єктів за допомогою роботизованих систем. Ці камери широко застосовуються в логістиці для виміру об'єму вантажів (рис. 4.5) з метою визначення вартості фрахту або транспортування, а також завантаження й розвантаження піддонів повністю в автономному режимі роботами, без переривання технологічних процесів.



Рисунок 4.5 – Вимір об'єму вантажу за допомогою ToF-камер безконтактним методом [3]

ToF-камерами можна оснащувати автоматичні самохідні візки, що дозволить автоматизувати процес логістики на виробництві. Для цього одна або декілька ToF-

камер у реальному часі здійснюють зйомку навколишнього простору, дозволяючи аналізувати знаходження оточуючих об'єктів і уникнути зіткнення з ними.

ToF-Камери можна використовувати для контролю руху на автодорогах. Зокрема, для виявлення пішоходів на переходах або на дорогах у темний час доби.

На рис. 4.6 [3] наведений комплект плат для розробки систем 3D ToF, пропонується компанією Analog Devices.

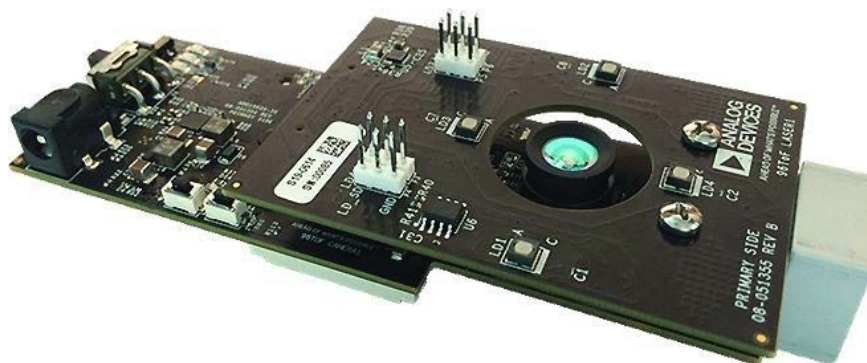


Рисунок 4.6 – Зовнішній вигляд комплекту плат для розробки систем 3D ToF [4]

На рис. 4.7 показаний результат роботи ToF-камери, наведеної на рис. 4.6.



Рисунок 4.7 – Зображення долоні на екрані телевізора отримане за допомогою ToF-камери

На екрані відображається зображення об'єкту та відстань до нього.

Використання зображення у форматі 2D разом з 3D-зондуванням може значно поліпшити якість інформації при вимірі відстаней між різними об'єктами

(рис. 4.8). Зокрема, 2D-зондування не дозволяє відрізнити особу реальної людини від її фотографії. Додаткова інформація про глибину дозволяє краще класифікувати людей, відслідковуючи їх особисті риси, особливості фігури, ходи й т.п. Визначення відстані може забезпечити високу якість розпізнавання осіб у юрбі, наприклад, для швидкого розпізнавання злочинця. Чим вище дозвіл і точність виміру відстані, тем краще працює алгоритм класифікації. Це може бути використане для надання доступу до мобільних пристроїв, санкціонованого доступу до службових приміщень і для підвищення безпеки в цілому.

Розглянуті системи можуть успішно застосовуватися в промисловості. Здатність точно вимірювати й класифікувати деталі в реальному часі в процесі виробничого процесу є важливим завданням. Точне визначення відстані допомагає ефективно розподілити простір складських приміщень. Деталі, які сходять із виробничої лінії, можуть бути швидко спрямовані в складальні цехи. Визначення відстані з високим дозволом дозволяє визначати краї будівельних або складських конструкцій у режимі реального часу (рис. 4.9), а також робити швидкі обчислення об'ємів різних об'єктів (рис. 4.5).



Рисунок 4.8 – Розпізнавання обличчя з використанням 3D-зондування [5]

Автономні транспортні засоби широко застосовуються на підприємствах. Вони повинні мати можливість швидкого переміщення по фабричному цеху або

складу. Технологія високоточного зондування відстані дозволить скласти карту виробничого простору в реальному часі, локалізувати транспортний засіб на карті й побудувати найбільш ефективний маршрут для його пересування. Одна із проблем впровадження подібних систем у промисловість полягає в захисті від перешкод, генеруємих датчиками подібних пристроїв і систем. Розроблювані в цей час протоколи для придушення завад дозволять таким системам працювати одночасно в зоні прямої видимості, не впливаючи одна на одну. Приклади використання ToF-систем для вимірювання відстані на виробництві наведені на рис. 4.9.



Рисунок 4.9 – Приклади використання ToF-систем для вимірювання відстані на виробництві

4.3 Лазерні далекоміри

4.3.1 Загальні зауваження

Лазерні далекоміри – найпоширеніше обладнання виміру дальності в промислових та побутових цілях (будівництво, полювання, туризм і т.п.). Таке обладнання забезпечує вимірювання дальності на відстані від 1 до 1500 м з точністю від 25 мкм до 1,5 м.

Принципи виміру дальності за допомогою лазерного випромінювання багато в чому подібні із принципами виміру за допомогою радіохвиль, але є й спеціальні "лазерно-оптичні" методи: дифракційний і триангуляційний.

Триангуляційний метод застосовується там, де необхідно високоточний вимір дальності в межах від декількох міліметрів до декількох метрів.

У якості джерела світла можна використовувати світлодіод або лазерний діод, у якості фотоприймача – прилад із зарядовим зв'язком (CCD), матрицю фотодіодів або позиційно-чутливий детектор (PSD). Останній являє собою монолітний детектор (фотодіод) у якому використовується поверхневий опір для одержання безперервної інформації про положення максимуму світлового потоку на поверхні. PSD більш точні й надійні в порівнянні з CCD.

Суть методу полягає в тому, що якщо відоме положення точок А і В, кути α і β , то можна однозначно визначити положення точки С (рис. 4.10). Відбитий від об'єкта лазерний промінь лінзою, що збирає, фокусується в точку на фотоприймачі, яка визначає відстань до об'єкта.

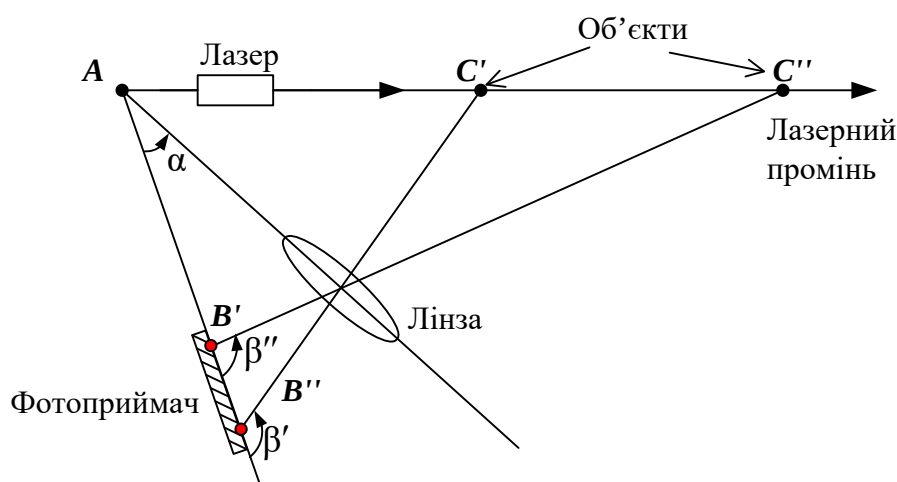


Рисунок 4.10 – До пояснення триангуляційного методу

Мінімальна й максимальна дальність виміру визначаються кутом α , ефективною довжиною фотоприймача і його розташуванням щодо точки А.

Для зменшення впливу фонового освітлення застосовують оптичні фільтри, що послабляють інтенсивність світла з довжиною хвилі, відмінної від довжини хвилі використовуваного лазера. Також застосовують алгоритм вимірів, який передбачає вимір струму PSD до й після включення лазера, а також кілька повторних вимірів, що дозволяють із високою вірогідністю визначити координату центру мас лазерної плями на поверхні PSD.

Кінцева точність обробки сигналу отриманого з PSD залежить від розрядності аналого-цифрового перетворювача (АЦП) і складності застосовуваного алгоритму.

4.3.2 Джерела лазерного випромінювання

Для формування променя потрібний стабільний по частоті й досить потужний лазер, який для вимірювання дальності може бути наступних типів [6, 7]:

- напівпровідниковий (на основі GaAs, In, Si);
- газонаповнений (найчастіше гелій-неонові, HeNe).

Гелій-неонові лазери – малопотужні (0.1...1 Вт), малогабаритні випромінювачі (резонатори довжиною 15...50 см), з довжиною хвилі 623 нм (червоне світло видимої частини спектру). Робоче тіло – суміш гелію й неону в пропорції 5:1 під низьким тиском (~300 Па). Енергія накачування подається від двох електричних розрядників з напругою близько 1000 В, розташованих у торцях колби.

Напівпровідникові лазерні діоди використовуються для мініатюрних і ефективних лазерних далекомірів. Їхні основні переваги: висока надійність, механічна міцність, низька напруга живлення, високий (до 50%) ККД, тривалий термін служби (до 100 тис. годин), мала інерційність, можливість перебудови довжини хвилі випромінювання, наявність великої кількості напівпровідників, що безупинно перекривають інтервал довжин хвиль від 0,32 до 32 мкм.

У напівпровідникових лазерах (НПЛ) збуджуються й випромінюють (колективно) атоми кристалічних ґрат. Це дозволяє одержати високу компактність (обсяг кристала $10^{-6} \dots 10^{-2}$ см) і показник оптичного посилення $10^4/\text{см}$.

Відмінність від звичайних світлодіодів – когерентність випромінювання (усі випромінені хвилі у фазі). Це досягається особливим станом кристалу що випромінює світло – стан з інверсією населеностей.

Застосовують наступні методи накачування напівпровідникових лазерів:

- інжекція носіїв струму через pn -перехід, гетероперехід або контакт метал-напівпровідник (інжекційні лазери);
- накачування пучком швидких електронів;
- оптичне накачування;
- накачування шляхом пробію в електричному полі.

Найбільший розвиток одержали напівпровідникові лазери (ПЛ) наступних двох типів: інжекційні й з електронним накачуванням.

Лазери інжекційного типу працюють в імпульсному режимі з вихідною потужністю до 100 Вт і в безперервному режимі з потужністю більш 10 Вт (GaAs) у близькій інфрачервоній (ІЧ) області ($\lambda = 850$ нм) і близько 10 мВт (Pbxsnl-xte) у середній ІЧ області ($\lambda = 10$ мкм). Недолік інжекційних лазерів – слабка спрямованість випромінювання, обумовлена малими розмірами випромінюючої області і відносно широкий спектр генерації в порівнянні з газовими лазерами.

Інжекційний лазер на pn -переході являє собою напівпровідниковий діод, у якого дві паралельні поверхні, перпендикулярні pn -переходу (рис. 4.11), утворюють оптичний резонатор (коефіцієнт відбиття від граней кристала $\approx 20\ldots 40\%$). Інверсія населеностей (тобто готовність до випромінювання) досягається при великій щільності прямого струму через діод (поріг генерації відповідає струму від 100 до 1000 А/см²). Для одержання досить інтенсивної інжекції застосовують сильно леговані напівпровідники.

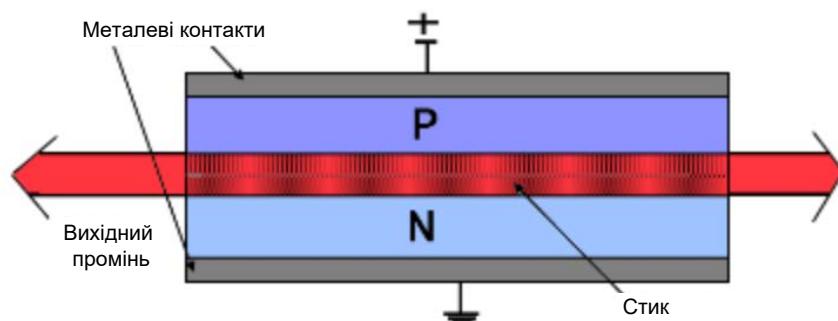


Рисунок 4.11 – Структура інжекційного лазера на pn -переході [8]

Інжекційні лазери на гетеропереході (з'явилися в 1968) являють собою, двосторонні гетероструктури. Активний шар (GaAs) укладений між двома напівпровідниковими гетеропереходами, один з яких (типу pn) служить для інжекції електронів, а другий (типу pp) відбиває інжектовані електрони, перешкоджаючи їх дифузійному розтіканню з активного шару (електронне обмеження). При однаковому струмі накачування в активному шарі гетероструктури досягається більша концентрація електронно-діркових пар й, отже, більше оптичне посилення, чим у лазерах на pn -переходах.

Інша перевага гетероструктури полягає в тому, що утворений активним шаром діелектричний хвилевід утримує випромінювання, що поширюється уздовж структури, у межах активного шару (оптичне обмеження), завдяки чому оптичне посилення використовується найбільше ефективно. Для НПЛ на гетеропереході необхідна щільність струму при $T = 300\text{ }^{\circ}\text{K}$ більш ніж в 10 раз нижче, чим у НПЛ на pn -переході, що дозволяє здійснити безперервний режим генерації при температурі до $350\text{ }^{\circ}\text{K}$.

Напівпровідникові лазери з електронним накачуванням

При бомбардуванні напівпровідника швидкими електронами з енергією $W \sim 10^3 \dots 10^6\text{ ЕВ}$ у кристалі народжуються електронно-діркові пари; кількість пар, створюване одним електроном, $\sim W/3\Delta E$ [6, 7]. Цей спосіб застосовується до напівпровідників з будь-якою шириною забороненої зони. Вихідна потужність такого лазера досягає 10^6 Вт , що пояснюється можливістю накачування великого обсягу напівпровідника. Достоїнство НПЛ із електронним накачуванням – можливість швидкого переміщення (сканування) електронного пучка по кристалу, що дає додатковий спосіб керування випромінюванням. Оскільки помітна частина енергії електронного пучка витрачається на розігрів ґрат кристала, то ККД обмежений ($\sim 1/3$), тобто на кожную електронно-діркову пару витрачається енергія $3\Delta E$, а випускається фотон з енергією $\sim \Delta E$.

НПЛ інжекційного типу випускають для комерційного застосування в різних модифікаціях. Деякі їхні різновиди представлені на рис. 4.12. НПЛ на рис. 4.12 мають вихідну оптичну потужність у безперервному режимі від 500 мВт до 4 Вт .

Квазінеперервні лазерні лінійки можуть мати пікову вихідну оптичну потужність до 150 Вт.



Рисунок 4.12 – Приклад твердотільного лазерного діода [9]

4.3.3 Типи лазерних далекомірів

Лазерні далекоміри випускаються в різних модифікаціях [10]:

- малогабаритні ручні "лазерні лінійки" із РКІ (рідкокристалічними індикаторами). Мають робочу дальність до декількох десятків метрів і високу точність виміру;
- далекоміри-біноклі з потужною оптичною системою й висновком результатів виміру на оптичну призму, поруч із об'єктом спостереження;
- стаціонарні військові або науково дослідницькі далекоміри мають високу точність при значних вимірюваних відстанях, мають потужну оптику й (часто) дистанційне керування.

Зараз лазерні далекоміри використовуються в наземній військовій техніки (артилерійські, танкові), і в авіації (далекоміри, висотоміри), і на флоті. У цей час ряд далекомірів прийнятий в арміях ряду країн.

4.3.4 Практичні застосування лазерних далекомірів

Перші дослідні зразки з'явилися вже через рік після появи лазера, і відносяться до 1961 р. Широке практичне застосування лазерів й безпосередньо лазерні далекоміри (ЛД), знаходять у військовій техніці.

Перший лазерний далекомір ХМ-23 пройшов випробування у В'єтнамі й був прийнятий на озброєння в армії США [11]. Він був розрахований на використання на передових спостережних пунктах сухопутних військ.

Джерелом випромінювання в ньому був лазер з вихідною потужністю 2,5 Вт і тривалістю імпульсу 30 нс. У конструкції далекоміра широко використовувалися інтегральні схеми. Випромінювач, приймач і оптичні елементи змонтовані в моноблоці, який має шкали точного відліку азимута й кута місця мети.

Живлення далекоміра здійснювалося від батареї напругою 24 В, що забезпечує до 100 вимірів дальності без підзарядки.

Значний розвиток далекоміри одержали в корабельних системах навігації, де було потрібно одержання значної дальності виміру при не дуже великій точності.

Лазерні далекоміри модульної конструкції випромінюють на довжині хвилі 1,064 мкм або 1,54 (1,57) мкм і забезпечують вимір дальності до 40 км із точністю ± 5 м. Характерним прикладом такого далекоміра є модель MOLEM фірми Zeiss Optronik GmbH (рис. 4.13). Цей далекомір випромінює промінь з довжиною хвилі 1,543 мкм. Енергія в імпульсі становить 10 МДж при тривалості імпульсу випромінювання 5 нс і повторі вимірів із частотою 1 Гц. Кутове розходження випромінювання становить 0,5 мрад, діапазон вимірюваних дальностей з точністю 5 м становить 50...39995 м.

Дистанція розрізнення цілей по дальності становить 20 м, можливо стробування по дальності із кроком 10 м. Маса 2,5 кг, габаритні розміри 180×124×112 мм, напруга живлення – 18...32 В, струм споживання менш 2 А, діапазон робочих температур від -35...63 °С.



Рисунок 4.13 – Типовий корабельний лазерний далекомір MOLEM [11]

Розвиток оптичних і радіоелектронних систем дозволив створити кілька поколінь космічних лазерних далекомірів, точність яких починаючи з кінця 60-х років до нашого часу виросла в сотні раз. Якщо перші лазерні далекоміри системи "Малий сажень" (прообраз сучасних систем наведення й визначення координат, таких як, наприклад GPS) мали середньоквадратичну погрішність порядку 2 м, то в 90-х роках погрішність становила 7...10 мм і продовжує зменшуватися. Космічні лазерні далекоміри (іноді сполучені з наземними), володіючи такою точністю, дозволяють виконувати наступні категорії завдань:

- вимір висоти орбіти супутника;
- вимір флуктуацій гравітаційного поля Землі по величині флуктуацій рівня океану в заданій крапці;
- спостереження за дрейфом материкових плит;
- точне визначення координат наземного об'єкта для наступного наведення на мету;
- пророкування сейсмічної активності місцевості по відносному підняттю рівня землі в заданих точках.

Крім військової й космічної техніки лазерні далекоміри також знайшли своє застосування в побутових умовах. Це лазерні рулетки й далекоміри-біноклі.

На рис. 4.14 показані лазерні рулетки різних виробників, застосовувані в будівництві .



Рисунок 4.14 – Лазерні рулетки різних виробників [12]

Максимальна дальність вимірів таких далекомірів від 30 до 500 м. Мінімальна дальність від 5 см. Похибка вимірювання від 5 до 0.5 мм. Лазер з довжиною хвилі 635 нм. Ступінь захисту – IP52...IP67, живлення – 2 елементи ААА (крім далекомірів, у яких передбачений обігрів і робота в несприятливих умовах). Кількість вимірів від одного комплекту елементів не менш 5000. Маса приладів 100...200 г. Гарантійний строк експлуатації не менш 12 місяців.

Додаткові функції (доступні не всі одночасно): підсвічування дисплея, зовнішні інтерфейси обміну даними, математичні обчислення площі, обсягу, збереження декількох останніх вимірів у пам'яті, можливість установки на штатив, дистанційного керування.

На рис. 4.15. наведено зовнішній вигляд лазерної рулетки Xiaomi Mileseeey Laser Ranging Tape Measure [13]. Головна особливість рулетки – вимірювання довжини за допомогою стрічки або лазера. Максимальна довжина стрічки – 5 м, за допомогою лазера можна вимірювати відстань до 60 м. Точність отриманих результатів 2 мм. Вбудована карта пам'яті та інтерфейс USB дозволяють зберігати результати вимірів і потім передати їх на ПК.



Рисунок 4.15 – Лазерна рулетка Xiaomi Mileseeey Laser Ranging Tape Measure [13]

Далекоміри-біноклі застосовуються на полюванні або в інших похідно-польових умовах (рис. 4.16) [14, 15]. Далекомір на рис. 4.16 використовує оптичну систему бінокля (зорової труби) для посилення прийнятого лазерного випромінювання, що дозволяє досягти дальності виміру до 1600 м. Точність вимірів не гірше 1 м. Час виміру не більш 1 с. Оптичне збільшення від 4 до 10 разів. Лазери ІК діапазону (830...950 нм). Вологозахищене виконання. Елементи живлення CR123 з наругою живлення 3 В. Кількість вимірів від одного комплекту елементів – не менш 1000. Маса приладів 880 грам. Гарантійний строк експлуатації не менш 36 місяців.



Рисунок 4.16 – Лазерні далекоміри-біноклі [14]

Додаткові функції (доступні не всі одночасно): багат шарове просвітління оптики, установка на штатив, визначення дистанції до найближчого в групі об'єкта, обчислення виправлень на кут нахилу місцевості, відображення дальності в ярдах або метрах, запис на згадку декількох останніх вимірів.

Окрім наведених пристроїв випускаються лазерні рівні для використання у будівництві (рис. 4.17) [16].



Рисунок 4.17 – Лазерний рівень [16]

Пристрої, що мають інтерфейси зв'язку, широко використовуються в системах IoT та PoT.

4.4 Оптичні датчики диму

Згідно з дослідженнями національної асоціації протипожежного захисту США, майже кожний четвертий (23%) випадок загибелі людей при пожежах навіть у такій розвиненому країні, як США, відбувається через те, що системи сигналізації про задимлення не працювали або були відключені. Тому наявність не тільки датчиків тепла, але й датчиків диму (продуктів процесу горіння – дрібних часток кіптяви), що з'являється при загорянні, є обов'язковим у сучасних автоматичних системах пожежогасіння.

Проблема надійності й точності роботи систем виявлення диму актуальна й на сьогоднішній день. Однією з найважливіших характеристик датчиків диму є ймовірність неправильних спрацьовувань. Неправильні спрацьовування є основним чинником, що спонукують споживачів знімати або відключати датчики протипожежної сигналізації, що при виникненні пожежі найчастіше приводить до трагічних результатів.

За принципом побудови датчики диму діляться на:

- іонізаційні – виявлення диму засноване на властивості іонізованого (у результаті нагрівання) повітря притягати частки димового потоку [17];
- оптичні (оптико-електронні) – виявлення засноване на вимірі оптичної щільності газо-повітряного середовища, яке міняється з появою часток диму [18, 19];
- аспіраційні, що забезпечують відбір і доставку проб повітря (аспірацію) через систему труб з отворами для забору повітря із приміщення, що захищається (зони) до обладнання виявлення ознаки пожежі (димув, зміни хімічного складу середовища) [20];
- лінійні – приймач ІЧ-випромінювання, установлений на одній осі й значному видаленні від передавача, реагує на ослаблення сигналу нижче заданого рівня [21].

Модифікацією лінійного датчика є обладнання, у якому випромінювач і приймач установлюються в одному корпусі, а ІЧ-промінь спрямований на

пасивний відбивач, розташований напроти датчика. Як впливає з наведеного переліку лінійні датчики також є оптико-електронними.

Найбільш ефективні іонізаційні датчики. Вони здатні виявляти вогнище загоряння не тільки на самій ранній стадії по появі летучих часток реакції горіння, але й реагують на будь-який їхній розмір, а також колір, що залежить від фізико-хімічних параметрів повітря в приміщеннях, що захищаються, так званий сірий і чорний дим, що недоступно більшості іншого автоматичного обладнання, що фіксують утворення димового потоку. Істотним недоліком таких датчиків є висока складність їх виробництва, технічного контролю й необхідність утилізації (деактивації) тільки на спеціалізованих підприємствах атомної промисловості через наявність у них радіоізотопних випромінювачів.

Тому найбільш широке поширення одержали оптичні датчики диму, принцип дії яких ілюструє рис. 4.18 [18].

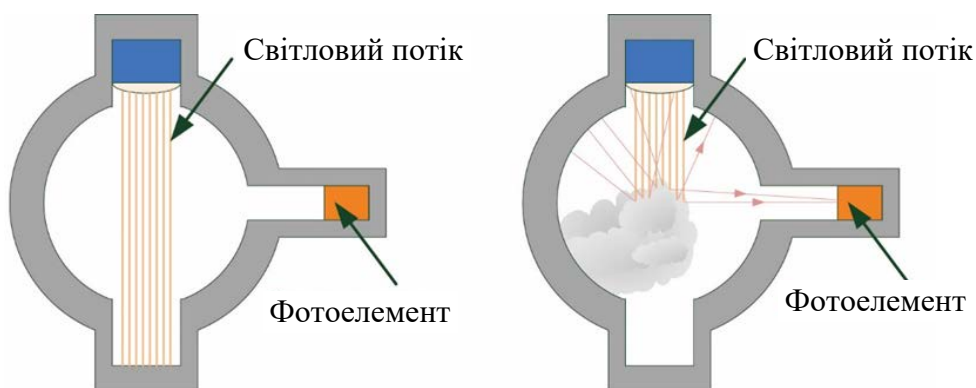


Рисунок 4.18 – Пояснення принципу дії оптичного датчика диму

При відсутності диму світловий потік, випромінюваний джерелом світла, не попадає на фотоелемент (будь-який приймач світла). Як тільки з'являється дим, частина світлового потоку починає відбиватися від часточок диму й попадає на фотоелемент, сигнал з виходу якого інформує про наявність диму в приміщенні. Можлива й інша конструкція датчика. Якщо джерело світла й фотоелемент розташовуються на одній осі, то при наявності диму частина світлового потоку

буде губитися й сигнал на виході фотоелемента буде зменшуватися, що буде свідчити про наявність диму.

Компанія Analog Devices випустила інтегровану в одному корпусі оптико-електронну систему виявлення диму ADPD188BI, що забезпечує роботу у двох діапазонах довжин хвиль оптичного випромінювання [18]. Система містить синє і інфрачервоне джерела світла на двох світлодіодах і два фотодіоди. Це дозволяє підвищити ймовірність виявлення диму при його малій концентрації. Для розширення функціональних можливостей системи в ній передбачено два додаткові входи для підключення зовнішніх датчиків. Наприклад, датчиків вмісту вуглекислого газу й температури.

Функціональна схема ADPD188BI наведена на рис. 4.19. Модуль містить два оптичні детектори. Перший фотодетектор (PDET1) має активну площу 0.4 мм^2 і підключений до третього входу ASIC, а другий фотодетектор (PDET2), площею 0.8 мм^2 , підключений до четвертого входу ASIC. У якості джерел світла використовуються синій світлодіод з довжиною хвилі випромінюваного світла 470 нм і інфрачервоний – довжина хвилі 850 нм.

Оптична система, що працює у двох різних діапазонах хвиль, дозволяє розрізняти дрібні частки диму, пили, і водяної пари. Вбудована в модуль інтегральна схема спеціального призначення (ASIC) включає блок обробки аналогового сигналу, 14-розрядний АЦП (14-BIT ADC), цифровий блок обробки сигналу, інтерфейси зв'язку I2C і SPI, і три незалежно програмовані джерела живлення світлодіодів (LED DRIVER).

Розташування оптичних компонентів ADPD188BI показане на рис. 4.20. Як випливає з рисунка, світлодіоди й фотодетектори не мають прямого оптичного контакту. Тільки з появою часточок диму або пари на фотоприймач будуть попадати відбиті промені світла.

Увесь робочий цикл ADPD188BI розбитий на два часові інтервали (рис. 4.21) [19]. У кожному часовому інтервалі здійснюється повний цикл роботи – від випромінювання світлодіодів до обробки отриманих даних. Налаштування драйверів світлодіодів і алгоритм обробки даних встановлюються для кожного інтервалу часу

незалежно за допомогою блоків TIME SLOT DATA. Для зниження енергоспоживання робочі цикли чергуються з інтервалами часу, коли датчик перебуває в режимі зниженого енергоспоживання (SLEEP).

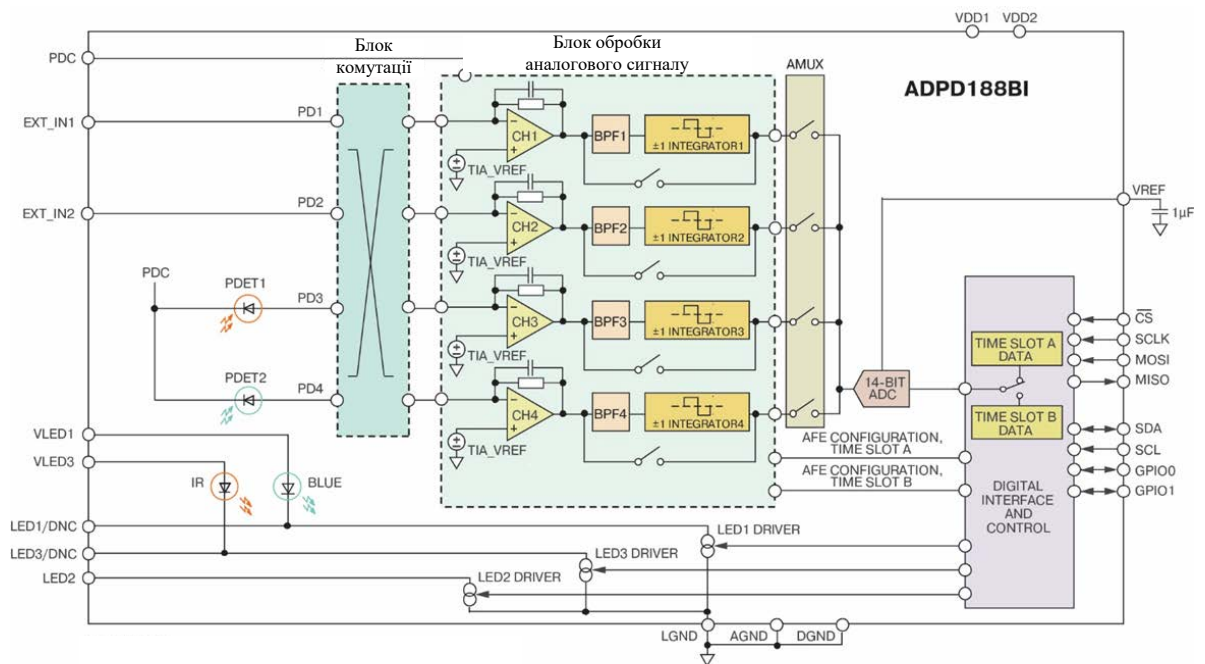


Рисунок 4.19 – Функціональна схема датчика диму ADPD188BI

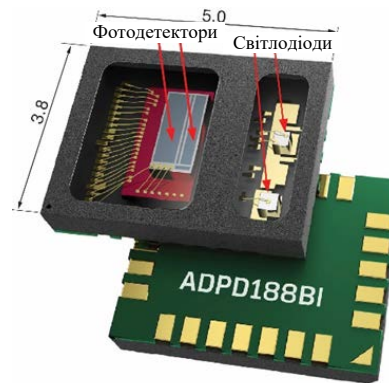


Рисунок 4.20 – Розташування оптичних компонентів датчика диму ADPD188BI [18]

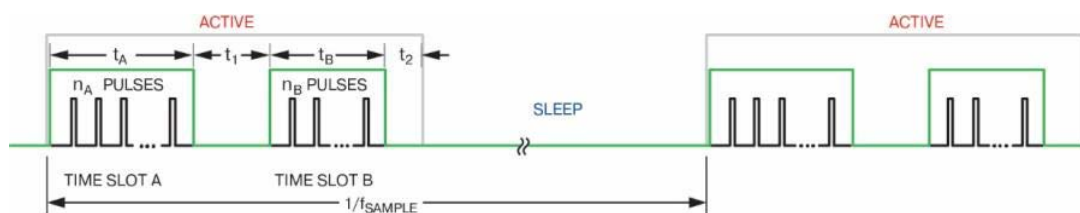


Рисунок 4.21 – Часові діаграми сигналів ADPD188BI в різних режимах [18]

Часові параметри циклів роботи датчика визначаються співвідношеннями:

$t_a = 25 + n_a \times 19$ [мкс], $t_b = 25 + n_b \times 19$ [мкс], $t_1 = 68$ мкс, $t_2 = 20$ мкс, де n_a і n_b , число імпульсів для часових інтервалів А і В, відповідно. Число імпульсів може бути задано від 1 до 255.

Частота взяття вибірок f_{sample} задається шляхом запису даних у регістр керування. В [15] наведені рекомендовані значення часових параметрів циклу роботи датчика. За замовчуванням рекомендується встановити частоту узяття вибірок рівну 32 кГц. У датчику ADPD188BI передбачений режим роботи із зовнішньою синхронізацією, сигнали якої необхідно подавати на вхід GPIO0 або GPIO1.

За допомогою блоку комутації підтримується кілька конфігурацій чотирьох вхідних каналів, залежно від налаштувань, внесених у регістр керування. Інтегровані фотодіоди можна підключити до входу каналів 3 і 4 або об'єднати їхні сигнали на вході каналу 1. Входи зовнішніх датчиків EXT_IN1 і EXT_IN2 можуть бути підключені до входів каналів 1 і 2 або об'єднані на вході каналу 2.

Сигнали, що надходять на входи блоку обробки аналогового сигналу, підсилюються й передаються на аналоговий комутатор AMUX або прямо з виходу підсилювача, або через смуговий фільтр і інтегратор. Аналоговий комутатор по черзі опитує виходи тих каналів, які задіяні й передає сигнал з виходу блоку обробки на вхід АЦП.

Завдяки можливості проводити математичну обробку результатів вимірів, зокрема здійснювати усереднення до 128 вибірок сигналу, еквівалентна розв'язна здатність АЦП змінюється залежно від числа імпульсів, що зазнають обробці. При обробці одного імпульсу розв'язна здатність АЦП становить 14 розрядів, а при числі імпульсів від 64 до 255 – 20 розрядів. При числі імпульсів від 64 до 255 і проведенні усереднень по 128 реалізаціях еквівалентне число розрядів зростає до 27.

Відмінною рисою детектора диму ADPD188BI є відсутність димової камери. Безкамерні детектори диму швидше реагують на появу диму. Достоїнством таких

датчиків є здатність оптики випромінювати розсіяний світло. Вартість таких датчиків значно нижче чому з камерами диму, а конструкція – значно простіше.

Недоліком таких датчиків є те, що їх оптика піддається впливу навколишнього середовища. Це може привести до того, що світильники, розташовані неподалік від датчиків, можуть викликати його неправильне спрацьовування. Тому всі датчики повинні проходити випробування на сліпучий вплив. Ціль цього випробування – показати, що на чутливість димової сигналізації не виявляє надмірного впливу близькість штучних джерел світла або вплив денного світла. Цей тест застосовується тільки для оптико-електронних датчиків диму.

4.5 Лазерні та інфрачервоні датчики охорони периметру

4.5.1 Загальні зауваження

Датчики руху для охорони периметра будинку – дуже поширений спосіб контролю за територією, що оточує основний об'єкт: двір, земельну ділянку, стоянку, склад і т.д. Це потрібний елемент будь-якої складної охоронної системи. Спеціальні датчики периметра (бар'єр) для системи охорони периметра – основний вид обладнання, яке можна використати для цього [22, 23].

Система охорони периметра спрацьовує при спробі порушника перетнути зовнішній фізичний або умовний кордон. Якщо людина опиниться в зоні виявлення датчика, сигналізація сповістить про це зацікавлені особи.

Вуличні датчики периметра встановлюються уздовж зовнішньої межі ділянки під охороною. Детектори розміщуються на огорожі, а за її відсутності – на штативах безпосередньо на території. Кожен сповіщувач "відповідає" за вузьку зону певної протяжності.

Пристрої підключаються до центрального блоку сигналізації, який обробляє сигнали, що надходять по кабелю або радіоканалу. При спрацьовуванні датчика централь реагує відповідним чином – вмикає сирену, сповіщає користувачів (смс), передає сигнал тривоги на пульт охорони.

Склад системи лазерної охорони периметра залежить від площі території, яку необхідно контролювати, а також від технології побудови датчиків. Розрізняють інфрачервоні та фотоелектричні бар'єри. Перші доцільно використовувати для зведення високої "стіни", фотоелектричні системи охорони периметра будинку мають значно більше можливостей щодо збільшення довжини "стіни", тоді як її висота досягає не більше 30 сантиметрів.

Датчики охорони периметра ділянки великої площі потребують більш дорогих бар'єрів високої потужності. Розраховуючи, скільки датчиків периметра, якого типу і потужності знадобиться для побудови системи, важливо чітко визначити довжину і висоту стіни, яка найбільш ефективно і раціонально впорається зі своїм завданням у конкретних умовах. Навіть незначна економія може нівелювати роботу всієї системи.

4.5.2 Лазерні датчики охорони

Променеві лазерні датчики руху, охорони периметра, території засновані на дії лазерного променя відбиватися від перешкоди, визначати його розміри, напрямок та швидкість руху.

Лазерні датчики мають досить високу вартість, порівняно з іншими видами датчиків. Датчики внутрішнього виконання можуть бути застосовані як додаткова система охорони сигналізації в банках, в окремих приміщеннях, де зберігаються цінності.

У моделі RLS-2020i, наприклад, створюється кут опромінення 90 градусів, який розгортає датчик з дальністю 20×20 метрів (рис. 4.22) [24]. В іншій площині промінь має ширину кілька сантиметрів.

Такий датчик утворює лазерну "стіну", при перетині якої людини або якогось предмета спрацює сигналізація, тобто датчик подає сигнал на контрольну панель. Так само дана модель є у вуличному виконанні, маючи підвищений клас захисту від опадів, температури та вологості.



Рисунок 4.22 – Лазерний датчик RLS-2020i [24]

Крім "сухих контактів", датчик має Ethernet вихід, який можна адаптувати з роботою системи IP-відеоспостереження та керувати роботою поворотних відеокамер.

Датчик можна встановити на стіні, відсікаючи вертикальною площиною ("стіною") прохід до місця зберігання чогось (рис. 4.23) [24].

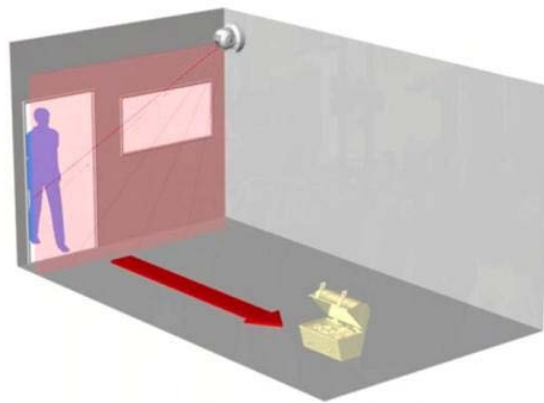


Рисунок 4.23 – Встановлення лазерного бар'єру при вході в приміщення [24]

Якщо датчик встановити під іншим кутом, повернувши на 90 градусів, можна відсікти пролаз через стелю. У цьому випадку створюється захисна стіна в горизонтальній площині (рис. 4.24) [24].

Датчики можуть налаштовуватися не тільки на людину, але і на предмет, при перетині яким лазерного променя спрацює лазерний датчик, розімкнувши свої сухі контакти і відправивши інформацію через Ethernet.

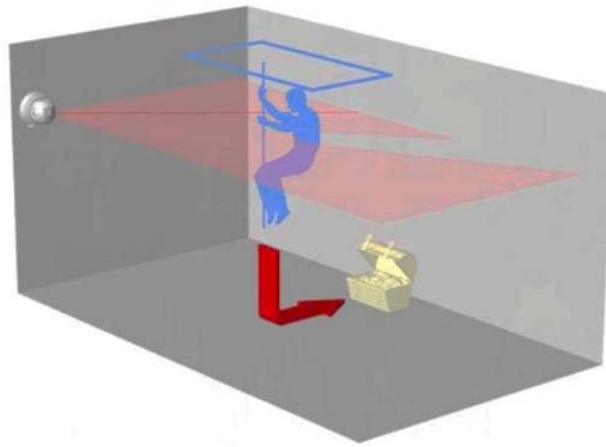


Рисунок 4.24 – Лазерний бар’єр RLS-2020i для захисту у горизонтальній площині [24]

Вуличні варіанти лазерних датчиків охорони периметра можуть захищати підступи до будівлі на території. На рис. 4.25 наведена вулична модель лазерного датчика охорони периметра RLS-3060SH [23].



Рисунок 4.25 – Лазерний датчик RLS-3060SH для встановлення на вулиці [23]

Принципова відмінність датчика у тому, що кут, створюваний лазером, дорівнює 180 градусів, а дальність виявлення об’єктів – 30 метрів. Встановивши такий датчик по центру огорожі, можна захистити периметр завдовжки до 60 метрів. Висота установки визначається наприклад за 1 метр від землі, з урахуванням трави та кучугур. Таким чином, формується горизонтальна захисна площина (рис. 4.26) [25].

Якщо цей лазерний датчик розташувати на стовпі, висотою, наприклад 5 метрів, то можна сформувати вертикальний бар’єр.

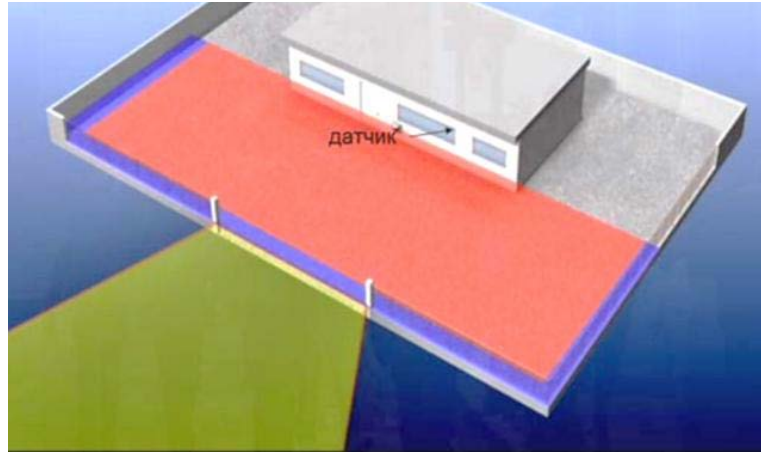


Рисунок 4.26 – Формування горизонтального захисного бар'єру [25]

4.5.3 Інфрачервоні датчики охорони периметра

Перший зовнішній рубіж охорони створюється за допомогою вуличних датчиків периметру різних типів [26, 27]:

- активних ІЧ-бар'єрів;
- пасивних ІЧ-детекторів.

У системах безпеки приватних будинків найчастіше використовуються активні ІЧ-датчики, які ефективні на відносно прямих ділянках без кущів, колючого дроту та інших перешкод. Пасивні інфрачервоні детектори призначені для охорони невеликих ділянок (наприклад, воріт двору).

Активні променеві інфрачервоні датчики створюють вузький бар'єр висотою від 60 см до 3 м. Бар'єр складається з 2...10 променів – в залежності від кількості променевих модулів. Чим більше променів – тим вище, а, отже, надійніше захисна "стіна".

Охоронна зона формується приймачем (фотоприймальним блоком) і передавачем, які встановлюються один навпроти одного. Діоди приймача випромінюють ІЧ-промені, а фотодіоди приймають їх. Сигналізація периметра спрацьовує при перекритті людиною двох або більше променів.

При виборі активного ІЧ-бар'єру треба звертати увагу на наступні характеристики:

- довжина променю – 50...200 метрів, різні показники для приміщення (більше) і вулиці (менше);
- горизонтальний і вертикальний кут формування променів;
- тип підключення – проводове, без проводове;
- ступінь захисту від вологи і пилу – для вулиці не менше IP64;
- діапазон робочих температур – від -25...30 до +5...60 °С (для суворих зим можна придбати нагрівачі, які встановлюються всередині корпусів приймача і передавача);
- можливість регулювання чутливості.

Розглянемо деякі датчики активних ІЧ-бар'єрів [9, 10].

ІЧ-бар'єр Lightwell LBX-100

Двопроменевий вуличний інфрачервоний бар'єр, довжина ІЧ-променю на вулиці 100 м, в приміщенні 300 м (рис. 4.27) [18]. Робочий діапазон температур від -25 до 55 °С, ступінь захисту IP65. Живлення від джерела постійного струму 12 В, струм споживання 150 мА. Габаритні розміри 9,9×211,5×74,7 мм.



Рисунок 4.27 – ІЧ-бар'єр Lightwell LBX-100 [26]

6-променевий ІЧ-бар'єр Lightwell LBW-60-6

Основні характеристики Lightwell LBW-60-6 (рис. 4.28) [26]:

- проводований;
- кількість інфрачервоних променів 6;
- довжина ІЧ-променю 60 м;
- горизонтальний кут налаштування променю 180 градусів (± 90 градусів) ;
- вертикальний кут налаштування променю нерегульований;
- швидкість відгуку не більше 40 мс;
- виходи реле на замикання та розмикання (30 В/1 А);
- напруга живлення 11...18 В постійного струму;
- струм споживання не більше 90 мА;
- ступінь захисту IP65;
- діапазон робочих температур від -25 до 55 °С;
- висота 108 см.



Рисунок 4.28 – 6-променевий ІЧ-бар'єр Lightwell LBW-60-6 [26]

На ринку України доступні датчики з кількістю променів від 1 до 12 [16].

Контрольні питання

1. Що означає поняття ToF-технологія?
2. Яким чином вимірюється відстань у ToF-системах?
3. Який пристрій використовується для вимірювання об'єму чи глибини об'єктів?
4. Які методи вимірювання відстані вам відомі?
5. Що таке тріангуляційний метод вимірювання розмірів об'єктів?
6. Які методи побудови датчиків диму Вам відомі?
7. Що означає термін "безкамерний датчик диму"?
8. В чому полягають переваги безкамерних датчиків диму?
9. Яку функцію виконують лазерні та інфрачервоні бар'єри?

Перелік посилань

1. Time of Flight або ToF Analog Devices. Url: https://www.analog.com/ru/applications/technology/3d-time-of-flight.html?icid=3dtof-tile_ru_hp. (дата звернення: 25.02.2024).
2. Time-of-Flight: The Advancing Technology for 3D Vision Tasks. Url: <https://www.baslerweb.com/en/learning/3d-vision-tasks/>. (дата звернення: 25.02.2024).
3. В. Романов Технологія 3D Time of Flight підтримує персональне фітнес-тренування у домашніх умовах. Електронні компоненти і системи, 2023. №3(243). с. 46-48.
4. CCD TOF Signal Processor. Url: <https://www.analog.com/media/en/technical-documentation/data-sheets/ADDI9036.pdf>. (дата звернення: 25.02.2024).
5. Emitters and Invisible “Light”. Url: <https://lumileds.com/company/blog/infrared-emitters-and-invisible-light/> (дата звернення: 25.02.2024).
6. Джерела лазерного випромінювання. Url: <https://deps.ua/ua/katalog/laser-radiation-sources.html> (дата звернення: 25.02.2024).
7. Напівпровідниковий лазер. Url: <https://wiki.cusu.edu.ua/index.php/%D0%9D%D0%B0%D0%BF%D1%96%D0%B>

- 2%D0%BF%D1%80%D0%BE%D0%B2%D1%96%D0%B4%D0%BD%D0%B8
D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BB%D0%B0%D0%B7%
D0%B5%D1%80 (дата звернення: 25.02.2024).
8. Semiconductor lasers. Url: https://www.daenotes.com/electronics/microwave-radar/semiconductor-laser#google_vignette (дата звернення: 25.02.2024).
 9. Червоний лазерний діод. Url: https://www.rcscomponents.kiev.ua/product/chervonyi-lazernyi-diod-liniiia-650nm-5mw_194356.html (дата звернення: 25.02.2024).
 10. Лазерні далекоміри. Url: https://simvolt.ua/dalekomri/?gad_source=1&gclid=Cj0KCQiAuou6BhDhARIsAIfgrn6Iwb09L1Tzf-8v4Vc4z3JX1TK2yKGe2s3uT2DmzpMvD7FuHRvnM3waAkMUEALw_wcB (дата звернення: 25.02.2024).
 11. Який далекомір використовують військові? Url: <http://uk.lumispot-tech.com/news/what-rangefinder-does-the-military-use/> (дата звернення: 25.02.2024).
 12. Лазерная рулеткаю. Url: <https://www.olx.ua/uk/dom-i-sad/instrumenty/q-%D0%BB%D0%B0%D0%B7%D0%B5%D1%80%D0%BD%D0%B0%D1%8F-%D1%80%D1%83%D0%BB%D0%B5%D1%82%D0%BA%D0%B0/> (дата звернення: 25.02.2024).
 13. Лазерна рулетка Xiaomi Mileseeey Laser Tape Measurer Blue DT10
Url: <https://vogmarket.com.ua/ua/p1538718962-ruletka-lazernaya-xiaomi.html?srsItd=AfmBOooYzynR6LX28UVNz-7NxdVgYrG6WY6VUZurwGsr4ZyuKd1uwPam> (дата звернення: 25.02.2024).
 14. Бінокль-далекомір Bushnell. Url: <https://hunterstore.com.ua/ua/p186126580-binokl-dalnomer-bushnell.html> (дата звернення: 25.02.2024).
 15. Бінокль Bushnell Fusion 1 Mile ARC з лазерним далекоміром. Url: https://military.pl/ua/p/bushnell/binokl-bushnell-fusion-1-mile-arc-z-lazernim-dalekomirom-10x42-8188?cd=20455536630&ad=147698503850&kd=&gad_source=1&gclid=CjwKCAiA3ZC6BhBaEiwAeqfvyoU3CA6oS00U7SiJ_N4ETAr5vr8eDNqhMTKu-g1RcTs0tEPwXRUY5BoCwIoQAvD_BwE (дата звернення: 25.02.2024).

16. Лазерний рівень нівелір Fixit Laser Level Pro 3. Url: <https://mpr-kip.com/ua/p519203927-lazernyj-uroven-nivelir.html> (дата звернення: 25.02.2024).
17. Іонізаційні пожежні сповіщувачі. Url: <https://fireman.club/statyi-polzovateley/ionizatsionnyie-pozharnyie-izveshhateli/>. (дата звернення: 25.02.2024).
18. Оптико-електронні пожежні сповіщувачі. Url: <https://fireman.club/statyi-polzovateley/optiko-elektronnyie-pozharnyie-izveshhateli/>. (дата звернення: 25.02.2024).
19. Integrated Optical Module for Smoke Detection. Url: <http://www.analog.com/media/en/technical-documentation/data-sheets/ADPD188BI.pdf>. (дата звернення: 25.02.2024).
20. Пожежний аспіраційний сповіщувач. Url: <https://fireman.club/statyi-polzovateley/pozharniy-aspiratsionnyiy-izveshhatel-preimushhestva-i-nedostatki/>. (дата звернення: 25.02.2024).
21. Лінійні пожежні сповіщувачі. Url: <https://fireman.club/statyi-polzovateley/lineynyie-pozharnyie-izveshhateli-tipyi-pravila-montazha-plyusyi-i-minusyi/>. (дата звернення: 25.02.2024).
22. Охорона периметра. Url: https://www.bezpeka-shop.com/ua/catalog/okhrana_perimetra/. (дата звернення: 25.02.2024).
23. Охорона периметра. Url: <https://guardmaster.com.ua/ik-bar-er-lightwell-lbw-60-6/>. (дата звернення: 25.02.2024).
24. RLS-2020I Indoor LiDAR Grade 3. Url: <https://www.optex-europe.com/products/indoor-intrusion-detection/rls-2020i> (дата звернення: 25.02.2024).
25. RLS-3060SH-PoE. Url: <https://www.asl-ademco.de/B/RLS-3060SH-PoE.html> (дата звернення: 25.02.2024).
26. ІЧ-бар'єр Lightwell LBX-100 AF з режимом "антитуман". Url: <https://recorder.com.ua/IK-barer-Lightwell-LBX-100-AF-s-rezhimom-antituman-Aktivnie-IK-izveshchateli-591652> (дата звернення: 25.02.2024).

5 ДАТЧИКИ ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ ТА СИСТЕМ БЕЗПЕКИ

5.1 Класифікація датчиків систем пожежної сигналізації та охорони

При вирішенні технічних завдань охорони в першу чергу необхідно вибирати такі пристрої, основні параметри яких забезпечують високу надійність виконання покладених на них функцій. Системи пожежної сигналізації фіксують появу диму, підвищення температури або перевищення концентрації угарного газу та формують сигнал тривоги. В залежності від складності системи внаслідок сигналу тривоги можуть включатися системи пожежогасіння або інформація передається у пожежну охорону. Системи охоронної сигналізації фіксують факт несанкціонованого доступу на охоронювану територію, передають сигнал тривоги, наприклад, на пульт охорони й включають виконуючі пристрої. Системи охоронної сигналізації включають: датчики; пульт-концентратор; виконуючі пристрої [1].

Датчик – чутливий елемент, що перетворює контрольований параметр в електричний сигнал. Особливість датчиків для систем охоронної сигналізації полягає в тому, що вони реєструють, в основному, неелектричні величини. Вимір неелектричних величин -- складне завдання й при цьому датчики повинні забезпечувати високу надійність і вірогідність контролю. Надійність датчиків забезпечується, в основному, цифровими методами обробки сигналів. Датчики поєднуються в зони. Під зоною розуміється один або кілька датчиків, що опікують певний об'єкт або ділянку об'єкта.

Датчики (сповіщувачі) руху в системах охорони можна класифікувати по різних параметрах [1].

По способу передавання сигналу діляться на:

- проводові;
- безпроводові.

По принципу дії діляться на:

- контактні;
- безконтактні.

По принципах перетворення в електричний сигнал:

- омічні (шлейфи);
- датчики розбиття скла;
- магнітно-контактні, магнітні (герконові);
- ударно-контактні;
- активні інфрачервоні датчики руху й присутності;
- індуктивні;
- фотоелектричні датчики;
- мікрохвильові датчики;
- ультразвукові датчики;
- вібродатчики;
- датчики температури;
- датчики наявності пару і газів.

5.2 Пожежні датчики

5.2.1 Що таке пожежний сповіщувач

Датчики-сповіщувачі – це пожежні технічні засоби, що передають повідомлення про виниклу пожежу на приймально-контрольний прилад (ПКП). Звичайно, кріпляться на стелі. Сповіщувачі встановлюються на різні об'єкти й використовуються з урахуванням того середовища, у якому вони будуть перебувати [1, 2]. Сучасні сповіщувачі пожежної сигналізації встановлюють у будинках, квартирах, в офісах і на підприємствах.

Протипожежна система може сповістити про незначне загоряння пожежну службу вчасно. Якщо система сигналізації додатково підключена до системи пожежогасіння, то вогнище загоряння буде погашене дуже швидко, після виявлення потенційної загрози.

Найчастіше використовуються наступні типи сповіщувачів: димовий, тепловий і полум'я [1].

Сповіслювачі пожежних систем працюють по одному алгоритму. Коли в приміщенні виникає дим, з'являється газ або полум'я, датчики реагують, посилаючи сигнал на пульт (панель) пожежної сигналізації. Коли сигнал оброблений і виявлена загроза, формується команда включення звукової сирени, а по мережі на пульт керування диспетчера приходить інформація про пожежу в певному місці.

Поганими сповіслювачами вважаються такі, які ідентифікують тільки вогонь. Найкращими є сповіслювачі що містять одночасно датчики диму, газу й температури (рис. 5.1) [2].



Рисунок 5.1 – Пожежний сповіслювач із датчиками диму, температури й складу повітря [2]

5.2.2 Види датчиків пожежної сигналізації

Розглянемо датчики, які використовуються для виявлення загоряння.

Теплові датчики

Реагують на зміну температури в приміщенні. Можуть установлюватися в будь-якому місці будинку. Теплові сповіслювачі (рис. 5.2) [3] рекомендується використовувати в запиленому, загазованому, агресивному середовищі або при низьких температурах. Тому що такі сповіслювачі можна використовувати в агресивному середовищі, вони часто використовується в промислових системах пожежної безпеки.



Рисунок 5.2 – Зовнішній вигляд теплового сповіщувача FT-A2 [3]

Теплові сповіщувач діляться на [3]:

1. Граничні;
2. Диференціальні;
3. Комбіновані.

Граничний (або максимальний) сповіщувач спрацьовує при подоланні припустимого рівня температури в приміщенні. По такому принципу реалізовувались найперші моделі теплових сповіщувачів. Вони формують сигнал про пожежу, коли вогонь уже розгорівся й температура значно зросла, що утрудняє гасіння пожежі.

Диференціальний сповіщувач аналізує швидкість підвищення температури в приміщенні. Якщо швидкість зміни температури відхиляється від норми, сповіщувач подає сигнал про початок пожежі.

Комбінований – поєднує властивості першого й другого типів сповіщувачів. Спрацьовує, якщо фіксується занадто швидке нагрівання повітря і якщо температура досягла граничного значення. Є універсальним, більш надійним і затребуваним у системах пожежної сигналізації.

Димові сповіщувачі

Датчики диму або димовловлювачі – більш ефективні через конструктивні особливості. Вони реагують на появу в повітрі дрібних часток – диму або аерозолі. Реакція на дим може допомогти запобігти пожежі ще на стадії тління. На рис. 5.3 наведено зовнішній вигляд датчика диму [4].



Рисунок 5.3 – Димовий сповіщувач [4]

За принципом побудови датчики диму діляться на:

- іонізаційні – виявлення диму засноване на властивості іонізованого (у результаті нагрівання) повітря притягати частки димового потоку;
- оптичні (оптико-електронні) – виявлення засноване на вимірі оптичної щільності газо-повітряного середовища, яке міняється з появою часток диму [3];
- лінійні – приймач ІЧ-випромінювання, установлений на одній осі й значному видаленні від передавача, реагує на ослаблення сигналу нижче заданого рівня [3];
- точкові димові пожежні датчики випромінюють у навколишній простір імпульси світла, які розсіюються, якщо в повітрі немає диму, а при наявності диму або аерозолі світло відбивається від дрібних часток, зважених у повітрі, і датчик спрацьовує, формуючи сигнал тривоги (випромінювач і фотоприймач розташовані в одному корпусі) [3];
- аспіраційні, що забезпечують відбір і доставку проб повітря (аспірацію) через систему труб з отворами для забору повітря із приміщення, що захищається (зони) до обладнання виявлення ознаки пожежі (дим, зміни хімічного складу середовища) [3].

Лінійні протипожежні датчики диму також мають випромінювач і приймач розташовані на одній осі (лінії). Інший варіант реалізації – випромінювач і приймач розташовані в одному місці а світло відбивається від дзеркала. На чутливий елемент за допомогою інфрачервоного світлодіода відправляються імпульси світла. При відсутності диму сигнал надходить на фотоприймач, що свідчить про відсутність пожежі. З появою диму світловий потік, що попадає на фотоприймач послабляється або припиняється й датчик формує сигнал тривоги.

Модифікацією лінійного датчика є обладнання, у якому випромінювач і приймач установлюються в одному корпусі, а ІЧ-промінь спрямований на пасивний відбивач, розташований напроти датчика. Як впливає з наведеного переліку лінійні датчики також є оптико-електронними.

Особливістю простих точкових датчиків (що мають один випромінювач і один фотоприймач) є не сприйняття чорного диму. Вони вимагають підтримки чистоти в приміщенні й регулярного очищення. Неправильні спрацьовування можуть викликатися появою пари й наявністю комах.

Датчики полум'я

Світлові сповіщувачі або "полум'я" реєструють відкрите полум'я в приміщенні або вогнища загоряння реагуючи на інфрачервоне й ультрафіолетове випромінювання (рис. 5.4) [5].



Рисунок 5.4 – Сповіщувач появи полум'я [5]

Устаткування достатнє дороге й використовується на великих промислових підприємствах. Використовується на об'єктах, де підвищення й перепади

температур регулярно, де постійно спостерігається задимленість і загазованість. Тому пожежа в таких місцях детектується за допомогою сповіщувачів полум'я.

Однак такі сповіщувачі можуть реагувати на іскри при зварюванні. Для усунення цього недоліку на сповіщувачі полум'я встановлюються додаткові оптичні фільтри. Застосовуються звичайно в нафтогазовій промисловості.

Сповіщувачі наявності газу

Сповіщувачі реагують на зміст чадного газу (рис. 5.5) [1, 6] й інших різновидів газу в приміщенні. Сповіщувачі використовуються на об'єктах з газовим устаткуванням, водонагрівачами, казанами і т.д. Якщо вентиляція справляється погано, концентрація газу може бути досить великою у приміщенні, і датчик про це проінформує.



Рисунок 5.5 – Сповіщувач чадного газу PoliceCam PC-1811CO [6]

Комбіновані сповіщувачі

Ці сповіщувачі (рис. 5.6) [2] найточніші, тому що містять датчики температури, диму й складу повітря (наявності чадного газу). Їх можна настроїти, наприклад, підключивши тільки детектування диму.



Рисунок 5.6 – Комбінований сповіщувач [2]

Ручні сповіщувачі

Найпростіший сповіщувач включається людиною. Звичайно, це кнопка, яка може включати сирену (найчастіше) і сповіщати систему пожежної сигналізації про подію (рис. 5.7) [7]. Кнопка перебуває в спеціальному корпусі, який прикріплений до стіни.



Рисунок 5.7 – Ручний сповіщувач про пожежу [7]

Додаткова класифікація пожежних сповіщувачів

Датчики пожежної сигналізації можна класифікувати й по інших параметрах. Часто, саме додаткова класифікація допомагає зробити вибір на користь потрібного для конкретного завдання сповіщувача.

По типу переданих сигналів

Сповіщувачі можуть мати однорежимними або дворежимними.

Однорежимний сповіщувач формує сигнал тривоги по одному параметру. Наприклад тепловий датчик реагує на підвищення температури. Це може привести до того, що у випадку несправності датчика, повідомлення про пожежу не буде сформовано. Виявити несправність такого датчика можна тільки при його фізичній перевірці.

У дворежимних сповіщувачах контролюється ще один параметр. Наприклад, він крім сигналу про пожежу з певною частотою повідомляє що пожежі немає. Якщо ж друге повідомлення не приходить на пульт керування (контрольну панель), можна зробити висновок, що датчик вийшов з ладу.

Багаторежимні сповіщувачі передають інформацію про характер несправності. Наприклад, обриви кабелю, ушкодження модуля зв'язку або чутливого елемента, і т.д.

По локалізації

Сповіщувачі по цьому параметру діляться на:

- точкові – одиничний датчик під конкретну мету;
- багатоточкові – сповіщувачі оснащені декількома датчиками різних видів;
- лінійні (рис. 5.8) – моніторинг території уздовж установленної лінії (можуть бути парними або одиночними).



Рисунок 5.8 – Лінійний датчик диму Артон АРТОН-ДЛ [8]

По типу інтерфейсу зв'язку

По типу інтерфейсу зв'язку діляться на проводові і безпроводові [3]. Проводові підключаються до пожежної контрольної панелі за допомогою двопроводової або чотирьохпроводової лінії зв'язку. Живлення датчиків здійснюється від пожежної контрольної панелі по проводах лінії зв'язку. Цей інтерфейс використовується найчастіше.

Однак при встановленні сучасних систем пожежної сигналізації у старих будинках, де прокладання проводових ліній зв'язку утруднено або економічно недоцільно, використовують безпроводові датчики.

Живлення безпроводових датчиків здійснюється від вбудованих батарей або акумуляторів. Такі датчики містять у своєму складі передавач, а для прийому сигналів від датчиків використовується, так звана, централь.

Безсумнівним лідером у виробництві таких датчиків є Українська компанія Ajax Systems [9, 10].

Вибір типу сповіщувачів

Процес вибору повністю залежить від місця установки й мети установки сповіщувачів.

Тепловий – простий, недорогий і невибагливий до місця установки.

Оптичний димовий – складний, дорогий й примхливий до очищення як самого обладнання, так і повітря.

Комбінований (оптичний і тепловий датчики) – найбільш прийнятний з погляду фіксації пожежної небезпеки, але вартість такого сповіщувача висока. На рис. 5.9 наведений зовнішній вигляд деяких пожежних сповіщувачів.



Рисунок 5.9 – Зовнішній вигляд пожежних сповіщувачів [3]

Компаній, які випускають пожежні сповіщувачі, досить багато. Найбільш відомою компанією в Україні є компанія Ajax Systems, що випускає безпроводові сповіщувачі з датчиками диму й чадного газу.

5.2.3 Безпроводові датчики систем пожежної безпеки

Розглянемо безпроводові датчики пожежної сигналізації на прикладі датчиків компанії Ajax Systems [9, 10].

Датчик температури та диму зі змінними батареями FireProtect

Основні характеристики датчика (рис. 5.10) [10]:

- виявлення диму оптичним сенсором;
- алгоритм HazeFlow для фільтрації хибних тривог, спричинених задимленням;
- вимірювання температури термопарою;
- вбудована сирена з рівнем звукового тиску 85 дБ;
- робота автономна чи у системі Ajax;
- дальність радіозв'язку з хабом до 1300 м на відкритій місцевості;
- керування та налаштування через застосунки Ajax;

- строк роботи без заміни батареї до 4-х років.



Рисунок 5.10 – Датчик температури та диму зі змінними батареями FireProtect [10]

Датчик температури, диму та чадного газу зі змінними батареями FireProtect Plus

Основні характеристики датчика аналогічні характеристикам датчика FireProtect. Додано хімічний датчик для виявлення концентрації чадного газу.

Датчик температури, диму та чадного газу з незмінними батареями FireProtect 2

FireProtect 2 – це датчик нового покоління, розроблений для миттєвого розпізнавання пожежі (рис. 5.11). Унікальна димова камера не вимагає регулярного очищення, працює в двох спектральних діапазонах, відрізняє дим від пари, термістор швидко реагує на горіння синтетичних матеріалів, а програмне забезпечення мінімізує хибні спрацювання. Все це відповідає найсучаснішим стандартам пожежної безпеки. Датчик має продуману конструкцію та кріплення, що у поєднанні з налаштуваннями у смартфоні забезпечує простий та швидкий монтаж.

Випускається 2 модифікації датчиків – FireProtect 2 SB із вбудованими незмінними батареями, FireProtect 2 RB зі змінними батареями [10].



Рисунок 5.11 – Датчик температури, диму та чадного газу з незмінними батареями FireProtect 2 SB [10]

Основні характеристики датчиків FireProtect 2 [10]:

- виявлення диму оптичним сенсором в 2-х різних діапазонах спектру;
- захищена від пилу та комах димова камера;
- алгоритм HazeFlow для фільтрації хибних тривог, спричинених задимленням;
- вимірювання температури терморезистором;
- хімічний датчик для виявлення концентрації чадного газу;
- вбудована сирена з рівнем звукового тиску 85 дБ;
- робота автономна чи у системі Ajax;
- дальність радіозв'язку з хабом до 1700 м на відкритій місцевості;
- керування та налаштування через застосунки Ajax;
- можливість утворення мережі і синхронного формування тривоги всіма датчиками за 20 с;
- радіозв'язок Jeweller з модуляцією TDMA, шифруванням та можливістю регулювання потужності передавача;
- строк роботи FireProtect 2 SB без заміни батареї до 7 років.

З іншими датчиками компанії Ajax Systems можна ознайомитись на сайті компанії [9].

5.2.4 Установка сповіщувачів пожежної сигналізації

Кожний сповіщувач має обмежену площу обслуговування. Для збільшення площі обслуговування необхідно використовувати кілька таких датчиків. Якщо відома площа обслуговування одного сповіщувача й площа приміщення, то нескладно розрахувати необхідне число сповіщувачів [11, 12].

Встановлюють сповіщувачі на стелі (рис. 5.12) [13], рідше на стінах. В офісних приміщеннях та громадських будинках сповіщувачі можуть встановлюватися за стельовим простором.



Рисунок 5.12 – Установка пожежного сповіщувача на стелі [13]

5.2.5 Різновиди систем пожежної сигналізації

Існує декілька способів побудови систем сигналізації. Коротко розглянемо їх основні відмінності [11,12].

Гранична. Це найбільш простий вид – настроюються на певне максимальне значення, наприклад, температури. При перевищенні показників, спрацьовує сповіщувач.

Адресно-опитувальна. У цій системі кожному сповіщувачу привласнюється адреса на об'єкті. Крім того, панель керування самостійно запитує про стан сповіщувача. Плюсом такого варіанта реалізації є більш своєчасне інформування про погрозу.

Адресно-аналогова. Між датчиком і панеллю керування розміщаються приймально-контрольні прилади (рис. 5.13). Вони проводять аналіз даних, що

надійшли,, порівнюють із попередніми результатами. При цьому кількість неправильних спрацьовувань значно зменшується.

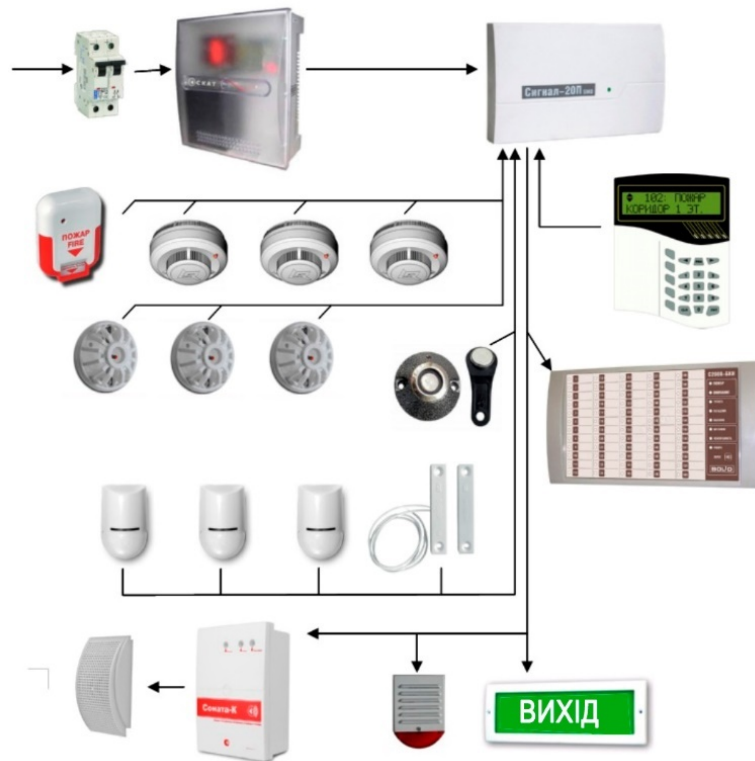


Рисунок 5.13 – Приклад структури пожежної сигналізації з використання граничних сповіщувачів [14]

Інтегрована. При одержанні попередження про ризик відключаються електрика, вентиляція, запускаються процеси димовидалення, сповіщення, аварійного освітлення.

На одну пару проводів можливий монтаж до 20 сповіщувачів. Це утрудняє швидке виявлення вогнища, тому що складно визначити місце, звідки був поданий сигнал.

Адресно-опитувальна система

Устаткування може настрюватися на наступні положення: норма, увага, пожежа, несправність і інші.

Перемикання режимів роботи здійснюється автоматично без участі персоналу. Адресні сповіщувачі не тільки сигналізують на ПКП (прилад

контрольно-приймний) про свій стан, але й передають код адреси. Незважаючи на те, що до одному каналу зв'язку можуть підключатися до 200 сповіщувачів, виявити несправність або місце спрацьовування можна дуже швидко.

Адресно-аналогова система

Її відмінність від попередньої в тому, що між сповіщувачем і ПКП перебуває приймально-контрольний прилад (ППКП). Усі дані від сенсорів отримує ППКП, аналізує їх, порівнює з порогом чутливості.

Інтегрована система

Вона поєднується із системами, що забезпечують увесь комплекс захисних заходів: димовидалення, пожежогасіння, сповіщення, контролю доступу. При погрозі відключаються вентиляція, електропостачання (крім аварійного), знімається блокування виходів, спрацьовує димовидалення.

Оповіщувачі систем пожежної сигналізації

З їхньою допомогою відбувається інформування людей про небезпеку. Вони бувають: звуковими (рис. 5.14), мовними, комбінованими, світловими [15, 16].



Рисунок 5.14 – Сирени та світлові оповіщувачі пожежної сигналізації [15]

У будь-якому місці будинку, де необхідне попередження про погрозу поширення вогню, рівень гучності повинен бути вище припустимого рівня шуму, але не перевищувати припустимий поріг 110 дБ. Світлові оповіщувачі встановлюються над евакуаційними виходами.

5.3 Датчики системи безпеки

5.3.1 Омічні сповіщувачі (датчики розбиття скла)

Омічні сповіщувачі – самий простий тип сповіщувачів [17]. Вони являють собою тонкий металевий провідник, спеціальним способом закріплений на охоронюваному предметі чи конструкції (рис. 5.15). Будь-який фізичний вплив на охоронюваний об'єкт приводить до розриву провідника, чим порушується цілісність шлейфу.

Омічні сповіщувачі "Фольга" та "Фольга-З" призначені для блокування від розбивання конструкцій з скла, підданих впливу вібраційних і ударних навантажень, при температурі навколишнього середовища від -40 до +50 °С. Ці сповіщувачі застосовуються для блокування скляних конструкцій, де не пред'являються підвищені вимоги до інтер'єру (склади, приміщення виробничого й господарського призначення).

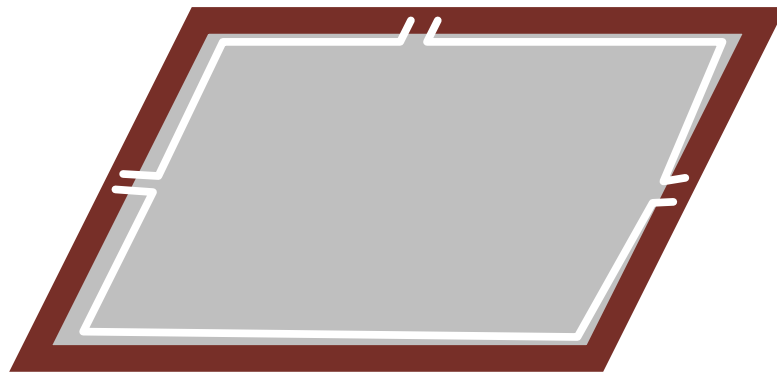


Рисунок 5.15 – Приклад розташування омічних сповіщувачів на склі [17]

Сповіщувачі поставляються рулонами при ширині стрічки 10 і товщині 0,02 мм. Допускається застосовувати алюмінієву фольгу товщиною 0,008...0,03 мм і шириною 6...10 мм. Сповіщувач Фольга-З складатися з фольги, що містить шар для самоприклеювання і затискачів. Клейовий шар покритий захисною плівкою. Сповіщувачі поставляються у вигляді рулонів довжиною 5...20 м, шириною 10 і товщиною 0,014 мм. Блокування алюмінієвою фольгою роблять шляхом приклеювання її по периметру скляних полотен на відстані 2...10 мм від бічної

сторони дерев'яної рами, 10...15 мм від металевої рами, до 50 мм від нижньої сторони рами в сухих, опалювальних приміщеннях, 150...200 мм від нижньої сторони рами у вологих і неопалюваних приміщеннях.

Допускається робити блокування фольгою по периметру скла на 2/3 загальної висоти від нижнього краю.

Для захисту прорізів зі склопрофілів, склоблоків фольга повинна приклеюватися по середині кожного склопрофіля, склоблока. Фольгу наклеюють на скло внутрішніх рам (дверей) з боку приміщення що охороняється. Фольга приклеюється до скла клеєм "Контакт" або аналогічним. Замість клею допускається використовувати олійну фарбу, ґрунтовку, цинкове білило, синтетичні фарби, епоксидні емалі. Забороняється застосовувати фарби на основі штучної оліфи. Колір фарби повинен бути підібраний по кольору рами або по вимогах замовника.

Омічний сповіщувач "Провід" призначений для захисту будівельних конструкцій (двері, люки, ворота, некапітальні стіни, перегородки й т.п.). Використовується провід перерізом не більш 0,2 мм². Провід прокладають по внутрішній стороні будівельних конструкцій по всій площі паралельно контурним лініям і кріплять скобами із кроком не більш 200 мм. Під скобу слід підкласти нерозрізану поліхлорвінілову трубку довжиною 10 мм. Відстань між проводами повинна бути не більш 200 мм.

При відкритому способі прокладання провід кріплять безпосередньо до поверхні будівельної конструкції з наступним захистом його від випадкових (або навмисних) ушкоджень фанерою, оргалітом або іншим матеріалом. При схованому способі прокладки провід прокладають і кріплять у борознах глибиною й шириною не менш двох діаметрів проводу з наступною шпаклівкою й зафарбовуванням. При будь-якому способі прокладки проводу на кожні 5 м² поверхні що блокується повинна бути встановлена коробка для відведення на максимальній висоті будівельної конструкції.

Блокування внутрішніх металевих ґрат повинна проводитися оповиванням горизонтальних і вертикальних прутів проводом із кроком витка 30...70 мм. У місцях перетинання прутів ґрат на проводі роблять вузол, який повинен

охоплювати обидва прутки. Перехід проводу з одного прута на інший повинен проводитися по будівельному прорізу схованим способом у штробі. Провід у штробі кріплять із наступною шпаклівкою. У місцях кріплення на провід надягають нерозрізану поліхлорвінілову трубку довжиною 10 мм. Ґрати з металевих трубок допускається блокувати пропусканням проводу через усі трубки.

По закінченню монтажу ґрати й провід офарблюють олійною фарбою одного кольору.

5.3.2 Контактні датчики систем охоронної сигналізації

У цій якості найчастіше використовують геркони, мікроперемикачі, кнопки, контактні групи від електромагнітних реле [18, 19].

Геркони як датчики, що реєструють переміщення, що реагують на двері, що відкривається, вікно й т.п., одержали, мабуть, найбільше поширення, і насамперед через їхню високу надійність і довговічності. Магніточутливі електроди геркона, один з яких зміщується, розміщені в запаяному скляному балоні, заповненому інертним газом (рис. 5.16).

При наближенні постійного магніту до геркону він спрацьовує – розімкнута контактна пара замикається, і триелектродний геркон перемикається. Очевидно, триелектродний геркон може бути використаний у якості як нормально замкнутого контактного датчика НЗКД, так і нормально розімкнутого НРКД.

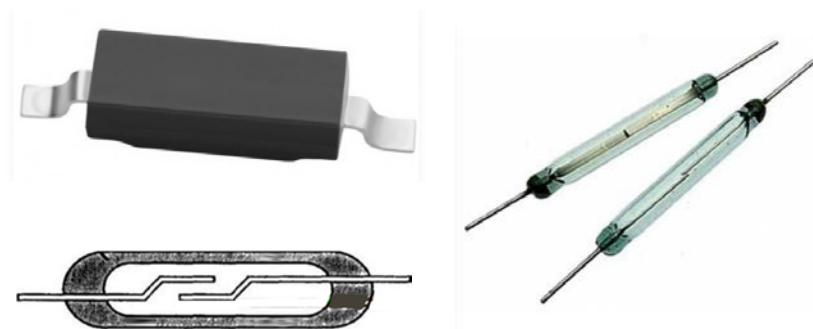


Рисунок 5.16 – Конструкція замикаючого геркона та його виконання у пластмасовому чи скляному корпусах [18]

Звичайно сам геркон розміщують нерухомо – врізають, наприклад, у дверну або віконну коробку, стінку шафи, а керуючий їм магніт вклеюють у спеціальний отвір в рухливій частині прорізу – у торець дверей, у віконну стулку й т.п. Їхнє взаємне розташування повинне бути по можливості постійним, тому що напруженість магнітного поля в міру видалення магніту від геркона швидко убиває. Герконовий датчик неважко замаскувати. На рис. 5.17 наведено приклад встановлення датчика на дверях розумного будинку [19].



Рисунок 5.17 – Приклад встановлення датчика на дверях розумного будинку [19]

Основні параметри герконів вітчизняного виробництва наведені в табл. 5.1.

Таблиця 5.1 – Основні параметри герконів вітчизняного виробництва

Тип геркона	Параметр						
	1	2	3	4	5	6	7
МКА-52141	100...200	3	5000	3	1	1000	53/5,4/80
МКА-52142	300	3	10000	3	0,1	до 1000	52/5,5/90
МКА-52202	180...300	8	380	4	0,3	2500	52/7/-
МК17	30...80	10	80	–	0,2	до 10000	20/3,1/45,6
МКА-10501	16...35	10	90	–	0,3	2000	10/2,3/41
МКА-10701	18...45	0,5	10	–	–	до 1000	10/1,8/25
МУК-1-1А-1	35...90	2	115	0,5	0,3	до 50000	21,5/-/40
КЭМ-2	21...64	1	180	0,25	0,15	до 100000	20/-/46
МК-16-3	35	1	30	0,01	0,15	1500	16/-/-
МК-10-3	13...40	0,8	36	0,1	0,3	до 20000	10/-/30.5
МКА-10113	14...25	0,8	36	0,1	0,3	до 10000	10/-/42.5

Параметри в табл. 5.1:

- 1 – магніторухійна сила спрацьовування, А;
- 2 – час спрацьовування, мс;
- 3 – максимальна напруга, що комутується, В;
- 4 – максимальний струм, що комутується, А;
- 5 – опір контактів, Ом;
- 6 – максимальне число комутацій, тис.;
- 7 – габаритні розміри, мм (довжина балона/діаметр балона/загальна довжина).

5.3.3 Датчики руху та розбиття скла для систем охоронної сигналізації

Як і в пожежній сигналізації, так і в пристроях систем охоронної сигналізації важливо правильно спроектувати та змонтувати всю систему. Важливо правильно підібрати тип та кількість датчиків.

Саме вони передають на контрольну панель відомості про зміну ситуації на об'єкті, що охороняється. Датчики класифікуються за типом сигналу, який вони відстежують. Нижче наведено перелік основних типів датчиків, які використовуються при встановленні охоронної сигналізації [20].

Акустичні датчики, як ясно з назви, реагують на гучні звуки певного діапазону. Цей діапазон відповідає звуку розбитого скла. Тому ці датчики встановлюють там, де є ризик проникнення через вікно (рис. 5.18) [3].



Рисунок 5.18 – Акустичний датчик розбиття скла Crow GBD-2 [3]

Інфрачервоний, об'ємний та лінійний (променевий) датчики – це датчики руху. Вони контролюють джерела тепла в приміщенні (рис. 5.19) [20]. Відстежується не сама наявність джерела тепла, а тільки його переміщення. Тому пасивні джерела тепла (прилади опалення) не стають причиною помилкових спрацьовувань. Плюсами цих датчиків вважається пасивний режим роботи – вони нічого не випромінюють, а тільки сканують температурні зони в приміщенні.

Окремо варто сказати про **відміну лінійного від об'ємного датчика**. Останній сканує приміщення не тільки від стелі до підлоги, але і має горизонтальний градус сканування. Лінійний та променевий датчики сканують тільки область безпосередньо перед ними. Причому променевий датчик складається з двох елементів, розташованих один проти одного. Між ними проходить ІЧ промінь і якщо сигнал не доходить до другого датчика, то спрацьовує сигналізація. Втім, і ці види датчиків можна обійти, тому їх нерідко застосовують разом з іншими видами охоронних датчиків.



Рисунок 5.19 – Датчик руху і розбиття скла U-Prox PIR Combi White [20]

Ультразвукові датчики. Як і ІЧ датчики, ультразвукові фіксують переміщення. Але використовують для цього не оптико-термальний спосіб, а акустичний, заснований на ефекті Допплера [21].

Акустичні датчики що використовують ефект Допплера використовуються як датчики руху (рис. 5.20). Поки в приміщенні відсутні об'єкти що переміщуються, сигнал на виході датчика відсутній. Коли з'являється об'єкт що

переміщується, датчик формує сигнал завдяки тому, що при відбитті від такого об'єкту частота випромінюваного сигналу та прийнятого відбитого відрізняються. Датчик порівнює частоти випромінюваного і відбитого сигналів і на основі порівняння формується (чи ні) сигнал тривоги.



Рисунок 5.20 –Ультразвуковий датчик руху [21]

Крім того, існують **ємнісні** датчики, які вимірюють ємність об'єму приміщення та спрацьовують при її зміні.

Вібраційні датчики спрацьовують при вібрації, приміром стін або підлоги.

На рис. 5.21 наведено зовнішній вигляд безконтактних датчиків руху [22].



Рисунок 5.21 – Зовнішній вигляд безконтактних датчиків руху [22]

5.4 Компоненти систем пожежної сигналізації

Системи пожежної сигналізації містять як мінімум 2 основних компоненти – сповіщувачі здатні приймати та передавати інформацію відносно виявлення пожежі та прилади приймально-контрольні пожежні (ППКП) [23-28]. Окрім цього, такі системи можуть містити звукові та світлові оповіщувачі, модулі перетворення інтерфейсів та різноманітні пристрої розширення функціональних можливостей.

Оповіщувач – звуковий або світло-звуковий пристрій, призначений для оповіщення людей про необхідність евакуації з зон, де була виявлена пожежа.

Зона – визначена частина захищуваних приміщень, в якій встановлено один чи декілька компонентів і для якої передбачено загальну індикацію стану.

Прилади приймально-контрольні пожежні – це пристрої, завданням яких є виявлення та відповідне сповіщення та протидія пожежі. Такі пристрої здатні ефективно сприймати та аналізувати сигнали, отримані від підключених до приймально-контрольного приладу датчиків. У свою чергу, залежно від типу може не тільки сповістити про небезпеку, а й ефективно боротися з нею. Це можливо завдяки тому, що деякі моделі пожежних ППК є настільки просунутим і складним автоматизованим комплексом, що здатні подавати сигнали і керувати різними установками для пожежогасіння.

Пожежні ППК в залежності від способу підключення додаткових пристроїв можна поділити на:

- проводові;
- безпроводові.

Перевагою безпроводових пожежних ППК є можливість підключення до нього різних сповіщувачів та іншого обладнання без використання проводів та кабелів. Однак безпроводові системи мають обмежену відстань між ППКП та датчиками, що залежить від матеріалу стін будівлі, їх товщини та кількості стін між пристроями пожежної сигналізації. До того ж, на дальність та надійність зв'язку впливають електромагнітні завади, що створюються при роботі різного обладнання, електродвигунів та систем управління ними, а також при

зварювальних роботах. З наведеного вище витікає, що більш надійними є проводові пожежні прилади прийому-контролю, які, у свою чергу, поділяються на:

- адресні;
- аналогові.

Адресні пожежні приймально-контрольні прилади проводять постійний моніторинг системи, так зване опитування сповіщувачів. В результаті такого опитування пожежний адресний приймально-контрольний прилад у найкоротші терміни зможе отримати сигнал про порушення в роботі або втрату працездатності якогось із сповіщувачів, що до нього підключені. Така розвинена система моніторингу дозволяє підключати до адресного пожежного приймально-контрольного приладу велику кількість сповіщувачів, а відповідно використовувати такий вид пожежної ПКП на великих об'єктах.

Якщо говорити про аналогові, або неадресні системи пожежних ППКП, то такі пристрої здатні контролювати всього кілька шлейфів, що дозволяє використовувати їх на невеликих об'єктах.

Контрольні питання

1. Для чого використовують геркони?
2. Який принцип дії геркона?
3. Як довго може працювати геркон без виходу з ладу, чи яку кількість спрацьовувань він допускає?
4. Який принци дії датчику диму?
5. Чи використовують датчики температури в системах пожежної сигналізації?
6. Який принцип дії датчиків температури?
7. Який діапазон вимірювання температури за допомогою напівпровідникових датчиків температури?
8. Які принципи дії датчиків руху вам відомі?
9. Який принцип дії ультразвукового датчику руху?
10. Який принцип дії інфрачервоного датчика руху?

Перелік посилань

1. Класифікація пожежних сповіщувачів. Url: <https://ista.ua/information/klasyfikatsiia-pozhezhnykh-spovishchuvachiv/> (дата звернення: 1.03.2024).
2. Адресний і комбінований пожежний сповіщувач. Url: <https://fireman.club/presentations/osnovnye-svedeniya-ob-ustanovkakh-avtomaticheskoy-pozharnej-i-oxranno-pozharnej-signalizacii/> (дата звернення: 1.03.2024).
3. Тепловий датчик. Url: https://www.bezpeka-shop.com/ua/catalog/datchiki_teplovye/ (дата звернення: 1.03.2024).
4. Niet leverbaar. Url: <https://www.bol.com/be/nl/p/sanbo-rookmelder-inclusief-montage-materiaal-inclusief-batterijen-brandmelder-rook-melder-brand-alarm-brandalarm-rookmelder-rook-alarm-rook-detector/9200000127688846/> (дата звернення: 1.03.2024).
5. Пожежні сповіщувачі полум'я. Url: <https://t-bezpeka.com/pozhezhni-spovishhuvachi-polumya/> (дата звернення: 1.03.2024).
6. Датчик чадного газу PoliceCam PC-1811CO. Url: <https://policecam.com.ua/ua/oborudovanie/oxrannaya-signalizatsiya/datchiki-i-sireny/policecam-rc-1811-co> (дата звернення: 1.03.2024).
7. Ручні пожежні сповіщувачі. Url: https://www.bezpeka-shop.com/ua/catalog/ruchnye_sryvateli/. (дата звернення: 1.03.2024).
8. Датчик диму лінійний Артон АРТОН-ДЛ. Url: <https://www.bezpeka-shop.com/ua/product/datchik-dyma-arton-arton-dl/> (дата звернення: 1.03.2024).
9. Професійна система безпеки. Url: <https://ajax.systems/ua/> (дата звернення: 1.03.2024).
10. Пожежні датчики. Url: <https://ajax.systems/ua/products/fire-detection/> (дата звернення: 1.03.2024).

11. Пожежна сигналізація: все про проектування, монтаж та обслуговування. Url: <https://uep.dn.ua/posts/pozezna/uk/vklucat-pozezna-signalizacia-vse-pro-proektuvanna-montazu-ta-obslugovuvanna.php> (дата звернення: 1.03.2024).
12. Функції та види систем пожежної сигналізації. Url: <https://ista.ua/information/funktsii-ta-vydy-sps/> (дата звернення: 1.03.2024).
13. Як відключити автономну пожежну сигналізацію, що спрацювала в квартирі, під'їзді або офісі. Url: <https://euroservis.com.ua/ua/kak-otkluchit-srobotavshuu-avtonomnuu-pozharnuu-signalizatsiu-v-kvartire-podezde-ili-ofise/> (дата звернення: 1.03.2024).
14. Пожежна сигналізація. Url: <https://alex-security.com/articles/pozharnaya-signalizacziya-vidyi-funkczii-princzip-raboty-montazh.html> (дата звернення: 1.03.2024).
15. Сирени Pfannenberг. Url: <https://prom.ua/p549858655-sireny-pfannenberг.html> (дата звернення: 1.03.2024).
16. Знаки по безопасности. Url: <https://prom.ua/Znaki-po-bezopasnosti;2.html> (дата звернення: 1.03.2024).
17. Що таке датчики розбиття скла? Url: <https://security-shop.com.ua/ua/signalizaciya/datchiki-ohoronni/datchiki-rozbittya-skla>
18. Геркони. Url: <https://filur.net/ua/pasivni-komponenti/ustanovochni-elementi-ta-komutaciya/gerkoni> (дата звернення: 1.03.2024).
19. Як працює датчик відкриття дверей: що таке геркон та який принцип його роботи. Url: <https://ohrana.ua/uk/stati-i-obzory/kak-rabotaet-datchik-otkrytiya-dveri-sto-takoe-gerkon-i-princip-ego-raboty.html> (дата звернення: 1.03.2024).
20. Датчики тривожного сповіщення для сигналізації. Url: <https://securitylab.com.ua/okhrannaya-signalizatsiya/datchiki/drugie/> (дата звернення: 1.03.2024).
21. Multi-function Presence Sensor. Url: <https://www.hdlautomation.com/product100000214055838.html> (дата звернення: 1.03.2024).

22. Датчики охоронні. Url: <https://security-shop.com.ua/ua/signalizaciya/datchiki-ohoronni> (дата звернення: 1.03.2024).
23. Прилади приймально-контрольні пожежні. Url: <https://antifire.ua/ppkp/>. (дата звернення: 1.03.2024).
24. Пожежні приймально-контрольні прилади. Url: <https://worldvision.com.ua/ru/pozharnye-ppk/>. (дата звернення: 25.02.2024).
25. Приймально-контрольні прилади (ППК). Url: <https://shop-security.com.ua/rU/pozharnaya-signalizaciya/prybyory-ppk/> (дата звернення: 1.03.2024).
26. ППКП ТИРАС 16П. Url: <https://secur.ua/ppkp-tiras-16p.html>_(дата звернення: 1.03.2024).
27. Пожежний приймально-контрольний прилад на 4 неадресні зони. Тірас-4П. Url: <https://tiras.technology/products/tiras-4p/>. (дата звернення: 1.03.2024).
28. ППКП СКБ Електронмаш – Варта-1/2 (2 шлейфи) з телефонним комунікатором для пожежної сигналізації. Url: <https://www.bezpeka-shop.com/product/varta-1-2/>. (дата звернення: 1.03.2024).

6 "РОЗУМНИЙ" БУДИНОК ТА "РОЗУМНА" БУДІВЛЯ

6.1 Що таке "розумний" будинок?

Під "розумним" будинком (англ. Smart Home) прийнято розуміти систему домашньої автоматизації. Для того щоб представити чітке визначення, що таке розумний будинок, необхідно пояснити його призначення. Основним завданням, що покликана виконувати така система, є забезпечення безпеки й комфорту мешканців квартири або частки котеджу. Його функціональність дозволяє управляти різним устаткуванням (рис. 6.1), включаючи систему опалення, кондиціонування, освітлювальні прилади, сигналізацію й цей перелік росте з кожним днем. У ці системи звичайно включають і так званий мультимедіум – систему керування мультимедіа пристроями: телевізорами, проекторами, акустичними системами й іншими мультимедійними пристроями [1].

Концепція розумного будинку була придумана в минулому столітті в 70 роках [1, 2]. Це поняття вперше ввели в США в Інституті Інтелектуальних Будинків. Американці створили технологію, що забезпечує передачу по єдиному проводовому з'єднанні різноманітних видів інформації для керування електроприладами. Розробка покликана була зробити більше комфортним життя мешканців інтелектуального житла. Ніяких інших цілей розроблювачі перед собою не ставили. Розумний будинок тієї пори вбудовувався в будинок на етапі його будівлі й застарів на момент здачі будинку в експлуатацію. Недосконала проводова система не поспівала за швидким розвитком телефонних, комп'ютерних і інших систем.

Офіційно система "розумний" будинок створена в 1978 р. завдяки появі кабельної технології X10 – шотландська компанія Pico Electronics розробила перший стандарт передавання даних, універсальний для всіх приладів домашньої автоматизації. Суть стандарту полягала в створенні шини, який будь-який виробник міг оснастити побутовий прилад, будь то соковижималка або пилосос. Підключення здійснювалося через звичайні розетки, на додаток використовувались модулі зв'язку, пульти й програма керування для комп'ютерів. Цей стандарт

застосовувався лише для зміни режимів роботи різного устаткування. Застосовувався цей стандарт в основному для керування освітлювальними приладами.

До розвитку концепції підключилася й Асоціація електронної промисловості, що стала ініціатором створення іншого універсального стандарту. Їхній протокол за назвою SEBus (споживча електронна шина) був модернізованим X10 і незабаром замінив прообраз на американському ринку.

"Розумний" будинок – це система датчиків і виконавчих пристроїв, об'єднаних в єдину систему що підтримує керування та налаштування роботою всіх систем з центрального пульта управління, а також за допомогою смартфона, планшета, комп'ютера або вбудованої сенсорної панелі [1, 2]. Обов'язковим елементом "розумного" будинку є центр керування, який підтримує зв'язок з іншими пристроями, отримує від них інформацію, яку потім передає на виконавчі пристрої, а також власнику на мобільний додаток (рис. 6.1) [2].



Рисунок 6.1 – Приклад складу системи "розумний" будинок [2]

Робота розумного будинку заснована на принципі виконання команд, причому одержувати їхній центральний контролер може як від людини, так і від сенсорів. Залежно від побажань користувача, спілкування із центральним контролером здійснюється за допомогою голосових команд, пульта керування або смартфона.

Системи розумного будинку можуть бути централізованими або децентралізованими. У перших керування всіма пристроями здійснюється з єдиного модуля, що дає можливість побудови складних схем автоматизації. Децентралізовані системи складаються з автономних ланцюжків приладів або навіть одиночних пристроїв. Такі рішення забезпечують більшу безпеку системи.

До центру керування розумним будинком, як правило, можна підключити дуже багато пристроїв, нерідко ліміт досягає декілька сотень.

Основними елементами "розумного" будинку є системи (рис. 6.2) [5]:

- клімат-контролю – керування теплою підлогою, опаленням, вентиляцією та кондиціонуванням;
- безпеки – системи відеоспостереження, сигналізації, датчики руху та відкриття дверей та вікон;
- освітлення – увімкнення/вимкнення світла, зміна яскравості та кольору освітлення залежно від побажань користувача;
- обліку ресурсів – розходу води, тепла, електроенергії та газу;
- контролю та запобігання протічкам води;
- керування мультимедіа – вимикати телевізор у заданий час, перемикати композиції на програвачі за допомогою голосового помічника і т.д.;
- керування побутовою технікою – запрограмувати прання на певний час, увімкнути кавоварку і т.д.



Рисунок 6.2 – Системи контролю та керування "розумного" будинку [5]

"Розумний" будинок максимально оптимізує, спрощує та автоматизує життя людини. Серед основних переваг системи смарт будинку варто відзначити:

1. Можливість дистанційного вмикання техніки. Виробники розумної техніки створюють спеціальні програми, які потрібно встановити на смартфон для роботи зі смарт-пристроєм, де б не знаходився користувач.

2. Голосове керування дозволяє вимкнути світло, приготувати каву, вимкнути мультиварку, включити телевізор та багато іншого.

3. Автоматичне оновлення. Смарт-пристрої мають модуль Wi-Fi або Bluetooth, завдяки чому можуть оновлювати програмне забезпечення автоматично, не вимагаючи втручання господарів.

4. Попередження надзвичайних ситуацій. У разі витoku газу, води або пожежі система швидко реагує та надсилає повідомлення на телефон та у відповідні міські служби.

Основним мінусом системи розумного будинку є висока вартість техніки та всіляких датчиків, а особливо неприємно, коли дорога техніка виходить з ладу і її потрібно ремонтувати.

Ще один недолік – складність монтажу. Не маючи потрібного досвіду, електрики та ремонтники часто можуть невірно змонтувати складну систему. Всі елементи в такій системі взаємопов'язані і не можна допустити навіть найменших помилок під час встановлення.

Деякі елементи розумного будинку потрібно встановлювати на етапі проектування чи монтажу квартири. Це стосується закладки комунікаційних кабелів, встановлення розумного освітлення та клімат-контролю.

"Розумна" будівля відрізняється від "розумного" будинку масштабами об'єкту автоматизації і наявністю або відсутністю деяких функцій. Наприклад, офісний центр не потребує встановлення систем управління мультимедійними пристроями, може бути відсутня система управління жалюзями. Але обов'язково повинна бути система вентиляції та кондиціонування повітря.

Крім забезпечення комфортних умов життя, система "розумний" будинок надає можливість істотно зменшити витрати на різні ресурси. Наприклад, створити розклад для включення опалення на щодня тижня. Перехід освітлювального й кліматичного устаткування в нічний режим і багато чого іншого.

6.2 Основні системи "розумного" будинку

6.2.1 Системи безпеки

Системи безпеки житла можуть включати системи охоронної, пожежної сигналізації, контролю доступу та відеоспостереження [3]. На рис. 6.3 наведені основні компоненти охорони "розумного" будинку [6].

Інфрачервоні сенсори руху, датчики задимленості, звукові сигналізатори, панелі систем охоронної сигналізації представлені на ринку в величезній кількості. Вже звичними стали домофони з моніторами.



Рисунок 6.3 – Системи безпеки "розумного" будинку [6]

Для відеоспостереження використовуються цифрові системи відеоспостереження з серверами на основі комп'ютерів та IP-відеокамер або аналогових камер, підключених через плати вводу відео до ПК або безпосередньо до відеореєстраторів (рис. 6.4) [3].



Рисунок 6.4 – Елементи систем відеоспостереження [3]

6.2.2 Системи підтримки мікроклімату

Тепловий комфорт в приміщеннях визначається взаємодією та якістю роботи систем теплозабезпечення, вентиляції та кондиціонування повітря. Сприйняття теплового комфорту кожною людиною дуже індивідуальне. Існують визначені

рамки 18...22 °С, та дехто відчуває навіть зміни температури в межах одного градуса. Так само індивідуальне і сприйняття вологості повітря.

Системи мікроклімату мають в своєму складі радіатори, конвектори, теплі підлоги, системи кондиціювання повітря. Високий рівень комфорту забезпечують системи зонного контролю, які управляють узгодженою роботою джерел тепла та холоду в визначеній зоні або приміщенні [4].

Якщо в житлових приміщеннях встановлюється система припливно-втяжної вентиляції, то утилізація тепла повітря, що видаляється з приміщень, на основі рекуператорів (пластинчатих, роторних, гліколевих) надає можливість суттєво економити енергію.

Регулювання мікроклімату у приміщенні також дає змогу обирати час виконання функцій забезпечення комфорту, таких як автоматичне відкривання та закривання вікон, жалюзі або ролетів у певний час доби [7]. Наприклад, інтенсивна вентиляція, так зване промивання приточним повітрям, може проводитися до прибуття перших працівників. Улітку функція "зворотного охолодження у нічний час" використовує прохолодне нічне та ранкове повітря для природного охолодження приміщень, у такий спосіб скорочуючи витрати енергії на охолодження (рис. 6.5) [7].



Рисунок 6.5 – Регулювання мікроклімату в приміщенні спортивного залу з природним провітрюванням [7]

Крім того, для кожної кімнати можна вибрати різні сценарії або різний рівень енергоспоживання, наприклад, комфорт, режим очікування, заощадження (зменшення вночі) або безпечна експлуатація будівлі. Сценарії можна перемикаєти за допомогою програм таймера, звітування про присутність або кнопок вручну. Крім того, можна вибрати додаткові сценарії з оптимальною інтенсивністю освітлення, вентиляції та захисту від сонця, наприклад зустрічі, презентації або офісна робота.

6.2.3 Зв'язок через шини будівлі або безпроводовий зв'язок

Попит на комфорт і універсальність в управлінні системами опалення, освітлення та контролю доступу для заміського будинку, а також офісного комплексу зростає. У той же час ефективне використання енергії стає все більш важливим. Люди хочуть комфортного, екологічного та безпечного місця для життя та роботи, і саме тут починається автоматизація. Однак більшої зручності та безпеки разом із меншим енергоспоживанням можна досягти лише завдяки розумному управлінню та контролю всіх задіяних продуктів. Це справжня проблема, так як система має на увазі багато проводів від датчиків і виконавчих пристроїв до центру управління. Для професіоналів така маса проводки також означає більші зусилля з проектування та монтажу, підвищений ризик пожежі та високі витрати. Ось де застосовується KNX [8].

Автоматизація не повинна бути складною. Для цього просто необхідна система, яка усуває проблеми ізольованих пристроїв, забезпечуючи зв'язок всіх компонентів на одній спільній мові. Тип пристрою, який ви хочете використовувати, більше не має значення. Чи хочете ви керувати освітленням, жалюзі, системами безпеки, енергоменеджментом, опаленням, вентиляцією, системами кондиціонування, системами сигналізації та

Для забезпечення надійної комунікації між актуаторами (виконавчими пристроями) та датчиками доступні різні системи шин (наприклад, KNX чи BACnet). Також використовуються радіосистеми (включно з ZigBee, Z-Wave,

EnOcean та KNX-RF). Вони дають змогу автоматизувати будівлі ретроспективно без потреби у складній кабельній проводці (рис. 6.6) [8].

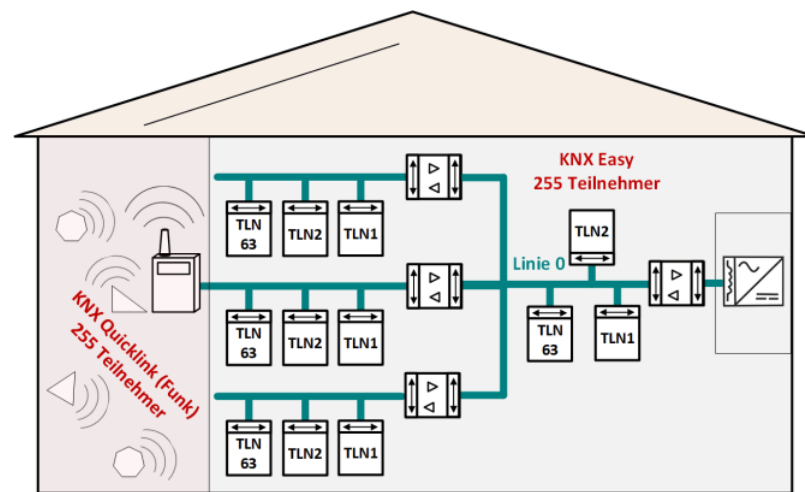


Рисунок 6.6 – Використання шини KNX для автоматизації будинку [8]

Головною перевагою шини KNX є можливість формування децентралізованої системи, що дозволяє зберегти відмовостійкість всього проекту навіть при відмові того чи іншого пристрою на шині.

6.2.4 Системи контролю якості повітря

Важливою складовою, що впливає на якість повітря, є вміст CO₂ та іонів у повітрі. Постійний приплив свіжого повітря знижує втомлюваність, підвищує імунітет людини та зменшує вміст шкідливих мікроорганізмів в приміщенні.

Наприклад система моніторингу якості повітря AQMesh – містить електрохімічні датчики для вимірювання якості повітря в приміщеннях та на відкритому повітрі, що пропонує локалізовану інформацію про якість повітря та аналіз даних у режимі реального часу (рис. 6.7). AQMesh вимірює ключові забруднювачі в атмосферному повітрі, використовуючи кращу технологію малих електрохімічних датчиків у поєднанні із запатентованою обробкою даних [9], отриманою внаслідок великих глобальних порівнянь даними. Система поєднує в собі надійну апаратну платформу з опціями безпроводового зв'язку, GPRS-

зв'язком, хмарною обробкою даних та безпечним онлайн-доступом. AQMesh виробляється у Великобританії і має винятково високу якість, ґрунтуючись на багаторічному досвіді розробки обладнання для моніторингу навколишнього середовища в суворих умовах та відповідно до міжнародних стандартів.

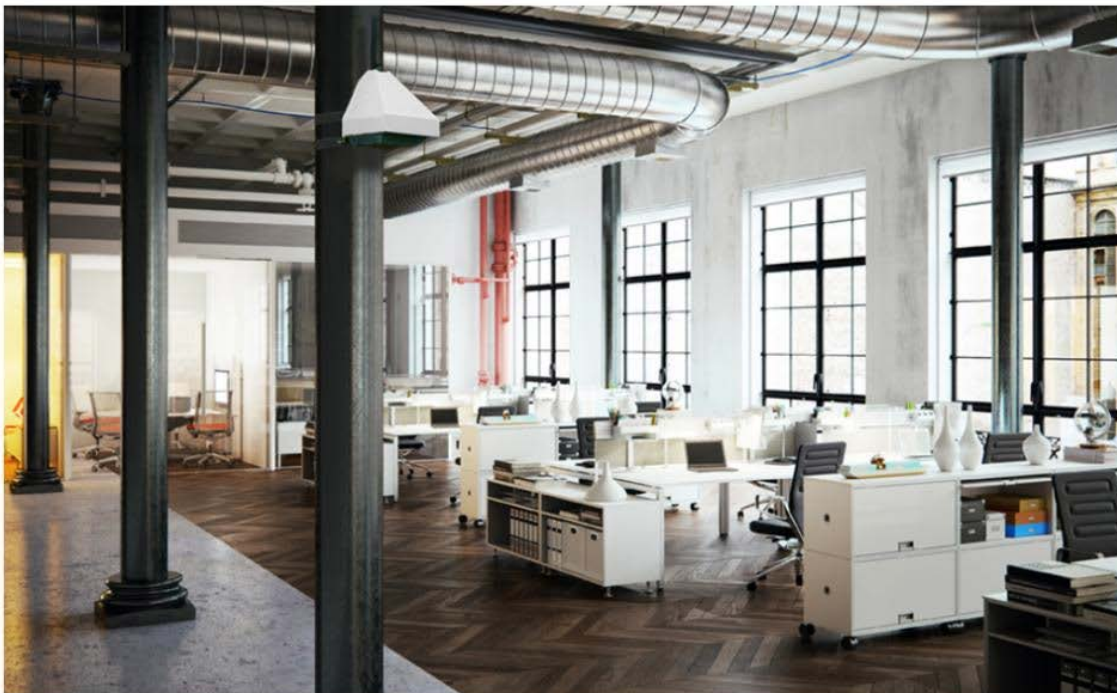


Рисунок 6.7 – Система AQMesh для вимірювання якості повітря в приміщеннях та на відкритому повітрі [9]

6.2.5 Системи освітлення

Системи освітлення забезпечують потрібний комфортний рівень освітлення. Світлові сцени можуть створити приємну атмосферу, яка буде відповідати настрою господаря [10-13]. М'які відтінки, що зручні при перегляді телевізійних програм, можуть змінити яскраві вогні, коли в будинку свято та багато гостей.



Рисунок 6.6 – Автоматизована система освітлення [10]

6.2.6 Інші системи "розумного" будинку

Системи економії енергоспоживання

Енергоспоживання житла залежить від якості теплоізоляції, а також від енергозберігаючих можливостей енергоємних систем мікроклімату та освітлення [14].

Тому в сучасних системах освітлення використовують світлодіодні світильники, які мають низьке енергоспоживання та можуть створювати безліч кольорів та відтінків за допомогою контролерів.

Також на ринку вже з'явилися системи природного освітлення зі світловими каналами. Вони забезпечують можливість передавання сонячного світла, що падає на дах будинку, у внутрішні приміщення.

Якщо раніше актуальним було завдання забезпечення малого енергоспоживання будинку, аж до нульового рівня (Zero Energy), то зараз є досить багато прикладів, коли житловий будинок може успішно генерувати енергію, а власник може продавати її надлишок. Ефективні теплові насоси, сонячні колектори та сонячні панелі надають таку можливість. Їх вартість постійно знижується при значному підвищенні вартості енергоносіїв.

Інформаційні та розважальні системи

Музичний центр, телебачення, домашній кінотеатр, Інтернет. Природне бажання користувача об'єднати все в одному мультимедійному комплексі, щоб для управління використовувати один, а не три-п'ять пультів дистанційного управління. Щоб звукове та візуальне обладнання підтримувало функцію "йди за мною" (follow me), супроводжуючи вас, коли ви переходите з кімнати в кімнату, або один мультимедійний комплекс забезпечував одночасно різну звукову та відеотрансляцію для різних мешканців за їхнім бажанням.

6.3 Технології автоматизації

Так само, як і у великих будівлях, системи управління для житлових будинків створюються на основі розподілених систем управління. Обмін даними між пристроями виконується згідно фізичних та логічних протоколів, які характеризують тип комунікаційної шини (Bus) [8]. Наприклад, фізичний протокол RS-485 визначає тип прийомопередавачів пристроїв та характеристики кабелю для прокладання комунікаційної мережі. За протоколом RS-485 працюють пристрої з логічними протоколами Modbus RTU, ASCII, BACnet MS/TP та інші. Пристрої з Modbus TCP, BACnet Ethernet, BACnet IP здійснюють обмін даними в мережі Ethernet. Пристрої з протоколами LON та KNX також мають певні вимоги до мереж передавання даних.

У сучасному помешканні вже звичними середовищами для передавання даних стали локальна мережа на основі структурованої кабельної мережі або безпроводових технологій Wi-Fi. Є пристрої, що забезпечують передавання даних по мережі електроживлення будівлі. Для обміну даними між сенсорами і контролерами існують чимало рішень на основі безпроводових технологій ZigBee, Mesh, Z-Wave, LoraWan, Smartmesh, Bluetooth і інших, спеціально розроблених для автоматизації будівель.

Так звані "закриті" системи автоматизації розробляються і підтримуються одним розробником або вузькою групою виробників. Відкриті системи базуються

на відкритих комунікаційних протоколах, що підтримуються великими групами розробників і асоціаціями виробників. Опис відкритого протоколу надається безкоштовно або за певну плату.

Для автоматизації будівель існують спеціалізовані стандартні протоколи, що описують змінні, об'єкти, сервіси, які використовуються в технологіях систем управління будівлями. Статус міжнародного стандарту ISO (International Organization for Standardization) мають такі протоколи:

- BACnet – Building Automation Control Network – ISO 16484-5;
- LonWorks – Local Open Network – ISO/IEC 14908, Parts 1, 2, 3, and 4;
- KNX – ISO/IEC 14543-3.

З відкритих протоколів, призначених для автоматизації малих будівель, квартир та приватних будинків найбільш відомі і популярні KNX і LON. BACnet системи застосовуються частіше в великих будівлях, хоча вони також можуть успішно вирішувати завдання автоматизації житла. Багато підсистем можна автоматизувати на основі відносно недорогого устаткування з відкритим промисловим протоколом ModBus.

Функція централізованого управління інтегрованої системи надає можливість управління всіма системами в будівлі з одного переносного пульта чи сенсорної панелі.

Для узгодженої та максимально ефективної роботи різних систем необхідно їх інтегрувати. Для цього створюється концепція системи автоматизації та взаємодії різних підсистем – схеми, сценарії, режими.

Взаємодію систем з різними комунікаційними протоколами забезпечують програмні чи апаратні шлюзи.

Як приклад – KNX-шлюзи Intesis для систем Daikin, які надають можливість повної інтеграції систем кондиціонування повітря в проект на основі технології KNX за досить низьких витрат [6].

Функція централізованого управління інтегрованої системи надає можливість управління всіма системами в будівлі з одного переносного пульта чи сенсорної панелі. Крім того можна в будь-який час переглянути звіт про стан

систем та обладнання. Система може надати власнику інформацію про будь-яку попередньо запрограмовану подію – тривогу, несанкціоноване проникнення, витік води чи вихід температури за встановлені межі.

Сучасна будівля постійно розвивається, оснащується новими, більш сучасними системами, які оновлюються швидкими темпами, особливо на рівні розважальних та комунікаційних систем. Отже, в проєкті повинна бути передбачена можливість такого розвитку.

6.4 Вимоги до функціональності систем "розумного" будинку

Вимоги до функціональності можуть бути різними у системного інтегратора і власника житла – кінцевого користувача системи. Для житлових будівель характерним є те, що як і інтер'єр квартири або особняка, система управління створюється за індивідуальним проєктом [5]. Власник виступає повноправним співавтором системи автоматизації свого житла.

Вільно програмовані контролери надають можливість програмування практично будь-яких алгоритмів роботи устаткування та його взаємодії. Контролери, що конфігуруються, призначені для роботи згідно з алгоритмами, які попередньо запрограмовані, і допускають лише обмежене налаштування параметрів.

Для власника житла важливим є дизайн настінного сенсора, пульта дистанційного управління, сенсорної панелі. Адже це ті пристрої, через які він взаємодіє з системою автоматизації. Їх привабливий зовнішній вигляд, простота і зручність в експлуатації істотно впливатимуть на сприйняття та оцінку якості всієї системи. Через них він сприймає і всю автоматику.

На нашому ринку присутні практично всі відомі виробники систем автоматизації. У кожного з них є панелі та пульти для автоматизації житла. Задовольняючи смаки споживачів, виробники намагаються максимально розширити їх кольорову гаму, фактуру, форму.

Як і сприйняття захищеності та комфорту, дуже індивідуальне у людини і сприйняття дизайну.

6.5 Що необхідно автоматизувати в першу чергу у розумних будинках?

У першу чергу потрібно приділити увагу безпеці (охоронна, протічка води, газу, оповіщення), системі опалення й диспетчеризації роботи ліфтів, також не можна стороною обходити комунікаційні системи. Контроль температури опалення, диспетчеризація систем безпеки й роботи ліфтів проводиться віддалено в ЖКГ. Всі тривожні сигнали повинні надходити як у відповідні служби забезпечення, хазяїнові квартири або котеджу, так і на центральний пульти у ЖКГ. Також хотілося б відзначити потребу в прокладці достатньої кількості проводів під слабкострумове керування аудіо- і відеопристроями [5].

Автоматизація будинків не самоціль. Вона потрібна для досягнення максимального рівня комфорту й безпеки при мінімальних витратах на експлуатації будинку. Для будь-якого власника в першу чергу цікаві системи безпеки й автоматизація енергоємних систем – освітлення, теплопостачання, вентиляції й кондиціонування повітря, що призначені для зниження рівня платежів за газ, тепло, електроенергію. Вартість енергоносіїв і тарифи будуть безупинно збільшуватися. Отже, потрібно контролювати споживання й знижувати його через оптимальне автоматичне регулювання, що забезпечує автоматика тепло-пунктів, котелень, систем вентиляції, системи диспетчеризації будинків.

Якщо підходити до питання автоматизації раціонально, то спочатку необхідно з'ясувати, що ми хочемо домогтися в підсумку від впровадження такої системи автоматизації, і скільки це буде коштувати. У більшості випадків від автоматизації очікують більше раціонального використання ресурсів, і отже економії коштів, або підвищенні комфорту проживання за рахунок рятуння людини від деяких рутинних дій і перекладання їх на плечі системи автоматизації.

Тому що саме рахунки за комунальні послуги турбують усіх без винятку власників житла, як мінімум раз на місяць, те й почати потрібно, напевно, із цієї

проблеми. Найбільші витрати традиційно йдуть на підтримку необхідного мікроклімату в приміщенні (охолодження/опалення) і освітлення. Підтримуючи комфортну температуру, вдається істотно знизити витрати на опалення, іноді до 40%. Подальшим розумним кроком може бути застосування електронних термостатичних головок. Даний пристрій дозволяє автоматично знижувати температуру в приміщенні в нічний час, що дозволяє домогтися додаткової економії й комфорту.

Для зменшення витрат на освітлення використовують сенсори освітленості та присутності. Наступним кроком може бути інтеграція в єдину систему й забезпечення взаємозалежної роботи систем підтримки клімату, освітлення, контролю доступу й безпеки, різних мультимедійних пристроїв у будинку, те, що отримало назву "розумний будинок".

6.6 Системи управління освітленням

Для управління системами освітлення на сьогодні використовують в основному систему KNX та DALI (Digital Adressable Lighting Interface). У системі KNX, як найбільш універсальній передбачена підтримка пристроїв з інтерфейсом DALI [8].

DALI призначені для керування електронними технічними приладами, що розташовуються на відповідній шині, такими, як наприклад, світлодіодні або люмінесцентні лампи. Наприклад, майстер-модуль KL6811 (рис. 6.7) [11] компанії Beckhoff дозволяє здійснювати підключення й керування пристроями DALI за допомогою системи вводу-виводу:

- DALI дозволяє гнучко управляти освітленням при мінливих умовах;
- KL6811 дозволяє підключати до 64 ведених пристроїв DALI;
- модуль DALI містить у собі інтегроване джерело живлення 24 В постійного струму з гальванічною розв'язкою від мережі змінного струму;

- за допомогою програмного забезпечення KS2000 можна виконати основне налаштування, а також групування й визначення світлових сценаріїв DALI-пристроїв.

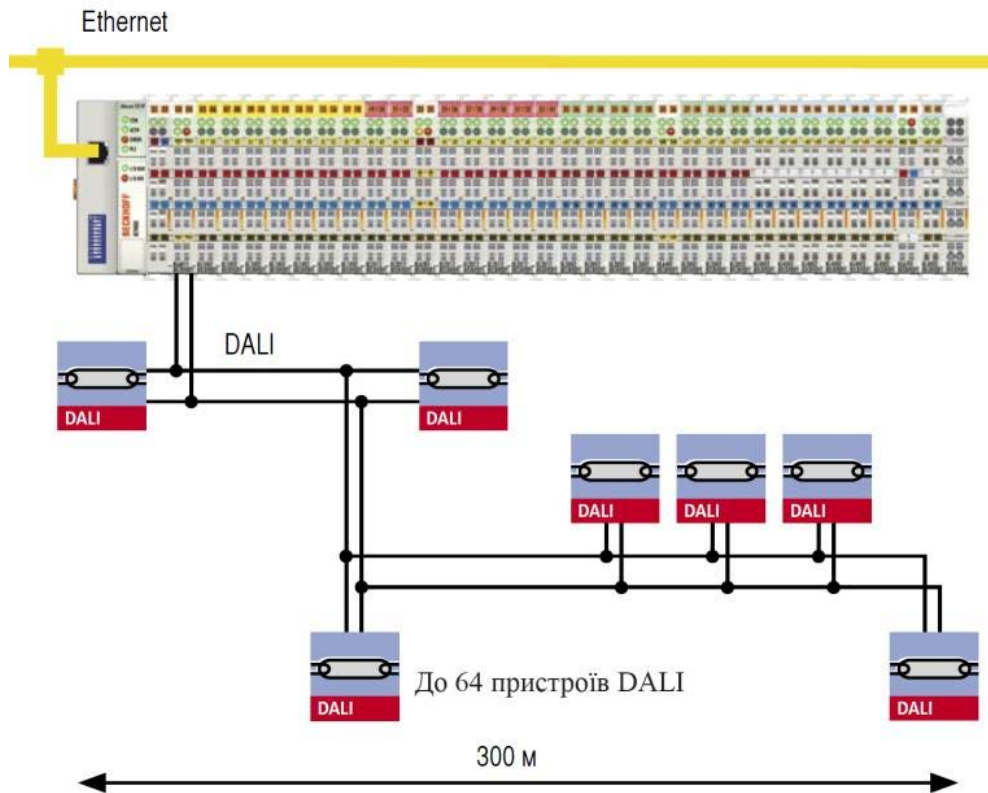


Рисунок 6.7 – Підключення майстер-модуля KL6811 до пристроїв DALI [11]

Для під'єднання пристроїв з різними інтерфейсами призначені пристрої узгодження інтерфейсів. Приклади деяких пристроїв компанії Beckhoff наведені в табл. 6.1 [11].

Компанія Siemens випускає велику кількість модулів, що призначені для управління освітленням. Зовнішній вигляд таких модулів наведений на рис. 6.8 та 6.9.

Таблиця 6.1 – Модулі компанії Beckhoff для перетворення інтерфейсів

Інтерфейс	Пристрій перетворення інтерфейсів/контролер вузла шини			
	CX	BK	BC	BX
Ethernet TCP/IP	+	+	+	+
EtherCAT	+		—	—
Lightbus	+	+	+	—
Profibus	+	+	+	+
Interbus	—	+	+	—
CANopen	+	+	+	+
DeviceNet	+	+	+	+
Modbus	+	+	+	—
RS485	+	+	+	+
RS232	+	+	+	+
USB	+	+	—	



DALI

Перемикачі
навантаження

Димери

Управляючі
пристрої

Рисунок 6.8 – Модулі Siemens для управління освітленням [10]

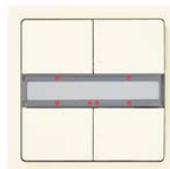
Датчик
присутностіКлавішні
перемикачі

Рисунок 6.9 – Пристрої Siemens для управління освітленням [10]

Розглянемо характеристики деяких модулів управління освітленням.

Зовнішній вигляд модуля на два канали управління N 141/21KNX/DALI Gateway Twin plus наведений на рис. 6.10 [12].



Рисунок 6.10 – Модуль N 141/21KNX/DALI Gateway Twin plus [12]

Основні характеристики модуля:

- підтримує аварійне освітлення та роботу з сенсорами присутності;
- для зв'язку через KNX EIB з електронними баластами з інтерфейсом DALI;
- виходи DALI відповідно до IEC 62386, кожен для зв'язку з 64 DALI ECG Ed.1 та DALI-2 та щонайменше 10 сенсорами;
- інтегрований блок живлення зі входною напругою змінного струму в діапазоні 110...240 В, 50...60 Гц або 120...240 В постійного струму для живлення електроніки шлюзу та виходу DALI;
- максимальна вихідна напруга DALI 19 В;
- стійкий до короткого замикання;
- визначення неправильного підключення напруги під час введення в експлуатацію;
- визначення, чи підключена неправильно лінія передавання до виходу DALI;
- світлодіодний дисплей для відображення режиму роботи та повідомлень про помилки;
- кнопка для перемикання між шиною та режимом прямої роботи;

- одна пара кнопок для ввімкнення / вимкнення всіх підключених пристроїв DALI;
- один світлодіод на вихід DALI для сигналу стану всіх підключених світильників у прямому режимі;
- налаштована поведінка на несправність шини (автономний режим);
- налаштування попередньо завантажених програм без програмного забезпечення (ETS), планувальник дня, тижня, дати та додаткової астро-функції;
- управління всіма підключеними світильниками разом у режимі трансляції;
- сигнал стану та відображення відмови лампи;
- розрізнення автономних аварійних світильників з одним або двома пристроями DALI;
- початок самостійного тестування кожного окремого інвертора та повідомлення результату тесту через шину або збереження в постійній пам'яті з моніторингом простору пам'яті об'єкту.

Універсальний модуль димера для плавного регулювання яскравості освітлення 5WG1 554-1DB31. Зовнішній вигляд димера наведений на рис. 6.11 [13].



Рисунок 6.11 – Універсальний димер 5WG1 554-1DB31 [13]

Основні характеристики універсального димера 5WG1 554-1DB31:

- чотири виходи для перемикання та затемнення резистивного, індуктивного та ємнісного навантажень;
- номінальна робоча напруга змінного струму 230 В, частота 50 і 60 Гц;
- номінальна потужність на виході димера при температурі навколишнього середовища 45 °С до 300 ВА на вихід, до 1000 ВА з об'єднанням сусідніх виходів;
- системи захисту від перевантаження виходу, короткого замикання та підвищення температури;
- необслуговувані клеми для підключення та наскрізної проводки необроблених одножильних та багатожильних провідників 0,5...2,5 мм²;
- кнопки ручного керування на пристрої для перемикання, затемнення та активації режиму прямого режим;
- пристрій для монтування на DIN-рейці або для кріплення на рейці TH35 згідно з DIN EN 60715.

З іншими пристроями для управління освітленням можна ознайомитись у [3].

6.7 Драйвери управління світлодіодними світильниками

Драйвер для світлодіодного світильника – найважливіший елемент системи освітлення, що забезпечує необхідну яскравість, ефективність і тривалу експлуатацію джерел світла. З його допомогою відбувається трансформація змінного струму промислової мережі напругою 220 В в постійний струм потрібного значення [14].

Головна характеристика перетворювача для світлодіодних освітлювальних приладів – вихідний струм. Світлодіод досить чутливий до якості електроживлення. Якщо знижене значення струму приведе тільки до зменшення яскравості світильника, то підвищення струму вище номінального значення дуже швидко знижує ресурс цих джерел світла. Для забезпечення стабільного електроживлення (підтримки заданого струму через діоди) необхідна додаткова електронна схема – драйвер живлення, що у англійській літературі отримав назву Led Driver.

Якщо порівнювати драйвер і блок живлення, то в них є розходження в роботі. Драйвер – це джерело струму. Його завдання підтримувати саме певну силу струму через ланцюжок світлодіодів.

Завдання стабілізованого джерела живлення у формуванні саме стабільної напруги. На відміну від звичайного джерела живлення завдання драйвера сформувати необхідний струм через ланцюжок світлодіодів світильників. Залежно від числа світлодіодів випускаються драйвери з вихідною напругу 12, 24 або 36 В. При цьому вони забезпечують струм від 0,3 до 1 А, залежно від використовуваних світлодіодів.

При виборі драйвера потрібно врахувати:

- потужність, споживану світильником;
- вихідну напругу;
- максимальний вихідний струм.

Крім того, випускаються й регульовані джерела живлення, що дозволяє регулювати яскравість світильників.

Розглянемо параметри деяких драйверів світлодіодів компанії MEAN WELL [14].

Надійні драйвери світлодіодів серії XLG (рис. 6.12) відповідають класу захисту електротехнічного устаткування IP67 і орієнтовані на застосування в системах внутрішнього й зовнішнього світлодіодного освітлення (стадіонів, залізничних станцій, морських портів і т.п.), декоративного архітектурного підсвічування та ін. Крім того, їх можна застосовувати в системах освітлення для підсвічування вітрин і прилавків у супермаркетах і торгових центрах, а також як джерела живлення прожекторів і інших світлотехнічних пристроїв.

Драйвери світлодіодів XLG-50 підтримують режим роботи зі стабілізацією вихідної потужності в розширеному діапазоні вхідної напруги змінного (100...305 В) і постійного (142...431 В) струму.

Драйвери відповідно до рекомендацій стандартів EN61000 і EN61547 стійкі до імпульсів напруги амплітудою 6 кВ (лінія-земля) і 4 кВ (лінія-лінія). Конструктивно драйвери XLG-50 виконані в герметичному металевому корпусі з

габаритними розмірами 105×63×30 мм. Термін служби – 100 тис. годин при температурі корпусу 60 °С.



Рисунок 6.12 – Зовнішній вигляд драйверів серії XLG компанії MEAN WELL [14]

Основні технічні характеристики драйвера XLG-50 наведені в табл. 6.2 а його структура наведена на рис. 6.13.

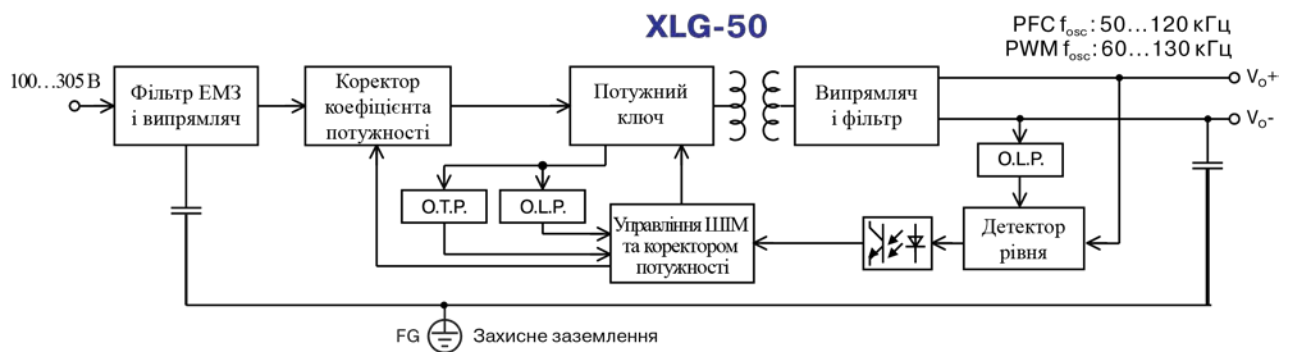


Рисунок 6.13 – Структура драйвера XLG-50

Драйвери забезпечують вихідний струм до 2 А і містять вбудований активний коректор коефіцієнта потужності. При входній напрузі 277 В і навантаженню 100% коефіцієнт потужності $PF \geq 0.92$, коефіцієнт корисної дії ККД – до 90%, споживана потужність при відсутності навантаження – менш 0.5 Вт. Графік залежності ККД від величини навантаження й входньої напруги наведений на рис. 6.14 [14].

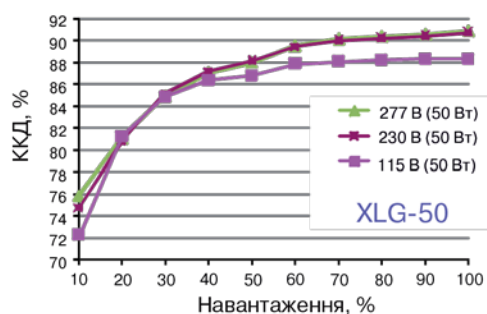


Рисунок 6.14 – Залежність ККД драйвера XLG-50 від навантаження [14]

Оскільки ККД знижується при зменшенні навантаження, найбільшу ефективність при використанні драйверів можна одержати в режимах роботи з найбільшим вихідним струмом.

У випадку експлуатації драйверів на висоті більше 2000 м над рівнем моря максимальна робоча температура знижується зі швидкістю $3.5\text{ }^{\circ}\text{C}/1000\text{ м}$ (у режимі примусового обдуву вентилятором) або $5\text{ }^{\circ}\text{C}/1000\text{ м}$ (якщо обдув не використовується). Драйвери XLG-50 витримують вібрації із прискоренням до 5 g у діапазоні частот $10\ldots 500\text{ Гц}$.

Драйвери XLG-50 відповідають рекомендаціям основних європейських і міжнародних стандартів по електромагнітній сумісності й безпеці.

У драйверах XLG-50 залежно від модифікації реалізовано кілька варіантів плавного регулювання вихідного струму й, відповідно, яскравості світіння світлодіодів. У драйверах для регулювання вихідного струму передбачене використання сигналу постійного струму напругою $0\ldots 10\text{ В}$, ШІМ-сигналу частотою $0.1\ldots 3\text{ кГц}$ із регульованою скважністю й амплітудою 10 В або зовнішнім резистором. У цьому випадку сигнали керування рівнем вихідного струму або зовнішній резистор підключаються до виводів драйвера DIM+ і DIM- (рис. 6.15). Крім того, вихідний струм можна регулювати за допомогою вбудованого потенціометра [14]. Основні характеристики драйвера світлодіодів XLG-50 наведені у табл. 6.2.

Таблиця 6.2 – Основні характеристики драйвера світлодіодів XLG-50

Параметр	Значення
Вихід	
Номінальний вих. струм, А	1
Макс. вих. напруга на х.х., В	57
Номінальна вих. потужність, Вт	50
Вих. напруга в режимі стабілізації струму, В	22...54
Рівень пульсацій вих. струму, % $I_{ном}$	± 5
Діапазон регулювання струму, А	0.53...2.1
Час старту, мс (вих. напруга. змінного струму, В)	500/100 (115/230)
Захист від КЗ, перегріву и перенапруги	+
Вхід	
Діапазон вхідної напруги, В	100-305 (AC) (47-63 Гц), 142-431 (DC)
Вхідний струм, А (вих. напруга. змін. струму, В)	0.57(115), 0.29 (230), 0.24 (277)
Коефіцієнт потужності PF (тип.)	PF ≥ 0.97 (115 В), PF ≥ 0.95 (230 В), PF ≥ 0.92 (277 В) при навантаженні 100%
Коефіцієнт гармонік (THD), не більше, %	10
ККД (тип.), %	90
Електромагнітна сумісність, безпека	
Електромагнітна сумісність (стандарти)	EN55015; EN61000-3-2 Class C (load $\geq 50\%$); EN61000-3-3; GB17743, GB17625.1; EN61000-4-2, 3, 4, 5, 6, 8, 11; EN61547 (лінія-корпус 6 кВ, лінія-лінія 4 кВ)
Стандарти безпеки	UL8750 (HL), CSA C22.2 No. 250.13-12, ENEC AS/NZS IEC EN61347-1, AS/NZS EN61347-2-13, IP65/IP67; GB19510.1, GB19510.14
Інші параметри	
Діапазон робочих температур, °C	-40...90
Відносна вологість повітря, %	20...95
Габаритні розміри, мм	105×63×30
Маса, кг	0.41/0.42
Строк служби, тис. годин	>50
Гарантія	5 років

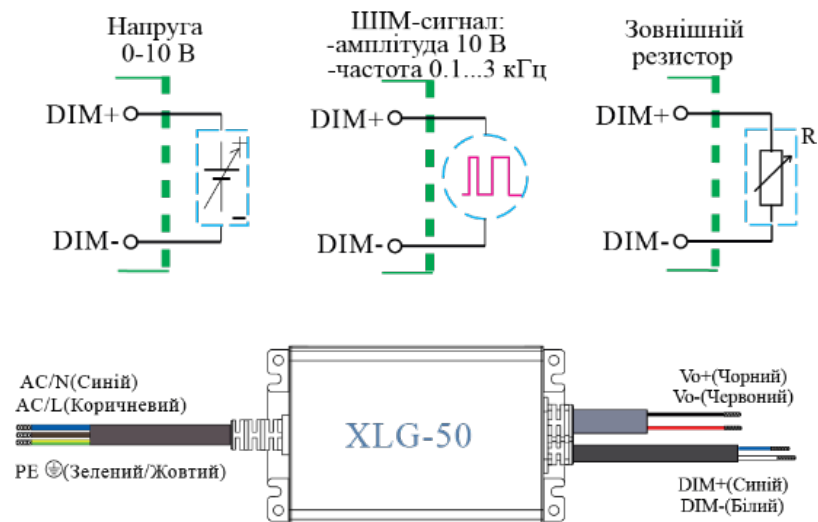


Рисунок 6.15 – Способи управління драйвером XLG-50

Драйвери XLG-240 підтримують режим роботи зі стабілізацією вихідної потужності в діапазоні входної напруги змінного (180...305 В) і постійного (142...431 В) струму. Конструктивно драйвери виконані в закритому металевому корпусі (IP67) габаритними розмірами 219×63×35.5 мм. Гарантійний строк роботи п'ять років. Драйвери XLG-240 витримують вібрації із прискоренням до 5 g у діапазоні частот 10...500 Гц. Орієнтовний термін служби – 60 тис. год при температурі корпусу 75 °С.

6.8 Світлодіодні лампи та світильники

6.8.1 Світлодіодні лампи

Для виробників світильників важливо знати параметри світлодіодів, драйверів світлодіодів та димерів. Але для тих хто встановлює системи освітлення а також для приватних споживачів цікава інформація про готові вироби для освітлення – лампи, світильники, прожектори та інші прилади освітлення [15, 16].

Світлодіодні лампи на сьогоднішній день є найекономічнішим джерелом світла. Розглянемо з яких елементів складається світлодіодна лампа та які її основні параметри (рис. 6.16).



Рисунок 6.16 – Конструкція світлодіодної лампи [15]

Світлодіодна або LED-лампа складається з чотирьох основних частин:

1. Колба з розсіювачем. На відміну від колб ламп розжарювання і люмінесцентних ламп, вона не б'ється, оскільки зроблена з пластику, а не скла. Також, вона не нагрівається. Колби бувають двох видів – матова і прозора. При виборі світлодіодної лампи, варто віддати перевагу пристрою з матовою колбою. Вона призначена для рівномірного розсіювання світла по всій площі приміщення. Колба, виконана з прозорого скла, призначені для декоративного освітлення.

2. Плата зі світлодіодами. 90% тепла, що випромінюється світлодіодами, припадає на плату. Тому, важливо, щоб вона була з алюмінієвою підкладкою. На сторону, яка розташована біля радіатора, наноситься термопаста, яка забезпечує ефективне відведення тепла від світлодіодів до радіатора.

4. Драйвер світлодіодів один з основних елементів світлодіодних ламп. Завдяки йому, струм передається від джерела живлення до лінійки світлодіодів. Драйвер впливає на якість світла, (мерехтіння, стабільність яскравості, можливість управляти яскравістю) а також на ресурс роботи лампи. Драйвер запобігає пульсації, а отже світлодіодні лампи не мерехтять. Завдяки йому наші очі не втомлюються від штучного освітлення. Також, завдяки цьому пристрою, лампи

можуть працювати до 10 тисяч годин навіть при перепадах напруги у мережі змінного струму.

4. Корпус лампи з цоколем. Основна задача корпусу лампи – вмістити усі внутрішні елементи та організувати якісне відведення тепла. У ранніх моделях LED-ламп використовувалися дуже складні конструкції корпусу. Вони були виконані з масивного алюмінію у вигляді радіаторів, що дозволяло дуже ефективно відводити тепло, яке випромінюється елементами драйвера і світлодіодами, але при цьому дуже їх здорожувало. Згодом виробники знайшли компромісне рішення: поєднання тонкостінного алюмінієвого стакану з термопластиком. Ця пара цілком справляється із завданням тепловідведення при відносній дешевизні конструкції, що зробило світлодіодну лампу доступнішою за ціною. Всі елементи драйвера розташовуються усередині стакану. Він з одного кінця закритий цоколем, а з іншого – алюмінієвою пластиною (друкованою платою), на якій розташовані світлодіоди. Іноді на цій же пластині розташовують елементи драйвера. Цоколь – це частина лампи, за допомогою якої пристрій прикріплюється до патрона люстри. Як і в лампах розжарювання, цоколь в світлодіодних лампах має багато модифікацій – від E14 і E27, які найчастіше використовують у побуті, до MR, які застосовуються для точкового освітлення.

6.8.2 Світлодіодні світильники

З розвитком LED-технологій все частіше в магазинах можна зустріти не тільки люстру, до якої потрібно купувати лампочки, а й готові світильники які значно менші за розмірами. Світильники випускаються різної потужності і в залежності від площі приміщення можна підібрати світильник що буде забезпечувати комфортне освітлення [15, 16].

На рис. 6.17 наведений приклади зовнішнього вигляду побутових світильників.



Рисунок 6.17 – Зовнішній вигляд побутових світильників [16]

Можливості світлодіодних світильників

Мабуть найзручнішою функцією світлодіодних світильників стала можливість дистанційного керування як з допомогою пульта ДУ, що йде в комплекті до розумного світильника, так і через підключення до телефону через Bluetooth для окремих моделей. Вартість світильників з дистанційним керуванням на сьогодні починається від 1300 грн і збільшується в залежності від потужності та кількості додаткових функцій світильника [16-18].

Серед інших цікавих функцій важливо виділити:

- регулюванням інтенсивності освітлення (диммер);
- регулювання колірної температури світла (від теплої до холодної)
- наявність таймера відключення
- режим нічної лампи
- можливість запам'ятовування налаштованого режиму.

Кожна з цих функцій робить світильник зручним для різних потреб. Таймер стане в нагоді людям, що люблять засинати перед телевізором, або ж регулярно забувають виключити світло на кухні, а режим нічника – найкраще використати для дитячої кімнати.

На рис. 6.18 наведено приклади освітлення з різною колірною температурою світильників [16].



Рисунок 6.18 – Приклади освітлення з різною колірною температурою [16]

До основних параметрів світлодіодних світильників відносяться [16]:

1. Колірна температура. Даний параметр вимірюється в кельвінах і визначає відтінок світіння. Можна орієнтуватися на наступні критерії вибору світлодіодних світильників:

- 2200...3000 К – прилади підходять для житлових і комерційних приміщень;
- 3400...4500 К – світильники можна використовувати в офісних і приміщеннях комерційного типу;
- 5000...6500 К і вище – світильники промислового і технічного призначення.

2. Енергоефективність. Основна характеристика економічності ламп є світлова віддача. Розраховується як відношення світлового потоку лампи в люменах до її потужності у ватах (лм/Вт).

3. Світловий потік. Величина світлового потоку (Ф) визначається як потужність випромінювання того чи іншого джерела світла, що викликає певне світлове відчуття в зоровому органі людини, і яка вимірюється в люменах (лм). Для прикладу звичайна лампа розжарювання потужністю 100 Вт створює світловий потік 1200 лм. А газорозрядна лампа 26 Вт характеризується світловим потоком у 1600 лм.

Під освітленістю E мається на увазі відношення світлового потоку до одиниці площі освітлюваної ним поверхні, тобто його поверхнева щільність. Ця величина нормується, як правило, в горизонтальній площині. При цьому в якості одиниці вимірювання освітленості використовується люкс (лк).

1 люкс відповідає світловому потоку в 1 люмен, який потрапляє на 1 м^2 освітлюваної площі.

Діапазон освітленості за різних умов поширення світла від різних джерел коливається від 1 до 20 лк на вулиці (за умов штучного освітлення) і в межах від 20 до 5000 лк у приміщенні. До речі, основною характеристикою економічності ламп є світлова віддача, що виражає відношення світлового потоку лампи в люменах до її потужності у ватах.

Як визначити світловий потік світлодіодної або енергозберігаючої лампи за потужністю. Відповідь можна знайти в табл. 6.3, в якій вказані визначені дослідним шляхом співвідношення між люменом та ватом для лампочок розжарювання, а також відповідні значення для світлодіодних ламп [16].

Таблиця 6.3 – Порівняння світлового потоку ламп різної потужності

Лампа розжарювання, потужність, Вт	Світлодіодний прилад, потужність, Вт	Світловий потік, лм
40	4...6	400
60	9...10	700
75	10...11	900
100	12...14	1200

4. Пульсація світлового потоку. Не всі виробники вказують в паспортних даних своєї продукції цю характеристику. Однак даний параметр дуже важливий. При великих значеннях пульсацій людина дуже швидко втомлюється і це шкідливо для зору. Безпечною можна вважати пульсацію не більше 10%. Для виконання точних видів робіт потрібні прилади з пульсацією не більше 7%.

5. Клас IP захисту. Цей параметр відіграє важливу роль при виборі світлодіодних світильників для встановлення в виробничі приміщення з підвищеним вмістом пилу, в кімнати з підвищеною вологістю. В коді виду IPXX перше число означає, наскільки прилад захищений від попадання пилу та інших дрібних частинок під корпус. Друга показує ступінь захищеності від випадкового попадання крапель води, бризок.

Світильники, які використовуються в теплицях, повинні бути більш захищеними. Індекс IP таких приладів потрібно вибирати не менше 65. Світлодіодні світильники з IP 65 і вище можуть працювати в більш широкому температурному діапазоні (від -30°C до $+60^{\circ}\text{C}$). Крім того, такі моделі додатково можуть оснащуватися:

- запобіжниками PULS – для захисту від перепадів мережі;
- міцним корпусом, стійким до механічних пошкоджень;
- спеціальним розсіювачем, який рівномірно розподіляє світловий потік.

Світлодіодну продукцію, у якій IP нижче 44 не можна встановлювати в саунах, лазнях, поблизу джерел тепла. Для офісних і житлових приміщень досить IP20.

Як підібрати LED світильник по типу

Щодо колірної температури. До 3000 K – це тепла палітра. Світло від таких джерел схоже на випромінювання від ламп розжарювання. До 4500 K – нейтральне світло. Світлодіоди з нейтральною колірною температурою випромінюють світло, схоже на денне. Лампи в діапазоні 5000...6000 K рекомендуються для освітлення робочих поверхонь. Це холодна палітра. Світло біло-блакитне.

Не всі виробники вказують в паспортних даних своєї продукції таку характеристику, як пульсація світлового потоку. Однак даний параметр дуже важливий – при великих значеннях лампи шкідливі для зору. Безпечною можна вважати пульсацію не більше 10%. Для виконання скрупульозних видів робіт потрібні прилади з пульсацією не більше 7%.

Контрольні питання

1. Що мається на увазі під терміном драйвер світлодіодів?
2. Скільки проводів використовується в системі управління світильниками DALI?
3. Який основний параметр драйверу світлодіодів?
4. Для чого призначені димери в системах освітлення?
5. Чи можна здійснювати управління по шині KNX світильниками з інтерфейсом DALI?
6. Що необхідно автоматизувати в першу чергу у розумних будинках?
7. Що викликає мерехтіння світла у світлодіодних світильниках або лампах?
8. Чому світлодіоди розміщують на металевій друкованій платі?
9. Як знайти енергоефективність світильника якщо відомі значення світлового потоку та споживаної потужності світильника?

Перелік посилань

1. S. Ilesanansi, P. Santhiyaa, M. Vidhya Smart city using IoT/ International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04, Apr 2019. pp. 2619-2622.
2. 10 Most Common Smart Home Issues (and How to Fix Them). Url: <https://www.tandytech.com/cybersecurity/10-most-common-smart-home-issues-and-how-to-fix-them/> (дата звернення: 1.07.2024).
3. Що таке "розумний будинок" і навіщо він потрібен? Url: <https://stylus.ua/uk/articles/528.html> (дата звернення: 1.07.2024).
4. Безпека. Url: <https://www.smarthouse.ua/ua/bezopasnost.html>. (дата звернення: 1.07.2024).
5. Розумний будинок. Url: https://12-220.zp.ua/rozumnyy_budynok/ (дата звернення: 1.07.2024).
6. Охорона будинку. Url: <https://sg-ukraine.com.ua/services/object-security/ohrana-doma/> (дата звернення: 1.07.2024).

7. Приточне повітря завдяки регулюванню мікроклімату у приміщенні. Url: <https://www.geze.ua/uk/cikavi-novini/temi/reguljuvannja-mikroklimatu-u-primishchenni>. (дата звернення: 1.07.2024).
8. Короткий вступ до протоколу KNX. Url: <https://knx24.com/news/basics/knx/> (дата звернення: 1.07.2024).
9. AQMesh система моніторингу якості повітря. Url: https://aep.kiev.ua/shop/portable_air_quality_monitoring/aqmesh-sistema-monitoring-kachestva-vozdruha/ (дата звернення: 1.07.2024).
10. Управління освітленням. Url: <https://www.siemens.com/ua/uk/produkty/avtomatyzatsiya-ta-bezpeka-budivel/systemy-avtomatyzatsiyi-ta-dyspetcheryzatsiyi-budivel/gamma-instabus/upravlinnya-osvitlennyam.html> (дата звернення: 1.07.2024).
11. Перелік продукції виробництва Beckhoff. Url: <http://ria-group.com.ua/beckhoff-2/> (дата звернення: 1.07.2024).
12. N 141/21 KNX / DALI Gateway Twin plus. Url: <https://support.industry.siemens.com/cs/document/87445450/n-141-21-knx-dali-gateway-twin-plus-product-database-and-application-description?dti=0&dl=en&lc=ru-BY> (дата звернення: 1.07.2024).
13. Universal dimmer N 554D31. Url: https://cache.industry.siemens.com/dl/files/037/109757037/att_947021/v1/5WG1_554-1DB31_tpi_en_DS01.pdf (дата звернення: 1.07.2024).
14. LED драйвери (Джерела живлення для світлодіодів) Mean Well. Url: https://meanwell.in.ua/led_drivers_m/?srsltid=AfmBOooGTgcpsu7MJtt0eRBFbMlTY4uZOFChyAAzZPkRzjeN28wPCRj (дата звернення: 1.07.2024).
15. Будова світлодіодної лампи. Url: <https://ledtest.vestum.ua/uk/study/budova-svitlodiodnoi-lampi/>. (дата звернення: 1.07.2024).
16. Як правильно вибрати світлодіодний світильник. Url: <https://vencon.ua.ua/articles/kak-vybrat-svetodiodnyj-led-svetilnik> (дата звернення: 1.07.2024).

17. Освітлення в системі "Розумний Дім": переваги та функціонал. Url: <https://svetilnikof.com.ua/ua/blog/osveshchenie-v-sisteme-umnyi-dom-preimushchestva-i-funktsional>. (дата звернення: 1.07.2024).
18. Енергоефективність. Url: <https://www.kresc.com.ua/energy-efficiency.shtml> (дата звернення: 1.07.2024).

7 СИСТЕМИ БЕЗПЕКИ ТА ПОЖЕЖНОЇ ОХОРОНИ

7.1 Системи пожежної охорони

7.1.1 Загальні зауваження

Системи пожежної охорони складаються з декількох основних частин [1, 2]:

- панель контрольна пожежна (ПКП);
- датчики температури (теплові);
- датчики диму.

Додатково можуть встановлюватись датчики газу (або універсальні датчики, що контролюють температуру, наявність диму та чадного газу) та датчики відкриття дверей. Окрім того можуть додатково встановлюватись додаткові панелі пожежної сигналізації, ручні сповіщувачі про пожежу, сирени звукового оповіщення, табло з написами (вихід чи зображенням людини що біжить). У складних системах можуть бути встановлені додаткові елементи – пристрої пожежогасіння, пристрої передавання даних та інші. Панелі контрольні пожежні (ППК) можуть бути замінені програмованими логічними контролерами.

До ППК можуть підключатися також датчики охоронної сигналізації. Наприклад для того щоб захистити приміщення де знаходиться ППК від втручання зломисників в систему пожежної сигналізації. Для охорони доступу до таких приміщень потрібна постановка й зняття з охорони.

Постановка й зняття з охорони

Постановка й зняття з охорони здійснюються прикладанням до зчитувача електронного ключа або картки, як у системах контролю доступу (буде розглянуто пізніше). Недоліком є уразливість зчитувача, що розташовується зовні охоронюваного об'єкта. Варіантом розв'язку може бути розташування зчитувача усередині закритого приміщення. У такому випадку, щоб при відкритті дверей не спрацювала сигналізація, шлейф, у який включені датчики, що контролюють вхід у приміщення, підключаються до шлейфа із запрограмованою затримкою на спрацювання.

Клавіатура

В деяких системах замість ключа або картки використовується клавіатура для зняття з охорони. Такі системи дозволяють задавати, так званий, код для зняття з охорони "під примусом". Якщо такий код був уведений замість звичайного, на пульт – а такий функціонал має сенс у тому випадку, якщо сигналізація підключається на пульт охорони, формується сигнал тривоги про напад, при цьому ніяких інших сигналів система не подає. Клавіатура вразливий пристрій і встановлюється усередині приміщення, а шлейф, що контролює вхід, програмується на роботу із затримкою.

Радіобрелки

У багатьох пристроях сигналізації використовують для зняття/постановки радіобрелки, що здійснюють управління по радіоканалу. Переваги очевидні: немає необхідності виносити якусь частину системи за межі охоронюваної зони, у такий спосіб знижується фізична уразливість ОПС. Однак сигнал із брелка може бути перехоплений і підроблений, а сам брелок може бути украдений або просте загублений.

Дзвінок або SMS

Деякі моделі охоронних панелей, оснащені GSM-модулем і можуть управлятися за допомогою дзвінка або SMS.

Інтерфейси для оповіщення

Контрольний прилад має контакти, які замикаються при спрацьовуванні датчика (так звані "сухі контакти", включаючи сирену або маячок. Використання виняткове світло-звукового способу оповіщення має сенс у тому випадку, якщо призначення сигналізації налякати зловмисника й привернути увагу. На сухі контакти також може бути підключений автодозвонювач (пристрій, який при тривозі телефонує по заданих номерах і відтворює записане голосове повідомлення. Для дозвону використовується як міська телефонна мережа, так і мобільні мережі зв'язку. Багато сучасних охоронних панелей мають вбудований GSM-модем.

SMS-оповіщення

Оповіщення за допомогою відправлення коротких повідомлень на мобільні номери використовуються в системах охоронної сигналізації для житла й малого бізнесу. Контрольна панель містить GSM-модуль, використовуваний як для відправлення повідомлень, так і для віддаленого керування сигналізацією.

Протокол Contact ID

Охоронно-пожежна сигналізація, що підключається на пульт групи швидкого реагування, використовує для подачі сигналів протокол Contact ID – набір DTMF-сигналів, що передаються як правило по лініях міської телефонної мережі або за допомогою стільникового зв'язку. За допомогою цього протоколу передається більш детальна інформація про обладнання, що спрацювало, а також може здійснюватися вилучене керування контрольною панеллю.

У якості ліній зв'язку іноді використовується Інтернет як у вигляді проводового Ethernet, так і мобільного – через GPRS. Однак не всі пульти підтримують таке підключення.

Розглянемо деякі елементи систем пожежної безпеки.

7.1.2 Панелі контрольні пожежні

7.1.2.1 Загальні зауваження

Панелі контрольні пожежні (ПКП) призначені для підключення сповіщувачів, подачі на них живлення, формування сигналу тривоги та включення необхідних пристроїв та передавання повідомлень [3].

Контрольна панель охоронно-пожежної сигналізації (інша назва контрольний прилад) призначена для приймання й обробки сигналів від датчиків. Фактично, контрольна панель це головне обладнання в системі охоронно-пожежної сигналізації (ОПС), яким визначаються функціональні можливості сигналізації. Для того, щоб вибрати контрольну панель, необхідно визначитися з основною термінологією й функціональними можливостями таких пристроїв.

Системи пожежної сигналізації містять як мінімум 2 основних компоненти – сповіщувачі здатні приймати та передавати інформацію відносно виявлення пожежі та прилади приймально-контрольні пожежні (ППКП) [3-8]. Окрім цього, такі системи можуть містити звукові та світлові оповіщувачі, модулі перетворення інтерфейсів та різноманітні пристрої розширення функціональних можливостей.

Оповіщувач – звуковий або світло-звуковий пристрій, призначений для оповіщення людей про необхідність евакуації з зон, де була виявлена пожежа.

Зона – визначена частина захищуваних приміщень, в якій встановлено один чи декілька компонентів і для якої передбачено загальну індикацію стану.

Прилади приймально-контрольні пожежні – це пристрої, завданням яких є виявлення та відповідне сповіщення та протидія пожежі. Такі пристрої здатні ефективно сприймати та аналізувати сигнали, отримані від підключених до приймально-контрольного приладу датчиків. У свою чергу, залежно від типу може не тільки сповістити про небезпеку, а й ефективно боротися з нею. Це можливо завдяки тому, що деякі моделі пожежних ППК є настільки просунутим і складним автоматизованим комплексом, що здатні подавати сигнали і керувати різними установками для пожежогасіння.

Пожежні ППК в залежності від способу підключення додаткових пристроїв можна поділити на:

- проводові;
- безпроводові.

Перевагою безпроводових пожежних ППК є можливість підключення до нього різних сповіщувачів та іншого обладнання без використання проводів та кабелів. Однак безпроводові системи мають обмежену відстань між ППКП та датчиками, що залежить від матеріалу стін будівлі, їх товщини та кількості стін між пристроями пожежної сигналізації. До того ж, на дальність та надійність зв'язку впливають електромагнітні завади, що створюються при роботі різного обладнання, електродвигунів та систем управління ними, а також при зварювальних роботах. З наведеного вище витікає, що більш надійними є проводові пожежні прилади прийому-контролю, які, у свою чергу, поділяються на [4-5]:

- адресні;
- аналогові.

Адресні пожежні приймально-контрольні прилади проводять постійний моніторинг системи, так зване опитування сповіщувачів. В результаті такого опитування пожежний адресний приймально-контрольний прилад у найкоротші терміни зможе отримати сигнал про порушення в роботі або втрату працездатності якогось із сповіщувачів, що до нього підключені. Така розвинена система моніторингу дозволяє підключати до адресного пожежного приймально-контрольного приладу велику кількість сповіщувачів, а відповідно використовувати такий вид пожежної ПКП на великих об'єктах.

Якщо говорити про аналогові, або неадресні системи пожежних ППКП, то такі пристрої здатні контролювати всього кілька шлейфів, що дозволяє використовувати їх на невеликих об'єктах.

Вибір пожежного приладу прийому-контролю (ППКП)

Для організації на об'єкті максимально ефективної пожежно-охоронної системи потрібно, при виборі пожежного приладу прийому-контролю, не лише звертати увагу на деякі тонкощі, а й заздалегідь визначитися з функціями, які покладаються на пожежно-охоронну систему об'єкта:

- розмір об'єкта – від цього показника безпосередньо залежить який тип пожежного ПКП необхідно вибрати та встановити;
- діапазон робочих температур та вологості у приміщенні, адже часом монтаж системи відбувається в умовах неопалюваного приміщення або приміщення з підвищеною вологістю повітря;
- ступінь захисту корпусу ППКП, в залежності від умов оточуючого середовища.

На ринку доступна велика кількість ППКП різних призначень, що випускаються різними виробниками. Наприклад на сайтах [7, 8] доступні ППКП Тірас, Артон, Лунь, Prime. На сайті [4] ще можна знайти ППКП Гамма, Електронмаш, Омега.

7.1.2.2 Прилади ПКП Тірас

Розглянемо, наприклад, прилади приймально-контрольні пожежні (ППКП) компанії Тірас, які випускаються у 4 модифікаціях [6, 7]:

- Тірас-4П – прилад приймально-контрольний пожежний на 4 зони;
- Тірас-8П – прилад приймально-контрольний пожежний на 8 зон;
- Тірас-16П – прилад приймально-контрольний пожежний на 16 зон;
- Тірас-16.128П – прилад приймально-контрольний пожежний на 16 зон з можливістю розширення кількості зон.

Зовнішній вигляд Тірас-16П наведено на рис. 7.1, а у відкритому вигляді – на рис. 7.2 [6].



Рисунок 7.1 – Прилад приймально-контрольний пожежний Тірас-16П [6]

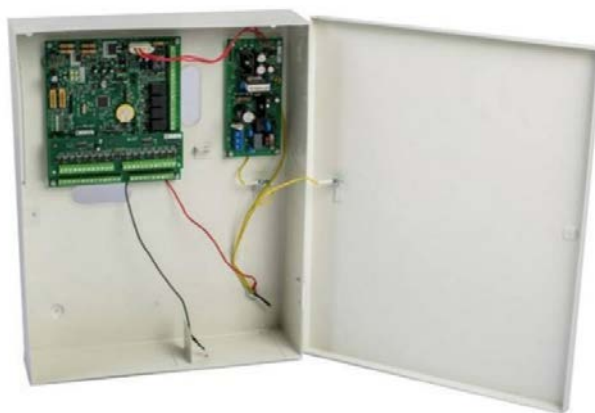


Рисунок 7.2 – Прилад приймально-контрольний пожежний Тірас-16П (зліва) та блок живлення (справа) у комутаційній шафі [6]

Прилад ППКП призначений для цілодобової централізованої пожежної охорони об'єктів та будівель, шляхом постійного контролювання шістнадцяти зон з можливістю розширення до 128 (шляхом розширення кількості зон за допомогою ППКП Тірас-4П, Тірас-8П та Тірас-16П). Прилад відповідає всім вимогам ДСТУ EN 54-2 та ДСТУ EN 54-4.

Він забезпечує безперервну цілодобову роботу в приміщеннях з регульованими кліматичними умовами при відсутності прямого впливу кліматичних факторів зовнішнього середовища, при температурі від мінус 5 до 40 °С та відносній вологості, не більше 93%.

Прилад забезпечує:

- використання пожежних сповіщувачів різних виробників та типів підключення;
- контролювання пожежних сповіщувачів та лінії їх підключення;
- 3 режими верифікації спрацювання сповіщувачів;
- керування оповіщувачами з контролюванням ліній їх підключення;
- передавання сигналів на АЗПЗ, ПУіЗ та прилади розширення;
- організацію ієрархічної системи пожежної сигналізації (СПС);
- отримання інформації від компонентів СПС (блоків живлення і т.п.);
- відображення стану приладу та режиму роботи на символному дисплеї;
- ведення журналу подій;
- автоматичну зарядку та контроль стану АКБ, автоматичний перехід на живлення від АКБ при відсутності напруги в мережі 220 В та зворотній перехід при відновленні напруги в мережі;
- передавання сигналів за допомогою додаткових модулів на ПЦПС через проводові (МЦА) та безпроводові канали зв'язку (МЦА-GSM), через локальну обчислювальну мережу (Ethernet-модуль M-NET.2 Tiras), які встановлюються додатково;
- керування, програмування та відображення інформації СПС на виносних панелях керування (ВПК);

7.1.2.3 Прилади ПКП Варта

Розглянемо ще один ППКП "Варта-1/2" Електронмаш (рис. 7.4) [8].



Рисунок 7.4 – Прилад приймально-контрольний пожежний
ППКП "Варта-1/2" Електронмаш [8]

ППКП Варта-1/2 (2 шлейфи) з GSM комунікатором – прилад приймально-контрольний пожежний. Це багатопроцесорна система збору та обробки стану пожежних шлейфів, сигналізації та керування різними вихідними сигналами.

Призначений для побудови систем пожежної сигналізації та автоматики різної складності, а також систем раннього виявлення надзвичайних ситуацій та техногенного захисту. Прилад забезпечує прийом та відображення інформації від усіх типів сповіщувачів та технологічних датчиків з подальшою передачею сигналу на виконавчі пристрої та/або спеціалізовані станції моніторингу об'єкта.

Прилад використовується лише у приміщеннях. Забороняється експлуатація пристрою у приміщеннях з агресивними домішками у повітрі, що викликають корозію.

Прилад містить:

- 4 рівнозначні шлейфи сигналізації ШС (стабілізована напруга живлення 24 В, обмеження струму 26 мА);
- два релейні виходи (у кожному реле 2 групи перемикаючих контактів 30 В 1 А постійного струму або 42 В 0,5 А змінного струму);

- один вихід "СЗО" (навантажувальна здатність 12 В 0.35 А з контролем КЗ та обриву);

- GSM комунікатор.

Кожен шлейф приладу може працювати за одним із 4 алгоритмів:

1. "Пожежний" – працюючий у двох режимах:

- без повторної перевірки – стан тривоги визначається збільшенням струму в ШС щонайменше ніж на 7 мА від поточного значення норми (при цьому значення струму має стати більше 26 мА, у цьому режимі підключаються ручні пожежні сповіщувачі;

- з перевіркою – при збільшенні струму в ШС на (2,5...7) мА від поточного значення норми видається повідомлення "Увага", відбувається автоматичне відключення живлення сповіщувачів у даному ШС на 6 с для скидання сповіщувачів, потім живлення на сповіщувачі в даному ШС подається і через 6 с і починається очікування підтвердження пожежі будь-яким станом шлейфу, відмінним від норми (спрацьовування, КЗ, обрив), а якщо протягом двох хвилин не буде підтвердження пожежі, ШС автоматично переводиться в черговий стан.

2. "Охоронний" – повідомлення "Тривога" видається при виявленні короткого замикання або обриву ШС.

- напруга живлення ШС 24 В;
- прилад зберігає працездатність ШС при опорі витоку між проводами ШС та/або між кожним із проводів ШС та "землею" не менше 50 кОм;
- прилад оцінює та видає повідомлення про зміну стану ШС при тривалості цієї зміни не менше однієї секунди та не видає при тривалості менше 100 мс;
- максимальний опір проводів пожежних ШС (без урахування опору виносних елементів) не більше 470 Ом;
- діапазон струму в колі ШС, при якому встановлюється черговий режим роботи від 5 до 17 мА;
- струм у колі ШС, який оцінюється як коротке замикання (КЗ), ≤ 26 мА.

При вимкненні живлення та зниженні напруги акумулятора нижче $10,8 \pm 0,2$ В прилад автоматично відключає ШС та переходить у стан "Несправність живлення". Зворотний перехід відбувається при подачі напруги живлення 220 В.

При зниженні напруги акумулятора до $10,5 \pm 0,2$ В акумулятор відключається.

Електроживлення приладу здійснюється від мережі змінного струму напругою 220 В та частотою 50 Гц та від акумуляторної батареї (резервного джерела) з номінальною вихідною напругою 12 В.

Потужність споживання від мережі змінного струму в черговому режимі не більше 10 ВА, максимальна не більше 50 ВА.

Акумуляторна батарея повинна бути кислотно-свинцевого типу герметична, що не обслуговується, перезаряджається з номінальною напругою 12 В і ємністю не менше 2.3 А·годин, здатна працювати в буферному режимі заряду.

Напрацювання на відмову приладу не менше 30000 годин.

7.1.2.4 Панель приймально-контрольна ОРІОН 8ТІ.2

8ТІ.2 – приймально-контрольний прилад, який використовується для побудови недорогої охоронної або пожежної сигналізації [3, 4]. Керування здійснюється за допомогою світлодіодної виносної клавіатури, яка має двоколірну індикацію. Відповідно до ситуації, управляти обладнанням можна не тільки через клавіатуру, але ще через електронні ключі моделі Touch Memory і через приймач "Оріон-Рк" [9]. Зовнішній вигляд панелі наведений на рис. 7.7, а основні параметри в табл. 7.1.



Рисунок 7.7 – Панель приймально-контрольна ОРІОН 8ТІ.2 [9]

Таблиця 7.1 – Характеристика панелі приймально-контрольної ОРІОН 8ТІ.2:

Параметр	Значення
Тип підключення	проводове
Максимальна кількість зон	8
Кількість груп	8
Кількість виходів (колекторних, релейних)	2
Напруга живлення шлейфа	12 В
Опір резистора шлейфа сигналізації	2,4...3,6 кОм
Канал комунікації	телефонна мережа
Кількість виходів сповіщення про тривогу	1
Протокол передавання даних	Міст, Селена
Програмування	через USB
Виконання	в корпусі
Клавіатура в комплекті	+
Блок живлення в комплекті	+
Touch Memory для управління	+
Напруга живлення/частота мережі	187-242 В/50 Гц
Акумулятор резервного живлення ємністю	7 А·год
Діапазон робочих температур	-5...40 °С
Габаритні розміри	125×93×33 мм
Маса	1600 г.

7.1.3 Підключення сповіщувачів

Розглянемо схеми підключення сповіщувачів на прикладі використання ППКП Тірас-16П [6]. З різними сповіщувачами виробник рекомендує схеми, що наведені на рис. 7.8 (для двопроводових сповіщувачів) та рис. 7.9 (для чотирьохпроводових сповіщувачів). Аналогічно підключаються сповіщувачі до ППКП інших виробників [6].

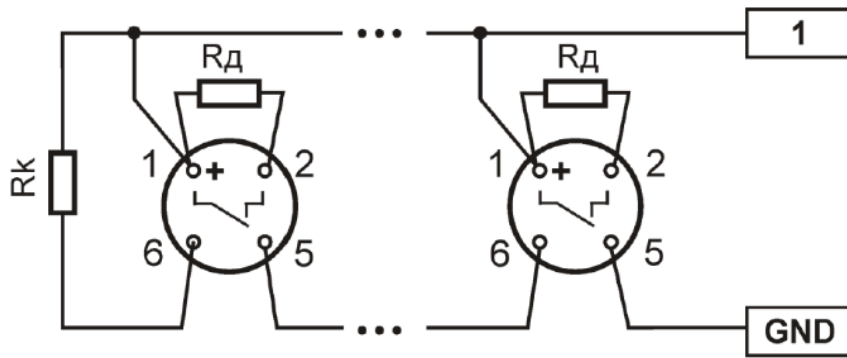


Рисунок 7.8 – Підключення двопроводових сповіщувачів до ППКП [6]

Підключення двопроводових сповіщувачів (сповіщувачі з нормально розімкненими контактами – Н.Р.) наведено на рис. 5.26. Кінцевий резистор R_k встановлюється в останньому сповіщувачі кола виявлення пожежі. Підключення сповіщувачів необхідно здійснювати через обмежуючий додатковий резистор R_d (рис. 5.26) опір якого залежить від типу сповіщувача. Опір R_d розраховується за формулою:

$$R_d = 1 \text{ кОм} - R_{\text{сп}},$$

де $R_{\text{сп}}$ – внутрішній опір сповіщувача після спрацювання (для сповіщувачів ТОВ "Тірас-12" – 560 Ом).

При використанні режиму роботи зон з верифікацією по спрацюванню двох сповіщувачів опір R_d розраховується за формулою:

$$R_d = 1,5 \text{ кОм} - R_{\text{сп}}.$$

Вибір опору резистора R_d здійснюється зі стандартного ряду номіналів, наприклад Е24: 470...820 Ом та 1 кОм.

Підключення чотирьохпроводових сповіщувачів (сповіщувачі з нормально замкнутими контактами – Н.З.) наведено на рис. 5.27. Кінцевий резистор R_k встановлюється в останньому сповіщувачі кола виявлення. Підключення здійснюється з використанням шунтуючих резисторів $R_{\text{ш}}$ номіналом 2,2 кОм, що

встановлюються на сповіщувачі, між контактами, які розмикаються при спрацюванні на сповіщувача (контакти 1 та 2 для сповіщувачів ТОВ "Тірас-12").

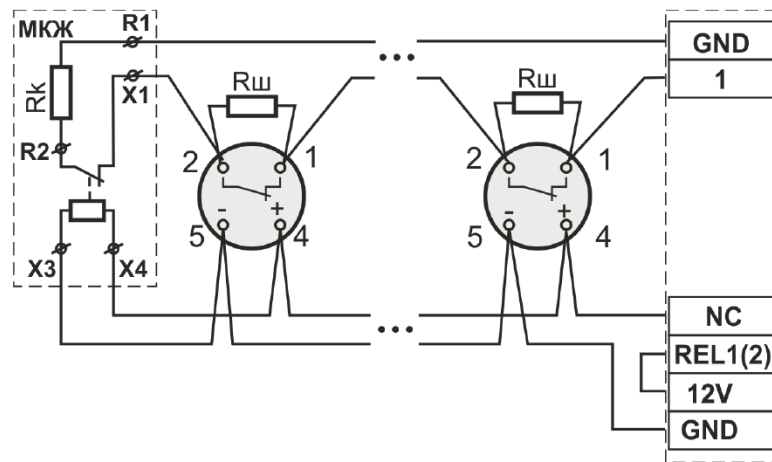


Рисунок 7.9 – Підключення чотирьохпроводових сповіщувачів з живленням від ППКП [6]

Для сповіщувачів, стан контактів реле яких не змінюється у разі вимкнення живлення, в коло живлення сповіщувачів потрібно встановити модуль контролю живлення (МКЖ). Підключення МКЖ виконувати згідно схеми на рис. 7.9 (нормально замкнутий контакт реле X1 включений в зону приладу, контакти X3, X4 необхідно підключити до виходу живлення сповіщувачів, між контактами R1 та R2 встановлюється кінцевий резистор R_k).

7.1.4 Підключення оповіщувачів

Приклади підключення оповіщувачів наведені на рис. 7.10. При живленні оповіщувачів від приладу ПКП необхідно встановити перемичку між входом USIR та виходом 12V. У випадку, коли струм споживання оповіщувачів перевищує навантажувальну здатність приладу, необхідно використовувати окреме джерело живлення для живлення оповіщувачів. При використанні оповіщувачів з низьким входним опором (наприклад, лампа розжарювання) послідовно з оповіщувачем необхідно включати діод (VD1, рис. 7.10,а) прямий робочий струм якого повинен

бути більшим за максимальний струм споживання оповісчувача. Кінцевий резистор кола виявлення оповісчувачів R_k [6].

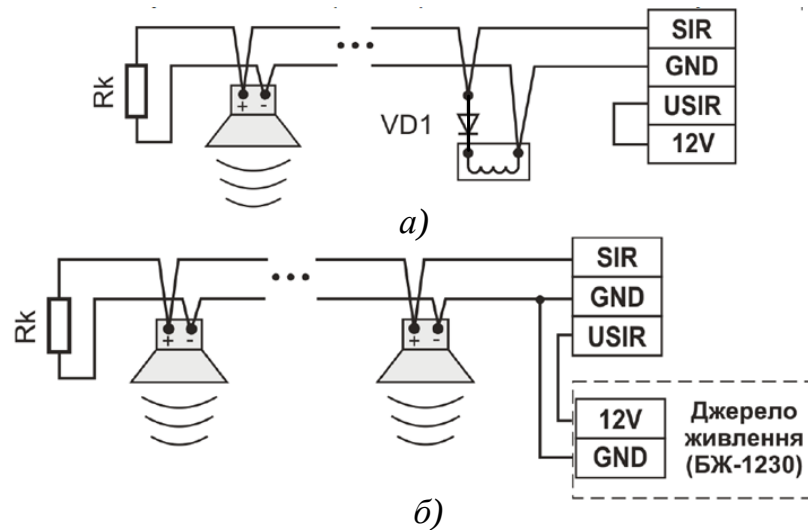


Рисунок 7.10 – Підключення оповісчувачів при живленні від ППКП (а) та при живленні від зовнішнього джерела живлення (б) [6]

7.1.5 Підключення безпроводових сповісчувачів Ajax

Для підключення безпроводових датчиків Ajax необхідно скористатись контрольними панелями цієї ж компанії [4, 10]. Компанія Ajax Systems випускає 7 типів контрольних панелей. Розглянемо деякі з них.

Контрольна панель Hub Plus

Інтелектуальна панель керування другого покоління з чотирма каналами зв'язку, новим потужним процесором, потроєним об'ємом оперативної пам'яті та подвоєною флеш-пам'яттю. Hub Plus контролює роботу всіх датчиків Ajax і миттєво сповіщає власника та охоронну компанію.

Використовує Wi-Fi, Ethernet, WCDMA та GSM для надсилання тривог на центральну станцію моніторингу та власнику системи. Надсилає сповіщення у разі відключення електроенергії та працює до 16 годин від резервної батареї.

Особливості Hub Plus:

- перевіряє працездатність датчиків кожні 12 секунд;
- автентифікація для запобігання підробці;

- виявлення завад у каналах зв'язку і шифрування повідомлень;
- сигналізація про втручання в роботу пристроїв.

Пульти керування гібридною системою безпеки Hub Hybrid

Пульт керування доступний у двох конфігураціях зв'язку – 4G і 2G.

Hub Hybrid – перша панель керування Ajax, що підтримує пристрої Jeweller і абсолютно нову лінійку продуктів Fibra. Проводові та безпроводові технології поєднуються для створення комплексного захисту незалежно від розміру об'єкта, сталевих чи бетонних перешкод. Безпеку підвищують інформативні сповіщення, фотоперевірка тривоги, контроль системи в реальному часі в додатку та сценарії автоматизації.

Особливості Hub Hybrid:

- 3 незалежних канали зв'язку;
- 8 ліній для підключення дротових пристроїв Fibra;
- перевірка фото тривоги за 9 секунд;
- до 3,5 днів роботи системи від резервного акумулятора;
- топологія кільцевого підключення проти саботажу;
- автоматизація систем безпеки.

З іншими контрольними панелями можна ознайомитись на сайті компанії [2].

7.1.6 Шлейфи сигналізації

Датчики підключаються до контрольного приладу, як правило, не окремо, а групами по кілька датчиків у кожній [10]. Одна група датчиків називається шлейфом. Фактично, шлейф це пара проводів під'єднаних до двох контактів на контрольній панелі, до яких підключаються кілька датчиків. Одна з характеристик контрольної панелі – це кількість контрольованих шлейфів. Призначення шлейфів може задаватися при програмуванні контрольної панелі, а може бути фіксованим [4-9].

Шлейф із затримкою для систем охоронної сигналізації

Якщо для зняття системи з охорони необхідно потрапити усередину охоронюваної зони, потрібно забезпечити, щоб сигналізація спрацьовувала з деякою затримкою, наприклад, при вході через двері, однак при проникненні через вікно або спрацьовуванні пожежного датчика сигналізація повинна включатися негайно. Для цього датчики, відповідальні за контроль входу, підключаються на окремий шлейф, який програмується на затримку спрацьовування, достатню для зняття системи з охорони.

24-годинна та інші зони

Датчики розбиття скла або руйнування стіни має сенс ніколи не знімати з охорони. Для цього їх можна підключити на окремий шлейф, що перебуває під охороною завжди. Крім того, на цей шлейф необхідно підключити тампери всіх датчиків, щоб зловмисники не могли знешкодити сигналізацію, коли вона знята з охорони (тампер – це спеціальний вимикач, що спрацьовує при спробі зняття датчика або розкриття його корпусу, їм обладнано багато охоронних датчиків). Датчики відкриття дверей можуть включатися в роботу за розкладом (наприклад у неробочий час). Для цього використовують різні шлейфи.

Живлення по шлейфу

Практично всі датчики, крім герконів, вимагають зовнішнього живлення. Датчики діляться на двопроводові й чотирьохпроводові. Живлення чотирьохпроводових датчиків здійснюється від окремого джерела живлення напругою 12 В (може бути і інша напруга живлення). Більшість пожежних датчиків і багато охоронних є двопроводовими, живлення яких здійснює охоронна панель по одній парі проводів.

Охоронні й пожежні шлейфи

Крім того, що пожежний шлейф ніколи не повинен зніматися з охорони, пожежний шлейф відрізняються від охоронного принципом сигналізації про спрацьовування. Охоронні датчики є нормально замкненими, тобто, у звичайному стані пари контактів, до яких підключається шлейф, замкнена, а при спрацьовуванні датчика відбувається розмикання (рис. 7.11).

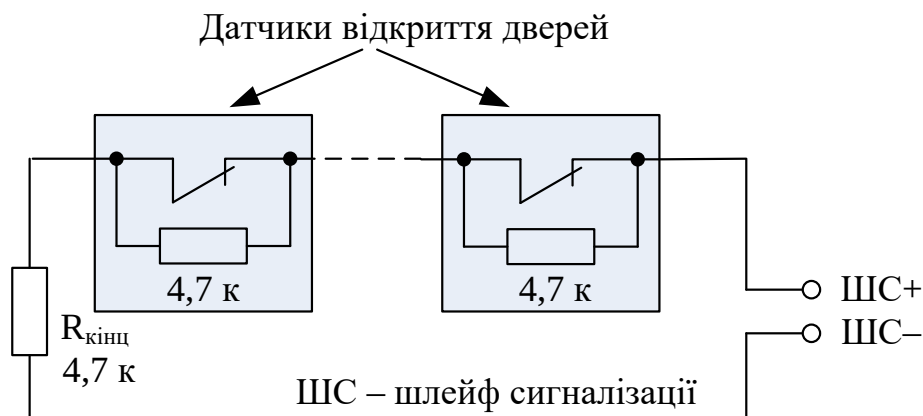


Рисунок 7.11 – Підключення охоронних датчиків до шлейфу

Якщо опір в нормальному стані (всі датчики мають замкнені контакти) дорівнює 4,7 кОм, то при спрацьовуванні одного з датчиків опір шлейфа буде становити 9,4 кОм. Якщо ПКП розрахована на спрацьовування одного датчика, то при такому опорі шлейфа буде сформовано сигнал тривоги. Можна налаштувати панель так, щоб спрацьовування було при розмиканні контактів двох датчиків – при опорі шлейфа 14,1 кОм. Опір резисторів може бути іншим (це залежить від типу датчика).

Кінцевий резистор ($R_{\text{кінц}}$) потрібен для того щоб контролювати стан шлейфа. Якщо буде обрив проводу, то опір шлейфу зростає до нескінченності і це є ознакою несправності. Аналогічно, ознакою несправності буде коротке замикання шлейфу.

Контакти пожежних датчиків нормально розімкнуті (рис. 7.12), а при спрацьовуванні датчика відбувається збільшення споживаного струму (але не замикання, що буде несправністю). Тому охоронні датчики включаються в шлейф послідовно; спрацьовування одного датчика або обрив лінії розімкне шлейф і спрацює тривога. Пожежні датчики включаються в шлейф паралельно.

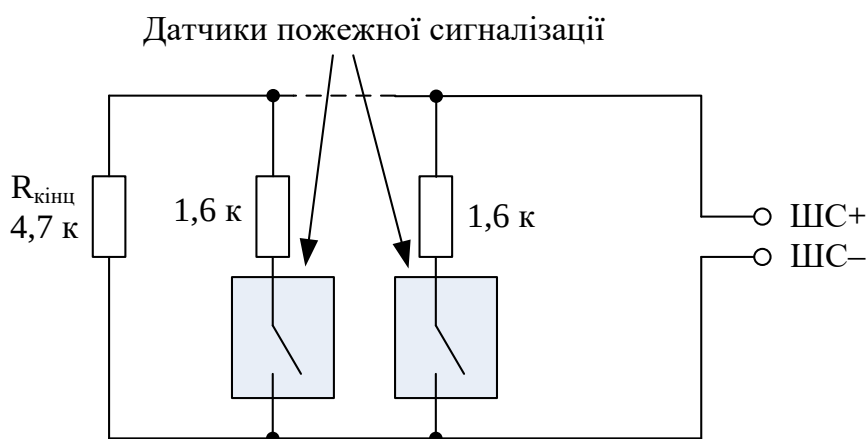


Рисунок 7.12 – Підключення пожежних датчиків до шлейфу

На рис. 7.13 наведено фото димового двоточкового сповіщувача Артон СП-2.1 [11, 12].

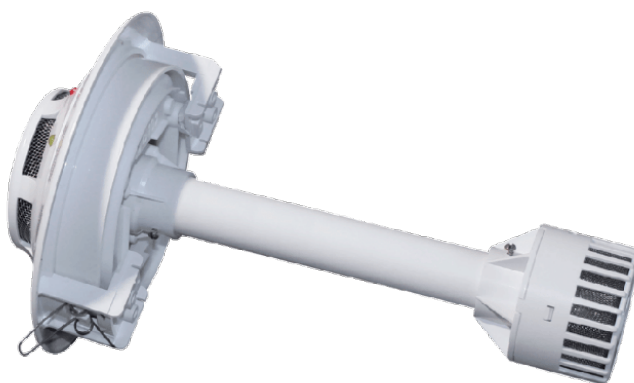


Рисунок 7.13 – Димовий двоточковий сповіщувач Артон СП-2.1 [11]

Схему підключення датчика диму СП-2.1 з живленням постійним струмом від шлейфу до контрольних панелей наведено на рис. 7.14 [11]. Опір резистора $R_{ок}$ зумовлюється типом ППК і може варіюватися в межах від 1 до 10 кОм.

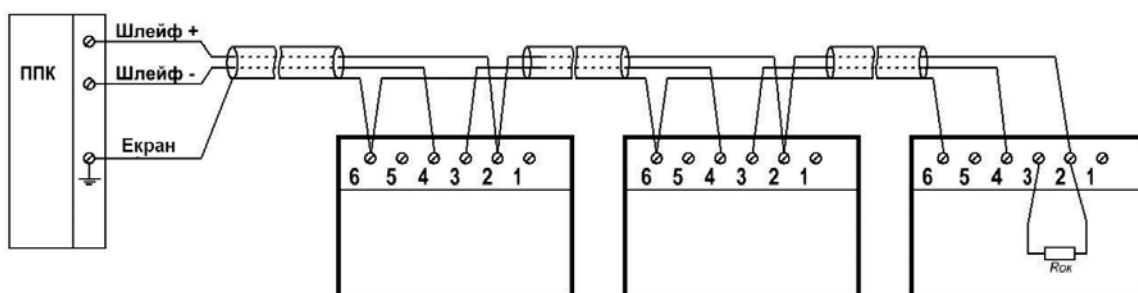


Рисунок 7.14 – Схема підключення сповіщувачів СП-2.1 до шлейфу з живленням постійним струмом від шлейфу [11]

На рис. 7.15 наведено схему підключення датчика диму СП-2.1 з зовнішнім пристроєм оптичної сигналізації (світлодіод VD1) з живленням постійним струмом від шлейфу.

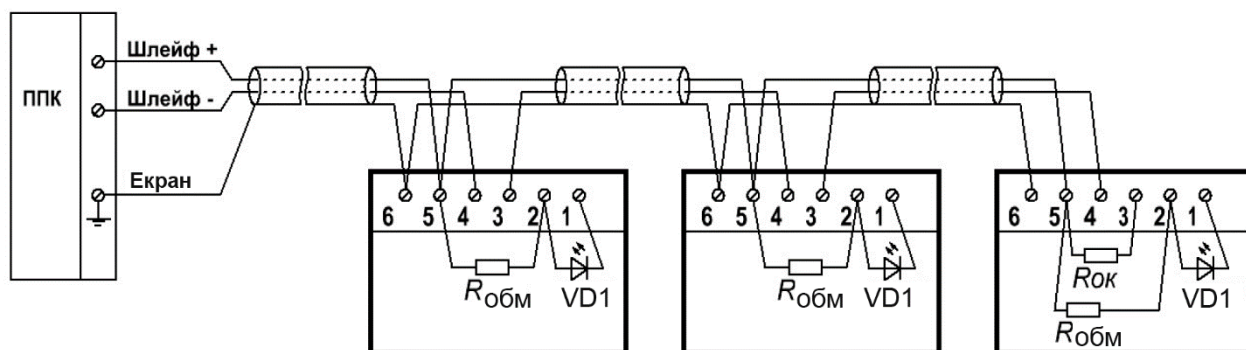


Рисунок 7.15 – Схема підключення сповісвачів СП-2.1 з зовнішнім пристроєм оптичної сигналізації до шлейфу з живленням постійним струмом від шлейфу [11]

Величина $R_{ок}$ залежить від типу ППК (діапазон припустимих значень від 1 до 10 кОм). Величина $R_{обм}=1,5$ кОм для напруги живлення шлейфу сигналізації (ШС) $U_{шс} = 24$ В. Для $U_{шс} = 15$ В $R_{обм}= 0,68$ кОм, а для 12 В – 0,36 кОм.

Чотирьохпроводові датчики підключаються до шлейфів сигналізації за схемою, що наведена на рис. 7.16. На рисунку наведено підключення не тільки датчиків пожежі чи безпеки, а і магнітно-контактний датчик (ДМК) на основі геркону. Як тільки двері в приміщення, де знаходиться контрольна панель, відкриваються, спрацьовує системи затримки спрацьовування шлейфа (щоб встигнути відключити сигналізацію). Якщо сигналізація не буде відключена, то спрацьовує сигналізація і формується сигнал тривоги.

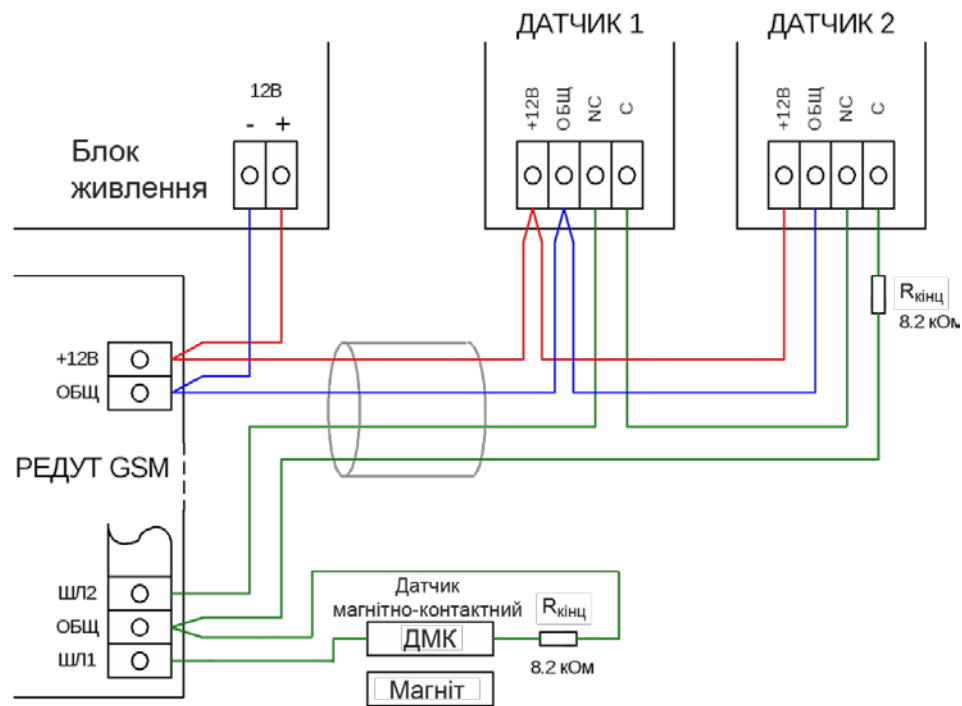


Рисунок 7.16 – Схема підключення чотирьохпроводового датчика

7.2 Системи контролю доступу

Система контролю доступу (СКД) – комплекс програмно-апаратних засобів, за допомогою яких можна дозволити / заборонити вхід і вихід через двері, турнікети, певному колу людей, а також контролювати пересування цих людей. Такі системи мають і іншу версію назви – системи контролю та управління доступом (**СКУД**) [14].

Системи контролю та управління доступом (СКУД, СКД) є ефективним рішенням для обмеження доступу в приміщення небажаних осіб, зручного і легкого надання фізичного доступу та адміністративного моніторингу подій проходів дозволеними особами, контролю трудової дисципліни і порядку співробітників.

СКУД розрізняються за ідентифікаторами, "ознаками" доступу. Найбільш популярні на сьогоднішній день є системи з наступними "ознаками доступу": безконтактної карти, відбитком пальця, радіобрелком. Однофакторні системи доступу дозволяють отримувати доступ тільки по карті, відбитку пальця, паролю, радіобрелку. Двохфакторні, трьохфакторні системи доступу дозволяють проводити

багатофакторну ідентифікацію доступу (карта + відбиток пальця, ПІН + відбиток пальця, карта або відбиток пальця + ПІН код та ін.) Останнім часом в якості ідентифікаторів стали використовувати радіочастотні мітки.

Контроль доступу одна з найскладніших, але в той же час одна з найбільш **функціональних систем безпеки, яка може реалізувати велику кількість різних функцій:**

- **облік робочого часу (контроль робочого часу)** – реєстрація часу приходу робочого персоналу на роботу і уходу, а також перебування на робочому місці;
- **управління точками проїзду автотранспорту** – фіксація проїзду автотранспорту на територію, ідентифікація і розпізнавання номерів автомобіля, реєстрація тривалості стоянки;
- **контроль проходження заданого маршруту** – можливість простежити шлях руху та місцезнаходження конкретної людини в означений момент часу з складанням карти переміщення;
- **контроль доступу** – безпосередньо дозвіл/заборона пересування по об'єкту, забезпечення санкціонованого доступу.

Крім того система контролю доступу дозволяє керувати різними пристроями, видавати звіти, зберігати базу даних працівників.

Основні елементи системи контролю і керування доступом:

- контролер системи доступу;
- зчитувач;
- термінал: контролер і зчитувач в одному корпусі;
- замок (електромагнітний замок або електромеханічний замок – служать для утримання дверей у закритому стані, керуються контролером);
- ідентифікатор (клавіатура, безконтактна картка, ключ, брелок, радіочастотна мітка, зчитувач відбитків пальців та ін.);
- турнікети (забезпечують пропуск по одній карті тільки однієї людини), хвіртка, шлагбаум;
- кнопки виходу;

- блоки живлення (забезпечують живленням основні елементи системи контролю доступу, зазвичай 12 В DC);
- доводчики (служать для примусового закриття дверей);
- геркони (формують сигнал стану дверей – відкрито/закрито);
- формувачі звукових сигналів (сповіщувачі тривожних ситуацій – невчасно закриті двері, злом дверей, злом терміналу і т.д.);
- програмне забезпечення: адміністрування системи, моніторинг у реальному часі, облік робочого часу.

Найпростіша система контролю доступу може бути побудована на замку або защібці і контролері з вбудованим зчитувачем. Більш складний і функціональний контроль доступу може бути об'єднаний в локальну мережу, управлятися за допомогою комп'ютера з відповідним програмним забезпеченням аж до організації контролю доступу з інтеграцією відеоспостереження та охоронної сигналізації.

Контролер – пристрій для управління замками. Дані що зчитуються з ідентифікаторів (ключів таблеток, карток тощо), порівнюються з даними, записаними в пам'ять, і за результатами порівняння формується сигнал відмикання або заборони відмикання дверей.

Зчитувач – пристрій передачі сигналу від ідентифікатора на контролер. Зчитувач може бути у вигляді клавіатури з кнопками для набору коду, може бути і комбінованим – клавіатура плюс зчитувач.

Ідентифікатори виконуються у вигляді карток, ключів-таблеток, брелків, іграшок, браслетів, годинників, наклейок і т.д.

Доводчики дверей – для закриття та керування станом дверей. Розрізняються способами закриття та утримання (зусилля утримання 40...400 кг).

Замок призначено для утримання дверей у закритому положенні. Використовуються замки декількох типів: механічні, магнітні, засувки і ригельні.

7.3 Контролери систем доступу

Контролер є основною ланкою системи контролю доступу. Контролери системи доступу відрізняються як зовні, так і функціонально. Найпростіші мають мінімальний, але достатній набір можливостей, необхідних для організації поділу прав доступу на об'єкті. Контролери системи доступу даного типу здатні запам'ятати кілька сотень ідентифікаторів, мають можливість підключення двох зчитувачів і одного виконавчого пристрою (турнікета, замку). Деякі з них мають вбудовану клавіатуру або зчитувач [15].

Більш складні контролери здатні запам'ятати кілька десятків, а в деяких випадках і сотень тисяч користувачів, можуть об'єднуватися в мережу і керуватися за допомогою спеціалізованого ПЗ. З їх допомогою можна організувати контроль доступу на великих об'єктах (заводах, навчальних установах, банках, аеропортах та ін.) з великим набором функцій: облік робочого часу, контроль проходження заданого маршруту, фотоідентифікація, управління паркінгом.

Деякі приклади контролерів [15-17] доступу наведено в табл. 7.2.

Окрім контролерів на одні двері (як автономних, так і мережевих) випускаються контролери на 2 та 4 двері (рис. 7.17) [15].

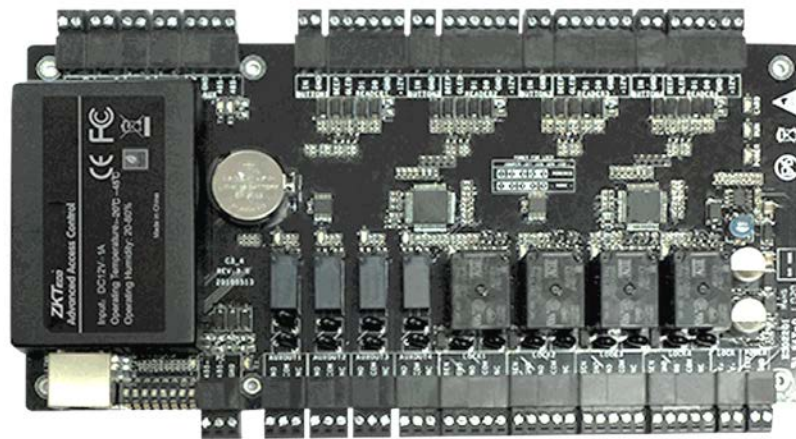


Рисунок 7.17 – Мережевий контролер доступу на 4 двері С3-400 [15]

Контролер доступу С3-400 підтримує:

- роботу з безкоштовним програмним забезпеченням ZKAccess 3.5;

- мережевий режим роботи по протоколу TCP / IP (Ethernet);
- розширений контроль доступу для управління 4 дверима або 2 турнікетами;
- роботу зі зчитувачами безконтактних карт по інтерфейсу Wiegand.

Таблиця 7.2 – Основні характеристики контролерів доступу

Тип	Параметри	Ціна, грн.
	Мережевий контролер CnM Secure Gate D1S2.NET Мережний IP контролер доступу D1S2.NET призначений для організації контролю доступу на 1 двері [5]. Налаштування й керування проводиться за допомогою ПО Cnm Secur Gate. У мережі може використовуватися необмежена кількість контролерів з можливістю дистанційного доступу. При пропаданні зв'язку із сервером, події зберігаються в пам'яті контролера. З появою мережі події можна вивантажити на сервер. Зберігання даних здійснюється в базі MS Access або MS SQL. Докладніше: https://nadzor.ua/product/cnm-secure-gate-d1s2net	3192
	Мережевий контролер Tecsar Trek T12-rs Мережний контролер Tecsar Trek T12-rs призначений для організації проходів через 1 двері, використовуючи комбінацію: зчитувач – зчитувач / зчитувач – кнопка [6]. При установці двох зчитувачів на точку проходів можна вести облік робочого часу й контроль трудової дисципліни. Крім того, контролер може управляти електромагнітними, електромеханічними замками або електромеханічними засувками. Відмінною рисою даного мережного контролера є простота налаштування. Вона проводиться через програмне забезпечення Tecsar Trek. Контролер працює з базами даних Access, MS SQL. Для підключення зчитувачів і клавіатур використовується інтерфейс Wiegand 26/34 біт, а для встановлення зв'язку контролерів у мережі – RS-232/RS-485. Можливо з'єднання з комп'ютером (сервером), при наявності конвертера RS-485 - USB. Докладніше: https://nadzor.ua/product/tecsar-trek-t12-rs	2240

Продовження табл. 7.2.

	Комплект автономної СКД на 1 двері Готовий комплект для організації контролю доступу на одні двері [7]. У комплект входить усе необхідне устаткування й інструкції для налаштування й монтажу. В основі системи лежить автономний контролер Tecsar Trek SA-TS21 із вбудованим зчитувачем проксі-карт і клавіатурою. Корпус антивандальний металевий, клас захисту IP65. Встановлюється панель зовні й усередині приміщення, наприклад, у бізнес центрах, розважально-торговельних центрах, магазинах, складах і т.п. Вхід у приміщення може здійснюватися: по паролю або за допомогою проксі-карти. У комплект поставки входить 5 ключів-брелоков Tecsar Trek Em- Marine. Для виходу із приміщення служить алюмінієва кнопка виходу Tecsar Trek AK-2RB, яка встановлюється зі зворотної сторони дверей. За фізичне блокування дверей відповідає електроригельний замок Yli Electronic YB-100S, який утримує двері в закритому стані до розблокування за допомогою контролера. Докладніше: https://nadzor.ua/product/komplekt-avtonomnoj-sk-d-no4-na-1-dver	2918
	Комплект автономної СКД №1 на 1 двері Самий бюджетний набір для організації контролю доступу на одні двері. У комплект входить усе необхідне устаткування й інструкції для налаштування й монтажу. В основі системи лежить автономний контролер Yli Electronic YK-168N із вбудованим зчитувачем проксі-карт і кодовою клавіатурою. Корпус обладнання виготовлений із пластику. Встановлюється панель усередині приміщення, наприклад, у бізнес центрах, розважально-торговельних центрах, магазинах, складах і т.п. Вхід у приміщення може здійснюватися: по паролю або за допомогою проксі-карти. У комплект поставки входить 5 ключів-брелків Tecsar Trek Em- Marine 1,6 мм. Для виходу із приміщення служить кнопка виходу Atis Exit-Kio, яка встановлюється зі зворотної сторони дверей. За фізичне блокування дверей відповідає електромагнітний замок Tecsar Trek EL-180, який утримує двері в закритому стані із силою до 180 кг, до розблокування за допомогою контролера. Докладніше: https://nadzor.ua/product/komplekt-avtonomnoj-sk-d-no1-na-1-dver	2611

7.4 Різновиди систем СКУД

Враховуючи загальні технічні вимоги та методи випробувань, СКУД підрозділяються [14]:

- за способом управління;
- числу контрольованих точок доступу;
- функціональними характеристиками;
- виду об'єктів контролю;
- рівню захищеності системи від несанкціонованого доступу.

Всі СКУД діляться на чотири класи.

СКУД 1-го класу – малофункціональні системи малої місткості, що працюють в автономному режимі і здійснюють допуск всіх осіб, які мають відповідний ідентифікатор. У такій системі використовується ручне або автоматичне керування виконавчими пристроями, а також світлова або / та звукова сигналізація.

СКУД 2-го класу – багатфункціональні системи. Вони можуть бути однорівневими і багаторівневими і забезпечують роботу, як в автономному, так і в мережевому режимах. Допуск осіб (груп осіб) може здійснюватися за датою, тимчасовими інтервалами. Система здатна забезпечити автоматичну реєстрацію подій і автоматичне керування виконавчими пристроями.

СКУД 3-го і 4-го класів, як правило, є мережевими. У них використовуються більш складні ідентифікатори і різні рівні мережевої взаємодії (клієнт-сервер, інтерфейси зчитувачів карт Віганда або магнітних карт, спеціалізовані інтерфейси та ін.)

На рис. 7.18 наведені складові елементи системи контролю і управління доступом [19].



Рисунок 7.18 – Складові елементи системи контролю і управління доступом [19]

Існує дуже багато різновидів СКУД різних виробників, а також її компонентів. Незважаючи на унікальність кожної конкретної системи контролю доступу, вона містить 4 основні елементи: ідентифікатор користувача (карта-перепустка, ключ), пристрій ідентифікації, керуючий контролер і виконавчі пристрої. Загальна схема СКУД показана на рис. 7.19.

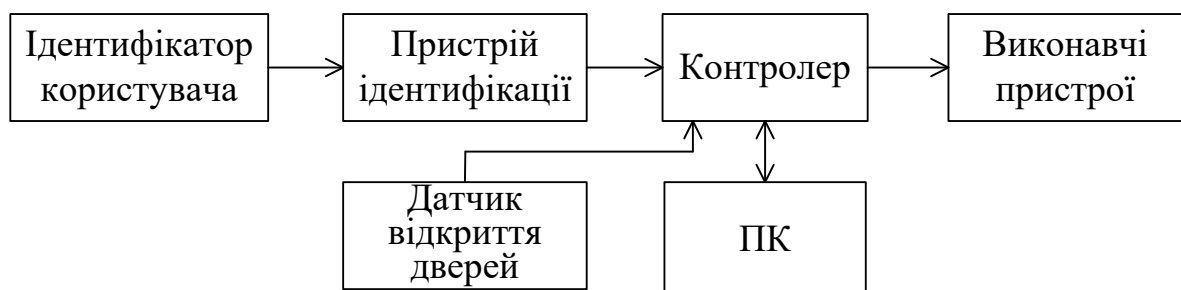


Рисунок 7.19 – Загальна структурна схема СКУД

Роботу системи контролю та управління доступом можна в спрощеному вигляді описати таким чином. Кожен співробітник або постійний відвідувач організації отримує ідентифікатор (електронний ключ) – пластикову картку або брелок, в якому міститься індивідуальний код. Електронні ключі видаються в результаті реєстрації перерахованих осіб за допомогою засобів системи. Паспортні дані, фото (відеозображення) і інші відомості про власника електронного ключа заносяться в персональну електронну картку. Персональна електронна картка власника й код його електронного ключа зв'язуються один з одним і заносяться в спеціально організовані комп'ютерні бази даних.

Біля входу в будівлю або в приміщення, яке підлягає контролю встановлюються зчитувачі, які зчитують з карток їх код та інформацію про права доступу власника картки і передають цю інформацію в контролер системи.

У системі, кожному коду поставлена у відповідність інформація про права власника картки. На основі зіставлення цієї інформації і ситуації, при якій була пред'явлена картка, система приймає рішення: контролер відкриває або блокує двері (замки, турнікети), переводить приміщення в режим охорони, включає сигнал тривоги і т. д. Всі факти пред'явлення карток і пов'язані з ними дії (проходи, тривоги і т. д.) фіксуються в контролері і зберігаються в комп'ютері. Інформація про події, що викликані пред'явленням карток, може бути використана в подальшому для одержання звітів по обліку робочого часу, порушень трудової дисципліни та ін. На підприємствах можна виділити чотири характерні точки контролю доступу: прохідні, офісні приміщення, приміщення особливої важливості, і в'їзд / виїзд автотранспорту.

Залежно від способу перевірки прийнято розрізняти кілька видів СКУД:

- ручні (визначення істинності особи здійснюється контролером на основі пред'явленої перепустки з фотографією власника);
- механізовані (фактично та ж ручна перевірка з елементами автоматизації зберігання і пред'явлення перепусток);

- автоматизовані (ідентифікація користувача і перевірка особистісних атрибутів здійснюється електронним автоматом, а аутентифікація та прийняття рішення про надання доступу проводиться оператором КПП);

- автоматичні (вся процедура перевірки та прийняття рішення здійснюється комп'ютером).

При виборі структури системи і її апаратури, необхідно приділяти особливу увагу ретельному аналізу її характеристик. До основних характеристик СКУД відносяться:

- вартість;
- надійність функціонування;
- швидкодія;
- час реєстрації користувача;
- ємність пам'яті;
- стійкість до зловмисних дій;
- ймовірність помилкового відхилення законного користувача (помилки 1-го роду);
- ймовірність помилкового надання доступу незаконному користувачеві (помилки 2-го роду).

7.5 Приклади побудови функціональної схеми системи безпеки та пожежної сигналізації

Для побудови функціональної схеми системи безпеки та пожежної сигналізації потрібно знати не тільки склад систем, а ще необхідно знати які інтерфейси зв'язку є у обраних приймально-контрольних панелях та контролерах СКУД.

На рис. 7.20 наведено приклад такої системи. До її складу входять:

- сповіщувач пожежний тепловий ИПК-7 "Прем'єр" – 12 шт. (<https://firmarion.com/products/spovischuvach-pozhezhnij-teplovij-ipk-7-premer>);

- сповіщувач пожежний диму ИПК-8 – 12 шт. (<https://ohrana.ua/datchiki/dymovoy-pozharnyy-datchik-spd-32-nz.html>);
- сповіщувач пожежний ручний ИПР-1 – 2 шт. (<https://ohrana.ua/datchiki/ipr-1-ip-54-izveshchatel-pozharnyy-ruchnoy.html>);
- сирена звукова С-03-12 – 2 шт. (<https://ohrana.ua/sireny/c-03-12.html>);
- контролер доступу Z-5R NET/8000 – 1 шт. (<https://control.ua/ua/iron-logic-z-5r-net-8000.html>);
- кнопка виходу СКУД YLI ISK-841A – 1 шт. (<https://securitylab.com.ua/yli-electronic-isk-841a/>);
- замок YLI ELECTRONIC YM-180N – 1 шт. (<https://worldvision.com.ua/yli-electronic-ym-180n-led/>);
- зчитувач ROSSLARE AY-CR11W – 1 шт. (<https://klaster.ua/ua/shop/kontrol-dostupa/schityvateli/schityvateli/schityvatel-rosslare-ay-sr11w-ros-aycr11w/>);
- датчик відкриття магнітоконтатний Алай COMK 3-4 (ІО 102-10-4) – 1 шт. (<https://ohrana.ua/uk/datchik-otkritiya-magnitno-kontaktuiy-alay-somk-3-4-io-102-10-4.html>);
- блок живлення SVS-12A3 12 В/3 А – 1 шт. (<https://ohrana.ua/uk/blok-pitaniya-svs-12a3-12-v-3-a.html>).

Всі сповіщувачі пожежної сигналізації мають двопроводове підключення і напругу живлення 12 В.

Система, що наведена на рис. 7.20 дозволяє здійснювати контроль доступу до однієї двері, контроль стану пожежної безпеки у декількох приміщеннях з використанням датчиків диму та теплових датчиків.

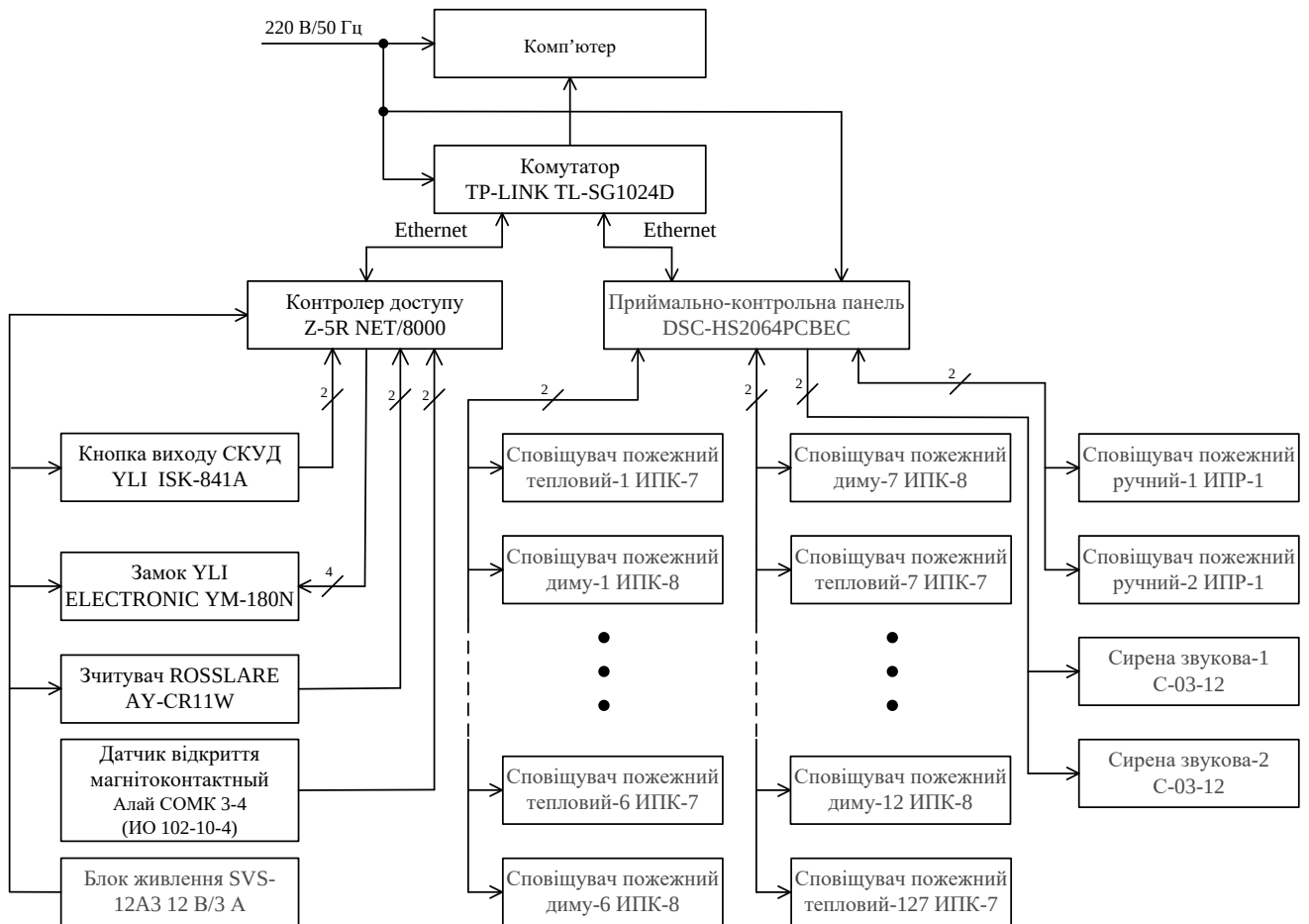


Рисунок 7.20 – Приклад функціональної схеми системи контролю доступу та пожежної сигналізації

Контрольні питання

1. Для чого призначені панелі приймально-контрольні
2. Що означає поняття зона?
3. Яка різниця у підключенні датчиків безпеки та пожежних датчиків до шлейфу?
4. Чим відрізняється підключення датчиків двопроводових від чотирьохпроводових?
5. Як здійснюється живлення датчиків пожежної та охоронної сигналізації?
6. Чи є різниця у підключенні живлення до двопроводових та чотирьохпроводових датчиків?
7. Які датчики повинні працювати у 24-годинній зоні?
8. Яким чином може передаватись оповіщення при тривозі?

9. Які функції виконують системи контролю та управління доступом?
10. Що входить до складу найпростішої системи СКУД?
11. Які функції виконують контролери СКУД?
12. Які ідентифікатори користувача вам відомі?

Перелік посилань

1. Пожежна сигналізація: все про проектування, монтаж та обслуговування. Url: <https://uep.dn.ua/posts/pozezna/uk/vklucat-pozezna-signalizacia-vse-pro-proektuvanna-montazu-ta-obslugovuvanna.php>. (дата звернення: 1.03.2024).
2. Функції та види систем пожежної сигналізації. Url: <https://ista.ua/information/funksii-ta-vydy-sps/>. (дата звернення: 1.03.2024).
3. Прилади приймально-контрольні пожежні. Url: <https://antifire.ua/ppkp/>. (дата звернення: 1.03.2024).
4. Пожежні приймально-контрольні прилади. Url: <https://worldvision.com.ua/ru/pozharnye-ppk/>. (дата звернення: 25.02.2024).
5. Приймально-контрольні прилади (ППК). Url: <https://shop-security.com.ua/rU/pozharnaya-signalizaciya/prybyory-ppk/> (дата звернення: 1.03.2024).
6. ППКП ТИРАС 16П. Url: <https://secur.ua/ppkp-tiras-16p.html>_(дата звернення: 1.03.2024).
7. Пожежний приймально-контрольний прилад на 4 неадресні зони. Тірас-4П. Url: <https://tiras.technology/products/tiras-4p/>. (дата звернення: 1.03.2024).
8. ППКП СКБ Електронмаш – Варта-1/2 (2 шлейфи) з телефонним комунікатором для пожежної сигналізації. Url: <https://www.bezpeka-shop.com/product/varta-1-2/>. (дата звернення: 1.03.2024).
9. Прилад приймально-контрольний охоронний "ОПІОН-4Т.2", "ОПІОН-4ТІ.2". Url: https://tiras.technology/wp-content/uploads/2022/09/or4ti2-4t2_ke.pdf. (дата звернення: 10.03.2024).
10. Професійна система безпеки. Url: <https://ajax.systems.ua/> (дата звернення: 1.03.2024).

11. Класифікація пожежних сповіщувачів. Url: <https://ista.ua/information/klasyfikatsiia-pozhezhnykh-spovishchuvachiv/>. (дата звернення: 1.03.2024).
12. Димовий двоточковий сповіщувач Артон СП-2.1. Url: <https://fire-stop.com.ua/ua/alarm/smoke-detectors/arton-spd21.html>. (дата звернення: 10.03.204).
13. Артон паспорт МЦИ 425239.001 ПС. Url: <https://fire-stop.com.ua/download/passport-arton-sp2.1.pdf>. (дата звернення: 10.03.204).
14. Системи контролю і управління доступом від А до Я. Url: <https://deps.ua/ua/knowegable-base/reference-information/7824.html> (дата звернення: 1.03.2024).
15. Мережевий контролер доступу на 4 двері СЗ-400. Url: <https://zktecoua.com.ua/products/setevoj-kontroller-dostupa-na-4-dveri-s3-400/>. (дата звернення: 10.03.204).
16. Мережевий контролер CnM Secure Gate D1S2.NET на 1 двері. Url: <https://nadzor.ua/uk/product/cnm-secure-gate-d1s2net>. (дата звернення: 10.03.204).
17. Мережевий контролер Tecsar Trek T12-rs. Url: <https://nadzor.ua/uk/product/tecsar-trek-t12-rs>. (дата звернення: 10.03.204).
18. Комплект автономної СКД №4 на 1 двері. Url: <https://nadzor.ua/product/komplekt-avtonomnoj-sk-d-no4-na-1-dver> (дата звернення: 1.03.2024).
19. Система контролю доступом. Url: <http://itnet.kg/service/sistema-kontrolja-dostupom/> (дата звернення: 1.03.2024).

8 ТЕХНОЛОГІЯ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

8.1 Технологія радіочастотної ідентифікації

8.1.1 Загальні зауваження

Метод автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів передаються (зчитуються або записуються) дані, що зберігаються в радіочастотних мітках (інші назви міток це транспондери або RFID-мітки) називається радіочастотною ідентифікацією (RFID – від англ. Radio Frequency Identification) [1-3].

Ця технологія автоматичної ідентифікації, що дозволяє автоматизувати процеси збору та обробки інформації безконтактним способом. Технологія використовується, щоб ідентифікувати, простежити, розсортувати і виявити необмежену кількість об'єктів, включаючи людей, тварин, документи, транспортні засоби, одяг, контейнери і т.д. Технологія також може бути використана для автоматизації технологічних та інших виробничих процесів у промисловості, автоматизації систем управління, організації систем контролю доступу та систем безпеки, для контролю та обліку робочого часу, для побудови логістичних систем, для захисту товарів та документів від підробок і в багатьох інших додатках.

Для забезпечення роботи системи радіочастотної ідентифікації не потрібно ні контакту зі зчитувачем, ні прямої видимості зчитувача на відміну від систем з використанням штрих-кодів та магнітних карт. Надійна робота гарантована при роботі в агресивному середовищі і несприятливих кліматичних умовах [1...4].

Розглянемо найпростішу схему радіочастотної ідентифікації, що складається з двох основних компонентів:

1. Зчитувач або рідер.
2. Мітка (тег від англ. Tag) – носій інформації. Як правило мітка включає приймач, передавач, антену і блок пам'яті для зберігання інформації.

Антенa зчитувача випромінює електромагнітні хвилі, а антенa мітки приймає ці хвилі і за рахунок прийнятого сигналу здійснюється живлення пасивної мітки. В

результаті чого мітка активізується і передає інформацію зчитувачу. Основні компоненти тегу (мітки) – інтегральна схема (чіп), що керує зв'язком зі зчитувачем і антена. Чіп має пам'ять, яка зберігає ідентифікаційний код або інші дані. Немає потреби в контактній або прямій видимості між зчитувачем і міткою. Мітки можуть бути приховані усередині тих об'єктів, які підлягають ідентифікації.

На рис. 8.1 наведена функціональна схема системи зчитувач – мітка.

Зчитувач складається з двох вузлів – передавача та приймача. Передавач посилає сигнал запиту для кожної мітки окремо, знаючи код мітки. Сигнал запиту через модулятор, що формує сигнал запиту для мітки на високій частоті, через атенюатор, підсилювач потужності (ПП) та смуговий фільтр (СФ) надходить в антену. Оскільки у зчитувачі використовується одна антена, то для розділення сигналів передавача та приймача використовується розщеплювач.

Антену передавача випромінює електромагнітні хвилі, які надходять до антени мітки. Сигнал з виходу антени надходить на випрямляч, який формує на своєму виході напругу живлення для чіпа мітки, який містить теж приймач і передавач, а окрім того вузол пам'яті і вузол управління або мікроконтролер.

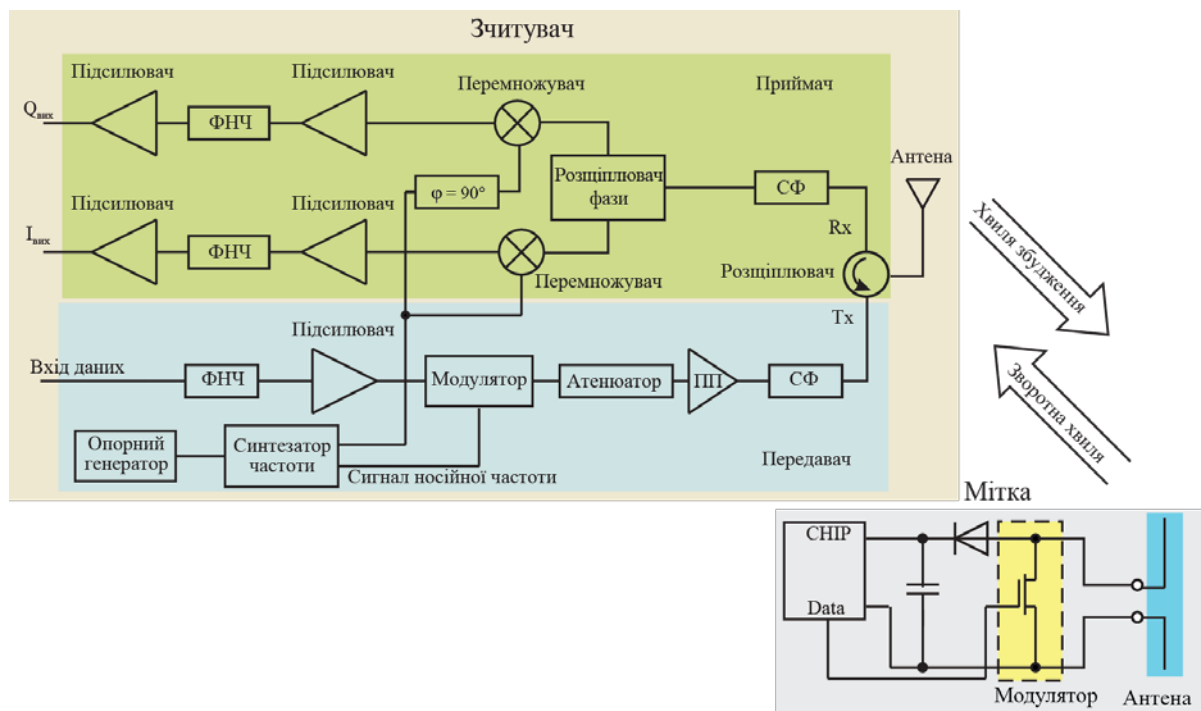


Рисунок 8.1 – Найпростіша система радіочастотної ідентифікації

Отримавши сигнал від зчитувача мітка генерує сигнал відповіді, (використовуючи дані записані в пам'яті мітки) і подає його на модулятор, з виходу якого сигнал відповіді надходить в антену мітки. Всі пристрої мітки мають наднизьке енергоспоживання – одиниці мкВт.

Сигнал приймається антеною зчитувача і через смуговий фільтр знаходить на демодулятор, що складається з розщеплювача фази, двох перемножувачів і фазообертача на 90 градусів. На виході демодулятора формуються дві складові, зсунуті по фазі на 90 градусів, які через підсилювачі і фільтри нижніх частот (ФНЧ) надходять на вихід приймача. Потім сигнали перетворюються в цифровий код і надходять у блок цифрової обробки (на схемі не показаний).

Технологія, найбільш близька до сучасної технології радіочастотної ідентифікації винайдена британцями в 1939 році – система розпізнавання "свій-чужий", що встановлювалася на літаках. Вона активно застосовувалася союзниками під час другої світової війни, щоб визначити, своїм або чужим є об'єкт в небі. Подібні системи до сих пір використовуються як у військовій, так і в цивільній авіації.

Засновником сучасної RFID-технології вважається Маріо Кардулло, який отримав патент США № 3713148 у 1973 ("Пасивний радіопередавач з пам'яттю"). Вперше пасивний пристрій на енергії відбиття був продемонстрований в 1971 році владі Нью-Йорка і іншим потенційним покупцям як пристрій з 16 бітами пам'яті для отримання мита на дорогах. Патент Кардулло передбачав використання радіохвиль, світла і звуку в якості засобу передавання інформації.

Перший патент США за № 4384288, пов'язаний власне з назвою RFID, був виданий Чарльзу Уолтону в 1983 році.

Етапи розвитку технології RFID ілюструє рис. 8.2.

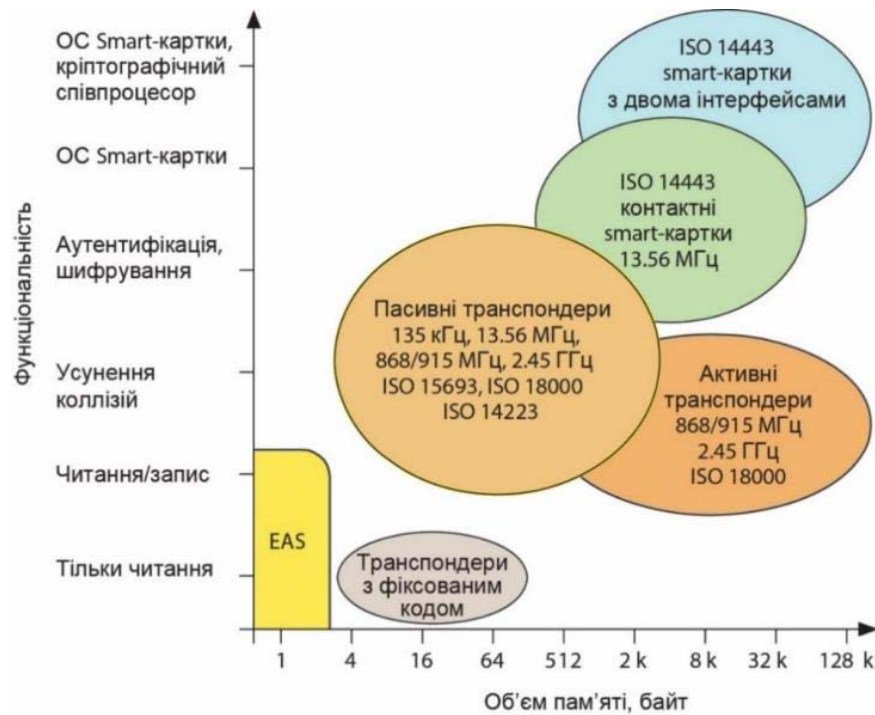


Рисунок 8.2 – Еволюція систем радіочастотної ідентифікації

8.1.2 Класифікація радіочастотних міток

На сьогодні існує велика кількість різних типів міток, працюючих в різних діапазонах частот, виконаних за різними стандартами, з пам'яттю для зберігання даних різного об'єму, призначених для встановлення на різних поверхнях і на об'єктах, виконаних з різних матеріалів [3].

Мітки розрізняються за типом живлення: активні, пасивні та напівактивні або напівпасивні. **Активні** мітки працюють від приєднаного або вбудованого джерела живлення, у зв'язку з цим вони можуть зчитувачами меншої потужності і забезпечують більшу дальність зв'язку.

Пасивні мітки працюють без джерела живлення, отримуючи енергію від електромагнітного поля випромінюваного зчитувачем. Пасивні мітки можуть бути меншими за розмірами і легше активних, зі значно нижчою ціною, мають практично необмежений термін служби.

Напівактивні або **напівпасивні** мітки мають вбудоване джерело живлення, які активують свою роботу при отриманні сигналу запиту від зчитувача. Так як енергія, що випромінюють такі мітки, зумовлена не тільки потужністю

випромінювання зчитувача, а і вбудованим джерелом живлення, вони можуть використовуватись на більших відстанях від зчитувачів. Дальність дії такої мітки може бути збільшена за рахунок внесення до неї додаткового каскаду підсилення сигналу запит, що надходить від зчитувача. Оскільки мітка більшу частину часу знаходиться в режимі очікування, що характеризується дуже низьким енергоспоживанням, то вона може працювати декілька років без заміни джерела живлення.

Активні і пасивні теги бувають наступних типів:

- тільки для читання;
- з читанням-записом;
- одноразово записувані (дані в них можуть бути занесені один раз користувачем).

Зовнішній вигляд деяких радіочастотних міток наведений на рис. 8.3.



Рисунок 8.3 – Зовнішній вигляд радіочастотних міток [5]

Конструкції деяких міток наведені на рис. 8.4.

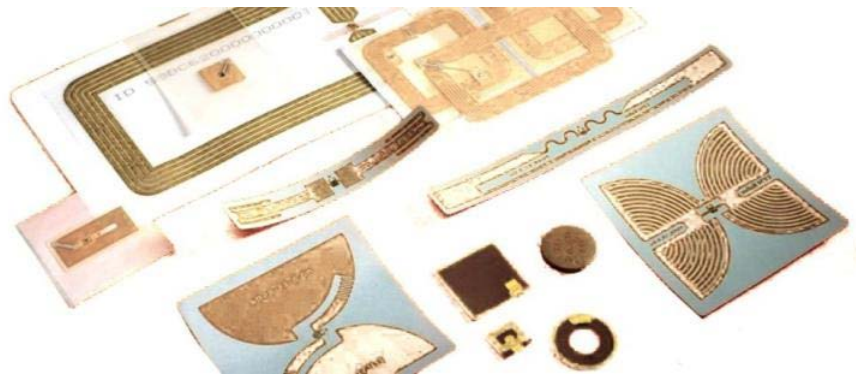


Рисунок 8.4 – Конструкції деяких радіочастотних міток [5]

8.1.3 Склад системи радіочастотної ідентифікації

Системи радіочастотної ідентифікації як правило складаються з трьох основних компонентів: зчитувача, радіочастотних міток і комп'ютерної системи обробки отриманих даних. Мітки, що закріплені на об'єктах, містять інформацію про об'єкт, яка дозволяє його ідентифікувати. Для збору інформації, яку містять в собі мітки, служать зчитувачі RFID [3, 5, 6].

Антени зчитувачів випромінюють електромагнітні хвилі, що активують мітку і дозволяють проводити зчитування даних з цієї мітки (для деяких типів міток запис і зчитування). Мітки можуть бути вбудовані в різні пристрої, а також у ворота, турнікети та інші об'єкти і дозволяють отримати інформацію про людей або предмети, що проходять через зону дії антени. У разі безперервного зчитування великої кількості міток електромагнітне поле випромінюється антеною зчитувача постійно або активується оператором, якщо постійне опитування не потрібно.

Сигнал, що надходить з антени зчитувача, демодулюється, розшифровується і передається в комп'ютер для подальшої обробки.

Типова структурна схема найпростішої системи радіочастотної ідентифікації наведена на рис. 8.5. В якості виконавчого пристрою часто використовується комп'ютер.

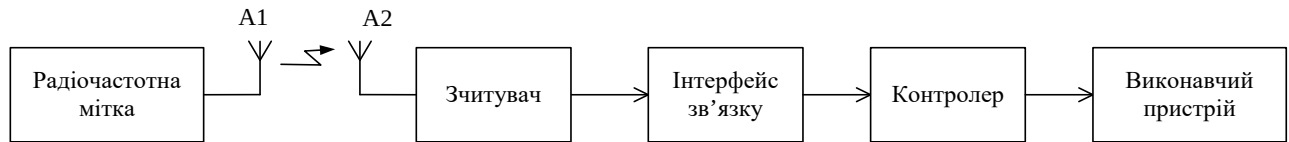


Рисунок 8.5 – Структурна схема найпростішої системи радіочастотної ідентифікації

Для передавання інформації по радіоканалу використовують коливання носійної частоти що модулюється. Використовується амплітудна модуляція або маніпуляція, під час якої змінюється амплітуда носійного коливання. На рис. 8.6 наведено приклад сигналів в системі радіочастотної ідентифікації у відповідності зі стандартом ISO 11785, що передбачає використання частоти носійного коливання 125 кГц [7].

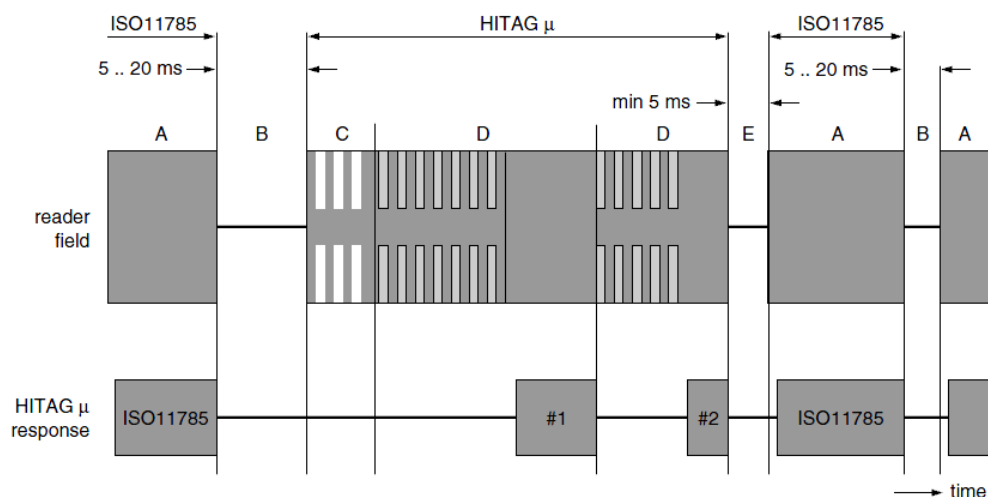


Рисунок 8.6 – Структура сигналів радіочастотного інтерфейсу для міток стандарту ISO 1785 [7]

Сірим на рис. 8.6 показано області де відсутні модуляція сигналу, тобто в цих областях формується гармонійний сигнал. Як слідує з рисунка є області де амплітуда змінюється на 100% від свого значення, а в інших областях зміна відбувається на 80%.

Інші способи модуляції це частотна (ЧМ) та фазова (ФМ). Але вони потребують набагато більш широкої смуги спектру і більш складних пристроїв для модуляції та демодуляції сигналів.

Такі особливості радіочастотних міток які дозволяють проводити зчитування інформації без безпосереднього контакту з об'єктом призводять до того, що поступово штрих-код передбачається замінити на відповідні електронні еквіваленти радіочастотних міток. Використання таких міток дозволяє спростити контроль за пересуванням товарів. Наприклад, уже сьогодні у книжкових магазинах використовуються такі мітки. Їх використання дозволяє запобігати крадіжкам книг. для цього на вході в магазин встановлюються зчитувач, який передає сигнал тривоги, якщо книга не оплачена і здійснюється спроба її вивезу з магазину. У великих супермаркетах найбільш дорогі товари теж оснащені таким мітками.

Використання радіочастотної ідентифікації має спростити електронні транзакції, що відбуваються між системами компаній, що ведуть товарообмін.

8.2 Основні переваги систем радіочастотної ідентифікації

До основних переваг систем радіочастотної ідентифікації відносять [2-4]:

1. Можливість перезапису даних. Дані записані у пам'ять мітки можуть перезаписуватися і доповнюватися багато разів (дані на штрих-коді не можуть бути змінені).

2. Система працює навіть при відсутності прямої видимості. Зчитувачу не потрібна пряма видимість мітки, щоб зчитувати дані що записані ній. Взаємна орієнтація мітки і зчитувача не грає ролі. Мітки можуть зчитуватися через упаковку, що робить можливим їх приховане розміщення. Для зчитування даних мітці досить потрапити в зону реєстрації на дуже короткий час (навіть при переміщенні на великій швидкості). Пристрою зчитування штрих-коду на відміну від зчитувача RFID, завжди необхідна пряма видимість штрих-коду для його зчитування.

3. Можлива велика відстань зчитування. Радіочастотна мітка може зчитуватися на значно більшій відстані, ніж штрих-код. Залежно від моделі мітки і зчитувача, радіус зчитування може становити до декількох метрів або навіть десятків метрів.

4. Великий об'єм даних, записаних у мітку. Мітка може зберігати значно більше інформації, ніж штрих-код. У мікросхемі мітки може зберігатися до 10000 байт інформації, в той час як штрихові коди можуть вмістити 100 байт (знаків) інформації, для відтворення яких знадобиться площа розміром з аркуш формату А4.

5. Підтримка зчитування декількох міток одночасно. Промислові зчитувачі можуть одночасно зчитувати дуже велику кількість (більше тисячі) міток в секунду. Для цього передбачено використання так званої антиколізійної функції. У той же час пристрій зчитування штрих-коду може одноразово сканувати тільки один штрих-код.

6. Зчитування даних радіочастотної мітки можливе при будь-якому її положенні. Для забезпечення автоматичного зчитування штрих-коду, існують вимоги розміщення штрих-кодів на товарній і транспортній упаковці. Для радіочастотних міток єдина умова – це знаходження мітки в зоні дії зчитувача.

7. Стійкість до впливу навколишнього середовища. Штрих-код легко пошкоджується (наприклад, вологою або забрудненням). У той же час випускаються радіочастотні мітки, що мають підвищений ступінь захисту від несприятливих умов робочого середовища. У тих областях застосування, де один і той же об'єкт може використовуватися велику кількість разів (наприклад, при ідентифікації контейнерів або зворотної тари), радіочастотна мітка має значні переваги при ідентифікації об'єктів, оскільки її не потрібно розміщувати на зовнішній стороні об'єкту.

8. Габаритні розміри, форма та конструкція мітки легко адаптуються до характеристик об'єктів і вимог системи контролю.

9. Можливість використання ідентифікації для рухомих об'єктів.

Об'єкти можуть знаходитися на великих відстанях від зчитувача (десятки метрів) і рухаються зі швидкостями до 300 км/год.

До недоліків радіочастотних міток можна віднести:

- відносно висока вартість;
- неможливість розміщення під металевими й електропровідними поверхнями;
- чутливість до перешкод у вигляді електромагнітних полів.

Вартість пасивної радіочастотної мітки, що працює на середніх частотах 13,56 МГц, становить:

- приблизно 1 долар при придбанні 1 шт;
- 0,2 у партії 100 шт;
- до 0,02 долара у партії понад 100 000 шт.

Таким чином, вартість радіочастотних міток значно перевищує вартість етикеток зі штриховим кодом на упаковці товарів. Зображення символу штрихового коду EAN-13, включене в загальне оформлення пакування, практично нічого не варто. У випадку використання етикетки з нанесеним на неї клеєм її ціна становить усього 0,02 долара. Тому на сьогодні використання радіочастотних міток розміщення коду EAN-13 на товарах масового попиту економічно не виправдане.

Разом з тим використання радіочастотних міток доцільно для захисту дорогих товарів від крадіжок або для забезпечення схоронності виробів, переданих на гарантійне обслуговування. У сфері логістики й транспортування вантажів вартість радіочастотної мітки може виявитися зовсім незначною в порівнянні з вартістю вмісту контейнера. Тому великі супермаркети можуть використовувати радіочастотні мітки на пакувальних ящиках, палетах і контейнерах.

8.3 Стандартизація систем радіочастотної ідентифікації

Існує велика кількість компаній, що випускають власні пристрої радіочастотної ідентифікації. При цьому зчитувачі виробництва однієї фірми можуть зчитувати інформацію своїх фірмових міток і можуть не розуміти мітки інших фірм. Через відсутність стандартів обладнання розрізняється за робочим частотам, за форматами збережених даних, за алгоритмами роботи і способам закриття даних.

В той же час сканери штрихового коду "розуміють" практично всі існуючі символіки. Існуючий стан в галузі штрихового кодування (за оцінками EAN International) є незадовільним: число основних, найбільш часто вживаних, кодів досягло чотирьох (EAN-13, EAN-8, UPC-A, UPC-E), в той час як в ідеальному для користувачів випадку це міг би бути один єдиний код EAN-13. EAN – European Article Numbering (Європейський товарний код) [8].

Областю діяльності EAN International є товарна нумерація, в якій RFID – це лише один із способів позначення номера товару поряд з штриховим кодуванням, оптичною, біометричною, магнітною ідентифікацією і т. д. Тому EAN International бачить мету стандартизації RFID в тому, щоб ця система, по-перше, була сумісна з існуючою системою EAN/UCC та витрати користувачів при впровадженні EAN/UCC були корисними для них.

Стандарти радіочастотної ідентифікації в ідеальному випадку повинні забезпечувати єдиний формат представлення даних. Міжнародним органом з стандартизації в галузі RFID є робоча група N4 (WG 4), утворена в серпні 1997 року в складі підкомітету з автоматичної ідентифікації (SC 31) об'єднаного технічного комітету N1 (JTC1) Міжнародної організації по стандартизації (ISO) – ISO/JTC1/SC31/WG4.

В даний час в якості міжнародного стандарту в області RFID прийнятий ISO 15693. Цей стандарт описує принцип передавання інформації, часові параметри сигналів в RFID-системах і т. д. У табл. 8.1 наведено перелік стандартів для RFID-систем, що працюють у різних частотних діапазонах [7].

Таблиця 8.1 – Міжнародні стандарти для різних частотних діапазонів RFID

Робоча частота	Стандарт	Призначення
125 кГц	ISO 14223 ISO 11784/11785	Розроблені для ідентифікації тварин (домашньої худоби), але досить широко використовуються в автомобілях
13,56 МГц	ISO 14443	Безконтактні смарт-карти для широкого кола додатків
13,56 МГц	ISO 15693	Безконтактні мітки для застосування в логістиці, ідентифікації товарів і т. д.
13,56 МГц	ISO 10373	Методи тестування
2,45 ГГц	ISO 18000	Безконтактні мітки для застосування в логістиці, ідентифікації товарів (зі збільшеною дальністю)

Перелік розроблених стандартів по системах RFID на кінець 2021 року можна знайти у [7]. У 2004 р. ISO/IEC прийняла єдиний міжнародний стандарт ISO 18000, що описує протоколи обміну в усіх частотних діапазонах RFID від 135 кГц до 2,45 ГГц. Діапазону НВЧ (860...960 МГц) відповідає стандарт ISO 18000-6A/B. З урахуванням технічних проблем, які проявлялися при зчитуванні міток класів 0 і 1 першого покоління, в 2004 р. фахівці Hardware Action Group EPCglobal створили новий протокол обміну між зчитувачем і міткою НВЧ діапазону – Class 1 Generation 2.

У 2006 р. пропозиція EPC Gen2 з незначними змінами була прийнята ISO/IEC в якості доповнення С до існуючих варіантів А і В стандарту ISO 18000-6, і на даний момент стандарт ISO/IEC 18000-6C є найбільш поширеним стандартом технології RFID в НВЧ діапазоні.

8.4 Области застосування систем радіочастотної ідентифікації

RFID-системи застосовуються в найрізноманітніших областях людської діяльності, коли потрібен оперативний і точний контроль, відстеження та облік численних переміщень різних об'єктів [1, 4, 5, 9]. Радіочастотні засоби ідентифікації застосовуються в основному для обліку одиниць товару в комерції, контролю переміщення та контролю в системах безпеки. А саме для електронного контролю за доступом та переміщеннями персоналу на території підприємств, управління виробництвом, товарними і митними складами (особливо великими), магазинами, видачою та переміщенням товарів і матеріальних цінностей.

На транспорті RFID-системи можуть забезпечити контроль, планування і управління рухом, інтенсивністю трафіку і вибір оптимальних маршрутів; на громадському транспорті вони служать для управління рухом, оплати проїзду та оптимізації пасажиропотоків. На їх базі можна створювати системи електронних платежів для всіх видів транспорту, що організують автоматичний збір даних і при необхідності нарахування оплати на залізницях, платних автомобільних трасах, на вантажних станціях і терміналах, платних автостоянках.

Приклади застосування систем радіочастотної ідентифікації в Європі наведені в табл. 8.2 [7]. В табл. 8.2 використані наступні позначення:

- LF – Low Frequency (низькочастотні мітки);
- MF – Medium Frequency (середньочастотні мітки);
- HF – High Frequency (високочастотні мітки);
- RO – Read Only (тільки для читання);
- WORM – Write Once Read Many (запис однократний, багаторазове зчитування);
- R/W – Read Write (запис і зчитування).

Таблиця 8.2 – Приклади використання систем радіочастотної ідентифікації

Найменування фірми	Тип мітки	Конструкція	Дальність зчитування	Робочі частоти	Сфери застосування
Agrotech Tabor	–	Імплантовані, в капсулах, пасивні мітки	0,5 м	134,2 кГц	Ідентифікація тварин
Amtech	Зчитувачі і пасивні мітки RW під захисним ковпаком	Зчитувачі і пасивні мітки RW під захисним ковпаком	15 м	315 МГц 2450 МГц 5,8 МГц	Ідентифікація транспортних засобів, залізничних и морських вантажів, майна, контроль руху, виробництво
Avonwood Developments (Eureka Systems)	Зчитувачі, активні і пасивні мітки RO, RW під захисним ковпаком и у вигляді бджів	-	3 м	132 КГц	Контроль доступу, ідентифікація майна, лабораторних зразків, транспортних засобів, тварин, виробництво, сортування багажу, ідентифікація персоналу
Baumer Ident	Зчитувачі, пасивні мітки RO, RW у вигляді брелків, бджів	Зчитувачі, пасивні мітки RO, RW у вигляді брелків, бджів	80-100 см	125 кГц	Виробництво, логістика
Diester Electronic	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів, брелків	-	8 м	125 кГц 100кГц	Контроль доступу, маркування майна, виробництво, обробка багажу, ідентифікація транспортних засобів, ідентифікація персоналу
Dialoc ID Technology	Зчитувачі, пасивні мітки RO у вигляді бджів, брелків	Зчитувачі, пасивні мітки RO у вигляді бджів, брелків	10 см	125 кГц 153 кГц	Контроль доступу, виробництво, ідентифікація персоналу
Euchner	Зчитувачі, пасивні мітки RO, RW у вигляді капсул, бджів, брелків	Зчитувачі, пасивні мітки RO, RW у вигляді капсул, бджів, брелків	25 мм	125 кГц 1,3 МГц	Контроль доступу, виробництво, ідентифікація персоналу, транспортних засобів, лабораторних зразків, електронні протиугінні системи
Feig Electronic	Зчитувачі, пасивні мітки RO, RW	Зчитувачі, пасивні мітки RO, RW	1,3 м	125 кГц	Контроль доступу, маркування майна, виробництво, ідентифікація транспортних засобів, лабораторних зразків, ідентифікація персоналу
GET	Бджі	Пасивні мітки RO, RW, бджі	70 см	125 кГц	Контроль доступу, ідентифікація персоналу
Identec	Зчитувачі, активні і пасивні RO мітки, бджі	–	4 м	131 кГц	Контроль доступу, маркування майна, виробництво, ідентифікація персоналу и транспортних засобів
Idesco	Зчитувачі, пасивні RO и RW мітки, капсули	–	45 см	24 кГц 250 кГц	Контроль доступу, маркування майна, виробництво, сортування багажу, ідентифікація транспортних засобів, лабораторних зразків, ідентифікація персоналу
ID Systems	Зчитувачі RFID	Активні и пасивні RO, RW мітки у вигляді капсул, брелків, бджів, імплантатів, поштових марок	1 м	25 кГц 13,56 МГц	Контроль доступу, маркування майна, виробництво, сортування багажу, ідентифікація транспортних засобів, лабораторних зразків, ідентифікація персоналу

Продовження табл. 8.2.

Найменування фірми	Тип мітки	Конструкція	Дальність зчитування	Робочі частоти	Сфери застосування
Industrial Auto ID	—	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	10 м	125 кГц 13,56 МГц	Контроль доступу, маркування майна, виробництво, сортування багажу, ідентифікація транспортних засобів, ідентифікація персоналу
Micro Design ASA	Зчитувачі, активні і пасивні мітки RO, RW	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	50 м	125 кГц 13,56 МГц 856 МГц 2,45 ГГц 5,8 ГГц	Контроль доступу, маркування майна, виробництво, сортування багажу, ідентифікація транспортних засобів, ідентифікація персоналу, стягування плати
Micro-Sensys	Зчитувачі, пасивні мітки RW у вигляді капсул, імплантатів	Мітки RO	5 мм (RW) 5 см (RO)	4,0 МГц (RW) 125кГц (RO)	Маркування майна, виробництво, ідентифікація лабораторних зразків
Nedar	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	1,2м(пасивн) 10 м (активн)	120 кГц	Маркування майна, виробництво, ідентифікація персоналу, транспортних засобів, тварин
Pepperl and Fuchs	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	Пасивні мітки у вигляді брелків, імплантатів	4 м	125 кГц 2,45 ГГц	Виробництво, ідентифікація персоналу, транспортних засобів
Scemtec	Зчитувачі RFID	Пасивні мітки RO, RW у вигляді капсул	2 м	125 кГц	Контроль доступу, маркування майна, сортування багажу, ідентифікація транспортних засобів, лабораторних зразків, газових балонів, ідентифікація персоналу, стягування плати
Sensormatic Electronics	Зчитувачі, пасивні мітки RO, RW	Зчитувачі, активні і пасивні мітки RO, RW	—	125 кГц 13,56 МГц 58 кГц 2,4 ГГц 134 кГц	Маркування майна, виробництво, ідентифікація персоналу, управління запасами, логістика
Siemens	-	Зчитувачі, активні і пасивні мітки RO, RW у вигляді капсул, бджів	1 м	—	Маркування майна, виробництво, ідентифікація транспортних засобів
Socymat	Пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	Зчитувачі RFID	—	13,56 МГц 125 кГц	Контроль доступу, маркування майна, виробництво, сортування багажу, ідентифікація транспортних засобів, персоналу
Socymat Ident Component	Пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів, поштових марок	—	1,2 м	125 кГц 13,56 МГц	Контроль доступу, маркування майна, виробництво, сортування багажу, ідентифікація транспортних засобів, персоналу, стягування плати, логістика

Продовження табл. 8.2.

Найменування фірми	Тип мітки	Конструкція	Дальність зчитування	Робочі частоти	Сфери застосування
Statec Technologies	–	Зчитувачі, пасивні мітки RO, RW у вигляді капсул	1 м	125 кГц	Виробництво
Statec Technology	Зчитувачі и пасивні мітки RW	Зчитувачі, мітки RO, RW у вигляді капсул, брелків, імплантатів	10 м	125 кГц 13,56 МГц 2,4 ГГц	Виробництво, ідентифікація транспортних засобів
STID	Зчитувачі RFID	Зчитувачі, активні и пасивні мітки RO, RW у вигляді капсул, бджів, брелків, імплантатів	70 см, 10 м	125 кГц 2,45 ГГц	Маркування майна, виробництво, ідентифікація транспортних засобів, персоналу, стягування плати
Tagmaster	Зчитувачі, активні мітки RO, RW у вигляді капсул, бджів	Зчитувачі, активні мітки RO, RW у вигляді капсул, бджів	4 м, 6 м	2,45 ГГц	Маркування майна, виробництво, ідентифікація персоналу, транспортних засобів, тварин
Traffic Supervision Systems	Зчитувачі и пасивні мітки RO, RW	-	80 см	125 кГц	Маркування майна, виробництво, ідентифікація транспортних засобів, стягування плати

На рис. 8.7 наведений приклад використання радіочастотної ідентифікації у тваринництві [10].

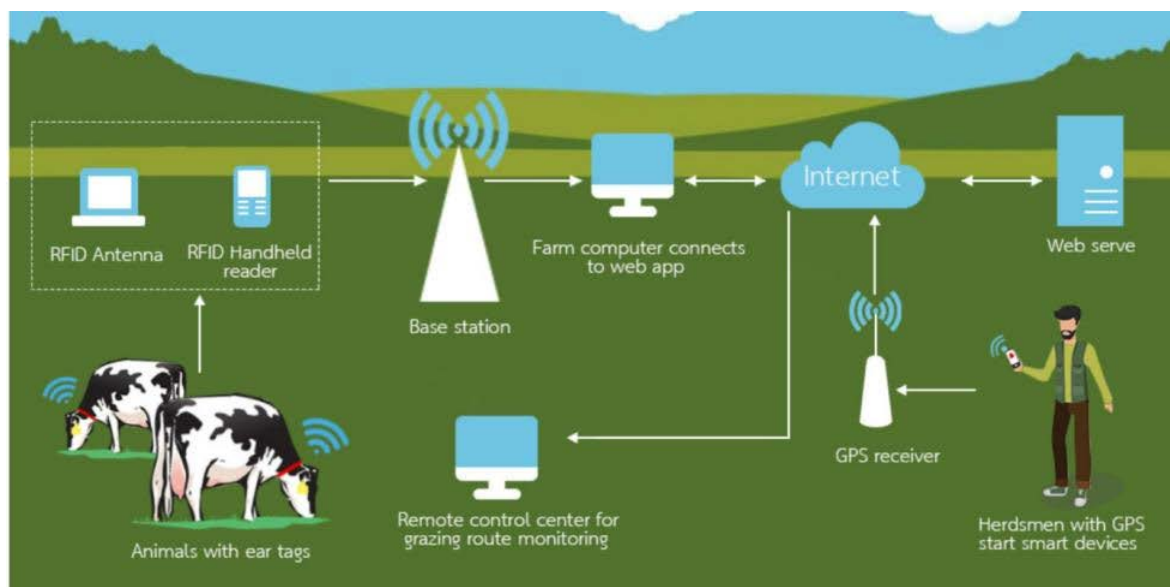


Рисунок 8.7 – Використання радіочастотної ідентифікації для контролю знаходження тварин [10]

Першим кроком у застосуванні технології RFID у тваринництві є встановлення RFID-міток на тваринах у вигляді постійного цифрового файлу та унікального ідентифікаційного атрибуту кожної домашньої тварини. RFID-мітка призначена для введення в чіп основної інформації про домашню тварину, таку як ім'я власника, характеристики тварини, імунітет, тип вакцини, виробник вакцини, номер виробничої партії, метод вакцинації, доза вакцинації, кількість імунітету і т. д. Тільки власнику тварини потрібно переносний зчитувач для отримання інформації про тварину на випасі. Мітки найчастіше розміщують у вухах тварини (рис. 8.8).

При утриманні тварин на фермах використовують як переносні так і стаціонарні зчитувачі [10].

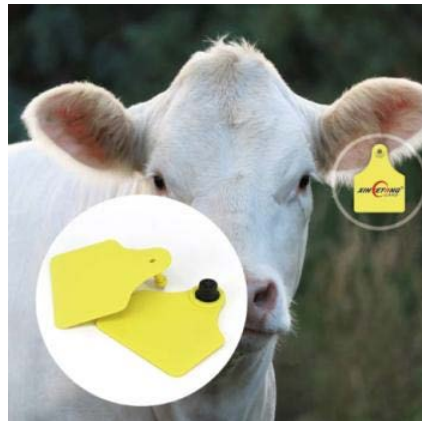


Рисунок 8.8 – Розміщення мітки на вухах тварини [10]

Окрім переліченої інформації мітка може містити інформацію про індивідуальний раціон годування тварини, що дозволяє підвищити продуктивність тваринництва.

Контроль домашніх тварин

В даний час багато країн і регіонів впровадили управління електронними логотипами RFID для домашніх тварин, наприклад, США, Канада, Австралія, Китай і т.д., що дозволяють з'ясувати місцезнаходження тварин у часі. Окрім того, такі мітки несуть інформацію про хазяїна та всі параметри тварини.

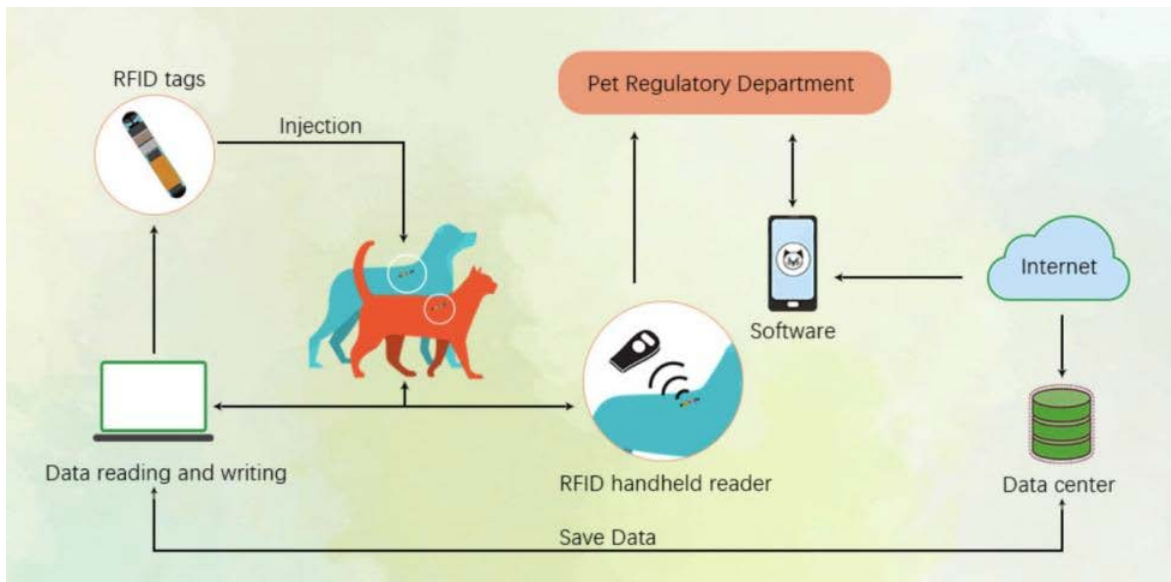


Рисунок 8.9 – Використання радіочастотної ідентифікації для контролю домашніх тварин [11]

Кожен вихованець, якому імплантований чіп, має глобальний унікальний ідентифікаційний номер (UID), який використовуватиметься як електронна ідентифікаційна карта тварини протягом усього її життя, оскільки термін служби чіпа перевищує 20 років. Крім того, чіп для домашніх тварин може записувати основну інформацію про домашніх тварин, включаючи ім'я, тип, стать, дату народження, фізіологічні характеристики та ім'я власника, адресу, контактну інформацію, тощо.

Регулюючі органи або лікарні для домашніх тварин можуть легко та швидко отримати інформацію про домашніх тварин, скануючи RFID-мітку для тварин. Система ідентифікації тварин RFID може також вимагати номер UID домашньої тварини, і ви можете отримати все більш і більш докладну інформацію про домашню тварину з бази даних домашніх тварин через Інтернет.

Використання RFID у великих бібліотеках

Система управління бібліотекою RFID не тільки надає читачам більш зручні та швидкі інтелектуальні послуги, такі як отримання та повернення книг, довідки тощо, але також покращує режим управління бібліотекою, підвищує ефективність роботи, знижує трудомісткість менеджерів та надає повне рішення для сфери застосування. бібліотеки (рис. 8.10) [12].



Рисунок 8.10 – Використання систем радіочастотної ідентифікації в бібліотеці [12]

Система включає систему робочого місця бібліотекаря, систему перетворення електронних етикеток, систему сертифікатів самообслуговування, систему самообслуговування та повернення, систему самообслуговування для сортування книг, систему інвентаризації колекції, систему контролю доступу, інтелектуальну систему навігації та пошуку та систему самообслуговування.

Ручна інвентаризація книжок, особливо інвентаризація книжок на книжкових полицях, потребує дуже багато часу і неефективна. RFID має можливість безконтактного, швидкого одночасного зчитування кількох етикеток на відстані та, що робить інвентаризацію швидкою, точною та ефективною. Більше того, за допомогою технології RFID легко знайти книги, яких немає на полицях. Персонал легко проводить інвентаризацію книг, значно заощаджуючи ручну працю та матеріальні ресурси.

Для маркування книг використовують гнучкі пасивні мітки (рис. 8.11) у вигляді наклейок [13].



Рисунок 8.11 – Наклейка з гнучкою пасивною RFID-міткою [13]

Ця наклейка з RFID-міткою працює на частоті 13.56 МГц і зазвичай розміщується на обкладинці книги. Вона має міцний клей на звороті, який нелегко відірвати після наклеювання, і цю бібліотечну наклейку можна надрукувати на принтері для етикеток. Це економічне рішення для ідентифікації та відстеження книг, яке робить управління бібліотекою інтелектуальнішим та зручнішим.

Використання RFID для управління контролем доступу

Система контролю доступу RFID не є чимось незвичайним у нашому повсякденному житті, оскільки має кілька функцій, а не традиційну систему контролю доступу.

Система контролю доступу RFID має всі функції традиційної загальної системи контролю доступу, а також дозволяє декільком людям швидко проходити та записувати особисту інформацію кожної людини, які входять та виходить одночасно.

Коли людина з RFID-картою проходить через ворота, інформація з картки автоматично збирається системою без ручного втручання, що робить керування контролем доступу зручнішим. RFID-мітки мають тривалий термін служби (до 10 років) і можуть багаторазово перезаписуватись.

Сфера застосування для контролю доступу дуже широка. Наприклад, для доступу до приміщення у готелях (рис. 8.12) [15].



Рисунок 8.12 – RFID-карта для контролю доступу в готелі [15]

Для контролю доступу до будинків найчастіше використовуються брелки (рис. 8.13), форма яких може бути різноманітною [16].



Рисунок 8.13 – Брелки для систем контролю доступу [16]

Найпростіші брелки наведені на рис. 8.14.



Рисунок 8.14 – Найпростіші брелки [17]

Економічним рішенням контролю доступу є використання Proximity Card, що дозволяють увійти до будівлі чи офісу, і представлені на рис. 8.12...8.14.

Використання RFID у лікарнях

RFID має широкі перспективи застосування у сфері лікарень та охорони здоров'я. Система управління лікарнею RFID може реалізувати взаємодію між пацієнтами та медичним персоналом, медичними установами, медичними пристроями. Крім того, RFID також відіграє велику роль в контролі стану пацієнтів, контролі доступу, управлінні пранням лікарняної білизни і т.д.

Система RFID у лікарнях також може запобігти втраті пацієнтів. Через RFID смарт-браслети (рис. 8.15), зчитувачі RFID, а також системи позиціонування та відстеження, медичні працівники можуть відстежувати фізичне місцезнаходження пацієнтів та швидко знаходити їх та впроваджувати для них відповідні медичні програми [15]. Таким чином, він може забезпечити цілодобове своєчасне спостереження за пацієнтами, забезпечити безпеку пацієнтів, знизити частоту нещасних випадків та підвищити рівень керування лікарнею.



Рисунок 8.15 – RFID-браслет для пацієнтів лікарень [15]

Управління ідентифікацією новонароджених

Браслет RFID має важливе застосування в акушерському управлінні ідентифікацією матері та дитини, контроль та перевірку особи дитини. У відділенні акушерства та гінекології великої лікарні загального профілю або пологового будинку новонародженого забезпечать браслет RFID, який може відзначити унікальну особу дитини та зіставити інформацію про дитину з інформацією матері.

Щоб визначити, чи тримаєте ви не ту дитину, вам потрібно лише порівняти інформацію про браслет RFID матері та дитини, щоб уникнути плутанини.

Коли хтось намагається вкрати новонародженого з лікарняної палати, пристрій ідентифікації RFID може виявити його в реальному часі, подати сигнал тривоги та повідомити охоронців останнє місцезнаходження вкраденої дитини. Крім того, якщо з дитини зняти етикетку, пристрій відразу подає інший сигнал тривоги, що вказує на місцезнаходження дитини.

Відстеження обладнання лікарень

Лікарняне обладнання коштує дорого, і зберігання медичних виробів має здійснюватися відповідно до суворих стандартів зберігання, що ускладнює та ускладнює управління лікарняними активами. В управлінні активами лікарень використання RFID-міток дозволяє отримати вдвічі більший результат з половиною зусиль, заощаджуючи час та трудовитрати на пошук обладнання, а також покращуючи здатність лікарні керувати активами.

Наприклад, встановлення активних або пасивних RFID-міток на переливних насосах, лікарняних ліжках, ношах, інвалідних візках та іншому рухомому майні може зробити процес пошуку та перевірки надзвичайно швидким і точним, більш ніж у 20 разів у порівнянні з традиційними методами. Крім того, за допомогою світлодіодних міток RFID, якщо деякі предмети втрачені, система може нагадати менеджеру складу про необхідність змінити місце зберігання за допомогою миготливих світлодіодних індикаторів.

RFID-мітки, що використовуються для контролю обладнання, зазвичай використовують діапазон 860...960 МГц, що дозволяє здійснювати контроль на відстані декількох метрів.

Окрім перелічених вище застосунків у лікарнях радіочастотна ідентифікація використовується для:

- контролю доступу в системі безпеки;
- відстеження хірургічних інструментів;
- управління аптеками лікарні і обліку дорогих ліків;
- управління реєстрацією в лікарнях;

- управління медичними відходами;
- контролю роботи пральні та переміщення лікарняної білизни.



Рисунок 8.16 – Бирка з АБС-пластику для лікарняного обладнання [15]

Використання радіочастотної ідентифікації у промисловості

В епоху Інтернету речей різні галузі покладаються на технологію Інтернету речей для досягнення стрибкоподібного розвитку. В даний час традиційна обробна промисловість гостро потребує трансформації. Технологія RFID, є ключем до інтелектуального виробництва. Оскільки автоматизація промислового виробництва стала тенденцією, інтелектуальні виробничі роботи та інше обладнання замінили більшу частину ручної праці, і виробничі потужності промислового виробництва поступово збільшуються. Отже, що RFID може принести до виробництва?

Застосування RFID у виробництві

Технологія RFID поєднує різні виробничі ланки в мережеву систему, надаючи матеріальну форму електронним міткам, що значно підвищує рівень автоматизації промислового виробництва. Вплив RFID на обробну промисловість широко, включаючи управління інформацією, виробництвом, контролем якості, відповідність стандартам, управління контролем обладнання, візуалізацію наявності продукції та її переміщенням на складах.

Управління виробничою інформацією

У виробничому процесі виробничих підприємств дуже важливо, щоб виробнича лінія забезпечувала своєчасний та точний зворотний зв'язок. Раніше реєструвати несправності можна було лише вручну під час виробництва, що потребувало багато часу та зусиль, а іноді й не могло бути дуже точним.

Комбінуючи RFID з існуючими виробничими інформаційними системами можна побудувати більш потужний інформаційний ланцюжок для своєчасного формування точних даних, що призведе до підвищення продуктивності, використання обладнання та вищого рівня контролю якості.

Стандартизований виробничий контроль

Система RFID може надавати безперервно оновлюванні потоки даних у реальному часі, що доповнює систему управління виробництвом. Інформація, що надається RFID, можна використовуватиме забезпечення правильного використання машин, устаткування, інструментів, деталей для безпаперової передачі даних та скорочення часу простою.

Крім того, коли сировина, деталі та вузли проходять через виробничу лінію, виробничий процес можна контролювати, змінювати або навіть реорганізовувати в режимі реального часу, щоб гарантувати надійність та високу якість продукції.

Відстеження якості

Якщо встановити обладнання для зчитування RFID-міток у кожній ланці виробничої лінії та використати RFID-мітки, які можна багаторазово зчитувати та записувати, на продукцію чи лоток, то коли продукція проходить через ці вузли, пристрій читання та запису RFID може зчитувати інформацію на етикетці та передавати інформацію в систему керування у режимі реального часу, забезпечуючи якість продуктів. .

Крім того, RFID та існуючі системи управління виробництвом можуть доповнювати одна одну. Для більшості компонентів виробничі системи управління можуть збирати інформацію, таку як ідентифікатори продукту, тимчасові мітки, фізичні атрибути, номери замовлень та партії кожного процесу, які можуть бути

перетворені на коди RFID та передані в ланцюжок поставок, щоб допомогти виробникам відстежувати та відстежувати історію продуктів.

Контроль обладнання

RFID-мітки прикріплені до обладнання дозволяють контролювати як місцезнаходження, стан доступності, характеристики продуктивності та інші параметри. Завдяки скороченню часу простою та ефективнішому обслуговуванню це може позитивно вплинути на дуже важливі виробничі параметри, такі як загальна ефективність пристрою.

Візуалізація складських запасів

Оскільки контрактне виробництво стає все більш важливим, стає критично важливим синхронізувати ланцюжок поставок і чітку видимість виробничого процесу. RFID підходить для програм будь-якого розміру (локально або поширюється на всю фабрику). RFID забезпечує повну візуалізацію вхідних, незавершених робіт, упаковки, транспортування та складування доти, доки вони, нарешті, не будуть відправлені до наступного пункту призначення у ланцюжку поставок, і все це пов'язано з управлінням інформацією.

Автоматичне керування виробничою лінією

Для виробничих цілей використовують мітки у захищених корпусах та у вигляді наклейок, які можуть встановлюватись на металеві поверхні. Найчастіше використовують мітки в діапазонах частот 860...960 МГц та 2,4 ГГц (рис. 8.17) [4].



Рисунок 8.17 – Мітки для використання в промисловості [4]

RFID-мітки можуть зручно та точно записувати інформацію про процес та інформацію про роботу лінії, задовольняти потреби гнучкого виробництва, значно

підвищувати швидкість та точність виробництва, підвищувати ефективність роботи, змінювати режим виробництва та скорочувати витрати.

Контрольні питання

1. Для чого призначені системи радіочастотної ідентифікації?
2. Що означає поняття радіочастотна мітка?
3. Яка різниця між транспондером, тегом та радіочастотною міткою?
4. У чому полягають переваги пасивних радіочастотних міток?
5. У чому полягають переваги активних радіочастотних міток?
6. Яким чином здійснюється живлення вузлів пасивних радіочастотних міток?
7. Які мітки забезпечують більшу дальність зв'язку – пасивні чи активні? Поясніть чому.
8. Чи впливає діапазон частот в якому працюють мітки на дальність зв'язку з мітками?
9. Яким чином можна використовувати радіочастотну ідентифікацію для обліку товарів?

Перелік посилань

1. Сандип Лахири RFID. Посібник з впровадження (The RFID Sourcebook) / Дудников С. – Кудиц-Прес, 2007. – 312 с.
2. Manish Bhuptani, Shahram Moradpour RFID Field Guide: Deploying Radio Frequency Identification Systems. – Prentice Hall; 1st edition (February 8, 2005). – 288 p.
3. Введення в радіочастотну ідентифікацію RFID. Url: https://masters.donntu.org/2004/fema/kvitkovsky/library/art6.htm_ (дата звернення: 17.04.2024).
4. К. Финкенцеллер Довідник з RFID. Теоретичні засади та практичне застосування індуктивних радіоприладів, транспондерів та безконтактних чіп-карт.. – Додека-XXI", 2008. – 496 с.

5. Pros and cons of RFID tags. Url: <https://www.starnfc.com/tag/what-are-rfid-tags-used-for/> (дата звернення: 17.04.2024).
6. Norbert Bartneck, Volker Klaas, Holger Schoenherr Optimizing Processes with RFID and Auto ID, 2009. – 268 p.
7. RFID_TOC. Url: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/rfid_toc.pdf (дата звернення: 17.04.2024).
8. EAN International International Article Numbering Association. Url: <https://www.iso.org/ru/organization/548498.html> (дата звернення: 17.04.2024).
9. RFID технологія для автоматизації обліку. Url: <https://remonline.ua/ru/blog/rfid-technology/>. (дата звернення: 17.04.2024).
10. RFID solution for livestock. Url: <https://yiio.com/solutions/rfid-solution-for-livestock/> (дата звернення: 17.04.2024).
11. RFID Animal Tracking and Identification. Url: <https://www.asiarfid.com/rfid-animal-tracking-and-identification.html> (дата звернення: 17.04.2024).
12. How RFID Library Management Systems Optimizes Workflows? Url: <https://www.gwrfid.com/rfid-for-library-management/> (дата звернення: 17.04.2024).
13. Why are more and more libraries using RFID technology? Url: <https://www.gialer.com/blogs/news-and-blogs/why-are-more-and-more-libraries-using-rfid-technology> (дата звернення: 17.04.2024).
14. RFID für Access Control Management, das Sie gerne wissen würden. Url: <https://www.asiarfid.com/de/rfid-for-access-control.html> (дата звернення: 17.04.2024).
15. RFID for Access Control Management You Would Like to Know. Url: <https://www.asiarfid.com/rfid-for-access-control.html> (дата звернення: 17.04.2024).
16. Leather keychain. Url: <https://www.shutterstock.com/ru/search/leather-keychain> (дата звернення: 17.04.2024).
17. RFID for Healthcare: What RFID Hospital Management offers? Url: <https://www.gwrfid.com/rfid-for-healthcare/> (дата звернення: 17.04.2024).

9 ТЕХНОЛОГІЯ NFC В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

9.1 Загальні зауваження

Абревіатура NFC (Near Field Communication) означає "Зв'язок на невеликих відстанях". Це технологія, що дозволяє здійснювати безпроводовий зв'язок між двома пристроям на невеликій відстані [1].

Технологія NFC відповідає розширенням стандарту ISO 14443 (стандарт, який описує протокол обміну, частотний діапазон і методи модуляції безконтактних пасивних карт ближнього радіусу дії). NFC була схвалена як стандарт ISO/IEC 8 грудня 2003, і пізніше як стандарт Ecma International. Ці стандарти визначають методи модуляції, кодування, швидкості передавання і структуру інтерфейсу пристроїв NFC, а також умови, необхідні для контролю за конфліктними ситуаціями під час ініціалізації [1]. Безпроводовий інтерфейс для NFC стандартизований в:

- ISO/IEC 18092, ECMA-340: Near Field Communication Interface and Protocol-1 (NFCIP-1);
- ISO/IEC 21481, ECMA-352: Near Field Communication Interface and Protocol-2 (NFCIP-2).

Пристрої NFC можуть взаємодіяти з існуючою раніше інфраструктурою зчитувачів, так як технологія об'єднує безліч раніше існуючих стандартів, включаючи ISO 14443, ISO 15693.

Пристрої NFC працюють на частоті 13,56 МГц та підтримують швидкість передавання даних 106, 216 та 424 кбіт/с. Розробляється варіант стандарту для більш високих швидкостей обміну даними за технологією NFC. Очікується, що він підвищить верхню межу для деяких додатків до 6,8 Мбіт/с [2].

Для передавання даних використовується індуктивний зв'язок між пристроями (аналогічний зв'язок між пристроями здійснюється в безпроводових зарядних пристроях). Максимальна дальність зв'язку приблизно 10 см. Типове значення 4...5 см, що забезпечує деякі переваги в безпеці при обміні даними [2].

Така мала відстань ефективного зв'язку пов'язана з тим, що поле у ближній від антени зоні складається з магнітного й електричного поля, однак магнітне поле практично є основним. Фактично зв'язок здійснюється через трансформатор без осердя з достатньо великою відстанню між обмотками. Загасання сигналу ближнього поля визначається коефіцієнтом $1/d^6$, де d – відстань між пристроями. Тому поле ближньої зони швидко послаблюється і поширюється приблизно в межах однієї довжини хвилі випромінюваного сигналу.

На рис. 9.1 показано як здійснюється обмін даними між пристроями NFC. Пристрій який ініціює зв'язок називається ініціатором, а пристрій, з яким потрібно встановити зв'язок – цільовим пристроєм.

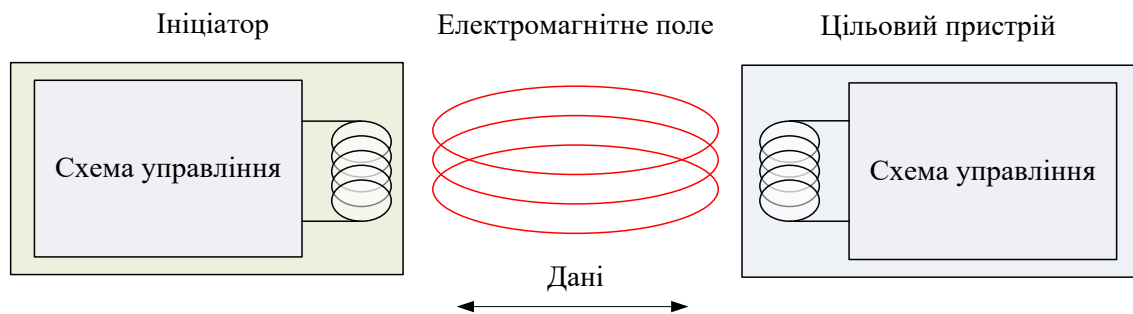


Рисунок 9.1 – Схема обміну даними між пристроями NFC

В антену ініціатора подається змінний струм який створює змінний магнітний потік. В результаті виникає змінний струм в антені цільового пристрою. Тобто сигнал потрапляє у цільовий пристрій.

Передача даних забезпечується за допомогою амплітудної модуляції (маніпуляції) сигналу (рис. 9.2 та 9.3). В свою чергу цільовий пристрій, щоб передати сигнал змінює струм у своїй антені за рахунок варіації імпедансу (опору). Зміна струму призводить до генерації магнітного поля цільового пристрою, яке взаємодіє з магнітним полем ініціатора. Ця взаємодія зароджує варіації струму в ініціаторі. Ці варіації струму ініціатор демодулює і отримує інформацію від цільового пристрою.

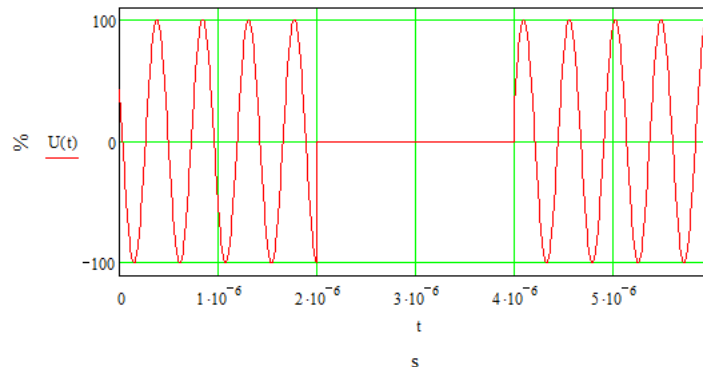


Рисунок 9.2 – АМ-сигнал з коефіцієнтом модуляції 100%

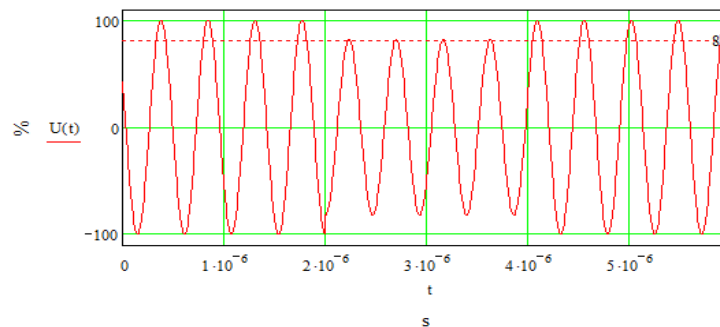


Рисунок 9.3 – АМ-сигнал з коефіцієнтом модуляції 10%

Амплітуда носійного колювання модулюється в залежності від значення біту даних, що передаються. Основною характеристикою амплітудної модуляції є коефіцієнт (глибина) модуляції – відношення різниці максимального та мінімального значення амплітуд модульованого сигналу до суми цих значень, представлене в процентах. Коефіцієнт модуляції обчислюють за формулою:

$$\frac{a-b}{a+b} \cdot 100\%$$

де a та b – максимальне та мінімальне значення амплітуди модульованого сигналу, відповідно.

Зв'язок між пристроями NFC встановлюється приблизно за 0,1 с [3]. Використовується 2 режими зв'язку між пристроями NFC – активний та пасивний.

Активний пристрій генерує власне електромагнітне поле. Пасивний пристрій використовує поле, створене активним пристроєм (власного електромагнітного

поля не генерує). Цільовий пристрій може бути як пасивним так і активним, на відмінну від ініціатора, який може бути тільки активним. Зв'язок може бути встановлено між двома активними пристроями, або активним і пасивним пристроєм, як показано в табл. 9.1 [4].

Таблиця 9.1 – Конфігурації зв'язку пристроїв NFC

Пристрій А	Пристрій В	Опис
Активний	Активний	Коли пристрій посилає дані, він генерує магнітне поле. В режимі очікування поле не генерується. Поле генерується пристроєм А та пристроєм В по черзі.
Активний	Пасивний	Магнітне поле генерується тільки пристроєм А
Пасивний	Активний	Магнітне поле генерується тільки пристроєм В

Активними пристроями NFC можуть бути смартфони, комп'ютери, термінали для оплати, планшети, фотоапарати.

Пасивні пристрої – NFC-мітки, можна використовувати для зв'язку з активними пристроями NFC. Мітка NFC схожа за схемою з RFID-міткою. Вона складається з мікрочіпа та антени. NFC-мітки зберігають та передають дані активним NFC-пристроєм. Коли зчитувач знаходиться близько до мітки, вона активується і передає дані на цей пристрій.

Основна перевага NFC в порівнянні з іншими безпроводовими технологіями полягає в низькій вартості і можливості використовувати в багатьох додатках. А з урахуванням простоти схеми і невеликої кількості елементів, мітки можна випускати з порівняно малими витратами.

Існує чотири базові типи міток (табл. 9.2). Ці типи форматів NFC-міток визначено в стандартах ISO 14443 Types A, B та Sony FeliCa [1]. Найбільш популярні моделі NFC-міток: Tec Tiles Tag, NTAG203, Xperia SmartTags NT2.

Таблиця 9.2 – Типи NFC-міток

	Тип 1	Тип 2	Тип 3	Тип 4
Стандарт ISO/IEC	14443 A	14443 A	JIS 63 19-4	14443 A/B
Сумісні вироби	Innovision Topaz	NXP MIFARE	Sony FeliCa	NXP DESFire, SmartMX- JCOP
Швидкість передавання даних	106 кбіт/с	106 кбіт/с	212,424 кбіт/с	106, 212, 424 кбіт/с
Об'єм пам'яті	96 байт, можливість розширення до 2 кбайт	48 байт, можливість розширення до 2 кбайт	Змінний, максимальний 1 Мбайт	Змінний, максимальний 32 кбайт
Застосування	Персональне використання, корпоративний ринок	Зберігання відео посилань, веб-адрес. Також, для додатку Sony Xperia's Smart Tag	Застосовується у додатках, що потребують високої ємності пам'яті.	Для зберігання візитних карток
Підтримка UID	Так	Так	Ні	Так
Блокування тільки для режиму зчитування	Так	Так	Так	Так
Підтримка анти-колізії	Ні	Так	Так	Так
Активний контент	Ні	Ні	Ні	Можливо

9.2 Режими роботи пристроїв NFC

9.2.1 Режим емуляції карти

Стандарт NFC передбачає 3 режими роботи для сумісних пристроїв:

- емуляції карти;
- зчитування/запису;
- взаємодії двох пристроїв.

Режим емуляції карти (англ. "card-emulation") дозволяє використовувати мобільний телефон для ідентифікації особи, контролю доступу та проведення грошових трансакцій. Пристрій NFC емулює роботу безконтактної карти і зовнішні

зчитувачі отримують дані, що зберігаються в пристрої NFC. При використанні цього режиму відпадає потреба в наявності банківської картки, готівки, квитків як фізичних об'єктів. Всі необхідні дані можуть зберігатись в одному пристрої – телефоні користувача. На рис. 9.4 наведений приклад використання мобільного пристрою в режимі емуляції карти [2].



Рисунок 9.4 – Використання пристрою NFC в режимі емуляції карти [2]

Технологія NFC була розроблена для використання у платіжних системах. В режимі емуляції карти пристрій поводить себе як смарт-карта. В системах запиту електронного ключа мобільний пристрій із інтерфейсом NFC представляє собою фізичний ключ або безконтактну смарт-карту і забезпечує контроль доступу.

9.2.2 Режим зчитування/запису

Режим зчитування/запису (англ. "reader/writer") дозволяє пристроям NFC встановлювати зв'язок з NFC-мітками. Такі мітки є пасивними пристроями. Основне призначення мітки полягає у зберіганні даних, які потім зчитуються активним пристроєм NFC. Мітки можуть бути вбудовані в плакати або банери, що знаходяться в громадських місцях, і містити або певну інформацію, або приводити активний NFC-пристрій в дію. На рис. 9.5 показано як здійснюється взаємодія між міткою та активним пристроєм [2].



Рисунок 9.5 – Взаємодія між міткою та активним пристроєм NFC в режимі зчитування/запису [2]

При використанні режиму зчитування/запису відправник знаходиться в активному режимі зв'язку, а приймач – в пасивному. Швидкість передавання даних – 106 кбіт/с. Для завантаження даних на мобільний пристрій користувача використовуються уніфіковані ідентифікатори ресурсу (URI) [1] двох класів – URN та URL.

Уніфікований вказівник місцезнаходження ресурсу (URL) – це URI, який, крім ідентифікації ресурсу містить інформацію про місцезнаходження ресурсу.

Уніфікована назва ресурсу (URN) – це URI, який тільки ідентифікує ресурс.

Пристрої NFC можуть взаємодіяти з пристроями стандарту ISO1443, тобто пристроями RFID. У табл. 9.3 показані основні відмінності між технологією NFC та RFID.

Таблиця 9.3 – Відмінності між технологіями NFC та RFID

Параметр	HF RFID	NFC
Робоча частота	13,56 МГц	13,56 МГц
Зв'язок	Односторонній	Двосторонній
Відстань сканування	До 1 м	До 10 см
Одночасне сканування	Так	Ні

9.2.3 Режим взаємодії двох пристроїв

Режим взаємодії двох пристроїв (англ. "Peer-To-Peer") дозволяє двом мобільним пристроям взаємодіяти між собою. Можливе двонаправлене з'єднання, тобто пристрій А надсилає дані пристрою Б, а пристрій Б може одночасно надсилати дані пристрою А. Використовуючи такий спосіб з'єднання, користувачі можуть обмінюватись візитними картками, фото, документами, тощо. На рис. 9.6 показано взаємне розташування пристроїв в цьому режимі [2].

За допомогою технології NFC неможливо обмінюватись відео та аудіо, але NFC можна використати для швидкого з'єднання двох пристроїв та подальшого обміну даними між ними за допомогою інших безпроводових технологій, наприклад, Bluetooth. При встановленні з'єднання через Bluetooth між двома пристроями виконується ряд операцій: пошук пристроями один одного, сполучення пристроїв, авторизація. Після виконання процесів пошуку, сполучення та авторизації починається передача даних. При використанні технології NFC можливо встановити зв'язок між пристроями швидше, ніж через Bluetooth.

У табл. 9.4 наведені відмінності технологій NFC та Bluetooth.

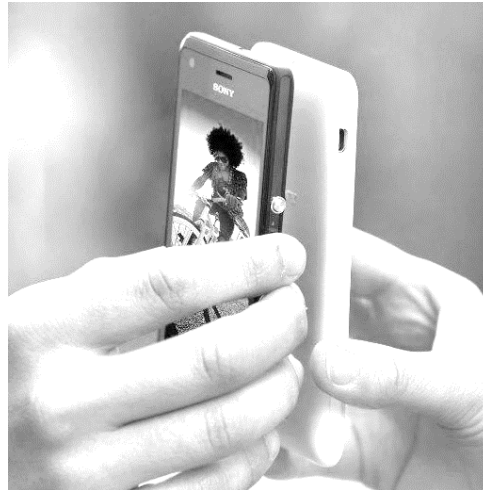


Рисунок 9.6 – Взаємне розташування пристроїв в режимі взаємодії [2]

Таблиця 9.4 – Відмінності технологій NFC та Bluetooth

Параметр	NFC	Bluetooth
Тип з'єднання	Point-to-point	Point-to-multipoint
Радіус дії	Менше 0,1 м	10 м
Швидкість передавання даних	424 кбіт/с	721 кбіт/с
Час встановлення з'єднання	Менше 0,1 с	Менше 6 секунд
Режими зв'язку	Активний, пасивний	Активний
Сумісність з RFID	Так	Ні

9.3 Приклади застосування технології NFC

9.3.1 Платіжні системи

Найбільш ефективно технологію NFC можна реалізувати за допомогою мобільних засобів телекомунікації, а саме телефонів та смартфонів, бо телефон практично завжди знаходиться з користувачем. не потрібно носити жодних додаткових пристроїв або карт. Апаратні засоби сучасного мобільного телефону можна використати для доступу NFC-модулів до систем стільникового зв'язку. Це

дозволяє завантажувати і передавати дані, у тому числі через SMS-повідомлення та глобальну мережу Інтернет [2, 3].

Підтримка режиму емуляції карти дозволяє використовувати телефони з NFC-модулями для проведення операцій через термінали платіжних систем. При цьому телефон може емулювати відразу кілька різних карт, дозволяючи користувачу обирати зручний для нього спосіб оплати і враховувати можливості конкретної платіжної системи.

9.3.2 "Розумні" плакати

Так називаються плакати (або інші об'єкти), в які вбудована пасивна мітка чи NFC-модуль із записаною інформацією. Коли користувач підносить мобільний телефон до NFC-модуля в нього автоматично завантажуються дані що записані у мітці. Наприклад, гіперпосилання, по якому телефон переходить на потрібний сайт для замовлення квитків, або забронювати місце в готелі після прибуття в аеропорт. У мітці можна розмістити і іншу інформацію. Наприклад, адресу готелю і багато чого іншого.

У режимі взаємодії двох NFC-пристроїв модуль на плакаті може зчитувати певну інформацію з пристрою користувача і на її основі формувати пакет даних. Наприклад, отримавши відомості про вподобання користувача, NFC-модуль може завантажити в його телефон список фільмів. Звичайно, частину цих процедур можна виконати вручну, але використання технології NFC робить їх виконання набагато швидшим. Також, з "розумних" плакатів можна завантажувати і більш об'ємну інформацію (буклети, путівники, карти та ін.).

Пасивна мітка, окрім плакатів, може бути фізично вбудована в будь-який об'єкт без жодних електричних зв'язків з ним. Пасивною міткою можуть виступати безконтактна смарт-карта, RFID-мітка або брелок.

9.3.3 Громадський транспорт

В громадському транспорті NFC-технології використовуються для вирішення цілого ряду задач:

- завантажувати розклад, карти і схеми;
- оплачувати проїзд і паркування;
- викликати таксі і потім передавати в його навігаційну систему адресу пункту призначення;
- виконувати багато інших операцій.

Для реалізації таких функцій можуть використовуватись "розумні" плакати та платіжні системи. Застосування технології NFC вигідно як пасажиром, так і водіям. По-перше, вона забезпечує комфорт у оплаті та додаткові сервіси, по-друге дозволяє заощадити значні кошти на паперових квитках і автоматах для їх продажу та ін.

9.3.4 Обмін інформацією

У багатьох випадках зручно передавати дані між двома NFC-пристроями, просто підносячи їх один до одного. Наприклад, так можна обмінятися контактною інформацією між двома мобільними телефонами (замість використання візиток).

Ще одним прикладом може бути ноутбук та цифрова камера. Наприклад, користувач хоче встановити Bluetooth-зв'язок між цими пристроями для обміну фотографіями. Bluetooth-лінія встановлюється шляхом близького знаходження пристроїв один до одного, а протокол запускається з використанням NFC. Це робить набагато легшим встановлення зв'язку для користувача з двома пристроями і виключає роботу з навігацією через меню для вибору правильного пристрою зі списку можливих партнерів зв'язку [4, 5].

9.3.5 Медицина

Надавши кожному пацієнту в лікувальних закладах свою NFC-мітку можна значно спростити лікувальний процес. Ця мітка міститиме інформацію про ім'я, адресу, вік, захворювання та необхідні ліки та процедури [1]. Таке застосування технології NFC може значно зменшити час що витрачається на заповнення різних форм як у паперовому так і у електронному вигляді.

Ще один приклад використання NFC-міток – біометричні паспорти.

Контрольні питання

1. Який принцип дії пристроїв NFC?
2. На яких частотах здійснюється зв'язок між пристроями NFC?
3. Яку швидкість передавання даних забезпечують пристрої?
4. Які режими зв'язку використовуються у пристроях NFC?
5. У чому полягає сутність режиму роботи емуляції карти?
6. У чому полягає сутність режиму роботи зчитування/запису?
7. У чому полягає сутність режиму роботи взаємодії двох пристроїв?
8. Чи можна передавати відео за допомогою пристроїв NFC?
9. Чи може пристрій NFC зчитувати дані з радіочастотних міток?
10. Як можна використати пристрої NFC в медицині?
11. На якій відстані можуть взаємодіяти пристрої NFC?

Перелік посилань

1. Prasad S. Halgaonkar , Sukmal Jain, V.M.Wadhai. NFC. A review of technology, tags, applications and security. International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, 2013.

2. Lou Frenzel "NFC Lets You Leave Your Cash And Credit Cards At Home" 2012. Url: <http://electronicdesign.com/energy/nfc-lets-you-leave-your-cash-and-credit-cards-home>. (дата звернення: 29.06.2024).
3. Ernst Haselsteiner and Klemens Breitfuß. Security in Near Field Communication (NFC). Strengths and Weaknesses, 2006.
4. Annika Paus. Near Field Communication in Cell Phones. Seminararbeit Ruhr-Universität at Bochum, 2007.
5. Rohde & Schwarz. Технологія NFC і проведення випробувань бездротового зв'язку ближньої дії, 2010. Url: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma182/1MA182_5rus_NFC_WHITE_PAPER.pdf. (дата звернення: 29.06.2024).

10 СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

10.1 Призначення систем охоронного відеоспостереження

Призначення охоронного телебачення полягає у підвищенні рівня безпеки об'єкта, тобто в мінімізації можливих наслідків небажаних впливів на людей, на матеріальні цінності і на інформаційні ресурси [1, 2]. Небажані впливи з зовнішньої (стосовно до охоронної зони) середовища можуть бути як усвідомленими (з боку кримінальних елементів), так і результатом техногенних катастроф або стихійних лих.

Охоронні **системи відеоспостереження** призначені для візуального спостереження за об'єктом, що охороняється, за допомогою відеокамер. Системи відеоспостереження дозволяють стежити одночасно за одним або кількома об'єктами (рис. 10.1) [3]. Камери відеоспостереження можна встановити як усередині приміщення, так і зовні. Завдання охоронної системи відеоспостереження полягає в наочному поданні відеоінформації про оперативну обстановку на контрольованому об'єкті.



Рисунок 10.1– Відеокамери для стеження за декількома об'єктами [3]

Найпростіша система відеоспостереження включає в себе одну або кілька відеокамер і монітор або телевізор. Камери відеоспостереження можуть встановлюватися на поворотних пристроях зовні або всередині приміщення і дозволяють здійснювати цілодобове стеження за територією, що охороняється (рис. 10.2). Спільно з системою відеоспостереження можна використовувати датчики руху (детектори), системи освітлення та інші додаткові пристрої.



Рисунок 10.2 – Внутрішня відеокамера Motorola Focus 66 WiFi HD Audio and Video Home Security Camera [4]

У системах відеоспостереження, розрахованих на використання декількох відеокамер, на екрані одного монітора можна одночасно показувати зображення від всіх відеокамер (рис. 10.3). Для цього служать **квадратори** (подільники екрану). Для послідовного виведення зображень використовуються **мультиплексори** (комутатори), які послідовно підключають відеокамери до монітора або телевізора [5].



Рисунок 10.3 – Відображення сигналів від декількох відеокамер на екрані монітора [5]

Охоронні системи відеоспостереження дозволяють створити гнучку і нарощувану систему безпеки, до якої можуть входити не тільки компоненти систем відеоспостереження, а й охоронно-пожежна сигналізація та системи контролю доступу.

Системи прихованого відеоспостереження використовуються для підвищення ефективності охорони і встановлюються там, де необхідно приховати факт спостереження. Завдання систем прихованого відеоспостереження – не вивчати відвідувачів, а контролювати ситуацію на території, що охороняється.

Шпигун лампочки з FULL HD, WiFi з 24-кратним ІК-світлодіодом нічного бачення та детектором руху з кутом огляду 120° – найкраща камера безпеки для квартири (рис. 10.4) [6]. Камера захована в лампочці зі стандартним цоколем E27, а також оснащена ІЧ-нічним підсвічуванням. Світлодіоди на лампочці призначені лише для нічного бачення, лампочка не світиться, тому вона не працює як звичайна

лампа. Відео зі звуком записується в роздільній здатності Full HD 1920×1080 пікселів із частотою 25 кадрів/с.

Завдяки з'єднанню Wi-Fi є можливість переглядати відео зі звуком у режимі реального часу на своєму ПК чи смартфоні. Камера працює з операційними системами Windows та Mac для ПК та Android та iOS для мобільних телефонів. Завантаживши безкоштовний мобільний додаток HD SMART IPC, можна керувати камерою за допомогою телефону. У програмі можна налаштувати якість запису, звук, обертання та перегортання зображення тощо. Також є можливість встановити режим виявлення руху, нічне бачення та перегляд збережених записів у камері.



Рисунок 10.4 – Система прихованого відеоспостереження [6]

10.2 Переваги систем охоронного телебачення

Перевага охоронного телебачення в порівнянні з іншими охоронними системами полягає в його високій інформативності (90% всієї інформації про навколишній світ людина отримує завдяки органам зору) [1]. Перевірити правильність функціонування систем безпеки, переконатися в реальності тривоги, сформованої сигналізацією (охоронною, пожежною, периметровою, антикрадіжковою, автомобільною) можна не тільки відвідуванням людиною місця події, а й дистанційно – за допомогою охоронного телебачення. Ще важливіше

запобігти інциденту, виявивши небезпечний рух на підступах до охоронюваної зони, розшифрувавши можливу загрозу по екрану відеомонітора, що особливо актуально для віддалених необслуговуваних об'єктів. З цим охоронне телебачення також успішно справляється.

Недосконалість будь-якої з систем безпеки в окремих випадках призводить до взаємного доповнення, деякого симбіозу систем, до спроб проектувальників інтегрувати різні системи в єдину систему безпеки, щоб істотно зменшити вплив слабких сторін кожної з систем, підвищити достовірність одержуваної оператором інформації. Інтеграція систем охоронного телебачення (на апаратному та/або програмному рівні) з іншими системами – це шлях підвищення рівня безпеки.

Повинно також враховуватися недосконалість зовнішніх охоронних датчиків, як і детекторів руху (у плані пропуску тривоги і формування сигналів помилкової тривоги). Це змушує створювати таку систему охоронного телебачення, яка буде відображати не тільки зону з джерелом тривоги, але і найближчі, пов'язані з нею зони, а також вести відеозапис не лише протягом часу прояву тривоги, але і до моменту виявлення причини тривоги, а також усунення цих причин.

10.3 Особливості обробки сигналів в охоронному телебаченні

Використовуваний в охоронному телебаченні стандарт на телевізійний сигнал спочатку розроблявся для ефірного телебачення з метою представлення спостерігачеві на одному екрані одного зображення. Основними вимогами при розробці стандарту було створення технічними засобами на екрані телевізора якісного зображення з урахуванням особливостей людського зору, раціонального використання частотного діапазону і сумісності різних систем телебачення (рис. 10.5).



Рисунок 10.5 – Формування якісного зображення в телевізійному мовленні

Завданням охоронного телебачення нерідко є формування на екрані монітора, що спостерігає оператор, одночасно декількох (іноді багатьох) зображень з різних контрольованих зон, запис і передача відеосигналів від багатьох відеокамер. Отримання і реєстрація цих зображень в режимі реального часу, тобто без втрати інформації, можна реалізувати лише при паралельній обробці відеосигналів, в іншому випадку (при використанні "перетворення в цифровий код" відеосигналів) рух об'єктів на екрані відображається переривчасто (проявляється так званий "строб-ефект").

У простих охоронних відеосистемах здійснюється мультиплексування сигналів. Проте зараз, як правило, здійснюється паралельна обробка інформації і виведення на 1 екран 16 відеоканалів в режимі реального часу. Це робить більш комфортною роботу оператора.

Необхідно відзначити, що **головним завданням охоронного телебачення є не отримання якісного зображення на екрані відеомонітора, а можливість формування достовірного судження про наявність тривожної ситуації.** У цьому плані спотворення зображення, неприпустимі в мовному телебаченні, виявляються прийнятними в охоронному телебаченні, а саме:

- частота зміни кадрів може бути істотно нижче 25 Гц;
- замість обробки двох полів може оброблятися тільки одне поле;

- передача кольору і передача градацій сірого можуть істотно відрізнятися від природної;

- нелінійні або геометричні спотворення не відіграють істотної ролі.

Тому в охоронному телебаченні широко використовуються компромісні рішення, при яких одні параметри "розмінюються" на інші, а саме [1, 2]:

- роздільна здатність на швидкість оновлення;
- чутливість на роздільну здатність;
- чутливість на швидкодію;
- коефіцієнт підсилення на смугу пропускання.

З іншого боку, набувають значимості деякі характеристики, що не оцінюються в мовному телебаченні (наприклад, можливість оператору контролювати зображення на екрані відеомонітора під гострим кутом огляду).

Для охоронного телебачення повинні враховуватися умови цілодобової експлуатації обладнання в реальних умовах життя і діяльності людини з урахуванням впливу навколишнього середовища (та інших людей).

Внаслідок прикладного характеру систем охоронного телебачення їх технічні рішення диктуються можливістю, простотою та економічною ефективністю практичної реалізації. Зокрема, одним з найважливіших параметрів систем охоронної сигналізації є зручність їх монтажу та введення в експлуатацію, завдяки чому використовується максимум стандартних рішень, що полегшують і прискорюють інсталяцію.

10.4 Класифікація цифрових систем відеоспостереження

10.4.1 Вступні зауваження

Сьогодні в експлуатації перебувають аналогові і цифрові системи відеоспостереження. Розглянемо системи, що зазвичай об'єднують поняттям "цифрові системи відеоспостереження" (ЦСВС) або із зарубіжної термінології DVR (Digital Video Recorder – цифровий записуючий пристрій). За кордоном поширені такі поняття [7]:

- DVR – в основному під цією аббревіатурою розуміють PC- або non-PC-пристрої; в першому випадку частіше вживають термін DVR-card, маючи на увазі плати як компонент для побудови PC-системи.

- IP-video – система, побудована на базі IP- або LAN-відеокамер або серверів (конверторів). У даному визначенні не відбитий момент наявності/відсутності ПЗ для запису, хоча зазвичай вважають, що ця та деякі інші функції в системі передбачені.

Дана класифікація не є єдино можливою. Так, виходячи зі способу побудови системи та її виконання всі ЦСВС можна поділити на три категорії.

1. ЦСВС, побудовані за допомогою плат перетворення в цифровий код і/або компресії відео на базі персональних, промислових або спеціалізованих комп'ютерів, із застосуванням багатофункціональних процесорів Intel і AMD і ОС Windows або Linux в будь-яких їх варіаціях (рис. 10.6) [8].



Рисунок 10.6 – Плата захоплення відеосигналів [8]

2. ЦСВС на базі так званих некомп'ютерних (non-PC) платформ. Само собою, в них теж є процесор і операційна система (наприклад, NiOS-ОС для вбудованих систем або Embedded Linux). Але здебільшого це закінчені пристрої, що не мають можливості модернізації ні за процесором, ні за кількістю каналів, рідко мають можливість поновлення внутрішніх мікропрограм у широкому сенсі (рис. 10.7) [9].



Рисунок 10.7 – Відеореєстратор для систем non-PC [9]

3. Третій напрям – це IP-відеоспостереження.

IP (мережеве) відеоспостереження – система відеоспостереження, що базується на цифрових мережах [10]. Будується із застосуванням мережових відеокамер або відеосерверів – пристроїв, що конвертують аналогове відео в цифрове і передають його мережею для зберігання, обробки і відображення.

Такі системи, як і в першому випадку, будуються обов'язково з використанням ПК (хоча для архівації можна обійтися і без комп'ютера, виконуючи запис на мережовий диск (NAS), але переглядати записане все одно доведеться через ПК). Однак на відміну від PC-систем, ті схеми, які відповідають за перетворення в цифровий код сигналу, компресію, а іноді й детектування, винесені в окремий блок, максимально наближений до відеокамери або розташований безпосередньо на ній. У IP-системах цифрові мережі використовуються для передачі відео та інших даних до сховища і монітора.

10.4.2 Огляд можливостей і сфер застосування існуючих систем

Незважаючи на те, що категорій лише три, перші дві представлені вже десятками, навіть сотнями систем, третя також скоро наздожене перші дві за кількістю виробників, пропонованих моделей і наданих ними можливостей [11].

Практика показує, що основну частку ринку, незважаючи якісні характеристики, займають добре розкручені і супроводжувані бренди (бренд – торговий знак компанії, яким вона диференціює свою продукцію від конкурентів). Нижче наведено рекомендації щодо вибору категорії устаткування.

У яких випадках переважно обирати **систему, що базується на ПК**:

1. Коли необхідно здійснювати відеоспостереження та запис на невелику кількість каналів (2...4) і в розпорядженні є будь-який (у тому числі домашній або офісний) комп'ютер.

2. Якщо є комп'ютер достатньої потужності (виходячи з кількості каналів та їх швидкості), який можна використовувати в цілях відеоспостереження або віддати цілком під виконання цих завдань.

3. Якщо однозначно відомо, що система буде розширюватися як в плані кількості каналів запису/спостереження, так і в плані збільшення кількості жорстких дисків.

4. Коли необхідна інтеграція з системами ОПС (охоронно-пожежна сигналізація) та СКД (система контролю доступу) або з іншими.

5. Коли необхідні серйозні можливості і настройки в плані визначення руху (активності).

6. Часто, особливо при побудові великих систем, що виходять за рамки 16 каналів, виникає необхідність поєднання різномірних систем. Такою можливістю володіють тільки інтегровані системи на базі ПК.

Щодо ринку **non-PC-пристроїв**, то у першу чергу споживачів приваблює простота застосування цього класу устаткування. Добре спроектований рекордер мало відрізняється в налаштуванні і використанні від побутового

відеомагнітофона. Через обмеженість функцій і відсутності "зайвих" компонентів поп-РС-пристрій надійніше комп'ютерного.

У якому випадку перевага надається поп-РС системам:

1. Насамперед, коли потрібні надійність і простота використання, не планується розширення системи і не потрібні додаткові можливості.
2. Система ЦСВС повинна працювати тривалий час автономно, без постійного контролю з боку оператора.
3. Не потрібна інтеграція з системами ОПС і СКД.
4. Рідко потрібна або зовсім не потрібна можливість копіювання або резервування архівів.

Категорія **систем ІР-відеоспостереження** поки ще не стала домінуючою з двох основних причин. По-перше, це практична відсутність системного програмного забезпечення, що дозволяє використовувати різні мережеві сервери і відеокамери для побудови ЦСВС. По-друге, недорогі пристрої не забезпечують досить високої якості, а мережеві відеокамери високої якості все ще мають високі ціни, що перевищують вартість РС- або поп-РС-систем з аналогічними параметрами. Однак ці недоліки стрімко сходять нанівець.

Споживачеві рекомендовано використовувати ІР-системи, якщо:

1. Немає можливості прокласти кабелі або можна використовувати існуючі кабельні мережі (СКС).
2. При необхідності легально, без отримання дозволу на частоти, використовувати безпроводовий зв'язок для організації системи.
3. Система розподілена і рознесена на великій території і є необхідність скоротити кількість кабельної розводки.
4. На об'єкті складна обстановка з завадами, і немає можливості використовувати аналогову передачу даних.
5. Необхідно віддалене спостереження з реєстрацією не в точці спостереження.
6. Необхідно знизити ймовірність перехоплення сигналів від камер спостереження.

Однак у IP-систем є і мінуси. Неможливо отримати нестиснене зображення і його необхідно декодувати для перегляду. Можливість детектування руху в основному буде обмежена можливостями самих IP-відеопристроїв або детектуванням за стисненим зображенням.

Системи, що базуються на ПК, є багатофункціональними і багатозадачними. Можна сформулювати деякі додаткові вимоги, яким повинна відповідати хороша ПК-система.

1. Система повинна дозволяти переглядати архівне відео, не перериваючи процесу перегляду "живого" відео (багато систем азіатського виробництва таку функцію не підтримують).

2. Забезпечення синхронного запису звуку (відсутність такої функції допустимо тільки для систем нижнього цінового діапазону).

3. Системи з програмним стисненням, що базуються на PCI-платах, нездатні записувати відео 25 кадрів/с з високою роздільною здатністю, починаючи вже від 8 каналів. У разі коли заявляється 400 кадрів запису на програмній системі з платами PCI 32 bit, мова завжди йде про роздільну здатність 320×240 або близьку до неї. Тому для збільшення роздільної здатності треба використовувати 64-розрядні пристрої.

4. Вибір PC-системи повинен давати додаткові можливості (у детектуванні руху, можливості тотального конфігурування та ін.).

5. Легальність ПЗ.

Non-PC-пристрої давно вже стали дуплексними і підтримують мережеві технології. Зростання конкуренції і зниження цін дозволяють відразу придбати досить багато додаткових функцій, які, можливо, і не потрібні. Потрібно звернути увагу на можливість копіювання архівів або підключення дисків з рекордера до комп'ютера для їх читання і копіювання.

Тепер, коли дуплексний режим в цих системах широко використовується (запис і одночасний перегляд "живого" відео), майбутнє за триплексним режимом – можливість запису, перегляду "живого" та архівного відео одночасно.

Приблизно в 70% пристроїв для компресії відео використовується JPEG або MJPEG (Motion JPEG): середній розмір кадру тут набагато більше, ніж в системах з використанням MPEG-2 або MPEG-4 (H.264). І хоча вартість таких систем вища, при зберіганні архіву протягом тривалого часу вартість жорстких дисків може виявитися більш високою, ніж різниця в ціні відеокамер і пристроїв компресії.

При виборі non-PC-систем кращим рішенням буде пристрій з НТТР-інтерфейсом. Це дозволить управляти системою з будь-якого комп'ютера, не встановлюючи програму-клієнт. Але слід пам'ятати, що НТТР менш захищений від мережових атак, особливо при роботі через глобальну мережу.

IP-системи швидко розвиваються. При їх виборі обов'язково слід передбачити наявність відео-серверів, кодеків типу MPEG-4 або H264 (для зменшення трафіку при передаванні даних). Дуже важлива частина IP-системи – ПЗ сервера. Саме ця складова перетворює набір окремих камер в систему. Тому особливу увагу необхідно звертати на можливості серверного ПЗ.

До основних переваг цифрових систем відеоспостереження слід віднести:

- високу якість відтворюваного відеозапису;
- високу швидкість доступу до відеоархіву;
- запис тільки тривожних подій;
- можливість збільшення і масштабування будь-якого кадру у цифровому форматі;
- миттєвий пошук і перегляд відеозапису за номером камер, датою і часом;
- можливість інтеграції з іншими комп'ютерними системами безпеки;
- легка трансляція відеоархівів за каналами зв'язку (Інтернет та ін.);
- можливість відправлення повідомлень тривоги електронною поштою і SMS;
- можливість експорту відеоінформації на сумісні зовнішні носії.

Трансляція відеозображення – одна з основних можливостей сучасних цифрових систем. Вона дозволяє, перебуваючи в офісі або на іншому робочому місці спостерігати за тим, що відбувається в зоні спостереження камер, які,

встановлені на віддалених об'єктах. Як правило, така можливість використовується для спостереження за виробничими процесами, або за особистими квартирами або будинками.

Для спрощення сприйняття викладеної інформації в табл. 10.1 наведені порівняльні характеристики різних типів цифрових систем з додатковою інформацією про кількість каналів у кожній категорії [12].

Таблиця 10.1 – Порівняльні характеристики цифрових систем відеоспостереження

Параметр	PC-based	Non-PC	IP-відео
Кількість каналів 25 кадрів/с в один блок	40	16	До 64
Кількість мультимплексованих каналів в один блок	64	16	Більш ніж 100
Максимальна роздільна здатність	768×576 (PAL)	720×576 (PAL)	3 мегапікселі і більше
Можливість оновлення	Не обмежена для ПЗ	Обмежена	Не обмежена для ПЗ
Можливість розширення	Можливо	Неможливо	Можливо
Відносна функціональність	Висока	Середня	Висока

Крім цифрових систем сьогодні також продовжують користуватися аналоговими. Переваги **аналогових систем відеоспостереження**:

- простота в налаштуванні і роботі;
- дозволяють наймати для обслуговування персонал меншої кваліфікації;
- висока надійність.

Недоліки:

- обмеженість функцій;
- вимагають постійного обслуговування (зміни та архівації касет, періодичного чищення і заміни відеоголовок відеомагнітофона).

Аналогові системи використовують там, де необхідно організувати відеоспостереження в невеликому числі приміщень і інформацію з відеокамер

записувати на відеоманітофон або спостерігати за тим, що відбувається на території, недоступній щохвилинному контролю (наприклад відкрити ворота автомобілю, що заїжджає).

10.5 Склад систем відеоспостереження

Залежно від категорії (виду) системи відеоспостереження до її складу можуть входити (рис. 10.8):

- відеокамери;
- мультиплексори;
- відеореєстратори (аналогові або цифрові залежно від системи);
- монітори;
- подільники зображень;
- сервери відеоспостереження;
- контролери управління;
- плати відеозахоплення;
- інтерфейси зв'язку;
- програмне забезпечення;
- блоки живлення.



Рисунок 10.8 – Склад простої системи відеоспостереження [13]

10.6 Приклади найпростіших систем відеоспостереження

На рис. 10.9 наведена узагальнена структурна схема аналогової системи відеоспостереження, що випускалася ще 15 років тому [14].

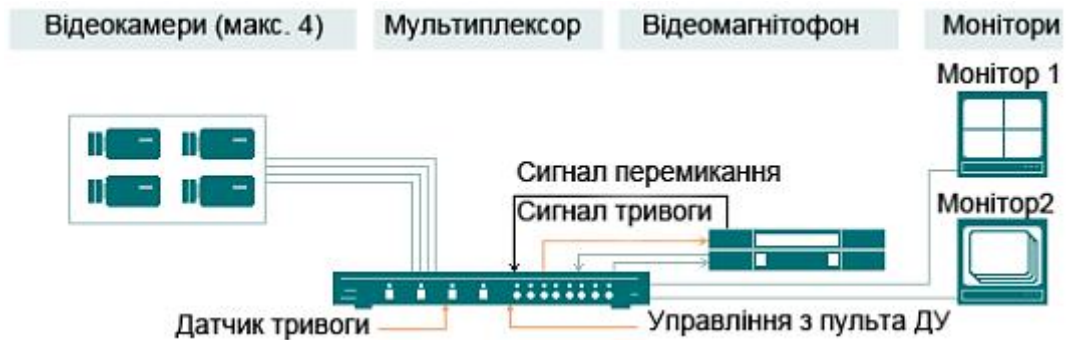


Рисунок 10.9 – Узагальнена структурна схема аналогової системи відеоспостереження [14]

Система у своєму складі має: мультиплексор MPX-MD4P, відеомагнітофон TLS-9924P, 4 відеокамери VCB-3455P, 4 об'єктиви VA-13VG308AS, 4 кронштейни VA-VCT31, монітор VM6615 та БЖ (блок живлення).

Комплект обладнання для професійної ч/б системи відеоспостереження з цілодобовою реєстрацією (рис. 10.10) [14] складається з таких елементів: мультиплексор MPX-MD162P, відеомагнітофон TLS-9924P, 16 відеокамер VCB-3455P, 16 об'єктивів VA-13VG308AS, 16 кронштейнів VA-VCT31, монітор VM6615 та БЖ.



Рисунок 10.10 – Узагальнена структурна схема професійної ч/б системи відеоспостереження [14]

Мультиплексор MPX-MD162P дозволяє здійснювати запис відеозображень одночасно від 16 підключених відеокамер VCB-3440P (рис. 10.11) [14].

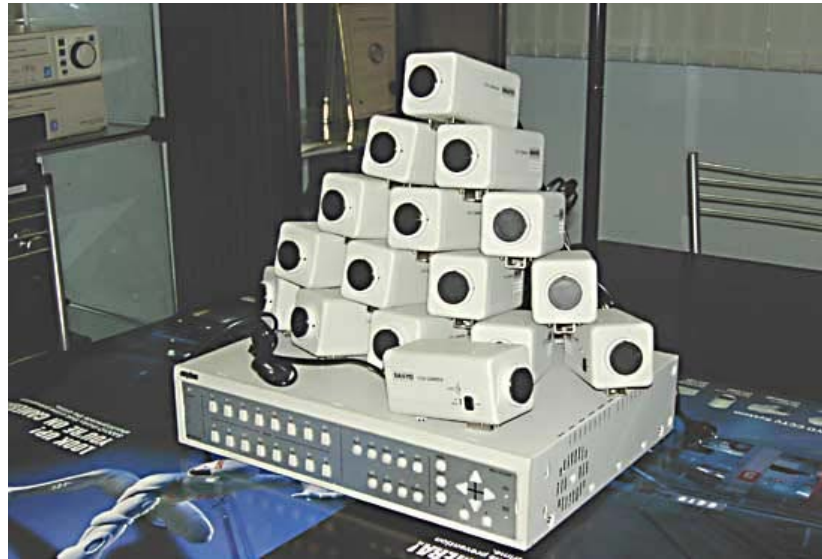


Рисунок 10.10 – Мультиплексор MPX-MD162P та 16 відеокамер VCB-3440P [14]

Комплект обладнання для невеликої системи відеоспостереження з цілодобовою реєстрацією (рис. 10.12) [14] містить: мультиплексор MPX-CD92P, відеомагнітофон TLS-9924P, 9 кольорових відеокамер VCC-5775P, 9 об'єктивів VA-13VG308AS, 9 кронштейнів VA-VCT31, кольоровий монітор VMC-8415FP, БЖ.

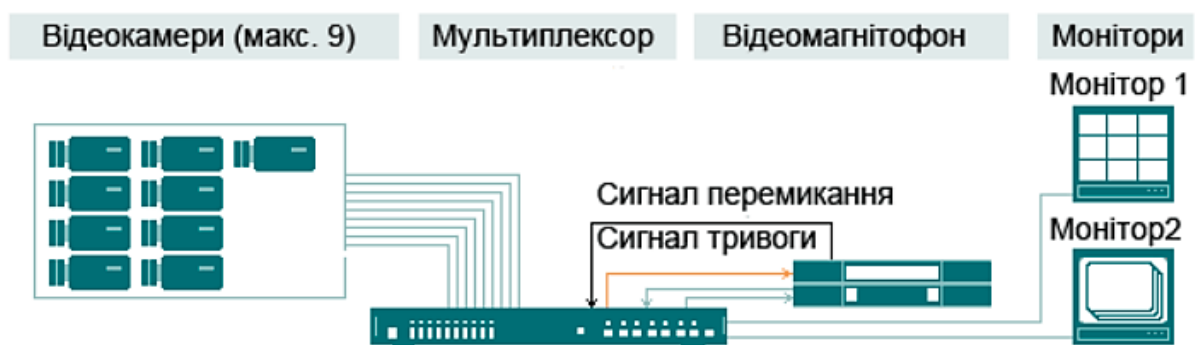


Рисунок 10.12 – Узагальнена схема системи відеоспостереження з цілодобовою реєстрацією [14]

Мультиплексори (MPX-MD4P, MPX-MD162P, MPX-CD92P) дозволяють здійснювати запис відеосигналів одночасно від всіх підключених відеокамер (VCB-

3455P, VCC-5775P) на відеомагнітофон і спостерігати на екрані монітора поточне зображення в мультиекранному режимі.

Відеомагнітофон тривалого запису TLS-9924P [14] використовується для запису подій, що відбуваються на протязі тривалого часу.

Підключивши два монітори, можна одночасно виводити зображення від різних відеокамер, а також спостерігати "живе" зображення від відеокамер і відтворене з відеомагнітофона.

Мультиплексори мають один недолік. Він полягає в тому, що при роботі режиму мультикартинки зображення, отримане з камер відеоспостереження, виходить переривчастим. Це пов'язано з цифровою обробкою зображення, яке пристрій здійснює в момент її передачі на екран монітора [14].

Всі мультиплексори, які зараз можна зустріти на ринку відеоспостереження, оснащені додатковими роз'ємами. Вони призначені для підключення таких додаткових пристроїв, датчики руху, а також іншого обладнання, яке бере участь у процесі забезпечення безпеки на об'єкті. Найчастіше мультиплексор використовують з двома моніторами. На екрані одного можна бачити картинку з зображенням всіх камер, які підключені до системи, а на екрані другого — зображення з відеокамери, яка веде спостереження за пріоритетною територією.

Крім того, мультиплексори оснащені детекторами активності, які дозволяють визначити, в якій частині об'єкта, що знаходиться під спостереженням, були помічені активні дії. В той момент, коли відбулися які-небудь зміни, мультиплексор видає сигнал, а картинка отримана з відеокамери відображається на моніторі. На рис. 10.13 наведений зовнішній вигляд сучасних мультиплексорів [15].



Рисунок 10.13 – Сучасні мультиплексори на 8 та 16 вхідних каналів [15]

На сьогоднішній день відеомагнітофони використовуються тільки у старих системах. У всіх нових системах найчастіше в системі відеоспостереження використовують відеореєстратори з вмонтованим жорстким диском. Кількість каналів запису такого відеореєстратора може становити від 8 до 25, а ємність жорсткого диска від 500 до 2000 Мбайт. Перед записом на диск зображення стискається для зменшення швидкості відеопотоку.

В залежності від конструкції і сфери застосування відеокамер реєстратори діляться на групи [16]:

1. Цифрові DVR реєстратори – це багатофункціональне обладнання, яке використовують для підключення до аналогових камер. Вони отримують сигнал по коаксіальному кабелю, стискають його, перетворюючи в цифровий формат, після чого зберігають картинку на жорсткому диску (HDD). Підключення аналогових відеокамер здійснюється через BNC-роз'єми. При використанні на невеликому просторі DVR-реєстратори не поступаються за якістю цифровим камерам.

2. Мережеві NVR відеореєстратори – застосовуються для підключення IP-відеокамер і записи цифрового відеосигналу зі збереженням інформації на жорсткому диску. NVR-реєстратори отримують зображення в стислому вигляді за допомогою технології Рое, яка дозволяє передавати дані і отримувати електроенергію для віддалених IP-камер через виту пару в мережі Ethernet.

3. Гібридні HVR реєстратори – професійне обладнання, що є перехідним між аналоговими і цифровими пристроями. Воно дозволяє отримувати зображення на IP-камери за допомогою кабелів типу Cat5 і Cat6. Підключення HVR до аналогових камер виконується через BNC-роз'єми. Гібридна апаратура необхідна для охорони складних об'єктів і великих територій, при цьому камери встановлюють як зовні, так і всередині приміщень.

Прикладом такого відеореєстратора може бути Dahua DH-DVR2404LF-S [16]. Відеореєстратор дозволяє під'єднати 24 відеокамери і здійснювати запис не тільки зображення, але і звукового супроводу від мікрофонів 16 камер. Його характеристики наведені в табл. 10.2 а зовнішній вигляд – на рис. 10.14.



Рисунок 10.14 – Відеореєстратор Dahua DH-DVR2404LF-S [17]

Таблиця 10.2 – Характеристики відеореєстратора DH-DVR2404LF-S

Кодек для стиснення зображення/звуку	H.264 / G.711
Операційна система	Вбудована, LINUX
Основні функції	Запис, відтворення, перегляд запису, запис і перегляд записаного раніше зображення, резервне копіювання, віддалене управління по локальній мережі.
Способи управління	З передньої панелі, за допомогою маніпулятора "мишка", пультом дистанційного управління, команди по локальній мережі
Кількість входів відеосигналу	24 канали, роз'єднувач типу BNC, розмах напруги відеосигналу 1 В, вхідний опір 75 Ом
Виходи зображення	1 HDMI, 1 VGA, 1 TV, 1 Spot
Входи для запису звуку	16 каналів, роз'єднувач типу BNC, канал 1 можна використати для двостороннього зв'язку
Вихід звукового сигналу	1 канал
Вбудований дільник екрану	1/4/9/16/25
Матричний вихід	1/4/9/16/25
Роздільна здатність при запису зображення *	D1 (704×576) / HD1(352×576) Field (704×288) / CIF (352×288)
Швидкість кодування	Основний потік: HD1/2CIF(Field)/CIF (1...25 кадр/с), D1 (1...12 кадр/с), Додатковий потік: CIF/QCIF (25 кадр/с)
Частота дискретизації (бітрейт)	32...2048 кбіт/с
Режими запису	Вмикання вручну, за розкладом, постійна, по спрацьовуванню датчика руху, відсутності зображення на екрані, відсутності відеосигналу, спрацьовуванню датчиків тривоги.

*Примітка: * За одиницю роздільної здатності при запису прийняте позначення CIF, що відповідає роздільній здатності 352×288 пікселів. Виходячи з цієї одиниці формуються такі позначення: 2 CIF має роздільну здатність 704×288 пікселів і позначається як Field, 4CIF – 704×576 і позначається як D1. Формат 352×576 позначається як HD1.*

Область застосування перелічених систем відеоспостереження: супермаркети, котеджі, видовищні заклади, шпиталі, виробничі підприємства, автостоянки, митні термінали, банки, закусочні з самообслуговуванням (бістро), невеликі магазини, клініки, виробничі приміщення, клуби.

Контрольні питання

1. Розкрийте зміст поняття "система охоронного відеоспостереження", її призначення та особливості.
2. В чому особливість систем прихованого відеоспостереження?
3. В чому суть компромісних рішень щодо параметрів сигналу в системах відеоспостереження?
4. Відмінності систем мовного телебачення від систем охоронного телебачення.
5. Які категорії ЦСВС сформовані на сьогоднішній день та які їх можливості?
6. Охарактеризувати особливості систем з РС-пристроями, їх застосування.
7. Охарактеризуйте особливості систем з non-РС-пристроями, наведіть приклади їх застосування.
9. Охарактеризуйте особливості систем IP-відеоспостереження, наведіть приклади їх застосування.
10. Назвіть переваги та недоліки аналогових систем відеоспостереження.
10. Опишіть склад та призначення елементів найпростішої системи відеоспостереження (за вибором).

Перелік посилань

1. Vlado Damjanovski CCTV: From Light to Pixels 3rd Edition. Butterworth-Heinemann; 3rd edition (October 2, 2013). 616 p.
2. Види систем відеоспостереження - вибір і огляд систем відеоспостереження. Url: https://secur.ua/articles/ua_vidi-sistem-videosposterezhennja-vibir-i-ogljad-sistem-videosposterezhennja.html (дата звернення: 26.11.2024).
3. Choosing the Right Long Range Security Camera. Url: <https://iottoday.com/blog/choosing-the-right-long-range-security-camera/> (дата звернення: 26.11.2024).
4. Motorola Focus 66 WiFi HD Audio and Video Home Security Camera. Url: <https://www.todayoutlet.store/?path=page/ggitem&ggpid=623676> (дата звернення: 26.11.2024).
5. Відеоспостереження для квартири. Url: <http://www.camservice.com.ua/flat/> (дата звернення: 26.11.2024).
6. Шпигун лампочки з FULL HD + WiFi + 24-кратний ІК-світлодіод з кутом 120 °. Url: <https://www.cool-mania.com.ua/spigunstvo/spigunski-kameri/spigun-lampocki-z-full-hd-wifi-24-kratnij-ik-svitlodiod-z-kutom-120> (дата звернення: 26.11.2024).
7. What is a Digital Video Recorder (DVR)? Url: <https://senstar.com/senstarpedia/what-is-dvr/> (дата звернення: 26.11.2024).
8. Плати відеозахоплення. Url: <https://smartel.ua/ua/platy-videozakhvata/?srsltid=AfmBOoqUxOGM2Px1JfVeIUHmZETpMU3JGLJRF9wEl4w9M11iDhrrp7Ge> (дата звернення: 26.11.2024).
9. Відеореєстратори. Url: <https://smartel.ua/ua/videoregistratory/> (дата звернення: 26.11.2024).
10. Відеоспостереження. Url: https://ic-trade.com.ua/videosposterezhennia/?utm_source=google&utm_medium=cpc&utm_campaign=pmax-videosp&utm_term=&gad_source=1&gclid=Cj0KCQiAgJa6BhCOARIsAMiL7V-

hi0osT9EPChC0MiQUgKkVnJAKc3oPFZepYdETllpVePA5Z4LFHyAaAhNnEALw_wcB (дата звернення: 26.11.2024).

11. 7 можливостей сучасного відеоспостереження. Url: <https://maxnet.ua/blog/7-vozmozhnostey-sovremennogo-videonablyudeniya/> (дата звернення: 26.11.2024).
12. 5 найважливіших характеристик ефективних систем відеоспостереження. Url: <https://worldvision.com.ua/articles/5-vazhneyshih-harakteristik-effektivnih-sistem-videonablyudeniya> (дата звернення: 26.11.2024).
13. Сучасна система відеоспостереження: з чого складається та як підібрати обладнання. Url: <https://eurodnepi.com.ua/suchasna-sistema-videosposterejeniya-z-chogo-skladatsya-ta-yak-pdbrati--ua/> (дата звернення: 26.11.2024).
14. Philips Retail камера безпеки і відеосистеми. Url: https://by.ebay.com/b/Philips-Retail-Security-Camera-Video-Systems/46974/bn_99581359 (дата звернення: 26.11.2024).
15. Мультиплексори систем відеоспостереження. Url: <http://tren.com.ua/multipleksori-sistem-videospostere/> (дата звернення: 26.11.2024).
16. Відеореєстратори для відеоспостереження. Url: <https://control.ua/ua/ohrannye-videoregistratory/> (дата звернення: 26.11.2024).
17. 24-канальний відеореєстратор Dahua DH-DVR2404HF-S. Url: <https://dahua-technology.com.ua/videoregistrator-dahua-dh-dvr2404hf-s> (дата звернення: 26.11.2024).

11 КОМПОНЕНТИ СИСТЕМ ОХОРОННОГО ВІДЕОПОСТЕРЕЖЕННЯ

11.1 Де потрібно використовувати відеоспостереження

Окремі камери або системи відеоспостереження встановлюють, щоб за чим-небудь стежити. Наприклад:

1. У будинку чотири квартири. Щоб зрозуміти, чи роблять діти домашню роботу, чим зайнята нянька, як себе почувають літні люди, не пробралися чи в будинок злодії й що роблять свійські тварини.

2. У під'їзді, у дворі, на паркуванні. Щоб з'ясувати, хто смітить на сходовій клітці, пише на стінах, псує газони й клумби або займає чуже паркувальне місце.

3. На дачі. Щоб побачити, хто здійснив проникнення в будинок, хто потоптався по грядках, як себе почувають рослини.

4. На невеликому підприємстві. Наприклад, у піцерії, кав'ярні або перукарні. Камера допоможе зрозуміти, у який момент із каси зникли гроші, куди поділися продукти, хто влаштовує вечірки з кальяном в офісі ночами. Можна влаштувати трансляцію з кухні, щоб покупці бачили, як роблять піцу.

5. На великих підприємствах і в офісних центрах. Камери доповнюють системи безпеки й дозволяють здійснювати візуальний контроль над приміщеннями й територією підприємства для запобігання несанкціонованого проникнення на територію й у службові приміщення.

За подіями можна спостерігати як у реальному часі, так і в записі – залежно від завдання. Більш складні й дорогі системи можуть бути оснащені контролем доступу, аналітикою, розпізнаванням осіб і багатьом іншим.

При виборі камери відеоспостереження оцінюють її технічні характеристики й умови, для яких вона призначена.

11.2 Основні параметри відеокамер

На ринку відеоспостереження існує два різних формати: аналоговий високого дозволу й цифровий – IP. Головна відмінність полягає в способі передавання

відеопотоку. Цифрова система може містити тільки камери, підключені до локальної мережі. Аналогова система може бути більш складною, тому що вимагає наявності обладнання для перетворення сигналу в цифровий код. Наприклад, плат захоплення відео, вбудованих у ПК, або відеореєстратора, що містить вузол аналого-цифрового перетворення.

11.2.1 Запис і зберігання відео

Камера потрібна, щоб зафіксувати, що відбуваються події й передати відеопотік для запису [1]. Відео можна записувати постійно (вимагає дуже великого обсягу пам'яті), за розкладом або по події або постійно. Відео можна записати на [2]:

1. Карту пам'яті MicroSD. Це найпростіший і дешевий варіант. Але якщо камеру украдуть, то разом з картою пам'яті й усім, що на ній записане.

2. Відеореєстратор або сервер. Недоцільно для малої системи, тому що потрібна купівля відеореєстратора або комп'ютера. З одного боку, це дороге, з іншого боку це більш безпечно і менше ризик втратити записи.

3. У хмару. Деякі китайські виробники пропонують записувати короткі відрізки відео або фото у свою хмару, наприклад, Cleverdog або Bitvision. У таких сервісів є істотний недолік – сервіс нестабільний і немає технічної підтримки. Платні хмарні сервіси беруть плату за час зберігання й обсяг збережених даних.

Щоб не записувати відео безупинно, камери можуть бути оснащені детекторами руху й програмами аналітики для включення запису по подіях.

Детектори руху практично є в більшості сучасних відеокамер [2]. Якщо в кадрі з'являється об'єкт, що рухається, то камера включає запис і зупиняє його, як тільки об'єкт перестає рухатися. Щоб не було неправильних спрацьовування (наприклад, на рух занавісок) багато камер дозволяють вибирати область, чутливість і розмір об'єктів, на які буде реагувати камера. У деяких камерах можна позначити лінію, після перетинання якої починається запис.

Деякі камери оснащуються тепловими інфрачервоними датчиками, здатними визначати об'єкти, які випромінюють тепло. Але вартість такої камери надто висока.

Випускаються камери з ПЗ, яке може вести підрахунок відвідувачів, малювати теплові карти спостережуваної території, відрізнити людей від свійських тварина або розпізнавати конкретних людей по обличчю, яке потрапило в кадр.

11.2.2 Дозвіл і кут огляду

Дозвіл відеокамери не єдиний, але дуже важливий для якості зображення параметр. Чим він вищий, тем чіткіше картинка й дорожче камера. Вимірюють дозвіл у мегапікселях. Для невеликих систем оптимальний дозвіл 2 мегапікселі. Також його називають Full HD, або 1080p [2].

Кут огляду вказують у градусах. Наприклад, якщо поставити камеру з кутом огляду 90 градусів по горизонталі в кут звичайної кімнати, ми побачимо зображення від стіни до стіни. Чим ширше кут огляду, тем легше розрізнити деталі, і навпаки. Досить часто в характеристиках указують кут огляду по діагоналі.

Цей параметр залежить від розміру матриці й фокусної відстані об'єктива. Кут буде ширше при меншій фокусній відстані й більшій матриці. Є камери, на яких можна міняти фокусну відстань і, відповідно, кут огляду. Це можливо завдяки варіофокусному об'єктиву. У такому об'єктиві лінза може рухатися ближче або далі від матриці. Залежно від моделі камери це можна робити вручну або віддалено. Для невеликих систем оптимальні об'єктиви з фіксованою фокусною відстанню 2,8 або 3,6 мм.

Для прикладу наведено два знімки. Вони зроблено однієї камерою, але з різною фокусною відстанню. Чим менше фокусна відстань, тим більше кут огляду, і навпаки. На рис. 11.1 наведена картинка для об'єктиву з фокусною відстанню 2,8 мм, а на рис. 11.2 – для об'єктиву з фокусною відстанню 12 мм.



Рисунок 11.1 – Зображення об'єкту при використанні об'єктиву з фокусною відстанню 2,8 мм, кут огляду по діагоналі 102 градуса [3]

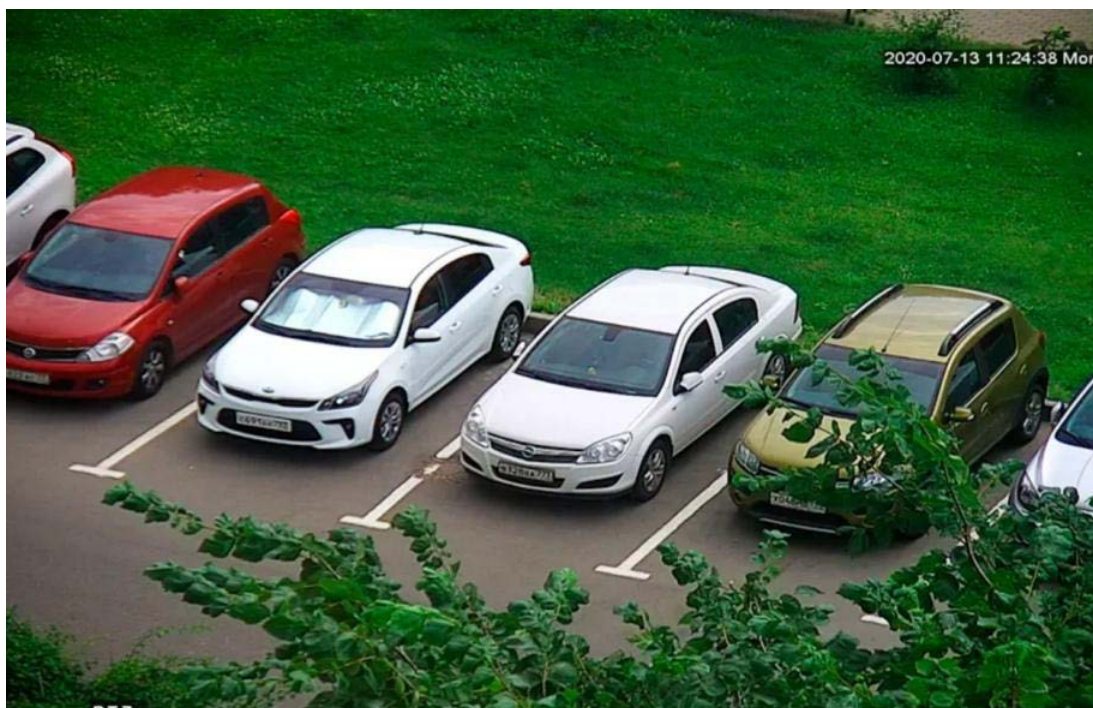


Рисунок 11.2 – Зображення об'єкту при використанні об'єктиву з фокусною відстанню 12 мм, кут огляду по діагоналі 102 градуса [3]

11.2.3 Підсвічування для нічного бачення

Використовується два різних способи підсвічування – світлодіодний і інфрачервоний. Звичайне світло може бути корисним, коли камера детектує рух і увімкне світло, щоб освітити простір перед камерою. Камер з інфрачервоним підсвічуванням набагато більше. Основний параметр – дальність підсвічування, яку звичайно вказують у метрах. Краще обирати підсвічування із приміткою SMART або EXIR [5]. Підсвічування SMART регулює яскравість залежно від близькості об'єкта до камери. Об'єкт може підійти впритул до об'єктива, але його особа при цьому не перетвориться в білу пляму. Підсвічування EXIR висвітлює краще й дає вночі більш чітку картинку. Підсвічування звичайним світлом дозволяє отримати кольорове зображення у темряві.

11.2.4 Можливість запису звуку

Мікрофон може бути вбудований у камеру, або є можливість підключити зовнішній. Також у камери може бути вбудований гучномовець, що дозволяє організувати двосторонній зв'язок через додаток, але якість звуку при такому зв'язку зазвичай дуже низька [3].

11.2.5 Наявність можливості встановлення карток пам'яті

Слот для карти пам'яті MicroSD. Чим більше обсяг підтримуваних карт пам'яті, тим краще. Але через постійний перезапис комірки пам'яті деградують і виходять із ладу, карту пам'яті потрібно міняти приблизно раз у два роки.

Важливо розібратися, як багато інформації може поміститися на карту пам'яті. Порахуємо, скільки даних повинне записатися за добу.

Двомегапксельна камера формує відеопотік зі швидкістю 4 Мбіт/с. Порахуємо, який об'єм інформації вона сформує за добу:

$$4 \text{ Мбіт/с} \times 60 \times 60 \times 24 = 345\,600 \text{ Мбіт за добу.}$$

Переведемо в більш звичні гігабайти: ділимо на 8, щоб одержати мегабайти, а потім на 1024, щоб одержати гігабайти:

$$345\,600 / 8 / 1024 = 42,19 \text{ Гбайт.}$$

Виходить, картки на 32 Гб, щоб записати інформацію за повну добу, не вистачить. Коли скінчиться місце, камера почне видаляти самі ранні файли й картка буде перезаписана 1,5 рази за добу. За рік набіжить 547 таких циклів перезапису. Найпростіша й дешева карта пам'яті витримає приблизно 150 циклів перезапису, дорога – 4000 циклів.

Звичайна карта пам'яті 32 Гбайт коштує 130 грн, спеціалізована для відеоспостереження такого ж обсягу – до 900 грн.

11.2.6 Формат стиснення інформації та чутливість камери

Для запису на будь-який носій для зменшення обсягу інформації відеосигнал піддають стисненню. Для цього використовують різні формати. Для запису у форматі mp4 використовують кодеки H.264, або H.265 та H.265+ – більш сучасний. При однаковій якості картини й тому самому обсязі носія камера з H.265+ запише три дні архіву, а з H.264 – тільки два.

Однак такий формат запису має свої недоліки. Оскільки здійснюється запис ключового кадру, а потім в наступних кадрах передається тільки зміна інформації по відношенню до ключового кадру, то при його втраті або пошкодженні буде втрачений цілий фрагмент запису.

Інший формат запису використовує технологію стискання jpeg і носить назву Motion JPEG. При використанні такої технології кожен кадр містить повну інформацію про об'єкт, що спостерігається камерою. При втраті одного кадру всі інші кадри залишаються непошкодженими.

Велике значення має такий параметр як динамічний діапазон (відношення максимального рівня сигналу до мінімального, виражене у децибелах).

Поняття "динамічний діапазон камери" означає максимально можливу кількість різних градацій яскравості в кадрі. Найкраща якість зображення досягається тоді, коли в полі зору камери всі об'єкти освітлені приблизно однаково. У цьому випадку наявний динамічний діапазон камери використовується найбільш ефективно, тобто всі об'єкти на зображенні добре видно, і вони мають достатню контрастність.

Для камер високої роздільної здатності набагато більше прикладів, коли умова рівномірного освітлення порушується – одна частина сцени на світлі, а інша в тіні. Наприклад, сонце і тінь від будинку, яскраве вікно і темний куток та інше.

Коли в кадр одночасно потрапляють і світлі, і темні ділянки, то градацій яскравості вже недостатньо (у системах відеоспостереження використовується 8-розрядне при перетворенні даних, тобто 256 градацій яскравості), щоб однаково якісно передати зображення від світлих і темних ділянок. Якщо налаштувати камеру на світлу ділянку, то все, що в тіні, стає просто чорним і нерозбірливим, якщо налаштувати на темну ділянку – виявляється засвіченою світла частина. Доводиться обирати щось одне, а іншу частину кадру втрачати, або знижувати загальну контрастність зображення, роблячи нерозбірливими багато деталей.

На рис. 11.3,а добре видно темні ділянки відображеної сцени, а світлі ділянки виявляються засвіченими, а на рис. 11.3,б – видно тільки світлі ділянки сцени, темні ділянки виявляються затемненими.

Ефективним вирішенням даної проблеми є застосування технологія HDRi (High Dynamic Range imaging – широкий динамічний діапазон) або WDR. Основний принцип – це отримання двох кадрів з різною витримкою, один налаштований на світлу ділянку сцени, а інший на темний ділянку сцени, а потім злиття цих кадрів в один, в якому присутні зображення і світлих і темних ділянок.



а)



б)

Рисунок 11.3 – Засвічені (а) і затемнені (б) ділянки зображення [5]

Камери з WDR (Wide Dynamic Range – широкий динамічний діапазон) дозволяють отримати якісну картинку при нерівномірному освітленні. Такий режим роботи реалізується програмним або апаратним способом. Програмний спосіб використовується частіше, але працює менш ефективно ніж апаратний. Апаратний додає порядку 20% до вартості камери, але відчутно поліпшує якість картинки. Starlight або Starvis – маркетингові назви технології, яка дозволяє одержати більш чітку картинку при поганому освітленні.

Людське око не сприймає більше 256 градацій яскравості, а зображення з широким динамічним діапазоном може містити набагато більше градацій яскравості. Через це зображення з широким динамічним діапазоном без зміни яскравості людське око сприймає частково. Щоб не губилися деталі занадто світлих і дуже темних ділянок зображень (не регулюючи яскравість для перегляду різних ділянок) необхідно стискати динамічний діапазон відеосигналу.

На рис. 11.4 наведено зображення, отримане після локально-адаптивного стиснення динамічного діапазону. На ньому видно одночасно і темна, і світла частини сцени на відміну від зображень, наведених на рис. 11.3. При цьому обидві частини сцени передаються без зниження контрастності, і, відповідно, без втрати деталей.



Рисунок 11.4 – Зображення, отримане шляхом локально-адаптивного стиснення динамічного діапазону [4]

Чутливість до світла вимірюють у люксах. Чим менше це значення в характеристиках, тим краще зображення при слабкому світлі. У камер з позначкою Starlight або Starvis цей параметр порядку 0,005 лк, а у звичайних – 0,01 лк. Камера при використанні технології Starlight передає кольорову картинку набагато краще ніж звичайна камера (рис. 11.5), яка при такому освітленні перемикається в чорно-білий режим.



Рисунок 11.5 – Картинка отримана з камери з використанням технології Starlight в нічний час [3]

11.2.7 Живлення камер

Вимоги до електроживлення звичайно зазначені в паспорті та на наклейці камери. Недорогі IP-камери мають напругу живлення 5 В і можуть живитись від зарядних пристроїв мобільних телефонів або через USB-порт.

Камера зі стандартним мережним портом Ethernet може отримати живлення через нього від роутера або комутатора з підтримкою живлення по крученій парі (POE – Power On Ethernet) або спеціального POE-інжектора. Крученої пари, підведеної до камери, у такому випадку досить, розетка й блок живлення на 5 В не потрібні. Комутатори й роутери, які підтримують POE, набагато дорожчі звичайних. Інжектор живиться від мережі змінного струму 220 В і коштує доволі дорого.

11.3 Особливості обробки сигналів відеокамер

11.3.1 Відеокамери "День/Ніч"

Використання монохромних камер (часто їх називають чорно/білими) і кольорових камер має свої переваги і недоліки. Кольорові камери більш інформативні, але мають меншу чутливість, що обмежує їх застосування в умовах слабкої освітленості. Основна причина зниженої чутливості кольорових камер – наявність фільтра, що вирізає інфрачервоний діапазон (ІЧ-діапазон).

Режекторний ІЧ-фільтр потрібен для забезпечення повнокольорового режиму роботи камери. Це пов'язано з тим, що матриці відеокамер чутливі до ІЧ-діапазону. Це дає збільшити чутливість камер в 2...3 рази.

Для того щоб камери були більш універсальними і могли працювати вдень як кольорові, а вночі як чорно-білі використовується два підходи.

У першому випадку, використовується кольорова камера, у якої перед матрицею встановлений режекторний ІЧ-фільтр і яка має вірну передачу кольору, але має невисоку чутливість. І вбудували в цю камеру механічний вузол, що прибирає режекторний ІЧ-фільтр при переході камери в монохромний режим. За

відсутності фільтра вдається домогтися реального підвищення чутливості камер в монохромному режимі. Такі камери часто називають TDN (True Day/Night) – "правильні" день/ніч, або ж виробники вказують наявність ICR (Infrared Cut Filter Removable) – прибирається режекторний ІЧ-фільтр (рис. 11.6).

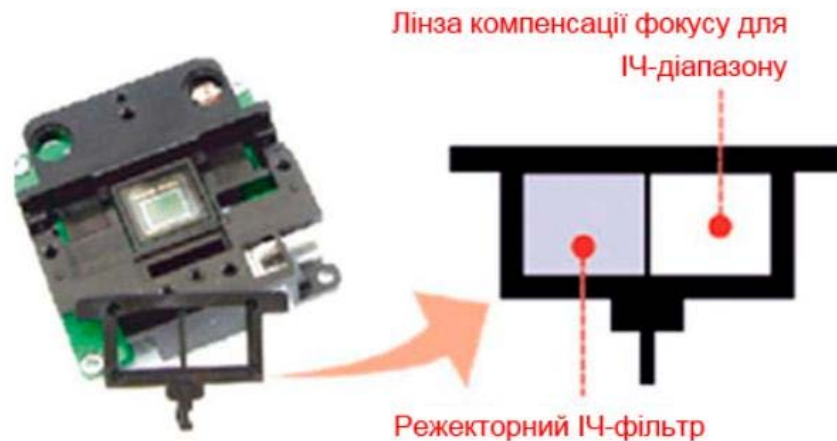


Рисунок 11.6 – Конструкція відеокамери з ІЧ-фільтром [5]

У другому випадку, використовується камера, у якої режекторного ІЧ-фільтру практично немає. Тобто, він є, але його смуга режекції (вирізання) не збігається з необхідною смугою для вірної передачі кольору. При переході в монохромний режим вимикається лише сигнал кольоровості, що дає несуттєву надбавку до чутливості камери (за оцінками різних фахівців, приблизно 20...50%). Однак ціна такого рішення виходить набагато нижче. На таких камерах видно спотворення кольорів. У відеокамерах з ІЧ-підсвічуванням також встановлюється "неповноцінний" режекторний ІЧ-фільтр.

11.3.2 Робота з ІЧ-підсвіченням

Щоб камера переходила в монохромний режим, вона повинна отримати сигнал, коли це робити. Раніше, майже завжди для цього використовували сигнал самої камери, схема автоматичного регулювання підсилення (АРП) формувала

сигнал перевищення певного порогу, і за цим сигналом відбувалося перемикання режиму.

Коли зображувана сцена темніє, камера формує команду прибрати фільтр. Матриця отримує потужний сигнал від ІЧ-підсвічування, тоді камера фіксує стан "світло", повертає фільтр. "Темно" – прибирає фільтр, "світло"...і так далі. Цей процес відбувається із затримкою (є спеціальні затримки для плавного переходу режимів). Камера може довго здійснювати такі переходи або може "зависнути" в одному з режимів.

Багато виробників встановлюють окремий сенсор, чутливий тільки до видимого світла і здійснюють перемикання режимів за його сигналом. Також випускаються камери з можливістю зовнішнього перемикання режимів, тоді сигнал перемикання можна брати від ІЧ-прожекторів (у деяких прожекторах формується цей сигнал і його можна використовувати).

11.3.3 Адаптивне ІЧ-підсвічування

Робота підсвічування від одного джерела (або сукупності ІЧ-світлодіодів) рідко буває ідеальною. Далекі об'єкти підсвічені менше, близькі – сильніше. Якщо порушник рухається на камеру з ІЧ-підсвічуванням в темряві, то коли він вдалині, зображення "дрібнуватиме" і його погано видно в темряві. Коли порушник поблизу, зображення пересвічене, і теж погано помітно деталі цього зображення. На середній відстані все начебто нормально, але важливо побачити порушника крупним планом.

Адаптивне підсвічування змінює яскравість залежно від енергії відбиття. При наближенні порушника до камери, яскравість підсвічування зменшується, і можна розглянути порушника детальніше [8]. У цьому і полягає заявлена перевага адаптивного ІЧ-підсвічування.

Однак досі не вдалося придумати алгоритм одночасного супроводу кількох цілей однією поворотною камерою, адже у випадку адаптивного підсвічування,

вона не зможе працювати одночасно з групою порушників, що знаходяться на різних відстанях від камери.

11.3.4 Компенсація яскравого засвічування

Функція компенсації яскравого засвічування (HLC – High Light Compensation) у деяких з виробників може називатися по різному (наприклад, Eclipse). Відомо, що камера опрацьовує рівень освітленості, змінюючи значення витримки електронного затвора або керуючи діафрагмою об'єктива. Яскраві ділянки в полі зору камери, що впливають на механізм налаштування затвора або діафрагми за середнім рівнем яскравості, призводять до непомітності деталей в темних ділянках. Якщо яскраві ділянки не враховувати під час розрахунку середньої яскравості, деталі в темних тонах будуть краще помітні. Цим і займається функція компенсації яскравою засвічування. Вона просто маскує яскраві ділянки, замінюючи їх сірим кольором.

Як приклад роботи такої функції, виробниками прийнято приводити чітке визначення номера автомобіля в умовах засвічування камери фарами цього ж автомобіля (рис. 11.7) [9]. Цей приклад дозволяє проілюструвати корисність компенсації яскравого засвічування.



а)

б)

Рисунок 11.7 – Зображення номерів автомобіля при виключеному (а) та включеному (б) режимі HLC [9]

Однак при установці системи телевізійного спостереження у вестибюлі будівлі зі скляним входом, слід врахувати, що, включивши таку функцію, користувач позбавляється можливості бачити вулицю. Там, як правило, завжди світліше і компенсація яскравою засвічування просто зафарбує всі зображення вулиці сірим кольором. Ілюстрацію інших функцій покращення зображення у складних умовах можна знайти у [9].

11.4 Особливості встановлення телевізійних камер для інтелектуальних відеосистем

Сьогодні відбувається загальний перехід від традиційних ТВ-систем до мережових. Це тягне за собою застосування різноманітних ІР-кодерів відеосигналу, в тому числі і з вбудованою відеоаналітикою. В результаті система відеоспостереження стає **інтелектуальною** – вона здатна самостійно інтерпретувати ситуацію в полі зору, приймати рішення і постачати користувача тільки необхідною інформацією [2]. Але "інтелект" системи може бути зведений до нуля при недотриманні простих правил.

Основні принципи встановлення та налаштування стаціонарних і PTZ-камер (Pan Tilt Zoom Camera – роботизована камера, що дозволяє автоматично змінювати панораму, масштаб і поворот камери в різних площинах) на об'єкті, призначених для роботи в складі інтелектуальної відеосистеми (ІВС), наведені нижче. Оскільки кожен об'єкт може мати специфічні вимоги з безпеки, і ці вимоги можуть змінюватися залежно від конкретних умов, інформація, наведена нижче, є базовою і підлягає доопрацюванню в кожному конкретному випадку.

Загальні принципи підключення стаціонарних і PTZ-камер до кодерів відеосигналу:

1. PTZ-камери повинні мати автофокус. Необхідно переконатися, що автофокус (AF – Auto Focus) включений.

2. Для PTZ-камер повинна бути відключена компенсація заднього засвічування (BLC) [9].

3. Камера повинна бути розташована таким чином, щоб виключити потрапляння прямих сонячних променів в об'єктив.

4. Якщо камера має вбудований стабілізатор зображення, його необхідно активувати.

5. Якщо камера має вбудований детектор руху, то його необхідно відключити.

6. Якщо PTZ-камера забезпечує маскування певних зон в полі зору, то цю функцію необхідно відключити.

7. Якщо камера має "нічний" режим із збільшеним часом накопичення, то цю функцію необхідно відключити.

11.5 Особливості перетворення відеосигналів з поворотних камер у цифровий код

Для контролю великих територій використовують поворотні відеокамери, які дозволяють шляхом зміни фокусної відстані об'єктива контролювати в денний час об'єкти на відстані 1...2 км (рис. 11.8) [7-8].



Рисунок 11.8 – Зовнішній вигляд поворотної відеокамери [7]

При використанні таких камер необхідно враховувати такі фактори:

- якщо необхідно здійснювати контроль на достатній відстані від об'єкта (понад 1500 м), доцільно застосовувати **ІР-відеосервери**, які здатні транслювати цифровий сигнал на будь-якій відстані;
- для перетворення в цифровий код зображень із поворотних камер підходить не будь-який АЦП і кодек.

АЦП і його драйвер, які використовуються для аналого-цифрового перетворення, можуть бути не розраховані на перетворення сигналів зі швидко змінюваними параметрами (в поворотній камері зображення змінюється досить швидко). Системи, які добре справляються із записом статичної фонові картинки, можуть бути зовсім неприйнятні для поворотних камер.

Роздільна здатність кадру. Більшість поворотних камер мають високу роздільну здатність. Вона не повинна мати роздільну здатність менше ніж 768×576 . Камера 2 мегапікселя має роздільну здатність 1920×1080 пікселів.

Деінтерлейсинг. При швидкій зміні фону особливо важливим є якість алгоритму деінтерлейсингу (процес перетворення черезрядкової розгортки в прогресивну – для відтворення відеозображень на сучасних телевізорах і дисплеях), який прибирає "гребінку" на зображенні (рис. 11.9).



Рисунок 11.9 – Зображення з ефектом інтерлейсингу [10]

Деінтерлейсинг – процес створення одного кадру з двох полів черезрядкового формату для подальшого виводу на екран з прогресивною розгорткою [11]. Застосовується в комп'ютерних системах обробки відео, плоскопанельних телевізорах і т. д.

Відеокамери швидко захоплюють послідовності кадрів (нерухомих зображень). Однак, телевізійні системи зчитують це записане зображення послідовно за допомогою сенсору зображення по одній лінії (рядками). В аналоговому телебаченні, кожен кадр розбивається на два послідовних поля, одне з яких містить всі парні рядки, друге непарні. Поля відтворюються послідовно на швидкості вдвічі більшій ніж стандартна частота кадрів. Наприклад, системи відео PAL і SECAM мають частоту в 25 кадрів/с або 50 полів/с, а система NTSC передає 29.97 кадрів/с або 59.94 полів/с. Такий процес розділення кадрів на поля з поділеною навпіл роздільною здатністю при подвійній частоті кадрів відомий як черезрядкова розгортка [11].

Оскільки черезрядковий сигнал відео має два поля одного кадру відзняті в різний час, він покращує сприйняття руху глядачем і зменшує мерехтіння завдяки ефекту інерції зору. Це дає ефективне подвоєння часової роздільної здатності в порівнянні з не черезрядковими кадрами (для частоти кадрів, що дорівнює частоті полів). Однак, черезрядковий сигнал потребує, щоб дисплей був здатен відображати окремі поля послідовним способом [11].

Кодек – пристрій або програма, здатна виконувати перетворення потоку даних або сигналу [12].

Кодеки можуть як кодувати потік/сигнал (часто для передачі, зберігання або шифрування), так і розкодувати – для перегляду або зміни у форматі, що більше підходить для цих операцій. Кодеки використовують при цифровій обробці відео й аудіо.

Особливо важливо обрати вірно кодек для поворотних відеокамер. Використання кодеку потокового стиснення типу MPEG і його різновидів не доцільно (оскільки при повороті відеокамери немає "змінюваних кадрів", всі кадри ключові). Крім того з'являється затримка реакції. При управлінні оператор не відразу бачить, куди повертається камера. Проблема з швидкими поворотними камерами в тому, що йде запізнювання відео на моніторі відносно реального часу. Особливо це сильно помітно на потокових кодеках, там затримка доходить до секунди. Коли на екрані монітора видно об'єкт, насправді він взагалі може в

реальності зникнути з поля зору камери. Керувати таким чином камерою практично неможливо.

Кодеки H.264 та H.265 також відносяться до потокового алгоритму стиснення. Більше того, його алгоритм допускає наявність лише одного ключового кадру на 1000 синтезованих. У випадках, де практично немає однакових областей, ми бачимо малоімовірну картину, яку намагається синтезувати алгоритм передбачення цього кодека. Для поворотних камер покадровому кодеку MJPEG альтернативи поки що немає.

Аналіз якості зображення. При використанні автоматичних режимів потрібен контроль за якістю картинки. Іноді доводиться стикатися з тим фактом, що купол камери вже давно забруднений, зображення спотворене краплями дощу або снігом. Тому доцільно, щоб система перетворення в цифровий код мала детектор перекриття огляду. На деяких купольних камерах вона може автоматично включити "двірник" або просто надіслати повідомлення службі техпідтримки.

Програмне забезпечення. Дуже часто оператору необхідно швидко перейти в певний режим камери ("день-ніч", "панорамування", "програма обходу території", "ручний режим", "захист від засвічування" та ін.). Для цього потрібні зручні засоби управління. Цифрове відео може приходити з запізненням, затримуючись у різних мережевих пристроях. У цьому випадку оператор не відразу бачить реакцію на свої дії, що значно погіршує якість стеження. Тому при використанні поворотних платформ потрібно звертати увагу на якість побудови мережевих сегментів, особливо шлюзів.

11.6 Конструкції відеокамер

Купольні відеокамери дозволяють здійснювати відеоспостереження з кутом огляду до 360 градусів (рис. 11.10) [7, 8].



Рисунок 11.10 – Купольні IP-камери [7, 8]

Такі камери можна розділити на три групи:

- стаціонарні купольні IP-камери з ІЧ-підсвічуванням;
- всепогодні пристрої з ІЧ-підсвічуванням – антивандальні IP-камери купольного типу, кожна з яких має клас захисту IP66 і діапазон робочих температур $-40...60\text{ }^{\circ}\text{C}$;
- класичні корпусні моделі.

Кожна група включає 3 види пристроїв – проводові IP-камери і моделі, що підтримують безпроводову передачу даних по мережах Wi-Fi і 3G.

Вуличні **аналогові відеокамери** і камери "день/ніч" окрім низької ціни відрізняються високими технічними характеристиками. Вони забезпечують відеоспостереження в повній темряві, мають клас захисту IP67 і стабільно працюють в температурному діапазоні $-40...60\text{ }^{\circ}\text{C}$. Випускаються в міцних алюмінієвих корпусах циліндричної форми, що виключає утворення бурульок у зоні спостереження відеокамери.

Зовнішній вигляд деяких камер наведений на рис. 11.11 та 11.12 [7-8].



Рисунок 11.11 – Зовнішній вигляд аналогової відеокамери
NEXT NRB-310D-6 з інфрачервоним підсвічуванням [8]



Рисунок 11.12 – Зовнішній вигляд аналогової відеокамери
NEXT NR-750LMWC-3516 [8]

Зовнішній вигляд поворотної відеокамери з ІЧ-підсвічуванням наведено на рис. 11.13 [7].



Рисунок 11.13 – Зовнішній вигляд поворотної відеокамери з ІЧ-підсвічуванням [7]

Безкорпусні камери випускаються для встановлення у різні об'єкти для маскування. На рис. 11.14 наведено зовнішній вигляд безкорпусної камери. Камери для таємного відеоспостереження повинні мати малі габарити. Можуть бути як з проводовим так і з безпроводовим інтерфейсом. На рис 11.15 та 11.16 наведені фото відеокамер для таємного відеоспостереження [13].



Рисунок 11.14 – Зовнішній вигляд безкорпусної відеокамери [13]



Рисунок 11.15 – Зовнішній вигляд безпроводової відеокамери JMK WS-208/309 для таємного відеоспостереження [13]



Рисунок 11.16 – Зовнішній вигляд безпроводової відеокамери таємного відеоспостереження [14]

Відеокамери зі змінною фокусною відстанню дозволять спостерігати об'єкти з високою якістю зображення на різних відстанях. На рис. 11.17 наведений приклад такої камери [7, 8].



Рисунок 11.17 – Зовнішній вигляд відеокамери з варіофокусним об'єктивом [7]

В офісних приміщеннях, при проведенні відеоконференцій часто використовуються настільні відеокамери (рис. 11.18) [15].



Рисунок 11.18 – Зовнішній вигляд настільних відеокамер [15]

При використанні відеокамер зовнішнього відеоспостереження, що працюють в жорстких умовах (висока вологість, широкий діапазон зміни температур, наявність пилу у повітрі і т.д.) використовують герметичні корпуси (рис. 11.19) [8].



Рисунок 11.19 – Зовнішній вигляд відеокамери в герметичному корпусі [8]

Контрольні питання

1. Що означає термін HDRi?
2. Чим WDR відрізняється від HDRi?
3. Для чого потрібно стиснення динамічного діапазону в системах відеоспостереження?
4. Для чого призначений режекторний фільтр ІЧ-діапазону?
5. Для чого використовується адаптивне ІЧ-підсвічування?
6. Яке підсвічування потрібно робити для формування кольорового зображення?

7. В чому особливості кодування сигналів поворотних відеокамер?
9. Як підвищити чутливість кольорової відеокамери у нічний час?

Перелік посилань

1. Vlado Damjanovski CCTV: From Light to Pixels 3rd Edition. Butterworth-Heinemann; 3rd edition (October 2, 2013). 616 p.
2. Види систем відеоспостереження - вибір і огляд систем відеоспостереження. Url: https://secur.ua/articles/ua_vidi-sistem-videosposterezhennja-vibir-i-ogljad-sistem-videosposterezhennja.html. (дата звернення: 26.03.2024).
3. Illustrations for the tinkoff journal. Url: <https://www.behance.net/gallery/85903657/ILLUSTRATIONS-FOR-THE-TINKOFF-JOURNAL#> (дата звернення: 26.11.2024).
4. <https://pxhere.com/ru/photo/1145511> (дата звернення: 26.11.2024).
5. Корисні функції в сучасних відеокамерах. Url: http://litetec.info/index.php?option=com_content&view=article&id=60 (дата звернення: 26.11.2024).
6. Відеокамери. Url: <https://agent-007.com.ua/videokamery> (дата звернення: 1.07.2024).
7. Відеокамери. Url: <https://klaster.ua/ua/shop/videonablyudenie/videokamery-ru/ip-videokamery/> (дата звернення: 1.07.2024).
8. Відеокамери. Url: <https://worldvision.com.ua/ip-kamery-videonabludeniya/> (дата звернення: 1.07.2024).
9. Технології, що поліпшують якість відеоспостереження. Частина I: BLC, HLC, DNR, WDR. Url: <https://pipl.ua/article/tehnologiyi-scho-polipshuyut-yakist-videosposterejennja-chastina-i-blc-hlc-dnr-wdr> (дата звернення: 1.07.2024).
10. Endelig et skikkelig HD-kamera. Url: <https://www.nettavisen.no/endelig-et-skikkelig-hd-kamera/s/12-95-1309993> (дата звернення: 1.07.2024).
11. Деінтерлейсинг. Url: <https://uk.wikipedia.org/wiki/Деінтерлейсинг> (дата звернення: 6.12.2024).

12. Кодек. Url: <https://uk.wikipedia.org/wiki/Кодек> (дата звернення: 6.12.2024).
13. Відеокамера з мікрофоном, відеоченят ZK-208B, Мінікамера. Url: <https://prom.ua/ua/p1715860064-videokamera-mikrofonom-video.html> дата звернення: 20.11.2024).
14. Mini Y2000. Url: https://ukrainian-goods.biz.ua/view_content.php?id=1080 дата звернення: 20.11.2024).
15. Камери відеоспостереження з кубічним корпусом. Url: <https://nadzor.ua/uk/videonablyudenie/kamery-videonabludenia/kubicheskiy> дата звернення: 20.11.2024).

12 ІНТЕРФЕЙСИ СИСТЕМ ІОТ

12.1 Призначення інтерфейсів

В англійській мові слово "інтерфейс" означає прошарок, середовище, що розділяє або єднальну різні об'єкти [1]. У нашій технічному побуті цифровий інтерфейс – система передавання даних між вузлами системи, різними системами, описана стандартом.

Застосування стандартизованого інтерфейсу забезпечує передавання даних між виробами різних розроблювачів. Дозволяє вести розробку вузлів паралельно й застосовувати готові вузли сторонніх виробників. Розроблювач системи, закладаючи в неї стандартизовані інтерфейси, може розраховувати на одержання зазначеної пропускну здатності, довжини ліній і інших параметрів. З іншого боку, необхідність дотримуватися стандарту може привести до подорожчання виробу. Дуже велика спокуса, обравши за основу більш-менш підходящий стандарт, не відповідати всім його вимогам, а адаптувати до конкретного завдання: змінити розрядність, функції або скоротити кількість керуючих сигналів, заощадити на шинних формувачах довгих ліній, що забезпечують підтримку, зв'язки й навантажувальну здатність, застосувати більш доступні роз'єднувачі.

У цьому випадку треба бути готовим до того, що розроблювальна система не буде відкритою, процеси її модернізації й нарощування сильно утрудняться, що в остаточному підсумку неминуче приведе до передчасного списання системи й заміни її на принципово нову.

Там, де потоки даних і відстань невелика, має сенс подумати про відмову від застосування інтерфейсу як системи. Швидше за все, дешевше буде передати кожний окремий сигнал "як є". Подібні розв'язки, насамперед, виправдані для зв'язку функціонально незакінчених вузлів (самостійне застосування яких або заміна більш досконалішими не передбачається). При ухваленні рішення потрібно враховувати фактор співвідношення параметрів прикладної (інтерфейсної) частини

виробу. Якщо хоча б один з нижчеперелічених параметрів інтерфейсної частини перевищує певний поріг, треба задуматися про альтернативний розв'язок:

- собівартість;
- споживана потужність;
- маса;
- габаритні розміри.

Поріг можна визначити на рівні 30...40%, для промислових застосувань він більше, для побутових – менше. У кожному разі рішення повинно прийматись індивідуально.

Волоконно-оптичні лінії зв'язку (ВОЛЗ) також є стандартизованими цифровими інтерфейсами. Для їхньої реалізації на ринку є велика кількість різноманітної елементної бази з високим ступенем готовності до застосування. Більшою перевагою ВОЛЗ є несприйнятливість до електромагнітних перешкод. Неметалічна природа середовища передавання даних забезпечує гальванічну розв'язку між портами. Пропускна здатність стандартизованих ВОЛЗ лежить вище пропускної здатності цифрових інтерфейсів з електричною природою сигналів. Головним недоліком ВОЛЗ є висока ціна кабельного й кінцевого устаткування. Через цей область застосування ВОЛЗ досить вузька:

- магістральні лінії великих телекомунікаційних систем;
- високопродуктивні системи збору даних для відповідальних застосувань;
- передавання мультимедійної інформації в професійних системах (реалізується на найдешевшій елементній базі).

Дорожнеча устаткування не дозволяє створювати розгалужені волоконно-оптичні мережі. Собівартість інтерфейсної частини може значно перевищувати собівартість цільового устаткування. Якщо в системі присутні потоки даних, що припускають застосування ВОЛЗ, то будується дворівнева система їх передавання. На ВОЛЗ реалізують верхній рівень, що з'єднує локальні підсистеми. Нижній рівень реалізується з використанням менш дорогих і продуктивних розв'язків.

У цей час на ринку є велику кількість готових розв'язків для реалізації портів різних інтерфейсів (особливо послідовних) у вигляді мікросхем, що вимагає

підключення невеликого числа зовнішніх елементів. Таким чином, організація стандартизованого інтерфейсу не вимагає більших витрат часу й не викликає значного збільшення масо-габаритних характеристик апаратури. Але в деяких випадках має сенс використовувати "полегшену" реалізацію інтерфейсу.

12.2 Типові реалізації цифрових інтерфейсів

12.2.1 Загальні зауваження

Реалізація стандартизованого інтерфейсу визначається документом (стандартом), що описують його [1]. **Дотримання стандарту забезпечує сумісність виробів різних виробників і гарантує одержання заявленої пропускну здатності.** Стандарти, у свою чергу, реалізують типові, уже кимсь винайдені й перевірені розв'язки кожний з яких має свої достоїнства й недоліки. Застосовані типові розв'язки можна вважати модулями, з яких створюються стандарти.

Перерахування застосованих типових розв'язків часто виноситься в заголовок стандарту й у його преамбулу. Інші модулі розпізнаються після аналізу тексту стандарту (рис. 12.1). Зовсім погано, коли така інформація може бути витягнута тільки з ілюстрацій. Це означає, що текст стандарту недостатньо докладно описує інтерфейс і можливі варіанти реалізації, що не забезпечують сумісність виробів різних виробників, або існують інші документи, що описують інтерфейс.

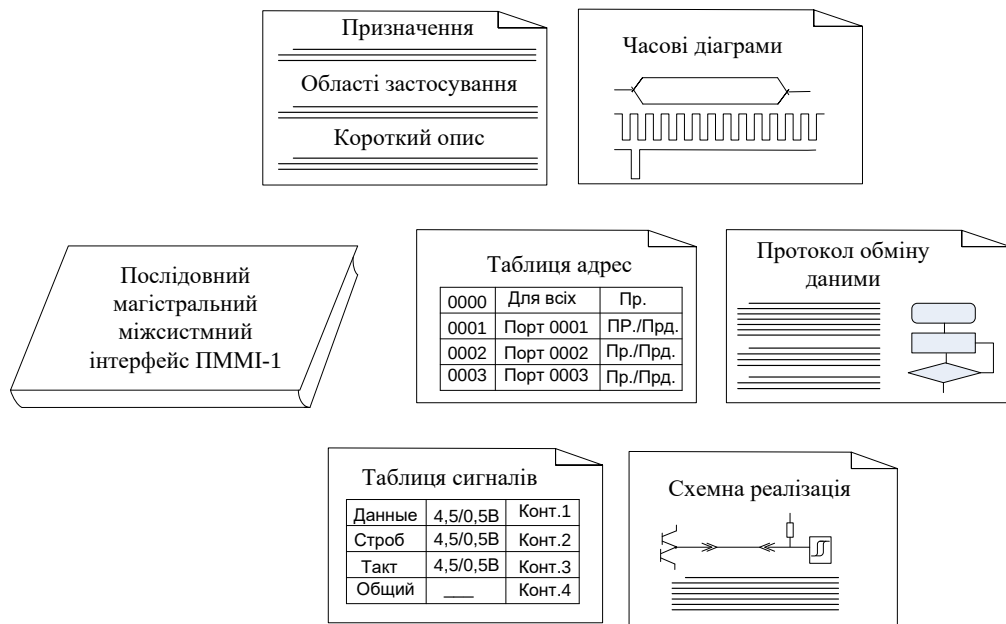


Рисунок 12.1 – Важливі складові частини документа, що описує інтерфейс [1]

12.2.2 Паралельні інтерфейси

При класифікації інтерфейсів дуже часто використовується критерій **паралельності-послідовності** передавання даних [1]. Це найважливіший параметр інтерфейсу. Його визначення – ключовий розв’язок розроблювача. Від нього залежить вартість апаратури й кабельного господарства, а також продуктивність інтерфейсу. У **паралельному інтерфейсі** кожний сигнал передається по окремій лінії. Лінії діляться на групи: шина даних, шина адреси, шина управління. Все-таки загальна кількість ліній повинна бути менше кількості переданих корисних сигналів (інакше виникає питання про доцільність застосування інтерфейсу). Часовий поділ у передавання корисної інформації застосовується на рівні зміни адрес і перемикання напрямків передавання даних.

Шина даних являє собою кілька ліній (по числу розрядів інтерфейсу). Передавачі є потужними ключами, захищеними від впливу реактивного опору лінії. Вони можуть бути відключені (переведені в стан високого імпедансу), що дозволяє працювати іншим передавачам на тій же шині. При включенні вони звичайно видають у шину даних інформацію з паралельного регістру передавання. Приймачі являють собою логічні елементи із декількома логічними рівнями. Вони

трансляють дані на паралельний регістр приймання. Дані записуються в регістр при наявності відповідних сигналів на шинах адреси й управління.

Шина адреси, якщо контролерами інтерфейсу можуть ставати кілька портів, будується аналогічно шині даних. Якщо контролером є завжди один порт – задача спрощується. Контролер має тільки передавачі без стану високого імпедансу, інші – тільки приймачі. При передаванні даних контролером шини адреси й даних працюють однаково. На обидві формується відповідна інформація. Ця інформація сприймається іншими портами в такий спосіб: адреса дешифрується й з нього формується сигнал дозволу-заборони приймання даних у кожному порту.

Шина управління будується по тим же правилам, що й шина адреси. Вона може бути спрощена заміною передавачів на схеми з відкритим колектором, тому що значущими сигналами на шині управління часто є тільки рівні логічного нуля.

Головне обмеження, що діє при застосуванні паралельних інтерфейсів, **довжина ліній зв'язку**. Велика кількість ліній визначає високу вартість погонного метра магістралі. Кабелі паралельних інтерфейсів звичайно мають недорогу просту конструкцію, наприклад, стрічкову. Використання коаксіальних і інших дорогих кабелів неможливо через їхню вартість, яка перевершує вартість електроніки. Реалізація ліній, що перевершують по довжині одиниці метрів, при високій пропускній здатності неможлива по технічних або економічних причинах. Друковані конструкції магістралей паралельних інтерфейсів по довжині звичайно не перевищують 1 метра. Вони мають широке поширення як системні магістралі модульних систем. Багатошарові друковані плати й з'єднувачі високої щільності дозволяють розташувати велику кількість ліній зв'язку на невеликих площах друкованих плат. При розміщенні інтерфейсу в межах однієї плати звичайно є можливість спростити реалізацію магістральних прийомопередавачів, що знижує вартість, габарити й енергоспоживання апаратури.

12.2.3 Послідовні інтерфейси

На відміну від паралельних, **послідовні інтерфейси не мають шин адреси, даних і управління** [1]. Уся корисна й службова інформація передається по єдиному інформаційному каналу. Цей канал може складатися з однієї сигнальної лінії й загального проведення (такі інтерфейси називають однопроводовими). Їхня перевага – у простоті комутаційного й кабельного господарства. **Недолік** даного класу інтерфейсів **у необхідності організації синхронізації портів** через інформаційний канал. Працюючи принципово асинхронно пристрою повинні обмінюватися даними без втрат і конфліктів. Спеціальні заходи на синхронізації знижують корисну пропускну здатність і надійність однопроводових інтерфейсів (ці проблеми успішно вирішені в інтерфейсі CAN) [6].

Багатопроводові інтерфейси, як правило, реалізуються простіше й мають краще співвідношення часу передавання корисної або службової інформації. Чим більше застосоване додаткових ліній зв'язку, тем це помітніше (рис. 12.2).

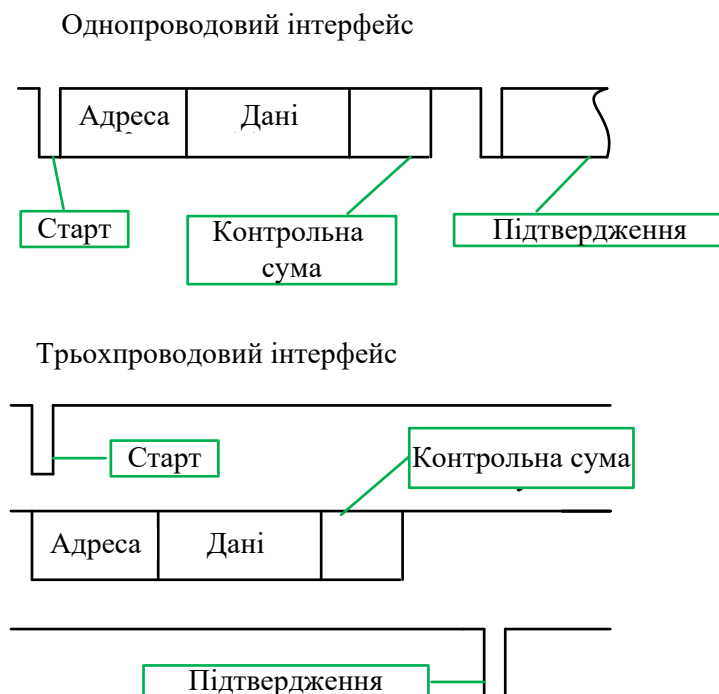


Рисунок 12.2 – Обмін корисною інформацією в однопроводовому інтерфейсі

Популярність послідовних інтерфейсів останнім часом пов'язана з появою спеціалізованої елементної бази, що дозволяє реалізувати порт інтерфейсу на одній

недорогій мікросхемі. Такі мікросхеми можуть з'явитися тільки при достатньому попиті на таку продукцію. Доступність спеціалізованих мікросхем розширює область застосування інтерфейсів за рахунок зниження вартості й поліпшення характеристик виробу. У цьому випадку має місце лавиноподібний процес росту ринку послідовних інтерфейсів.

Послідовні інтерфейси використовують кабельне господарство, роз'єми, площу друкованих плат у набагато менших кількостях, чим паралельні. У цей час цей фактор став дуже важливий не тільки в традиційних випадках (довгі лінії, мобільні пристрої), але й у більшості інших, що викликане ростом щільності інформаційних потоків на одиниці об'єму (або ваги) апаратури. У системах автоматизації дуже важливий фактор простоти обслуговування кабельного господарства, розміщеного на значній території.

У радіальних інтерфейсах, що з'єднують усього 2 порти, передавання даних від кожного з них може здійснюватися по окремій лінії. У цьому випадку з'являється принципова можливість одночасного (дуплексного) передавання даних в обох напрямках, що означає подвоєння пропускної здатності інтерфейсу й спрощення процедури арбітражу. Кількість ліній зв'язку в цьому випадку, як правило, подвоюється (рис. 12.3). У реальних системах найчастіше не вдається одержати подвоєння пропускної здатності через особливості алгоритму роботи пристрою. Лінії зв'язку занадто часто простоюють.

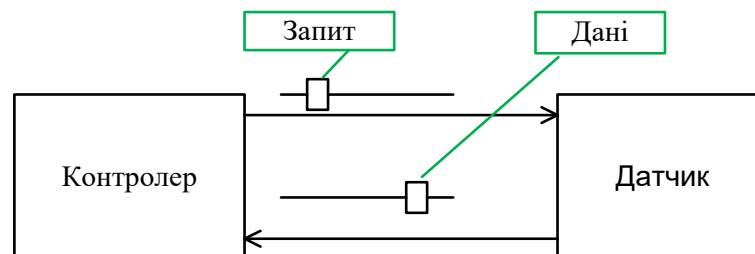


Рисунок 12.3 – Формування даних по запиту

12.3 Комунікаційні інтерфейси RS-232, RS-485 і RS-422

12.3.1 Загальні відомості про стандарт RS-485

Популярність інтерфейсів RS-232, RS-485 і RS-422 визначається невисокою вартістю портів і кабелів, а також стабільністю використання даних інтерфейсів у різних областях техніки, протягом тривалого часу різними виробниками. Підтримуються асинхронний і синхронний режими обміну даними.

Інтерфейс RS-232 побудований на уніполярних (однополярних) лініях передавання даних [1, 2]. Тому його продуктивність і максимальна довжина кабелю невеликі. RS-232 застосовується для підключення периферійного устаткування до персональних комп'ютерів. Кабельне господарство цього інтерфейсу недороге, що дає можливість використовувати окремі лінії для опитування, синхронізації й переривання. RS-232 є радіальним інтерфейсом, тому поняття адреси там відсутнє.

На рис. 12.4 показана послідовність керуючих сигналів інтерфейсу RS-232C. Вона має наступний фізичний зміст:

2. Установкою DTR (Data Terminal Ready – готовність контролера до обміну даними) контролер указує на бажання використовувати кінцевий пристрій.

3. Установкою DSR (Data Set Ready – готовність кінцевого пристрою до обміну даними) кінцевий пристрій сигналізує про свою готовність до роботи.

4. Установкою RTS (Request To Send – запит передавання даних. Сигнал готовності даних для передавання з контролера до кінцевому пристрою. У напівдуплексному режимі використовується для управління напрямком передавання даних) контролер запитує дозвіл на передавання й заявляє про свою готовність отримувати дані від кінцевого пристрою.

5. Установкою CTS кінцевий пристрій повідомляє про свою готовність до приймання даних.

6. Зняттям CTS кінцевий пристрій сигналізує про неможливість подальшого приймання (наприклад, буфер приймання заповнений) – контролер повинен призупинити передавання даних.

7. Установкою CTS кінцевий пристрій дозволяє комп'ютеру продовжити передавання (наприклад, у буфері з'явилося місце).

8. Зняттям RTS контролер інформує кінцевий пристрій про свою неготовність до обміну даними. Це може означати як заповнення буфера приймання контролера, так і відсутність даних для передавання в кінцевий пристрій.

9. Кінцевий пристрій підтверджує зняття RTS зняттям CTS.

10. Контролер повторно встановлює RTS для поновлення обміну даними.

11. Кінцевий пристрій підтверджує готовність до обміну установкою CTS.

12. Зняттям RTS контролер указує на завершення.

13. Кінцевий пристрій підтверджує зняття RTS зняттям CTS.

14. Контролер знімає DRT для переведення кінцевого пристрою в економічний або "сплячий" режим.

15. Кінцевий пристрій підтверджує зняття DRT зняттям DSR.

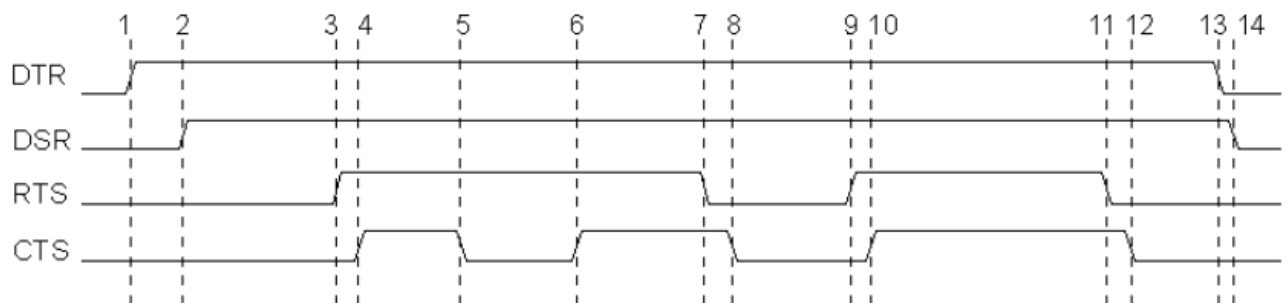


Рисунок 12.4 – Послідовність керуючих сигналів інтерфейсу RS-232C [2]

Інтерфейси RS-485 і RS-422 реалізовані на диференціальних лініях зв'язку, що забезпечує їх високу перешкодозахищеність. Звичайно застосовується кабелі із хвильовим опором 120 Ом. На кінцях ліній обов'язково розміщуються погоджувальні резистори. Активні системи узгодження не використовуються через невисокі швидкості передавання даних. Лінії RS-485 можуть бути довжиною до 1 кілометра. Інтерфейс RS-422 є "полегшеною" версією RS-485. У нього знижені

вихідні струми передавачів і, отже, менше навантажувальна здатність. Для поліпшення цих параметрів застосовуються повторювачі даних.

Інтерфейси RS-485 і RS-422 реалізують магістральний принцип обміну даними. У них може бути адресоване до 63 портів. Строго говорячи, RS-422 – радіальний інтерфейс, але багато виробників устаткування доповнюють його можливістю магістрального підключення й частковою сумісністю з RS-485 (зі зниженими параметрами по навантажувальній здатності). Рекомендаційний характер стандартів це цілком допускає. Розроблювач, що застосовує продукцію різних виробників, повинен бути уважним в аналізі параметрів виробів.

Завдання передавання даних між компонентами обчислювальної системи й периферійними пристроями на великі відстані в умовах підвищених шумів у промислових умовах є нетривіальною, а іноді й неможливою з використанням несиметричних ліній передавання. У той же час, що існують стандарти симетричних цифрових інтерфейсів дають розроблювачеві універсальний розв’язок для задоволення вимог побудови таких мереж. До таких інтерфейсів відноситься популярний стандарт RS-485, й стандарт CAN, що набирає популярність.

Стандарт передавання даних по двопроводовому багатоточковому послідовному симетричному каналу зв’язку RS-485 (Recommended Standard 485 або EIA/TIA-485-A) розроблений Electronic Industries Alliance (EIA) спільно с Telecommunications Industry Association (TIA). Він визначає тільки фізичні рівні передавання сигналів і не описує програмну модель і протоколи обміну на відміну від іншого популярного стандарту CAN.

RS-485 створювався для розширення фізичних можливостей передавання даних інтерфейсу RS-232. Його основними перевагами в порівнянні з RS-232 є:

- висока швидкість передавання даних – до 50 Мбіт/с;
- більша довжина лінії передач – до 1200 метрів;
- використання одного джерела живлення 5 В;
- використання симетричного методу передавання даних, що дозволяє підвищити завадостійкість, а також зменшити випромінювані перешкоди;

- можливість підключення декількох передавачів і приймачів.

Мала сприйнятливість до шумів диференціальної лінії разом з використанням крученому пари й широкого діапазону синфазної напруги дозволяють передавати дані по кабелю зі швидкістю 50 Мбіт/с або організовувати передавання даних на кілометрові відстані при малих швидкостях передавання за допомогою RS-485.

Тому що стандарт RS-485 описує тільки фізичний рівень процедури обміну даними, то всі проблеми обміну, синхронізації й опитування покладають на більш високий протокол, часто це стандарт RS-232 або інші протоколи верхнього рівня (Profibus, Modbus, DCON і т.п.).

Сам RS-485 виконує тільки наступні дії [2]:

- перетворює вхідну послідовність "1" і "0" у диференціальний сигнал;
- передає диференціальний сигнал у симетричну лінію зв'язку;
- підключає або відключає передавач драйвера по сигналу вищого протоколу;
- приймає диференціальний сигнал з лінії зв'язку.

На сьогоднішній день RS-485 стандарт є одним із широко застосовуваних для передавання даних з використанням симетричної лінії і його можна знайти практично в будь-якому додатку, що вимагає економічного й надійного зв'язку між двома або більш пристроями.

12.3.2 Топологія мережі RS-485

Мережа з використанням RS-485 будується по послідовній шинній схемі, тобто прилади в мережі з'єднуються послідовно симетричними кабелями [2]. Кінці ліній зв'язку при цьому повинні бути навантажені погоджувачими резисторами (рис. 12.5), опір яких повинен дорівнювати хвильовому опору кабелю зв'язку [1, 2]. Ці резистори виконують наступні функції:

- зменшують відбиття сигналу від кінця лінії зв'язку;

- забезпечують достатній струм через усю лінію зв'язку, що необхідно для послаблення синфазної завади за допомогою кабелю типу "кручена пари".

Часто при побудові такої топології в умовах підвищеного шуму додають фільтр синфазної складової шляхом заміни одного резистора навантаження на RC-фільтр нижніх частот (рис. 12.6). У цьому випадку важливо точно погодити величини використовуваних резисторів, щоб забезпечити однакову частоту зрізу обох фільтрів, тому що відмінність частот зрізу може привести до перетворення синфазного шуму в диференціальний шум, тим самим погіршуючи перешкодозахищеність системи.

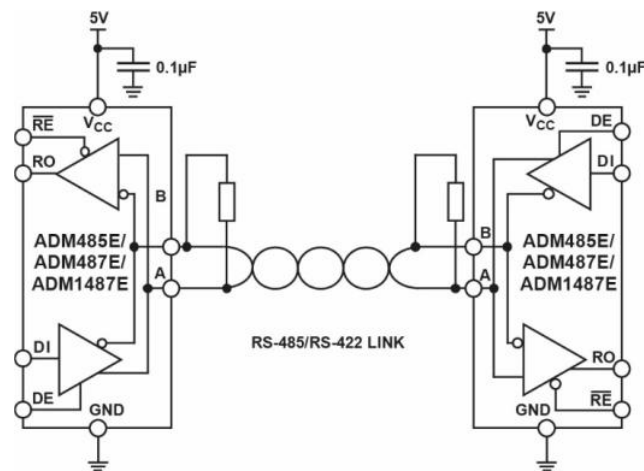


Рисунок 12.5 – Підключення трансиверів RS-485 до лінії зв'язку [3]

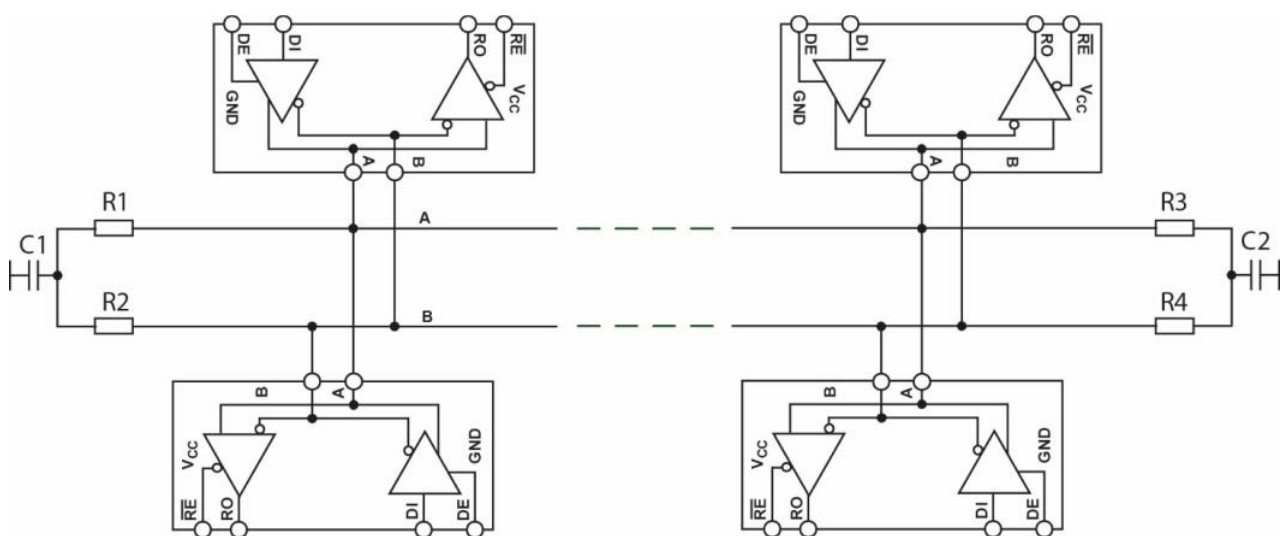


Рисунок 12.6 – Підключення трансиверів RS-485 до лінії зв'язку в умовах підвищеного шуму з фільтром синфазної складової [3]

Технічні характеристики інтерфейсу RS-485 [4].

У стандарті RS-485 для передачі та прийому даних використовується одна кручена пара проводів, іноді супроводжується екрануючим оплетенням або загальним проводом. Передача даних здійснюється з допомогою диференціальних сигналів. Різниця напруги між провідниками однієї полярності означає логічну одиницю, різниця іншої полярності – нуль.

Стандарт RS-485 обумовлює лише електричні та часові характеристики інтерфейсу.

Стандарт RS-485 не встановлює [4]:

- параметри якості сигналу (допустимий рівень спотворень, відображення у довгих лініях);
- типи з'єднувачів та кабелів;
- гальванічну розв'язку лінії зв'язку;
- протокол обміну.

Електричні та часові характеристики інтерфейсу RS-485 [4]:

- до 32 приймачів в одному сегменті мережі;
- максимальна довжина одного сегмента: 1200 метрів;
- лише один передавач активний;
- максимальна кількість вузлів у мережі 256 (з урахуванням магістральних підсилювачів).

Характеристика швидкість обміну/довжина лінії зв'язку [4]:

- 62,5 кбіт/с 1200 м (одна кручена пара);
- 375 кбіт/с 500 м (одна кручена пара);
- 500 кбіт/с (одна кручена пара);
- 1000 кбіт/с (одна кручена пара);
- 2400 кбіт/с 100 м (дві кручені пари).

Вихідний каскад повинен витримувати режим короткого замикання, мати максимальний вихідний струм 250 мА, швидкість наростання вихідного сигналу не менше ніж 1,2 В/мкс та схему обмеження вихідної потужності.

Устаткування для реалізації інтерфейсу випускає багато компаній. Одним з найбільших виробників ІМС для реалізації таких інтерфейсів є Texas Instruments.

12.3.3 Трансивери RS-485 Texas Instruments

Компанія Texas Instruments випускає порядку 180 різних пристроїв для реалізації трансиверів на основі інтерфейсу RS-485 [2]. У табл. 12.1 наведені основні характеристики деяких прийомопередавачів, що випускаються компанією Texas Instruments.

Таблиця 12.1 – Основні характеристики трансиверів RS-485 компанії Texas Instruments

Напруга живлення	Напівдуплексний трансивер	Особливості	Повнодуплексний ресивер
5 В	HVD3082E, HVD3085E, HVD3088E	Малий корпус, економічний	HVD308ÖE, HVD3083E, HVD3086E
	HVD20, HVD21, HVD22	Синфазна напруга -20...+25 В	
	HVD23, HVD24	Синфазна напруга -20...+25 В, частотна корекція	
	HVD1785, HVD1786, HVD1787	Синфазна напруга -20...+25 В, захист пінії 70 В	HVD1791, HVD1792, HVD1793
	LBC184	Захист від перехідних процесів	
	HVD1176	PROFIBUS	
	HVD96	Захист від перехресного включення (Sympol)	
	HVD09	9 каналів RS-485/422	
	ISO3082, ISO3088	4 кбайт ізольований RS-485	ISO3082, ISO3086, ISO3086T
3.3-5 В	ISO1176, ISOH76T	4 кбайт ізольований PROFIBUS	
	HVD08	Напруга живлення 3...5 В	
3.3 В	HVD1780, HVD1781, EIVD1782	Напруга живлення 3...5 В, захист лінії 70 В	
	HVD10, HVD11, HVD12	16 кбайт ESD, малий корпус	
		Із входом дозволу	HVD30, HVD31, HVD32
		Без входу дозволу	HVD33, HVD34, HVD35
		Мале споживання	HVD37

12.4 Однопроводовий інтерфейс CAN

CAN (Control Area Network) – послідовна магістраль, що забезпечує підключення в мережу "інтелектуальних" пристроїв вводу/виводу, сенсорів і виконавчих пристроїв деякого механізму або навіть підприємства (рис. 12.7). Характеризується протоколом, що забезпечує можливість знаходження на магістралі декількох пристроїв, що забезпечують передавання даних у реальному масштабі часу й корекцію помилок, характеризується високою завадостійкістю.

Для реалізації системи CAN випускається велика кількість мікросхем, що забезпечують роботу підключених до магістралі пристроїв, розробку яких починала фірма BOSCH для використання в автомобілях. У цей час CAN широко використовуваних не тільки в автомобілях, але в системах автоматизації промисловості [5].

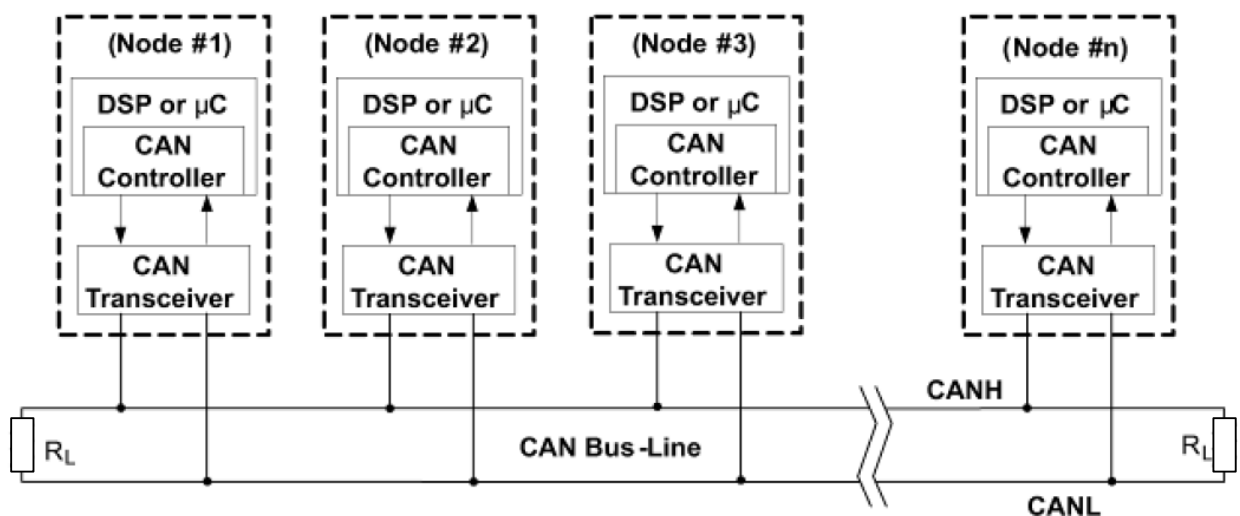


Рисунок 12.7 – Підключення пристроїв до шини CAN [5]

Основні параметри CAN-контролерів наведені в табл. 12.2.

Таблиця 12.2 – Основні параметри CAN-контролерів

Стандарт	ISO 11898
Швидкість передавання	1 Мбіт/с (максимум)
Дальність зв'язку	1000 м (максимум)

Продовження табл. 12.2.

Стандарт	ISO 11898
Характер сигналу, лінія передавання	диференціальна напруга, кручена пара
Кількість драйверів	64
Кількість приймачів	64
Схема з'єднання	напівдуплекс, багатоточкова

Характеристики інтерфейсу CAN [5, 6]:

1. Призначений для організації високонадійних недорогих каналів зв'язки в розподілених системах управління. Інтерфейс широко застосовується в промисловості, енергетику й на транспорті. Дозволяє будувати як дешеві мультиплексні канали, так і високошвидкісні мережі.

2. Швидкість передавання задається програмно й може бути до 1 Мбіт/с. Користувач вибирає швидкість, виходячи з відстаней, числа абонентів і ємності ліній передавання. У табл. 12.3 наведені дані про відповідність швидкості передавання й довгі лінії зв'язку.

3. Максимальне число абонентів, підключених до даного інтерфейсу фактично визначається навантажувальною здатністю застосованих прийомопередавачів. Наприклад, при використанні трансивера фірми PHILIPS PCA82C250 вона дорівнює 111.

4. Протокол CAN використовує оригінальну систему адресації повідомлень. Кожне повідомлення забезпечується ідентифікатором, який визначає призначення переданих даних, але не адреса приймача. Будь-який приймач може реагувати як на один ідентифікатор, так і на трохи. На один ідентифікатор можуть реагувати кілька приймачів.

5. Протокол CAN має розвитку систему виявлення й сигналізації помилок. Для цих цілей використовується порозрядний контроль, пряме заповнення бітового потоку, перевірка пакета повідомлення CRC-поліномом, контроль форми пакета повідомлень, підтвердження правильного приймання пакета даних. Інтервал Хемінга $d = 6$. Загальна ймовірність невиявленої помилки $4,7 \cdot 10^{-12}$.

6. Система арбітражу протоколу CAN виключає втрату інформації й часу при "зіткненнях" на шині.

7. Інтерфейс із застосуванням протоколу CAN легко адаптується до фізичного середовища передавання інформації. Це може бути диференційний сигнал, просто відкритий колектор і т.п. Нескладно робиться гальванічна розв'язка. Такий сигнал може передаватись по оптоволоконному кабелю.

8. Елементна база, що підтримує CAN, випускається в індустріальному виконанні.

В табл. 12.3 наведена відповідність швидкості передавання довжині лінії зв'язку.

Таблиця 12.3 – Відповідність швидкості передавання довжині лінії зв'язку

Відстань, м	25	50	100	250	500	1000	2500	10000
Швидкість, Кбіт/с	1000	800	500	250	125	50	20	10

12.5 Внутрішньомодульний інтерфейс I²C

Інтерфейс I²C, очевидно, найпростіший послідовний інтерфейс передавання даних [7]. Стандарт розроблявся для обміну даними між мікросхемами у межах однієї друкованої плати. Первісне призначення – тестування й ініціалізація ІМС. Оскільки підсистеми тестування не можуть становити більш 20% від робочої апаратури, в інтерфейсі I²C немає нічого зайвого – тільки те, без чого не можна обійтись. Реалізація ліній передавання даних і загальна ідеологія обміну даними нагадують інтерфейс CAN. Звідси й схожість позитивних рис: малі витрати часу на системні операції, зручний арбітраж і організація механізму пріоритетів, дешевина реалізації ліній обміну даними.

Інтерфейс I²C базується всього на двох лініях передавання даних. Вони побудовані однаково, за схемою "монтажного I". Буферні схеми ліній можуть бути легко реалізовані в будь-якій сучасній технології виготовлення мікросхем. Вихідні ключі – за схемою з відкритим емітером (затвором). Вхідні каскади звичайно

будуються за схемою тригера Шмідта. Обидві лінії є двонаправленими. Інформацію на них у ході обміну даними можуть видавати як контролер, так і кінцевий пристрій. На рис. 12.8 наведений приклад з'єднання пристроїв з використанням інтерфейсу I²C, а на рис. 12.9 – структура комутатора для інтерфейсу I²C.

Будь-який порт може ставати контролером, якщо в його структурі закладена така функція (табл. 12.4). На лінії обміну даними допустимі стани, наведені в табл. 12.5.

Таблиця 12.4 – Лінії обміну даними інтерфейсу I²C

Найменування лінія	Призначення лінії
SDA (Serial Data Line)	Послідовна передавання даних
SCL (Serial Clock Line)	Передавання сигналів синхронізації

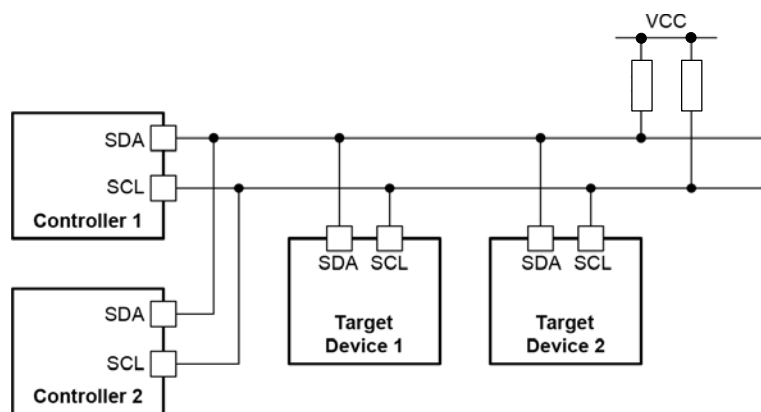


Рисунок 12.8 – З'єднання пристроїв з використанням інтерфейсу I²C [9]

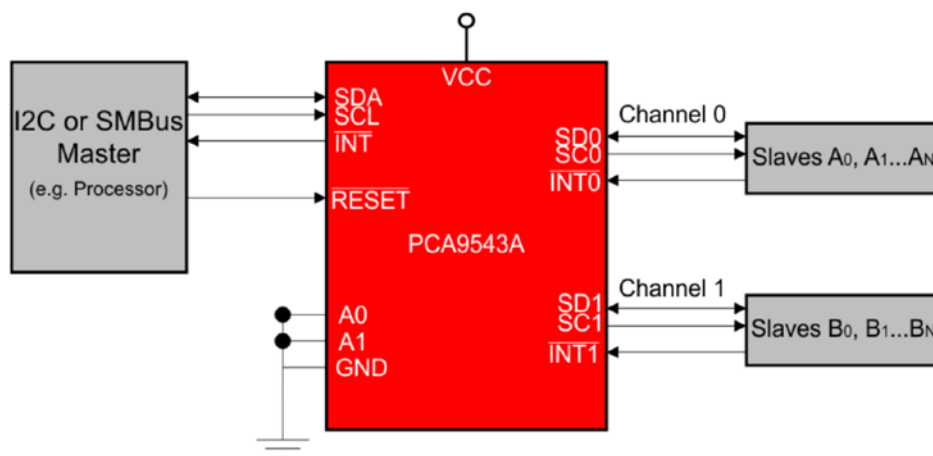


Рисунок 12.9 – Комутатор для інтерфейсу I²C [10]

Таблиця 12.5 – Припустимі стани ліній обміну даними інтерфейсу I²C

Значення	Рівень на лінії SCL	Рівень на лінії SDA
Шина вільна, зміна даних на лінії SDA, неготовність кінцевого пристрою	Низький рівень	Будь-яке
Передавання рівня логічного "0"	Високий рівень	Низький рівень
Передавання рівня логічної "1"	Високий рівень	Високий рівень
Сигнал "Початок передавання"	Високий рівень	Перепад з високого рівня на низький
Сигнал "Кінець передавання"	Високий рівень	Перепад з низького рівня на високий

Передавання починає будь-який порт (рис. 12.10). Він формує високий рівень на лінії SCL, а на лінії SDA формує сигнал "Початок передавання". Він являє собою перепад, в усі інших випадках сприйманий як збій. Порт, що передав сигнал "Початок передавання", вважає себе контролером, що захопив управління інтерфейсом. Він починає передавати адреси кінцевого пристрою зі старшого біта. Звичайно адреса складається з 7 бітів. Восьмим бітом передається ознака напрямку пересилання даних. Рівень логічного "0" означає передавання даних в кінцевий пристрій, рівень логічної "1" – приймання даних з кінцевого пристрою. Після приймання кожного байта, у тому числі адресного, приймач видає сигнал підтвердження у вигляді рівня логічного "0" на лінії SDA.

Підтвердження приймання адресного байта означає впізнавання кінцевим пристроєм своєї адреси. Якщо при цьому кінцевий пристрій не готовий почати обмін даними, воно фіксує рівень логічного "0" на лінії SCL. Оскільки лінія побудована за схемою "монтажного I", цей рівень буде залишатися на лінії, поки кінцевий пристрій його не знімає. Цим механізмом забезпечується функціонування асинхронного режиму обміну даними. Аналогічно він працює й при прийманні кожного біта

даних. При відсутності затримок, внесених кінцевим пристроєм, швидкість передавання становить 100 кбіт/с.

Передавання даних у тому або іншому напрямку здійснюється під управлінням позитивних синхронізуючих імпульсів на лінії SLC, формованих контролером. Після передавання кожного байта вставляється байт підтвердження, що свідчить про безпомилкове його приймання. Наприкінці операції обміну даними контролером формується сигнал "Кінець передавання".

Арбітраж функціонує аналогічно інтерфейсу CAN. Якщо кілька портів одночасно намагаються захопити управління, вони формують однакові стартові сигнали й починають передавати адресний байт. Усі передавальні порти контролюють реальний рівень сигналу на лінії SDA. Схема "монтажного И" виключає шинні конфлікти в такій ситуації, але в той момент, коли різні порти формують на лінії SDA одночасно рівні логічного "0" і логічної "1", що превалює логічний "0" є присутнім на шині (за рахунок "монтажного I").

Порт, що виставив рівень логічної "1", але, що виявив рівень логічного "0" на лінії SDA, вважає себе, що програли процедуру арбітражу. Таким чином, повідомлення із меншою адресою вважається більш пріоритетним. Виявивши цю ситуацію, порт, що передав рівень логічної "1", припиняє передавання й негайно переходить у режим приймання. Далі він працює як звичайний порт, що почав приймання адресного байта із самого початку обміну даними, і може виявитися кінцевим пристроєм до якого потрібно передати дані. У випадку трьох і більш одночасно захоплюючих шину портів арбітраж відбувається аналогічно. При збігу адресного байта процедура арбітражу триває з байтами даних, що надходять за ним [9].

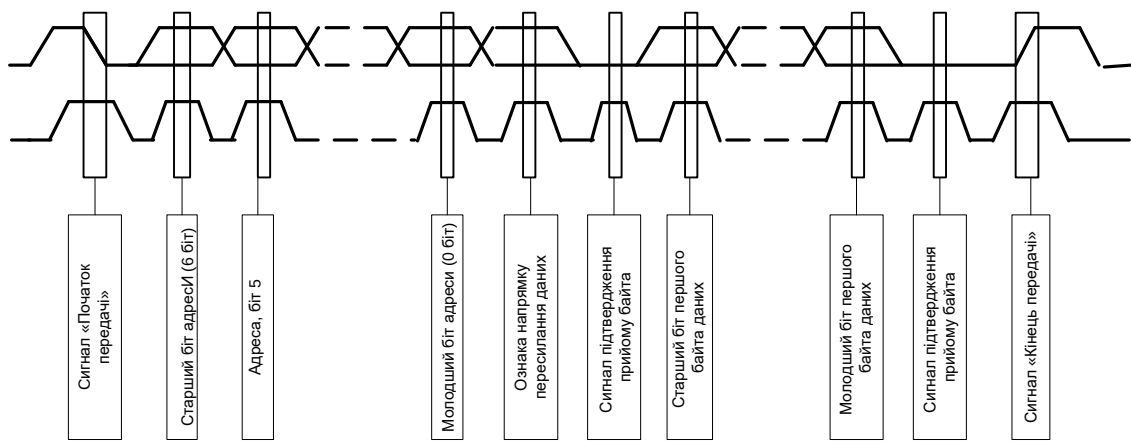


Рисунок 12.10 – Часові діаграми сигналів обміну даними по інтерфейсу I²C [9]

Обмін даними здійснюється максимально економічно за часом і без конфліктів на шині. Інтерфейс I²C допускає використання 10-бітної адреси, а також роботу на високій швидкості, що перевищує звичайну в 4 рази.

Порти I²C звичайно вбудовані у великі інтегральні схеми (ВІС), які випускаються для поставки на ринок і використання в різноманітних користувацьких системах. Розподіл адрес портів недоступний розроблювачеві системи. Адреси видаються виробникам ВІС комітетом РС по запиту виробників. Адреса конкретного типу ВІС завжди фіксована. Для виробів, яких може бути багато в одній системі, застосовується програмування декількох молодших бітів адреси за допомогою перемичок на друкованій платі. Така процедура розподілу адресного простору обмежує волю розроблювачів, практично не даючи переваг. Але звичайно цей недолік не сильно заважає розроблювачеві, тому що в реальних I²C системах застосовується обмежене число портів. Розміщається вся система на одній платі й не припускає стикування з іншими. Тому розроблювач завжди може знайти компроміс: відступити від стандарту при емуляції порту I²C у контролері і т.д.

Особливістю середовища передавання даних в інтерфейсі I²C є те, що всі порти розташовуються в межах однієї друкованої плати. За рахунок цього, а також за рахунок невеликої кількості ліній передавання даних реалізація систем на інтерфейсі I²C дуже економічна. Вимоги до буферних каскадів інтерфейсу дуже невисокі, їх собівартість, у порівнянні з найбільш близьким по реалізації інтерфейсом CAN, значно нижче. При стандартизації інтерфейсу I²C не

конкретизуються логічні рівні. Вони можуть бути різними залежно від напруги живлення утримуючих порти I²C мікросхем. Істотною перевагою I²C є дуже мала площа, займана інтерфейсними пристроями й лініями на друкованій платі. Споживана портами від джерела живлення потужність дуже мала, а, отже, малі й створювані перешкоди. Ця особливість дозволяє використовувати I²C у сенсорах, програмованих підсилювачах, схемах обробки малих сигналів.

12.6 Однопроводовий інтерфейс 1-wire

12.6.1 Загальні зауваження

Стандарт на даний інтерфейс створений фірмою Dallas Semiconductor. У цей час вона злилася з фірмою Maxim (яка в свою чергу злилася з компанією Analog Devices) [11]. Розробка інтерфейсу для виробів у двовиводному корпусі знадобилася для реалізації мікросхеми пам'яті в такому конструктиві. Пізніше інтерфейс був використаний для системи виробів у металевих таблеткових корпусах (рис. 12.11) [11]. Розширення функціональних можливостей систем з інтерфейсом 1-wire зажадало впровадження компонентів для нього в традиційних корпусах. Мережі на основі 1-wire звуться Microlan.



Рисунок 12.11 – Ключ iButton для систем контролю доступу [11]

Стандарт підтримується й просувається тільки фірмою Dallas Semiconductor. Завдяки цьому виробнику й ряду унікальних властивостей інтерфейс 1-wire застосовується в найрізноманітнішому устаткуванні, не ставши внутрішнім стандартом фірми. Компоненти з портами інтерфейсу 1-wire випускаються Dallas

Semiconductor, і розроблювачам практично не доводиться створювати схеми портів і досконально розбиратися у функціонуванні системи. Проте, інформація про нього корисна фахівцям для розуміння властивостей даних систем, а також тому, що ряд оригінальних розв'язків, закладених в стандарт, можуть бути використані поза контекстом 1-wire.

Орієнтованість 1-wire на двовиводні компоненти викликала до життя ідею "паразитного живлення". Для живлення портів і пов'язаних з ними цільових пристроїв по лінії передавання даних подаються імпульси, що заряджають вбудовані в порт конденсатори. Розряджаючись, вони забезпечують живлення.

По тій же причині виникли труднощі встановлення адрес пристроям, підключеним до системи. Прийнято записувати унікальну адресу пристрою при виготовленні у внутрішню пам'ять. Кожному пристрою властива індивідуальна адреса, що не повторюється за весь час виробництва. Якщо все, що вже випустив Dallas Semiconductor для 1-wire і ще випустить у майбутньому, об'єднати в одну величезну мережу, адреси портів не перекриються й конфліктів із цієї причини не виникне. Такий глобальний розв'язок привів до входу дуже довгих адрес, як показано на рис. 12.12.

Контрольна сума	Серійний номер виробу	Код типу виробу
1 байт	6 байт	1 байт

Рисунок 12.12 – Структура адреси порту інтерфейсу 1-wire

Настільки довга адреса пристрою знижує корисну продуктивність інтерфейсу. Навіть у невеликих системах, які частіше всього реалізуються за технологією 1-wire, циркулюють настільки довгі адреси. Треба помітити, що протокол 1-wire розрахований на як можна більш рідке вживання адрес при обміні даними.

У кожної 1-wire системі обов'язково присутня тільки один контролер, керуючий обміном даними й іншими операціями, усі інші порти є веденими

кінцевими пристроями. Вони можуть тільки відпрацьовувати команди контролера й виставляти переривання. Особлива роль контролера визначає різку відмінність його реалізації й функцій від кінцевих пристроїв:

Завдяки наявності в складі будь-якого пристрою унікальної індивідуальної адреси (відсутність збігу адрес для приладів, що випускаються Dallas Semiconductor Corp., гарантується самою фірмою-виробником), така мережа має практично необмежений адресний простір.

При цьому, кожний з однопроводових приладів відразу готовий до використання в складі 1-wire мережі, без яких-небудь додаткових апаратно-програмних модифікацій. Однопроводові компоненти є самотактуємими напівпровідниковими пристроями, в основі обміну інформацією між якими, лежить управління зміною тривалості часових інтервалів імпульсних сигналів в однопроводовому середовищі і їх вимір. Передавання сигналів, для 1-wire інтерфейсу, асинхронне й напівдуплексне, а вся інформація, що циркулює в мережі, сприймається абонентами або як команди, або як дані. Команди мережі генеруються майстром (рис. 12.13) і забезпечують різні варіанти пошуку й адресації ведених пристроїв, визначають активність на лінії навіть без безпосередньої адресації окремих компонентів, управляють обміном даними в мережі і т.д.

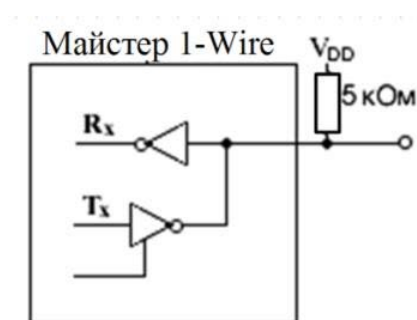


Рисунок 12.13 – Структура пристрою "майстер" інтерфейсу 1-wire [12]

Стандартна швидкість роботи 1-wire мережі, яка становить 15,4 кбіт/с, була обрана, по-перше, з урахуванням забезпечення максимальної надійності передавання даних на великі відстані, і, по-друге, з урахуванням швидкодії найбільше широко розповсюджених типів мікроконтролерів, які в основному

повинні використовуватися при реалізації провідних пристроїв однопровідної шини. Це значення швидкості обміну може бути зменшене до будь-якого можливого значення завдяки введенню примусової затримки між передачею в лінію окремих бітів даних. Або збільшене за рахунок переходу на спеціальний прискорений режим обміну (швидкість Overdrive до 125 кбіт/с), який допускається для окремих типів однопровідних компонентів на невеликій відстані, по не перевантаженій іншими приладами лінії зв'язку.

Особливо привабливою якістю технології 1-wire є виняткова простота налаштування й обслуговування мережі практично будь-якої конфігурації, побудованої по цьому стандарту. Дійсно, для початку роботи досить будь-якого персонального комп'ютера, недорогого адаптера 1-wire лінії, а також вільно розповсюджуваною фірмою Dallas Semiconductor Corp. програми Ibutton Viewer. При наявності цього невеликого числа складових контроль і управління мережею практично будь-якої складності, побудованої на базі стандартних однопровідних компонентів, організує протягом декількох хвилин. Програма Ibutton Viewer, у цьому випадку, дозволяє з максимальним комфортом для розроблювача ідентифікувати кожний з ведених однопровідних пристроїв на лінії й перевірити в повному обсязі правильність його функціонування в складі мережі.

12.6.2 Ведені однопровідні компоненти

Ведені однопровідні компоненти, що містять 1-wire інтерфейс, випускаються у двох різних корпусах. Або в корпусах MicroCAN, схожих зовні на дисковий металевий акумулятор, або у звичайних корпусах для монтажу на друковану плату. Футляр MicroCAN порожній усередині. Він виконує функцію захисту напівпровідникового кристала, що монтується в ньому, однопровідної мікросхеми, яка з'єднана із зовнішніми колами лише через дві, ізольовані один від одної, половинки корпусу, що є по суті контактними майданчиками для підключення однопровідної лінії. У подібних "таблеткових" корпусах поставляються, як правило, прилади iButton. Компоненти, які призначені для

використання в складі 1-wire мереж, упаковуються в пластикові корпуси, використовувані для виготовлення транзисторів і інтегральних схем. Такий підхід пояснюється тим, що на відміну від пристроїв iButton однопроводові прилади для 1-wire мереж часто мають більш двох виводів. Крім виводів, які потрібні для обміну даними по однопроводовій магістралі, вони мають у своєму розпорядженні додаткові виводи необхідні для забезпечення їх живлення й організації зовнішніх кіл, що зв'язують такі прилади з об'єктами автоматизації, наприклад, сенсорами або виконавчими пристроями.

Найбільш популярними веденими компонентами, на базі яких реалізована, мабуть, найбільша кількість застосувань, є цифрові термометри типу DS18S20. Переваги цих цифрових термометрів з погляду організації магістралі, у порівнянні з будь-якими іншими інтегральними температурними сенсорами, а також непогані метрологічні характеристики й гарна завадостійкість, виводять їх на перше місце при побудові багатоточкових систем температурного контролю в діапазоні від -55 до +125 °C. Вони дозволяють не тільки здійснювати безпосередній моніторинг температури в режимі реального часу, але й завдяки наявності вбудованої енергонезалежної пам'яті температурних уставок, можуть забезпечувати пріоритетну сигналізацію в лінію про факт виходу контрольованого параметра за межі заданих значень.

Більш досконалі прилади DS18B20 [14], швидкість перетворення, у яких визначається розрядністю результату, яка програмується майстром лінії безпосередньо в ході їх обслуговування. Цифровий код, зчитуваний з такого термометра, є прямим результатом обмірюваного значення температури й не має потреби в додаткових перетвореннях. А їх некалібрована, але в теж час більш дешева версія під позначенням DS1822, представляється оптимальним розв'язком для розроблювачів недорогих багатоточкових систем контролю температурних процесів. Для споживачів, що використовують тільки паразитний режим живлення однопроводової лінії, компанія Dallas Semiconductor Corp. випускає економічні двовиводні прилади – DS18S20-PAR, DS18B20-PAR, DS1822-PAR [14].

На рис. 12.14 наведено приклад використання декількох сенсорів з інтерфейсом 1-wire.

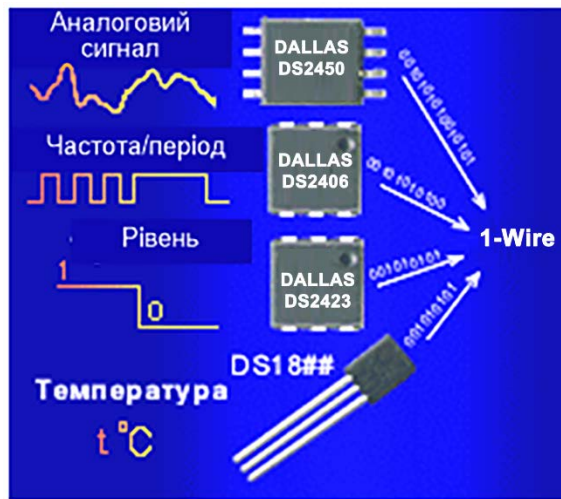


Рисунок 12.14 – Приклад використання декількох сенсорів для контролю параметрів об'єкта

Основними елементами, що лежать в основі фундаменту однопроводових мереж автоматизації, є універсальні здвоєні транзисторні ключі типу DS2406P [16], призначення яких наведено на рис. 12.15.

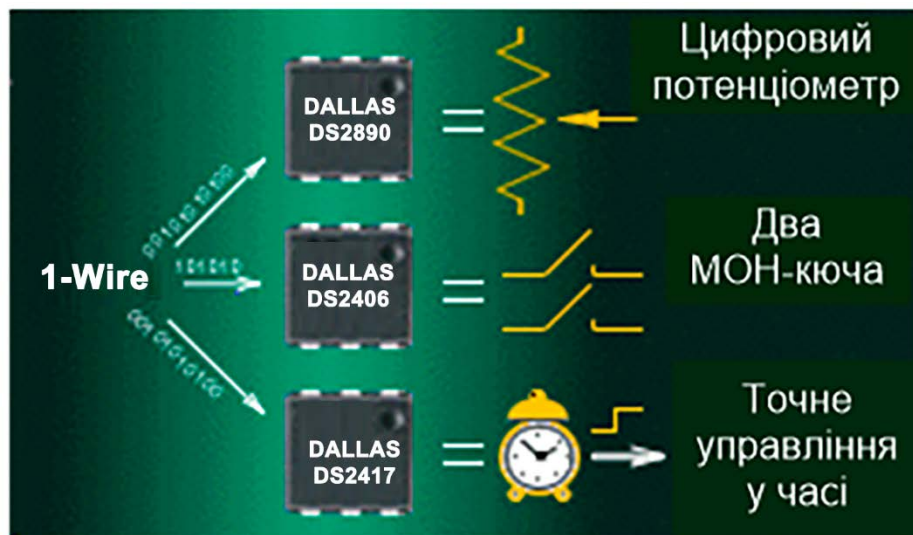


Рисунок 12.15 – Універсальні здвоєні транзисторні ключі для інтерфейсу 1-wire

На базі цих пристроїв може бути реалізована маса застосувань, і, насамперед, вузли контролю логічних станів (рівнів) і схеми обслуговування сенсорів, а також

різноманітні ключові схеми. Завдяки використанню цих компонентів здійснюється збір дискретної інформації з територіально розосереджених сенсорів (моніторів дверей, контакторів положення арматури, будь-яких сенсорів, що мають вихід ТАК/НІ, якість сенсори положення, проходу, присутності, пожежної й охоронної сигналізації і т.д.).

Подібні ж прилади забезпечують управління перемиканням будь-яких видів силового устаткування, які мають два робочі стани: включене/виключене (нагрівачів, кондиціонерів, моторів, вентиляторів, арматурних засувки і т.д.). Крім того, двонаправлені, індивідуально програмовані виводи DS2406P можуть бути використані для організації повільного послідовного інтерфейсу між локальним мікроконтролером і 1-wire мережею. Не дивлячись на невисоку швидкість при реалізації подібного способу обміну інформацією з однопроводової мережі, коли один біт даних передається за дві стандартні посилки, такий розв'язок є прийнятним і досить надійним для великої кількості конкретних застосувань.

12.6.3 Лінія зв'язку й топологія

Більшу роль при побудові 1-wire мереж відіграє виконання однопроводової лінії зв'язку. Як правило, такі лінії мають структуру, що складається із трьох основних провідників: DATA - шина даних, RET – зворотний або земляне проведення, EXT_POWER – зовнішнє живлення, що не тільки обслуговуються ведених пристроїв, але й зовнішніх щодо них кіл сенсорів і органів управління. Залежно від способу прокладки, сполучення з веденими пристроями й використовуваних при прокладці матеріалів, відповідно до табл. 12.6 розрізняють три основні варіанти якості організації 1-wire мереж, кожен з яких має на увазі використання особливої технології й аксесуарів при реалізації лінії [11].

Таблиця 12.6 – Параметри 1-wire мережі при різній довжині лінії

Класифікація лінії	Довжина лінії	Кількість ведених пристроїв	Тип використовуваного кабелю	Топологія	Майстер лінії
Короткі лінії	До 30 м	До 50 шт	4-хпроводний телефонний	Вільна	Пасивна підтяжка (резистор)
Середні лінії	До 100 м	До 200 шт	Кручена пари 5 категорії	Загальна шина	Активна підтяжка (DS2480, DS2490 або спеціальний схемний розв'язок)
Довгі лінії	До 300 м	До 300 шт	IEEE1394 (Firewire)	Загальна шина з єдиним стовбуром	Активна підтяжка з урахуванням струму в лінії

12.7 Оптичний інтерфейс із відкритим каналом Irda

В 70-х роках минулого століття з'явилися напівпровідникові джерела й приймачі інфрачервоного випромінювання, що дозволили реалізувати відкритий оптичний канал передавання даних на відстані до декількох метрів у межах прямої видимості. Поява подібної елементної бази викликала до життя численні системи зв'язку з їхнім використанням [16].

На цьому етапі не стояло завдання стандартизації інтерфейсу. Елементна база цифрової електроніки дозволяла будувати радіальні лінії обміну даними, часто односпрямовані, звичайно на мікросхемах середнього ступеня інтеграції. Такі розв'язки покривали потреба у зв'язку цільового пристрою, що носить, з базовим пристроєм. Ситуація змінилася з появою персональних комп'ютерів, які могли виконувати роль бази для декількох пристроїв, що носяться. У зв'язку із цим в 1993

році була створена організація виробників інфрачервоних інтерфейсів (Infrared Data Association), покликана стандартизувати подібні системи.

Повітряне середовище передавання даних розсіює випромінювання й не дозволяє організовувати кілька ліній або дуплексний режим роботи. Тому в стандарт на інтерфейс Irda закладений напівдуплексний режим. Створення мереж з більш ніж двох портів не передбачене, однак це не означає, що додаткові порти не можуть працювати тільки в режимі приймання. Повноцінна мережа може бути створена за рамками стандарту, шляхом додавання в посилку інформації про адресу.

Інтерфейс Irda розроблений як розширення стандарту RS-422. У форматі передавання даних багато схожого. Як наслідок, реалізація портів Irda і конвертерів COM – Irda не представляє труднощів, можна використовувати сумісну елементну базу. При передаванні даних імпульси випромінювання генеруються в однозначній відповідності із сигналами інтерфейсу RS-422.

Рівень логічного "0" передається в Irda коротким імпульсом. Рівень логічної "1" – відсутністю випромінювання (рис. 12.16) [16].

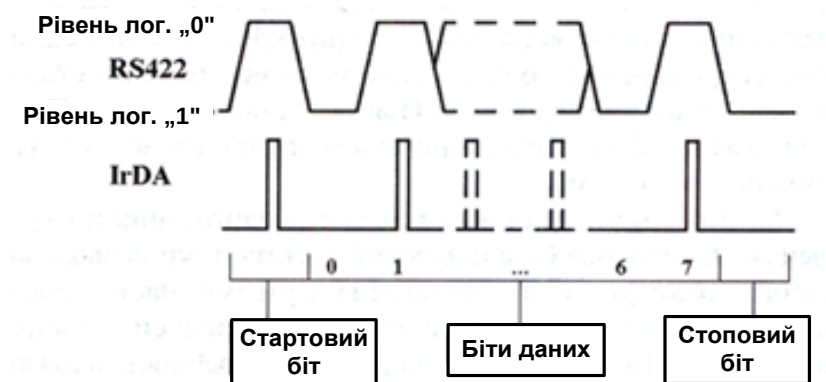


Рисунок 12.16 – Схожість формування сигналів інтерфейсів RS-422 і Irda [16]

Вільна лінія в RS-422 приймає значення логічної "1". Передавання починається з формування стартового біта рівнем логічного "0". По цьому імпульсу приймач синхронізується й починає приймання послідовних даних. Аналогічно в інтерфейсі Irda, при відсутності передавання не формується ніяких імпульсів, що

відповідає логічній "1". Початок передавання позначається імпульсом стартового біта, слідом за ним передаються дані. Столовий біт позначається рівнем логічної "1". Перешкодозахищеність, вірогідність і надійність такого каналу обміну – низькі. Відповідно інтерфейс Irda може бути використаний у невідповідальних додатках.

Для роботи компактних пристроїв дуже важливо невисоке споживання енергії від батареї. Тому імпульси передавача інтерфейсу Irda мають велику скважність. Тривалість імпульсу повинна бути рівна $3/16$ від часу передавання одного біта. Але імпульс не може бути коротше 1,63 мс. Такий імпульс формується при швидкості обміну даними 115,2 кбіт/с і вище (табл. 12.7) [17].

Оптичний прийомопередавач стандарту Irda часто виконується у вигляді приставки до універсального порту послідовного інтерфейсу UART. Така архітектура забезпечує дуже низьку вартість устаткування. На рис. 12.17 показана типова схема трансивера Irda. Електричний інтерфейс відповідає сигналам інтерфейсу RS-422. В табл. 12.7 наведені часові параметри імпульсів інтерфейсу Irda.

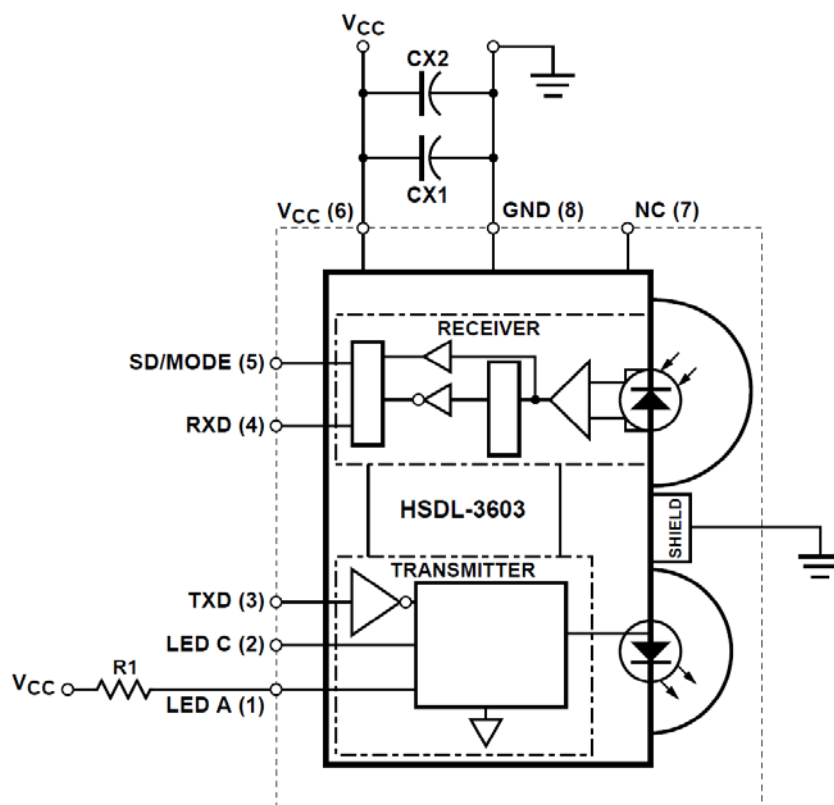


Рисунок 12.17 – Схема трансивера Irda HSDL-3603 [17]

Таблиця 12.7 – Часові параметри імпульсів інтерфейсу Irda

Швидкість передавання даних, кбіт/с	2,4	10,6	19,2	38,4	57,6	115.
Час передавання одного біта, мс	416	104	52	26	17,3	8,68
Тривалість імпульсу, мс, +0,22 мс	78,13	19,53	9,77	4,88	3,26	1,63

Конструктивно трансивер інтерфейсу Irda звичайно виконується у вигляді мікросхеми в корпусі із пластику, прозорого для інфрачервоного випромінювання (довжина хвилі в Irda рівна 880 нм, з допуском у межах 850 – 900 нм). Така конструкція технологічна й недорога у виготовленні й монтажі (рис. 12.18).



Рисунок 12.18 – Конструкція трансивера інтерфейсу Irda [18]

Дуже низька вартість реалізації, невеликі енергоспоживання й габарити, гальванічна розв'язка портів, простота програмування, відсутність проводів й роз'єднувачів роблять інтерфейс Irda привабливим для розроблювачів цивільних систем обміну даними. Тим більше що портами цього інтерфейсу оснащено багато пристроїв.

На зміну Irda поступово приходить радіоінтерфейс Bluetooth, який забезпечує більшу дальність, підтримує до 256 портів і має інші переваги.

12.8 Безпроводовий інтерфейс Bluetooth

Інтерфейси з безпроводовим середовищем передавання даних усе більш затребувані в сучасному світі й застосовуються для невідповідальних додатків. В 90-х роках XX століття найбільше поширення одержав інтерфейс Irda з відкритим

оптичним середовищем. Це було обумовлено простотою реалізації й дешевиною комплектуючих. Впровадження Irda дозволило уніфікувати з'єднання між різним периферійним устаткуванням і базовими пристроями (контролерами). Невелика продуктивність каналу обміну даними не дозволила використовувати оптичне середовище для більш складних завдань.

Набагато більші можливості має радіосередовище передавання даних. Її пропускна здатність набагато вище, не потрібно мати прямої видимості між портами, можлива реалізація повнодуплексного режиму. Такі властивості закладені в специфікацію стандарту Bluetooth [19-22]. Спочатку він розроблений консорціумом фірм – виробників мобільних електронних пристроїв. Пізніше розробка була підтримана IEEE, що й виразилося в створенні стандарту IEEE.802.15.1, що узаконив специфікацію Bluetooth. Робоча група IEEE.802.15 продовжує розробки в тому ж напрямку.

Конкуруючі розв'язки одержали набагато менше поширення, хоча не були суттєво гірше, а тільки не одержали потужної підтримки великих виробників. Архітектура інтерфейсу Bluetooth може бути, як магістральної, так і радіальної. У радіальному варіанті функціональність системи в частині передавання синхронних даних ширше.

Магістральний варіант реалізується за допомогою пікомереж. У кожен пікомережу входить один пристрій, що є контролером, і до 255 кінцевих пристроїв. Одночасно можуть бути активні тільки 8 портів. Інші перебувають у неактивному режимі до команди активізації від контролера. Пікомережі можуть взаємодіяти між собою, тому що контролер однієї з них може бути одночасно кінцевим пристроєм іншої (рис. 12.19).

Кожному виробу з Bluetooth при виготовленні привласнюється унікальний 27-розрядна адреса, як це прийняте в інтерфейсі 1-wire.

Радіообмін в Bluetooth відбувається на частотах від 2,4 до 2,4835 ГГц. Даний діапазон практично у всіх країнах є неліцензованим і може бути використаний вільно. У Франції й Іспанії він частково зайнятий під військові потреби. Увесь цей діапазон розділений на 76 каналів. У кожний момент часу обмін відбувається

тільки по одному з них. Після передавання одного пакета даних обмін переходить на інший канал. Частота переходів до 1600 Гц. Вибір каналів здійснюється по псевдовипадковому алгоритму, єдиному для пікомережі. У цьому алгоритмі однієї зі змінних є адреса контролера, тому для кожної пікомережі послідовність використання каналів різна. Для зовнішніх стосовно пікомережі пристроїв такий широкопasmовий сигнал подібний шуму, не сильно впливає на зв'язок в інших системах. Перешкоди від них також не сильно впливають на роботу пікомережі, тому що у випадку помилки обміну даними повторна передавання відбувається по іншому каналу.

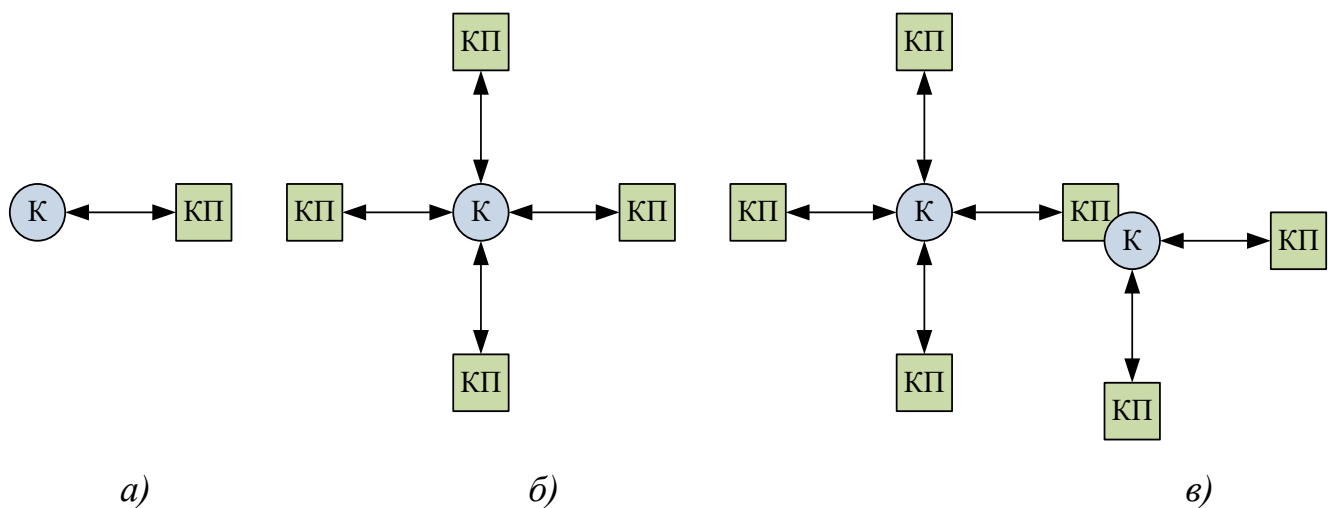


Рисунок 12.19 – Конфігурації пікомереж Bluetooth, радіальне з'єднання (а), типова пікомережа (б), зв'язані пікомережі (в)

На рисунку буквою К позначений контролер, а буквами КП – кінцевий пристрій. Будь-який порт інтерфейсу Bluetooth, що потрапив у зону дії пікомережі, намагається увійти в мережу. Контролер пікомережі не дозволяє цього до підтвердження оператора. Оператор може визнати новий пристрій "своїм", його унікальна адреса запам'ятовується контролером, і при наступному контакті втручання оператора вже не потрібно.

Інтерфейс Bluetooth підтримує синхронний і асинхронний режими обміну даними. Синхронний режим можливий тільки у випадку радіального з'єднання контролера з кінцевим пристроєм. Контроль передавання при цьому не ведеться.

Продуктивність інтерфейсу в синхронному режимі дає можливість організувати до 3 канатів передавання голосової інформації.

Асинхронний режим дозволяє досягти високої надійності обміну даними. У випадку помилки приймання передавання збійного пакета повторюється.

Стандартний пакет Bluetooth містить код доступу пікомережі (72 біта), заголовок (18 біт) і поле інформації (не більш 2745 біт) (рис. 12.20). Заголовок або інформація можуть бути відсутні. Код доступу ідентифікує пакети даної пікомережі. Він включає унікальну адресу контролера й контрольну суму.

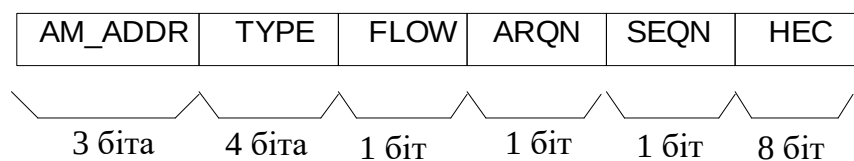


Рисунок 12.20 – Заголовок пакета Bluetooth

Заголовок містить поля:

- AM_ADDR – адреса кінцевого пристрою (3 біта);
- TYPE – код типу даних (4 біта);
- FLOW – готовність кінцевого пристрою (1 біт);
- ARQN – підтвердження правильності приймання (1 біт);
- SRQN – послідовність пакетів (1 біт);
- HEC – контрольна сума (8 біт).

Поле інформації може містити додаткові поля (підполя) даних і голосу.

Поява інтерфейсу Bluetooth пов'язана з розвитком елементної бази цифрової обробки сигналів. Реалізація порту Bluetooth неможлива без цифрового сигнального процесора. На нього ж звичайно покладає реалізація протоколів високого рівня. Невеликі розміри й споживання енергії привели до масового впровадження Bluetooth у цивільних мобільних пристроях. Масове впровадження природно привело до лавиноподібному падінню цін на комплектуючі. Усе це

робить застосування інтерфейсу Bluetooth дуже вигідним у різноманітних системах передавання даних.

Контрольні питання

1. Який інтерфейс з наведених забезпечує найбільшу дальність зв'язку?
2. У чому переваги інтерфейсу RS-485 перед інтерфейсом RS-232?
3. Які інтерфейси забезпечують економічний і надійний зв'язок між двома або більш пристроями?
4. В яких додатках найчастіше використовується інтерфейс CAN?
5. Чи передбачена корекція помилок в інтерфейсі CAN?
6. До чого призводить корекція помилок при передаванні даних – до збільшення, чи до зменшення завадостійкості?
7. Де знайшов використання інтерфейс 1-wire?
8. Наведіть приклади використання інтерфейсу Irda?
9. Де використовується інтерфейс I²C?
10. Скільки ліній зв'язку використовується в інтерфейсі Irda?
11. Скільки ліній зв'язку використовується в інтерфейсі 1-wire?
12. Скільки ліній зв'язку використовується в інтерфейсі CAN?
13. Скільки ліній зв'язку використовується в інтерфейсі I²C?
14. На якій відстані можна здійснювати зв'язок за допомогою інтерфейсу I²C?

Перелік посилань

1. Branden Hookway Interface. – MIT Press, 2014. 192 p.
2. RS232/RS485 Multiprotocol Transceivers. Url:
https://www.ti.com/lit/ug/tidua80/tidua80.pdf?ts=1732267730364&ref_url=https%253A%252F%252Fwww.ti.com%252Fsitesearch%252Fen-us%252Fdocs%252Funiversalsearch.tsp%253FlangPref%253Den-

- US%2526nr%253D1327%2526searchTerm%253Drs485+transceiver (дата звернення: 1.07.2024).
3. RS485 Driver. Url: <https://www.oemsecrets.com/articles/rs485-driver> (дата звернення: 1.07.2024).
 4. Стандарт Передачі Даних RS485. Url: <http://www.mika.ua/RS485> (дата звернення: 6.12.2024).
 5. Canbus Introduction. Url: <https://wiki.li-bat.com/comm/canbus/introduction/> (дата звернення: 1.07.2024).
 6. Протокол CAN. Url: <https://greenhouse.cv.ua/?p=623> (дата звернення: 1.07.2024).
 7. CAN transceivers. Url: https://www.ti.com/interface/can-transceivers/products.html?keyMatch=can%20transceiver&tisearch=universal_search (дата звернення: 1.07.2024).
 8. I2C інтерфейс. Url: <https://itmaster.biz.ua/directory/standarts/i2c.html> (дата звернення: 1.07.2024).
 9. A Basic Guide to I2C. Url: https://www.ti.com/lit/an/sbaa565/sbaa565.pdf?ts=1732601374021&ref_url=https%253A%252F%252Fwww.google.com%252F (дата звернення: 1.07.2024).
 10. PCA9543A. Url: https://www.ti.com/product/PCA9543A?keyMatch=PCA9543A&tisearch=universal_search&usecase=GPN-ALT (дата звернення: 1.07.2024).
 11. 1-Wire Devices. Url: <https://www.analog.com/en/product-category/1wire-devices.html> (дата звернення: 1.07.2024).
 12. Електронний ключ Touch Memory. Url: <https://око.укр/kontrol-dostupa/schityvateli-i-klyuchi/ehlektronnyj-klyuch-touch-memory/> (дата звернення: 1.07.2024).
 13. Інтерфейс 1-wire. Url: <https://схем.net/comp/comp53.php> (дата звернення: 1.07.2024).

14. Sensors and MEMS. Url: <https://www.analog.com/en/search.html?query=DS18%D0%9220&prodCats=Sensors%20and%20MEMS> (дата звернення: 1.07.2024).
15. DS2406 Dual Addressable Switch Plus 1Kb Memory. Url: <https://www.analog.com/media/en/technical-documentation/data-sheets/ds2406.pdf> (дата звернення: 1.07.2024).
16. IRDA. Url: https://ko.com.ua/irda_luchshe_pozdno_chem_nikogda_44351 (дата звернення: 1.07.2024).
17. IRDA приймально-передавачі. Url: https://kosmodrom.ua/irda-priymachi-peredavachi/proizvoditel__vishay?srsId=AfmBOooPHvaqF1tnGRNVgESO98QtTZQOY0Dme01Q48iXPCyI-FBXIu6D (дата звернення: 1.07.2024).
18. Agilent HSDL-3603 IrDA. Url: <https://www.datasheetbank.com/ru/datasheet-download/931707/1/AVAGO/HSDL-3603-007> (дата звернення: 1.07.2024).
19. David Kammer, Gordon McNutt, Brian Senese Bluetooth Application Developer's Guide: The Short-Range Interconnect Solution. Url: <https://vdoc.pub/download/bluetooth-application-developers-guide-the-short-range-interconnect-solution-5tlg44huc6r0>. (дата звернення: 1.07.2024).
20. Neal Stephenson, George F. Jewsbury, Stephen Bury Interface. – Paperback Published, 2005/ – 640 p.
21. Yan Yan, Qi Li, Heping Li, Xuejun Zhang and Lei Wang A home-based health information acquisition system. Health Information Science & Systems 2013, 1:12. Url: <https://link.springer.com/content/pdf/11.1186/2047-2501-1-12.pdf>. (дата звернення: 1.07.2024).
22. Bluetooth® Low Energy Application Developer's Guide. Url: <https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/wireless-connectivity/11469/1/Bluetooth%20Low%20Energy%20Application%20Developer%20Guide.pdf>. (дата звернення: 1.07.2024).

13 СИСТЕМИ КОНТРОЛЮ ТА КЕРУВАННЯ ПАРАМЕТРАМИ "РОЗУМНОГО" БУДИНКУ

13.1 Використання технологій Інтернету речей для побудови "розумних" будівель

На цей час розрізняють два поняття – "розумний" будинок та "розумна" будівля [1]. Поняття розумного будинку відноситься до індивідуальних жилих будинків (котеджів) та може бути віднесено до великих квартир у багатоповерхових будинках ("розумна" квартира).

Що стосується розумної будівлі, то це поняття відноситься до багатоквартирних будинків і навіть до невеликих мікрорайонів міста. Існує ще і поняття "розумного" міста, що відноситься вже до всього міста.

Термін "розумний" будинок у 1984 році запропонувала американська асоціація забудовників. Це скоріш поняття "розумної" будівлі. У цей період часу почався спад цін на електроприлади, що дозволило здійснювати будівництво офісів з високою функціональністю. А 90-х роках двадцятого сторіччя почали з'являтися інтелектуальні побутові прилади і технології зв'язку, що дозволили говорити про концепцію "розумний" будинок для індивідуального споживача та "розумна" квартира.

Система "розумний" будинок дає можливість контролювати стан приміщень і обладнання будинку та здійснювати керування пристроями, встановленими у будинку.

Для зручності користувачів в систему "розумний" будинок можуть бути включені:

- система керування електроживленням будівлі і його освітленням;
- система безпеки (охорона і протипожежна сигналізація, багатозональне відеоспостереження, захист від протікання води);
- системи контролю та керування споживанням води та газу;
- автоматичні електроприводи (віконних жалюзі, воріт, захисних ролет і т.д.);

- система контролю параметрів навколишнього середовища – температуру повітря, його вологість, швидкість вітру та інші (за потребою);
- системи контролю складу повітря, вентиляції, обігріву та кондиціонування повітря;
- системи для розваг і дозвілля (домашній кінотеатр, музичний центр та інше).

Одними з найпоширеніших є системи керування освітленням, що дозволяють включати та виключати світло у приміщеннях як автоматично, так і користувачем, управляти яскравістю освітлення, здійснювати контроль витрат електроенергії. Встановлюють аналогічні системи для контролю і керування витратами води та газу.

Системи контролю мікроклімату дозволяє не тільки підтримувати високий рівень комфорту, тобто вологості, температури і чистоти повітря, а і знизити енергоспоживання. Це можливо реалізувати завдяки можливості програмування роботи системи в різних режимах. Наприклад, при відсутності мешканців у будинку можна знизити температуру повітря у зимовий час, відключивши його обігрів.

Для керування всіма пристроями у будинках можна використовувати як проводові, так і безпроводові канали зв'язку. Найчастіше для організації "розумного" будинку використовуються проводові системи зв'язку. А для керування окремими пристроями – безпроводові системи зв'язку. Наприклад, для передавання даних від датчика розташованого на великій відстані від будинку, доцільно замість прокладання кабелю використати безпроводовий канал зв'язку. Але при виборі тієї чи іншої системи необхідно оцінювати не тільки вартість реалізації системи, а і її надійність.

13.2 Інсталяційна шина KNX

У сучасних системах автоматизації будинків використовується цілий ряд різних стандартів зв'язку. Одним з них є міжнародний стандарт (технологія) KNX (ISO/IEC 14543). В основі стандарту лежить шина EIB (European Installation Bus) [2, 3].

У лютому 1990 року була організована асоціація EIBA зі штаб-квартирою в м. Брюссель (Бельгія). Засновниками асоціації були 15 провідних європейських компаній: Siemens, Gira, ABB, Berker, Jung і інших. Основними завданнями асоціації були:

- просування на ринку технології EIB;
- контроль якості й сумісності устаткування, виробленого її членами;
- підготовка програм навчання фахівців.

Через кілька років уже близько 100 європейських і світових компаній пропонували сертифіковане устаткування під логотипом EIB. Учасники асоціації контролювали до 80% європейського ринку інсталяційних пристроїв. До кінця століття EIB була явним лідером у своїй області. У світі було встановлено більше 10 мільйонів пристроїв EIB. Однак у шини EIB були конкуренти - шина BatiBUS, що одержала поширення на півдні Європи, а також EHS (European Home System).

У травні 1999 відбулося об'єднання трьох європейських асоціацій автоматизації будинків EIBA (European Installation Bus Association), EHSA (European Home Systems Association) і BCI (BatiBUS Club International) в одну, котра згодом одержала остаточну назву "Асоціація KNX" – Konnex. Відбулося й злиття трьох технологій: EIB, EHS і Batibus.

На думку різних експертів, стандарт KNX на 80...90% заснований на технологію EIB. Це об'єднання – результат загальної інтеграції в Європі. Верховенство EIBA не ховалося всіма учасниками, саме тому в багатьох випадках використовується позначення EIB/KNX. Наприкінці 2003 року технологія була затверджена як європейські стандарти EN 50090 і EN 13321-1, а потім як міжнародний стандарт ISO/IEC 14543-3 [3], американський стандарт ANSI/ASHRAE 135 і китайський стандарт GB/Z 20965.

Всесвітня Асоціація KNX має партнерські угоди з більш ніж 11000 компаній-інтеграторів устаткування в 74 країнах, з більш ніж 50 технічними університетами й 112 центрами навчання [4].

KNX є єдиним у світі відкритим стандартом для контролю безпеки комерційних і житлових будинків. Використання KNX забезпечує реальні переваги для архітекторів, проектувальників і виконавців робіт, а також, у першу чергу, для власників і/або користувачів будинків:

1. Низькі експлуатаційні витрати й значне зниження енергоспоживання. Освітлення й опалення включаються тільки тоді, коли вони дійсно потрібні, наприклад, відповідно до заданих програм або у випадках присутності людей, що дозволяє заощаджувати електроенергію й фінансові ресурси. Освітлення може контролюватися автоматично відповідно до реальної інтенсивності денного світла, що допомагає забезпечувати мінімальний необхідний рівень яскравості освітлення на кожному робочому місці й знижувати енергоспоживання (включеними залишаються тільки ті джерела освітлення, які дійсно необхідні).

2. Економію часу. Зв'язування всіх пристроїв, що обмінюються між собою інформацією, за допомогою однієї загальної шини значно скорочує час проектування системи й час її установки. Програмний пакет ETS, загальний для всіх виробників і програмних додатків, дозволяє здійснювати проектування, налагодження й налаштування систем, що містять у своєму складі KNX-сертифіковані елементи. Оскільки цей програмний пакет є єдиним для всіх виробників, інтегратори систем можуть поєднувати в проекті продукти від різних виробників, що використовують різні канали для обміну інформацією (кручені пари, радіочастотні канали, електричні лінії або IP/Ethernet), у складі єдиної системи.

3. Гнучкість і здатність адаптуватися до майбутніх змін. KNX-система може бути легко пристосована до виконання нових завдань і розширена. Нові компоненти можна підключати до вже працюючої системи.

Щоб передавати керуючі сигнали до всіх компонентів, відповідальним за керування будинком, необхідна система, здатна взаємодіяти з окремими пристроями; для цього всі її компоненти повинні вміти “спілкуватися” між собою

єдиною мовою. Шинна технологія KNX, єдина для всіх виробників устаткування й програмних додатків, відповідає ці вимогам.

При використанні каналу передавання керуючих сигналів KNX, до якого підключаються всі інші шини (кручені пари, радіочастотні канали, електричні лінії або IP/Ethernet), підключені до них пристрою одержують можливість обмінюватися інформацією між собою. До шин можуть підключатися як сенсори, так і виконавчі механізми, необхідні для контролю устаткування, що управляє будинком, зокрема, систем освітлення, штор, жалюзі й ставень, систем безпеки, систем контролю енергоспоживання й опалення, вентиляції й кондиціонування повітря, сигнальних систем, систем моніторингу й дистанційного керування, вимірювального устаткування, систем керування аудіо й відео, великої побутової техніки, інтерфейсів комунальних систем і інших систем керування будинком і т.д. Всі ці функції можуть здійснюватися, контролюватися й відслідковуватися через єдину загальну систему, без використання яких-небудь додаткових центрів керування (рис. 13.1) [4].



Рисунок 13.1 – Деякі компоненти систем, заснованих на стандарті KNX, і їхні умовні позначення [5]

Системи, побудовані на основі KNX, є **децентралізованими** [4]. У їхній склад входять 3 основних типи пристроїв – сенсори, актуатори (тобто виконавчі механізми та пристрої) й системні пристрої.

1. Сенсори (датчики) – сенсорні настінні панелі й вимикачі; датчики температури, вологості, освітленості, диму, руху й т.д., пульти дистанційного керування, таймери й інших. Вони виконують реєстрацію різних зовнішніх подій, настання яких повинне викликати певну відповідну реакцію системи. Після настання такої події (натискання кнопки, перевищення температурою граничного значення й т.п.) сенсор посилає по мережі керуючу команду відповідному виконавчому пристрою.

2. Актуатори (виконавчі пристрої й перетворювачі) – регулятори сили світла (димери), релейні модулі, електродвигуни, модулі керування жалюзі й інших. Вони міняють свій стан (включене-виключено, відкрите-закрите й т.п.) відповідно до команд, що надходять від сенсорів, тим самим управляючи різним електроустаткуванням.

3. Модулі контролерів – логічні контролери, функціональні модулі, термостати й т.д. Забезпечують програмування й керування мережею. Модулі контролерів дозволяють реалізувати особливо складні алгоритми керування, коли, наприклад, поставлене завдання керування відразу декількома видами устаткування по даним, одержуваним одночасно від декількох сенсорів. Як правило, такі модулі не потрібні.

4. Системні пристрої – блоки живлення, інтерфейсні модулі, шинні з'єднувачі, повторювачі й інші, включаючи панелі й логічні модулі. Системні пристрої забезпечують працездатність і можливість налаштування мережі KNX.

Оскільки система децентралізована, то вихід з ладу кожного із пристроїв не вплине на роботу системи в цілому. При цьому висока надійність устаткування підтверджена сертифікатами й тестами головної асоціації Konnex.

Система є безпечною, тому що керуюча напруга дорівнює 24 В. Дані в системі можуть передаватися по:

- кручений парі з фіксованою швидкістю передавання 9600 біт/с;

- силової лінії (проводам живлення 230 В/50 Гц) зі швидкістю передавання 1200 біт/с;
- IP-мережі (EIB.net) – наприклад, Ethernet;
- радіоканалу в неліцензованих частотних діапазонах 868 і 433 МГц.

Підключені до шини пристрої можуть обмінюватися інформацією через загальний канал передавання. Для цього інформація упаковується в телеграму й передається по каналу зв'язку від сенсора до одного або декількох виконавчих пристроїв. При успішному передаванні й прийомі кожен пристрій (приймач) підтверджує одержання телеграми. При відсутності підтвердження передача повторюється ще два рази. Якщо й після цього підтвердження відсутнє, то процес передавання закінчується. Саме із цієї причини протокол KNX не є "промисловим", тобто його не можна застосовувати в додатках, пов'язаних з небезпекою для життя й здоров'я людей.

Телеграма – це послідовність знаків, які залежно від загального для них інформаційного змісту поєднуються в поля. Вона складається із блоків даних: службових і інформаційного, у якому повідомляється про подію (наприклад, натисканні кнопки), і контрольної інформації, що дозволяє виявити помилки передавання даних.

Передавання здійснюється модуляцією напруги в мережі, причому логічний нуль пересилається у вигляді імпульсу, з амплітудою приблизно ± 6 В. Відсутність імпульсу інтерпретується як логічна одиниця. Телеграми пересилаються пакетами по 8 байт. Пересилання синхронізується старт- і стоп-бітами. Є біт контролю парності [5].

Структура телеграми наведена на рис. 13.2.

Контрольне поле	Початкова адреса	Адреса призначення	Пріоритет і квітування	Довжина	Поле даних	Поле захисту інформації
8 біт	16 біт	16 + 1 біт	3 біта	4 біта	16×8 біт	8 біт

Рисунок 13.2 – Структура телеграми в системі KNX

Кожна телеграма стає видимою у функціональному блоці й відповідно її дані можуть бути оброблені. Блок відкидає KNX телеграми з адрес, які не включені в поле "Довжина". Наприклад: групова адреса 1/2/0 довжина: 10. Всі KNX телеграми з адресами 1/2/0...1/2/9 пройдуть через фільтр і будуть сприйматися блоком.

Дані контрольного поля й поля захисту інформації необхідні для безперебійного обміну телеграмами. Вони обробляються шинними пристроями (функціональними блоками), яким вони адресовані. Адресне поле містить вихідна адреса (адреса джерела сигналу) і адреса призначення (адреса одержувача). Адреса джерела сигналу завжди фізична адреса. Вона вказує, до якої зони й до якої лінії відноситься сигнал, що посиляє, прилад. Фізична адреса закріплюється при проектуванні за одним конкретним шинним пристроєм і використовується тільки для введення в експлуатацію й для сервісних функцій.

Адреса призначення визначає учасників комунікації. При цьому одержувачем, якому відправляється телеграма, може бути як окремий блок, так і група блоків, підключених до однієї лінії, або ж розподілених по різних лініях. Той самий функціональний блок може входити в різні комунікаційні групи (групові адреси). Групова адреса визначає комунікаційні відносини усередині системи. Поле даних служить для передавання безпосередньо самого інформаційного послання, наприклад, команд, повідомлень, настановних параметрів, даних вимірів і т.д.

Для запобігання колізій телеграм у мережі застосовується метод CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance – множинний доступ з контролем носійної й запобіганням конфліктів). Цей метод гарантує випадковий, безпроблемний доступ пристроїв до шини, при цьому без істотного зниження її максимальної пропускної здатності. При цьому гарантується, що спочатку будуть передані повідомлення з найвищим пріоритетом.

Для того, щоб система запрацювала необхідно не тільки встановити пристрої й з'єднати їх необхідними кабелями між собою й із силовою мережею, але й запрограмувати пристрої за допомогою програмного забезпечення ETS.

У межах однієї мережі кожний пристрій повинен мати індивідуальну фізичну адресу. Призначення адрес здійснюється за допомогою програмного забезпечення ETS [5]. Перед призначенням пристрою адреси він переводиться в режим програмування, як правило, шляхом натискання на спеціальну кнопку на лицьовій частині корпусу, при цьому для підтвердження режиму програмування загоряється червоний світлодіод.

Групові адреси можуть бути призначені активним пристроям системи поза залежністю від їхнього розташування й значень фізичних адрес. Виконавчим пристроям (одержувачам телеграм) може бути призначено кілька групових адрес, але сенсори можуть відправляти телеграму тільки по одній адресі. У складних системах, як правило, використовують трьохрівневу систему групової адресації (головна група/середня група/підгрупа).

Фізична адреса пристроїв має наступну структуру: Зона/Лінія/Пристрій. Наприклад, адреса 2/1/3 визначає третій пристрій у першій лінії другої зони. Для фізичної адреси зарезервованій 16 біт інформації. На рис. 13.3 показана структура адреси.

Зона	Лінія	Пристрій
XXXX	XXXX	XXXXXXXX
4 біта	4 біта	8 біт

Рисунок 13.3 – Структура фізичної адреси KNX-пристрою

При такій адресації до кожної лінії можна підключити до 64 пристроїв, як показано на рис. 13.4, а мережа KNX може включати до 14400 пристроїв без застосування підсилювачів ліній (15 зон по 15 ліній у кожній й по 64 пристрої, підключених до кожної лінії), як показано на рис. 13.5. Лінія може складатися як з одного сегмента, так і з декількох (максимум із чотирьох), з'єднаних за допомогою лінійних підсилювачів [5].

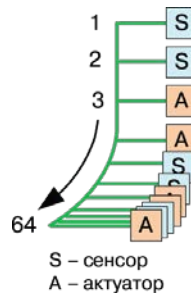


Рисунок 13.4 – Об’єднання пристроїв KNX у лінію [5]

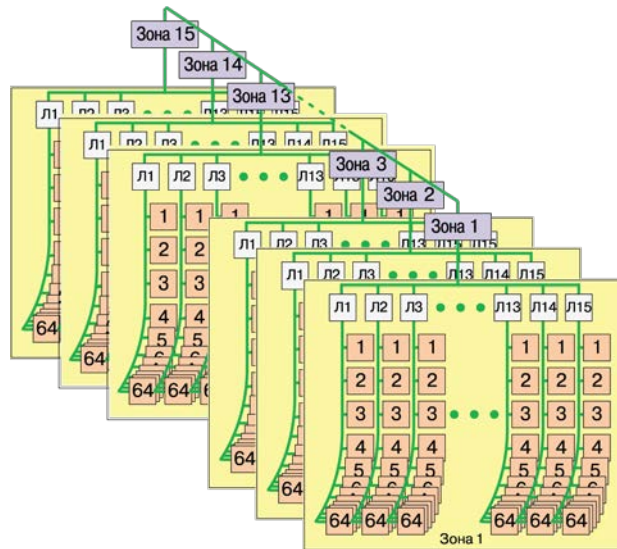


Рисунок 13.5 – Об’єднання ліній і зон KNX [5]

Для складних проектів створюється структура із груповими адресами. Найчастіше трьохрівнева – головна група/середня група/підгрупа. Трьохрівнева система групових адрес використовує 4 біти інформації для головної групи, 3 біти для середньої й 8 біт для підгрупи. Таким чином, можна використати максимально 16 головних груп (0...15), 8 середніх (0...7) і 256 підгруп (0...255).

За допомогою лінійних з’єднувачів (Л1...Л15 на рис. 13.5) до 15 ліній можуть бути підключені до головної лінії й об’єднані в одну зону. До головної лінії також можливе підключення до 64 шинних пристроїв. Максимальне число підключених шинних пристроїв скорочується зі збільшенням числа лінійних з’єднувачів.

Головна лінія повинна мати окреме джерело живлення й дросель. На зонній і головній лініях не допускається підключення лінійних підсилювачів.

Кілька зон можуть бути з'єднані між собою за допомогою зонної лінії, при цьому кожна зона підключається до зонної лінії через окремий зонний з'єднувач (на рис. 13.5 підсилювачі не показані). Зонна лінія повинна мати власне джерело живлення. До зонної лінії можливе підключення шинних пристроїв

Застосування шини KNX дозволяє значно спростити прокладку проводів у будинку. Традиційні рішення, у яких для керування кожною підсистемою передбачені окремі лінії, вимагають більших витрат на електропроводку, як показано на рис. 13.6. Крім цього, підвищується пожежонебезпека й знижується ремонтпридатність. Чим складніше система, тим складніше пошук несправностей, тому що силове проведення й проведення керування не відділені одне від одного.

В KNX силове проведення й проведення керування розділені (рис. 13.7) [5].

Між окремими пристроями. лінійного сегмента KNX існують наступні обмеження на довжину сполучних ліній при відсутності додаткових підсилювачів (рис. 13.8):

- відстань між пристроєм і блоком живлення не більше 350 м
- відстань між двома зв'язаними пристроями не більше 700 м
- максимальна довга лінійного сегмента 1000 м.

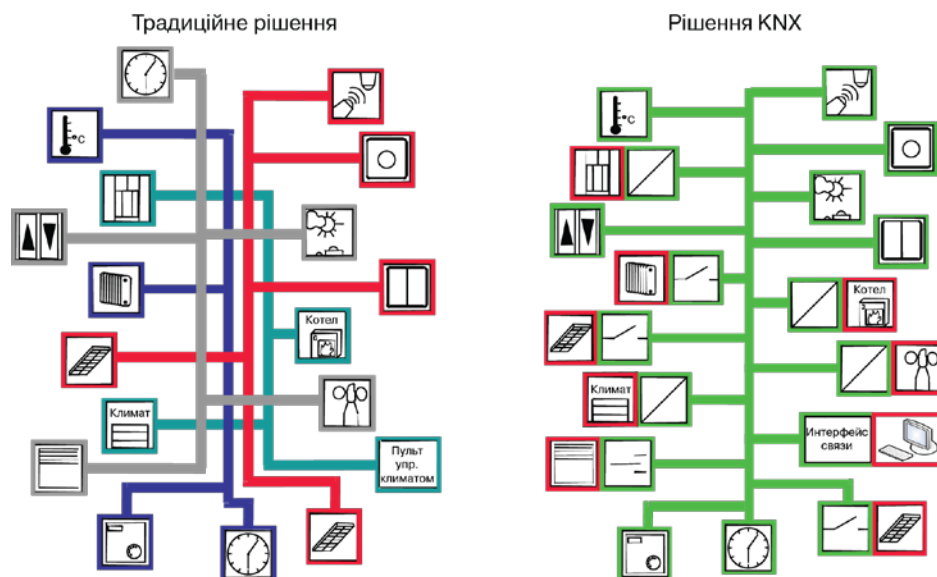


Рисунок 13.6 – Структура ліній зв'язку при традиційному рішенні системи керування і при використанні шини KNX [6]

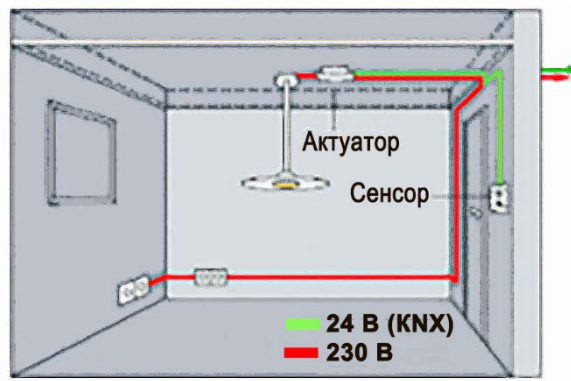


Рисунок 13.7 – Силове проведення й проведення керування шини KNX розділені [6]

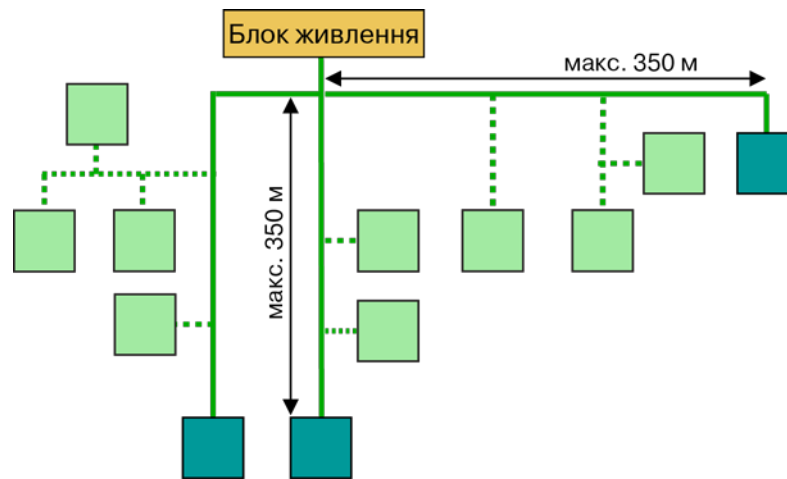


Рисунок 13.8 – Обмеження на довжину сполучних ліній у лінійному сегменті KNX

Для з'єднання пристроїв використовується стандартний кабель із двома парами проводів ($2 \times 2 \times 0.8$ мм). Одна пара проводів використовується для передавання сигналу й електроживлення 24 В (червоне й чорне проведення), а друга резервна (наприклад, для підключення резервного блоку живлення).

Структура шинного пристрою

Кожний шинний пристрій (наприклад, сенсорний вимикач, активатор димера або активатор жалюзі) має дві основних частини:

- шинний контролер (Bus Coupling Unit – BCU);
- прикладний модуль (Application Module – AM).

Шинні пристрої конструктивно виконуються як для установки на DIN-рейку, так і для схованого монтажу.

Дані керування надходять по шині на шинний контролер, що посиляє, одержує й зберігає таку інформацію, як власна фізична адреса, один або кілька групових адрес, а також прикладну програму з усіма необхідними параметрами. Координацію цих функцій виконує мікропроцесор. При виникненні несправностей або спадання напруги в мережі всі дані зберігаються, і шинні пристрої переводяться в передбачений програмою для цього стан. Передбачено можливість запрограмувати поведінку пристроїв після усунення несправностей і при відновленні напруги в шині до номінального значення.

Електроживлення

Живлення пристроїв KNX здійснюється безпечною напругою, максимальна величина якого не перевищує 30 В. Шина завжди надійно ізольована від силової електромережі, і дотик до шини безпечний. Електроживлення шини відповідає вимогам DIN EN 50090, тобто максимальна величина струму в шині обмежена й всі джерела живлення мають захист від короткого замикання в навантаженні.

Тому що телеграми передаються по тим же проводам по яких подається живлення на шинні пристрої, то для запобігання значного ослаблення сигналу команд джерело живлення підключається до шини через вбудований у нього дросель [5]. Опір дроселя для сигналу телеграм має значну величину й практично сигнали команд у шині не послаблюються (рис. 13.9). Тому що джерела живлення для KNX мають і другий вихід без дроселя, то його можна використати із зовнішнім проміжним дроселем для живлення іншої лінії.

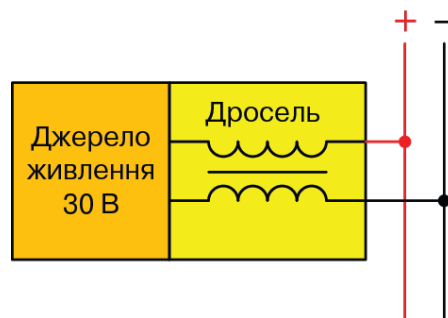


Рисунок 13.9 – Підключення джерела живлення до шини KNX

Керування по радіоканалу

У системі KNX передбачена наявність пристроїв, у яких прийом і передавання даних здійснюються по радіоканалу [6]. Щоб уникнути колізій при одночасній роботі декількох пристроїв по радіоканалах, кожний радіопередавач KNX відсилає в складі телеграми також свій серійний номер для розпізнання пристрою в мережі. Таким чином, на телеграми кожного передавача реагують лише ті приймальні пристрої, які настроєні на прийом сигналів від конкретного передавача.

Радіус дії радіосигналів у будинку обмежений. Це обумовлено загасанням радіосигналів при проходженні через стіни, перекриття й інші фізичні перешкоди. Розширити зону дії можна використавши повторювачі радіосигналів, що дозволяє здійснювати керування пристроями, розташованими на різних поверхах, по радіоканалу.

У радіосистемах KNX як метод модуляції застосовується частотна маніпуляція (Frequency Shift Keying – FSK). Частота носійного коливання 868.30 МГц (ISM-діапазон), швидкість передавання даних становить 16384 біт/с, максимальна потужність сигналу – 12 мВт. Час передавання радіосигналу кожним пристроєм, називаний також робітником циклом (Duty Cycle), становить приблизно 0.6 с. Більше докладну інформацію про структуру телеграми й інших параметрів пристроїв, що працюють із застосування радіоканалу, можна знайти в [3].

Проектування системи "розумного" будинку за допомогою програми ETS

Проектування й налагодження системи KNX здійснюються за допомогою програмного забезпечення ETS. Короткий опис системи ETS3 дано в [5]. У цей час випущена версія програмного забезпечення ETS5.6 [5]. Демонстраційна версія програми ETS5 Demo, розрахована на підключення п'яти пристроїв, може бути безкоштовно завантажена із сайту асоціації <https://www.knx.org>.

Крім того, пропонується програмне забезпечення KNX Virtual [7] – це додаток для Windows, що дозволяє протестувати роботу програми з п'ятьма пристроями в одному проекті й не потребуючої її установки на ПК. Програма дозволяє спроектувати:

1. Включення освітлення (включаючи сходи).
2. Включення освітлення (включаючи сходи) зі зворотним зв'язком.
3. Затемнення.
4. Керування жалюзі.
5. Керування опаленням (RTC).

При роботі програми KNX Virtual виводяться повідомлення про пристрої, які потрібні для проекту ETS, які можна завантажити через каталоги ETS [7].

При роботі з інстальованою на ПК демонстраційною версією програми в установках поставити "пташку" у рядку "Автоматично завантажувати відновлення каталогу". Для негайного відновлення натиснути кнопку "Негайне відновлення". Через кілька хвилин список доступних каталогів буде виведений у нижній частині вікна програми (рис. 13.10).

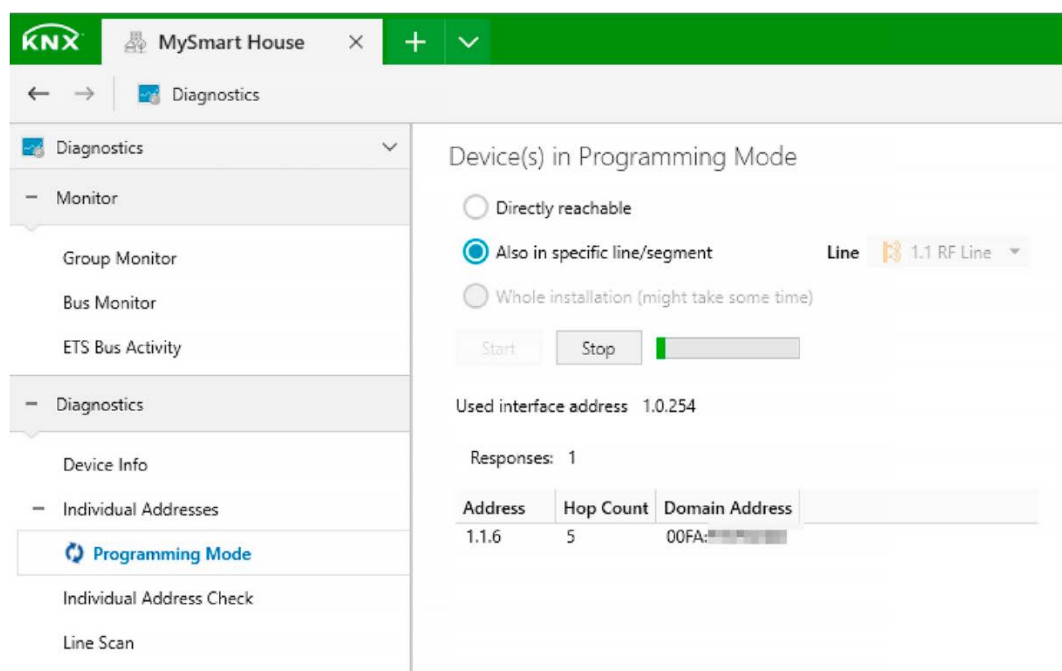


Рисунок 13.10 – Вікно програми ETS в режимі програмування [6]

Всі виробники KNX-пристроїв супроводжують свої вироби файлом-описом з розширенням *.vd1...*.vd5, призначеним для експорту в програму ETS. Завантаживши файл у програму, можна запрограмувати даний пристрій відповідно до необхідного алгоритму роботи й установити потрібні параметри.

На етапі проектування немає необхідності наявності самого пристрою й зв'язку із шиною EIB – досить мати програму ETS і бібліотеку файлів пристроїв, що входять у майбутню систему.

З порядком роботи із програмою можна ознайомитися в [7].

У цей час асоціація Konnex активно розвиває напрямок Інтернету речей. Для цього напрямку розроблені програмні продукти KNX IoT Software Tools: "**KNX Web service exporter**" і "**KNX Web service gateway**".

13.2 Пристрої для керування освітленням по шині KNX

13.2.1 Загальні зауваження

KNX є світовим стандартом (ISO/IEC 145433-3) керування житловими приміщеннями й будинками, пропонуючи на ринку безліч нових продуктів для систем візуалізації й автоматизації будинків. MEAN WELL, що є провідним виробником стандартних блоків живлення, просуває технологію керування автоматизацією будинків KNX з моменту випуску першого стандартного блоку живлення KNX-20E з технологічним стандартом KNX в 2017 році й постійно розширює номенклатуру виробів, призначених для систем KNX.

Наприклад, універсальний вимикач KAA-8R і регулятор яскравості KAA-4R4V, залежно від застосування вони підходять для різних джерел живлення MEAN WELL і драйверів світлодіодів. Ґрунтуючись на архітектурі KNX, системні інженери можуть легко програмувати через систему ETS роботу цих виробів [8].

Всі вироби **MEAN WELL** відповідають світовим стандартам безпеки й сертифікатам EMC/EMI. Клієнтам не потрібно чекати тривалий час перевірки й платити за дорогі збори за сертифікацію, що може привести до зриву графіка введення системи керування в експлуатацію.

Компанія MEAN WELL випускає продукцію для систем:

- керування внутрішнім освітленням;
- керування опаленням;
- керування шторами й жалюзі;

- комплексного керування енергоспоживанням.

13.2.2 Керування внутрішнім освітленням

У міру того, як поліпшується рівень життя людей, відповідно підвищуються вимоги до якості освітлення. Системи освітлення повинні не тільки прагнути до енергозбереження й високої ефективності, але й бути зручними, гнучкими й орієнтованими на людину. З розвитком технології інформаційних мереж технологія шин KNX стає усе більше поширеною, що сприяє розвитку індустрії інтелектуального будівництва. Ці фактори привели до розробки концепції "інтелектуальної системи керування освітленням". Архітектура системи складається із блоку живлення, що живить шину KNX. Перемикач або димер KNX використовується для керування драйвером світлодіодів. Для виконання цих завдань MEAN WELL розробила джерела живлення шини KNX-20E і KNX-40E, універсальний перемикач KAA-8R, димер KAA-4R4V [8]. Що стосується світлодіодних драйверів, MEAN WELL розробив безліч таких виробів і тому для вибору найбільш підходящого драйвера світлодіодів можна звернутися до веб-сайту компанії.

На рис. 13.11 схематично показані можливості системи керування освітленням, створеної на базі продукції MEAN WELL. Живлення всіх пристроїв керування KNX здійснюється по шині KNX. По ній же передаються й сигнали керування. Більш докладно про це можна прочитати в [5].

Актуатори KNX здійснюють керування світлодіодними драйверами. Залежно від типу драйвера (з димером чи ні) використовуються відповідні їм актуатори.

З огляду на те, що в експлуатації є велика кількість світлодіодних драйверів з інтерфейсом DALI (Digital Addressable Lighting Interface – стандартний цифровий протокол керування освітленням за допомогою таких пристроїв, як електронні баласты для люмінесцентних ламп і димери), MEAN WELL випускає пристрої керування такими драйверами (актуатори).

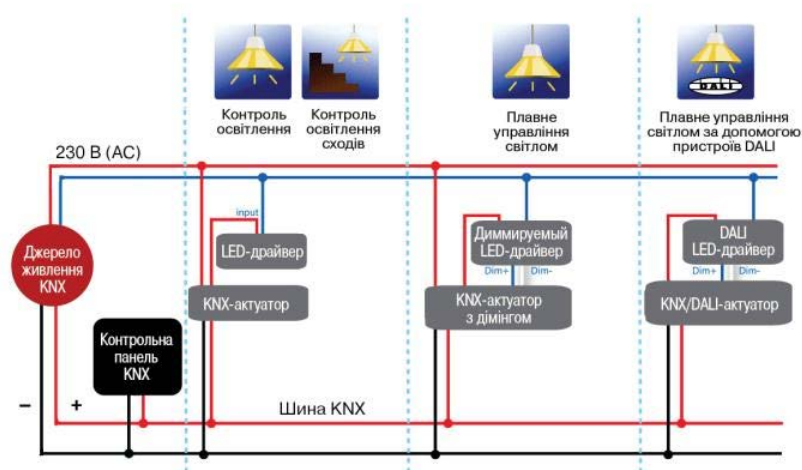


Рисунок 13.11 – Можливості системи керування освітленням з використанням продукції MEAN WELL [7]

13.2.3 Компоненти MEAN WELL для керування внутрішнім освітленням

8-канальний актуатор (комутатор навантаження) КАА-8R

Модуль КАА-8R [8] (рис. 13.17) призначений для керування люмінесцентними лампами, ємнісним і індуктивним навантаженням у системах автоматизації будинків, опалення, вентиляції й освітлення [10].



Рисунок 13.17 – Модуль КАА-8R [8]

Основні характеристики КАА-8R:

- 8 каналів керування;
- світлодіодні індикатори для кожного каналу;
- монтаж на DIN рейку;
- живлення здійснюється по шині KNX (21...31 В);

- програмування за допомогою ПО ETS 5.0;;
- ручне керування за допомогою кнопок на передній панелі
- програмування різних варіантів режимів і часу роботи;
- максимальний вихідний струм для модифікації;
 - КАА-8R - 16 А;
 - КАА-8R-10 - 10 А;
- сумарний максимальний вихідний струм 80 А (КАА-8R) і 56 А (КАА-8R-10);
- струм споживання не більше 6 мА;
- споживана потужність 180 мВт;
- вихід - бістабільне реле;
- максимальна ємність навантаження 220 мкФ;
- число циклів комутації не менш 10^6 ;
- діапазон робочих температур $-30...45\text{ }^{\circ}\text{C}$;
- відносна вологість 10...95%;
- габаритні розміри $72\times90\times57\text{ мм}$;
- маса 312 г.

Класи й ступінь захисту, безпека, рівень ЕМЗ і несприйнятливість до електромагнітних перешкод аналогічно КАА-4R4V.

Функціональна схема модуля наведена на рис. 13.18 і особливих пояснень не вимагає.

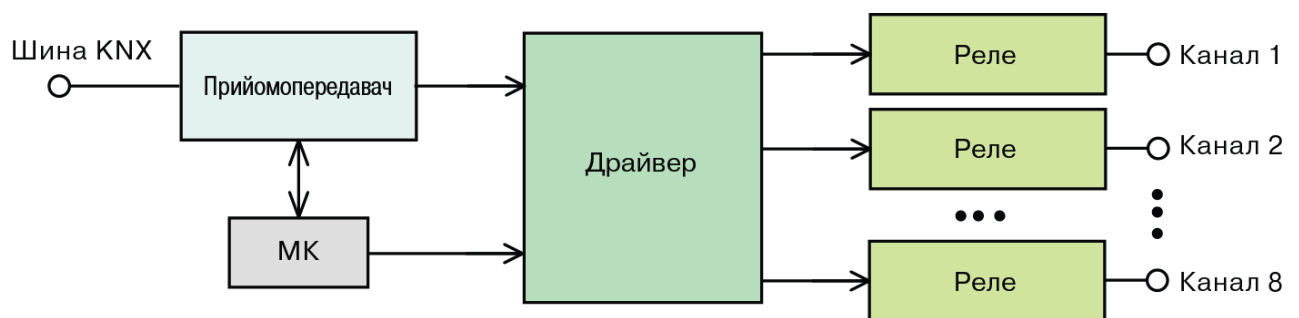


Рисунок 13.18 – Функціональна схема модуля КАА-8R

Припустима потужність, що віддає модуль КАА-8R у навантаження, залежно від її характеру наведена в табл. 13.1.

Таблиця 13.1 – Припустима потужність, що віддає модулем КАА-8R у навантаження

Тип навантаження	Максимальна потужність, Вт	
	КАА-8R	КАА-8R-10
Активне навантаження або нагрівачі	3680	2300
Лампи розжарювання	2300	2300
Галогенні лампи 230 В	2300	2300
Галогенні лампи із трансформатором	1300	1300
Лампи люмінесцентні некомпенсовані	2000	2000
Лампи люмінесцентні з паралельною схемою компенсації	1200	1200
Максимальне число трансформаторів	15	15
Електродвигуни для жалюзі	600	600

Джерело живлення KNX-20E-640 [9]

Сумісність із шиною KNX/EIB, інтегрований дросель, компактний корпус (ширина 3SU = 53,5 мм) для монтажу на DIN-рейку TS-35 / 7.5 або 15 (рис. 13.12).



Рисунок 13.12 – Джерело живлення KNX-20E-640 [9]

Основні характеристики джерела живлення:

- діапазон вхідної напруги 180...264 В (AC), 254...370 В (DC);
- частота мережі змінного струму 47...63 Гц;
- власне енергоспоживання на холостому ході < 0,5 Вт;

- 1 вихід 30 В с дроселем (для живлення шини);
- 1 вихід 30 В без дроселя;
- вихідний струм не більше 640 мА (сумарний);
- час включення 1 с, вимикання 50 мс;
- при відключенні сіткової напруги зберігає працездатність на протязі 200 мс;
- ККД до 86%;
- діапазон робочих температур -30...70 °С;
- відносна вологість 20...95%;
- ступінь захисту IP20;
- відповідність стандартам SELV, KNX, TUV, CE;
- кнопка скидання;
- захист від КЗ, перевантаження й перевищення вихідної напруги;
- захист від перенапруги категорії III згідно EN60664-1;
- охолодження за рахунок природної конвекції повітря;
- ізоляція класу I;
- світлодіодна індикація: нормальна робота/скидання/перевантаження;
- маса 215 г;
- гарантія 3 роки.

На рис. 13.13 наведена функціональна схема джерела живлення KNX-20E-640.

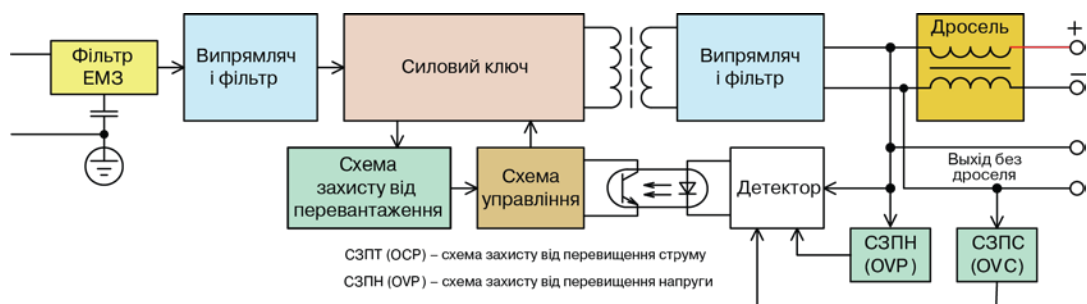


Рисунок 13.13 – Функціональна схема джерела живлення KNX-20E-640

Тому що живлення пристроїв, підключених до шини KNX, і передавання сигналів керування здійснюється по одній і тій же парі проводів, то для запобігання шунтування шини малим вихідним опір джерела живлення, у нього введений додатковий дросель. Команди керування передаються на високій частоті й опір дроселя для цих сигналів дуже великий.

Другий вихід джерела живлення може бути використаний для живлення пристроїв, не підключених до шини KNX.

Джерело живлення призначене для використання в системах освітлення, автоматизації будинків, безпеки, керування шторами й жалюзі, вентиляції й кондиціонування. На рис. 13.14 наведений приклад схеми підключення пристроїв різного призначення до шини KNX.

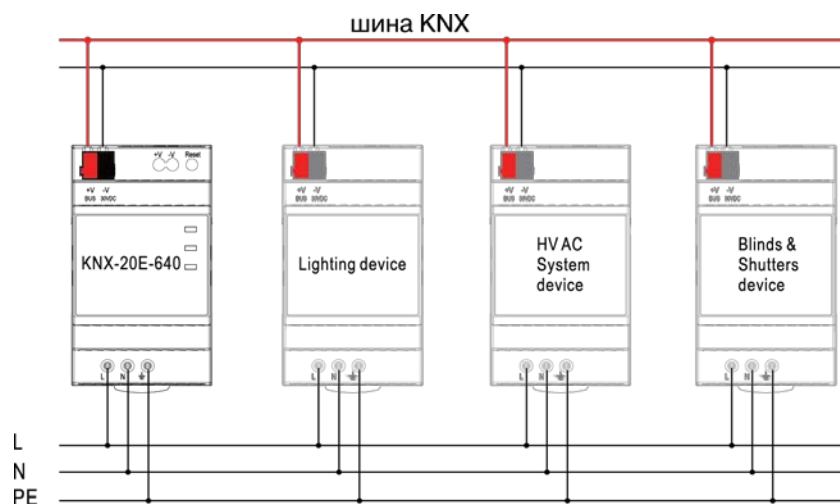


Рисунок 13.14 – Приклад схеми підключення пристроїв різного призначення до шини KNX [9]

КАА-4R4V – актуатор і димер для керування світлодіодними драйверами [10].

Модуль КАА-4R4V (рис. 13.15) призначений для керування світлодіодними драйверами, що підтримують режим регулювання яскравості (диммирования) [10].



Рисунок 13.15 – Модуль KAA-4R4V [10]

Застосування димера для керування світлодіодними джерелами живлення, з огляду на можливість організації вилученого керування, дозволяє істотно спростити роботу й поліпшити ергономіку систем освітлення, у тому числі з підтримкою різних сценаріїв. Індикація режиму роботи пристрою й поточного стану забезпечується світлодіодними індикаторами на корпусі. Релейні виходи сумісні з усіма типами світлодіодних драйверів MEAN WELL.

Компактна конструкція з модульною шириною 4SU (72 мм) робить його придатним для установки в розподільний щит на монтажних рейках 35 мм. На додаток до базової функції перемикачання, на виходах керування формується сигнал постійного струму, що змінюється в діапазоні 0...10 В для плавного регулювання яскравості світильників.

Модуль може бути використаний разом з датчиками руху в будинках для економії енергії. З появою об'єктів, що рухаються, у приміщенні модуль автоматично включить освітлення, а при довгостроково відсутності руху автоматично виключить світло.

Основні характеристики KAA-4R4V:

- 4 канали керування;
- світлодіодні індикатори для кожного каналу;
- монтаж на DIN рейку;
- живлення здійснюється по шині KNX (21...31 В);
- програмування за допомогою ПО ETS 5.0;
- ручне керування за допомогою кнопок на передній панелі;
- лінійний або логарифмічний закон зміни яскравості;

- програмування різних варіантів режимів і часу роботи;
- струм споживання не більше 11 мА;
- струм керування димером 50 мА (максимальне значення);
- максимальна відстань до об'єкта керування 100 м при перетині кабелю 1.5 мм²;
- максимальний струм на одному релейному виході 10 А;
- максимальна ємність навантаження 220 мкФ;
- діапазон робочих температур -30...45 °С;
- відносна вологість 10...95%;
- клас захисту ІІ згідно EN61140;
- захист від підвищеної напруги категорії ІІІ згідно EN60664-1;
- ступінь захисту ІР20, відповідно до EN60529;
- безпека відповідно до стандартів EN50491-3, EN60669-1, EN60669-2-1, EN60669-2-5;
- рівень електромагнітного випромінювання згідно EN50491-5-1,-2,-3, EN50090-2-2, EN60669-2-1, EN60669-2-5, EN63044-5-1,-2,-3;
- несприйнятливості до електромагнітних перешкод згідно EN50491-5-1,-2,-3, EN50090-2-2, EN60669-2-1, EN60669-2-5, EN63044-5-1,-2,-3;
- габаритні розміри 72×36×71 мм;
- маса 247 г.

Функціональна схема модуля КАА-4R4V наведена на рис. 13.16.

Прийомопередавач здійснює обмін даними з панеллю керування KNX. Мікроконтролер (МК) формує сигнали керування релейними виходами й пристроєм керування димерами. Для гальванічної розв'язки кіл керування й вихідних кіл модуля використовується ізолятор. Живлення пристрою керування димерами здійснюється за допомогою вбудованого DC/DC-перетворювача.

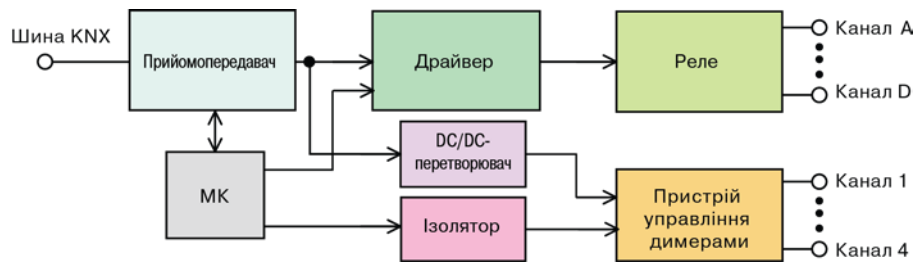


Рисунок 13.16 – Функціональна схема модуля KAA-4R4V

KDA-64 – модуль сполучення системи освітлення DALI із шиною KNX

KDA-64 (рис. 13.19) використовується для підключення цифрової системи освітлення DALI до шини KNX [11]. За допомогою цього модуля керування освітленням у приміщеннях вбудовується в систему керування будинком більшого високого рівня на базі системи KNX.



Рисунок 13.19 – Модуль KDA-64 [11]

Пристрій перетворить команди перемикання й затемнення з підключеної системи KNX у телеграми DALI і інформацію про стан із шини DALI у телеграми KNX. KDA-64 є пристроєм категорії 1 (відповідно до EN 62386-103). Це означає, що пристрій повинне використатися в сегментах DALI тільки з підключеними модулями контролю ECG. Живлення на модулі контролю подається від KDA-64. Наявність додаткового джерела живлення DALI не потрібно й не допускається.

Основні характеристики KDA-64:

- просте налаштування й установка;
- підключення до 64 драйверів DALI;

- вбудоване джерело живлення DALI (16...20 В, 250 мА);
- РК-дисплей 2×12 символів;
- керування освітленням за допомогою кнопок;
- керування освітленням через вбудований веб-сервер;
- налаштування до 16 груп освітлення DALI;
- налаштування до 16 сцен DALI;
- швидкість обміну інформацією з Ethernet 100 Мбіт/с;
- напруга живлення 100...240В (АС 50...60 Гц), 142...339 В (DC);
- струм споживання 0,1 А;
- споживана потужність не більше 7 Вт;
- діапазон робочих температур -5...45 °С;
- відносна вологість 5...93%;
- 3 роки гарантії;
- габаритні розміри 86×72×55 мм;
- маса 200 г.

Як показано на рис. 13.20 керування освітленням можна здійснювати як через шину KNX, так і по безпроводовому каналу зв'язку, використовуючи Ethernet.

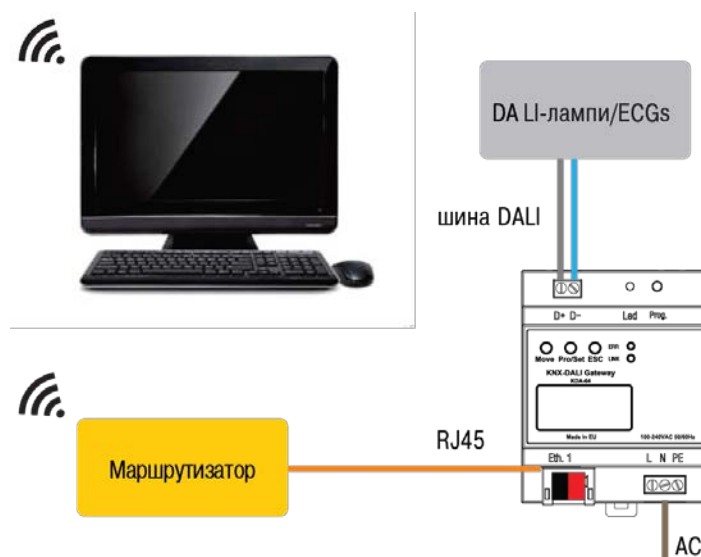


Рисунок 13.20 – Керування освітленням з використанням smart-телевізора й модуля KDA-64 [11]

KSI-01U – перетворювач інтерфейсу KNX/ USB

Модуль KSI-01U (рис. 13.21) призначений для двонаправленого перетворення інтерфейсу KNX/USB, що забезпечує гальванічно ізольований доступ до шини KNX [12]. Модуль може використовуватися для доступу до всіх пристроїв, підключеним до шини KNX, дозволяючи здійснювати керування системою KNX з персонального комп'ютера, включаючи введення в експлуатацію, адресацію, налаштування параметрів, діагностику, візуалізацію та інше.



Рисунок 13.21 – Модуль KSI-01U [12]

З'єднання між шиною даних KNX і ПК зі стандартним програмним забезпеченням, таким як ETS, ElTT і іншим програмним забезпеченням, виконується за допомогою драйвера FALCON. KSI-01U підтримує передачу "довгих" повідомлень (до 220 байт) і забезпечує роботу із програмним забезпеченням в операційних системах, не підтримуваних драйвером FALCON (наприклад, Linux).

Основні характеристики KSI-01U:

- USB тип B;
- напруга живлення 21...30 В (KNX) і 5 В (USB);
- діапазон робочих температур -5...45 °C;
- відносна вологість 20...90%;
- клас захисту IP20 відповідно до IEC60529;
- KNX-стандарт ISO/IEC 14543-3, EN50090, EN13321-1;
- відповідність стандартам безпеки EN50428 і EN62479;

- рівень електромагнітних випромінювання згідно EN50491-5, EN61000-3-3;
- несприйнятливість до електромагнітних завад згідно EN61000-4-2,3,4,5,6,11;
- середній час безвідмовної роботи 100 тис. годин;
- габаритні розміри 36×90×71 мм
- маса 60 г.

Схема підключення ПК до шини KNX наведена на рис. 13.22.

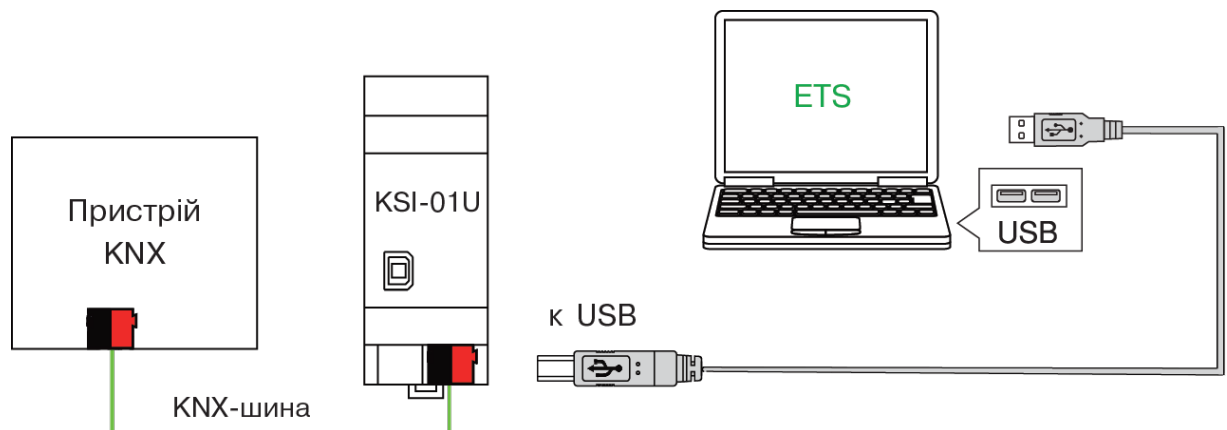


Рисунок 13.22 – Схема підключення ПК до шини KNX [12]

KNX-маршрутизатор KSR-01IP

Модуль KSR-01IP (рис. 13.23) призначений для маршрутизації й тунелювання KNXnet/IP і працює як місцевий з'єднувач IP KNX [13].



Рисунок 13.23 – Модуль KSR-01IP [13]

Живлення модуля здійснюється по шині KNX. Можливість адресації всіх шинних пристроїв у системі KNX дає можливість зробити мережні операції менш трудомісткими. Робочий стан, стан фільтрації, несправність і несправність зв'язку відображаються світлодіодами на передній панелі модуля. Пристрій ставиться до класу UPn (Universal Plug and play), і його убудоване ПЗ може бути оновлене через вбудовану веб-сторінку інтерфейсу.

KSR-01IP з'єднує Ethernet з KNX IP і KNX TP, два канали для введення в експлуатацію, адресації, налаштування параметрів, візуалізації й діагностики операцій між пристроями на шині KNX.

KSR-01IP може фільтрувати трафік відповідно до місця установки в ієрархії шинної системи по убудованих таблицях фільтрів для групового зв'язку. Фільтрація повідомлень може бути тимчасово відключена в будь-який час натисканням кнопки на пристрої. Час повернення до нормальної роботи налаштується в програмі ETS. Якщо буде потреба тимчасовий доступ до інших ліній можливий також без завантаження даних з ETS.

Основні характеристики KSR-01IP:

- напруга живлення 21...30 В (DC);
- струм споживання 20 мА;
- діапазон робочих температур -20...60 °С;
- відносна вологість 20...90%;
- клас захисту IP20 відповідно до IEC60529;
- KNX-стандарт ISO/IEC 14543-3, EN50090, EN13321-1;
- відповідність стандартам безпеки EN50428, EN62479 і EN60950-1;
- рівень електромагнітних випромінювання згідно EN50491-5, EN61000-3-3;
- несприйнятливості до електромагнітних завад згідно EN61000-4-2,3,4,5,6,11;
- середній час безвідмовної роботи 100 тис. годин;
- габаритні розміри 36×90×71 мм
- маса 70 г.

Схема з'єднання із пристроями KNX наведена на рис. 13.24.

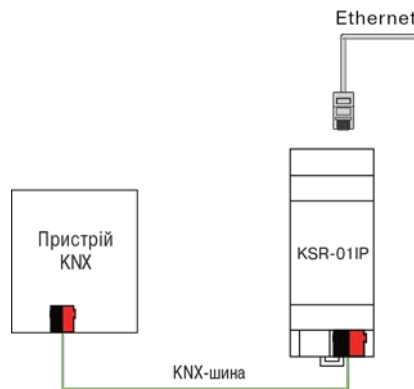


Рисунок 13.24 – Схема з'єднання модуля KSR-01IP із пристроями KNX [13]

13.3 Централізована система керування "розумним будинком"

13.3.1 Розподілена система керування

Централізованими системами називаються системи, які управляються з єдиного центру з використанням програмованого логічного контролера (ПЛК).

Розподілена система, розглянута вище, – це альтернативна розподілена шинна система. Наприклад, це KNX/EIB, HDL, Clipsal, Crestron – досить довго існуючі та поширені у всьому світі системи. Це системи, призначені саме для "розумного" будинку. Виробники обладнання для таких систем: Gira, VTicino, Jung, ABB та багато інших.

На рис. 13.25 показано систему керування освітленням "розумного будинку" з використанням шини KNX [4, 5].

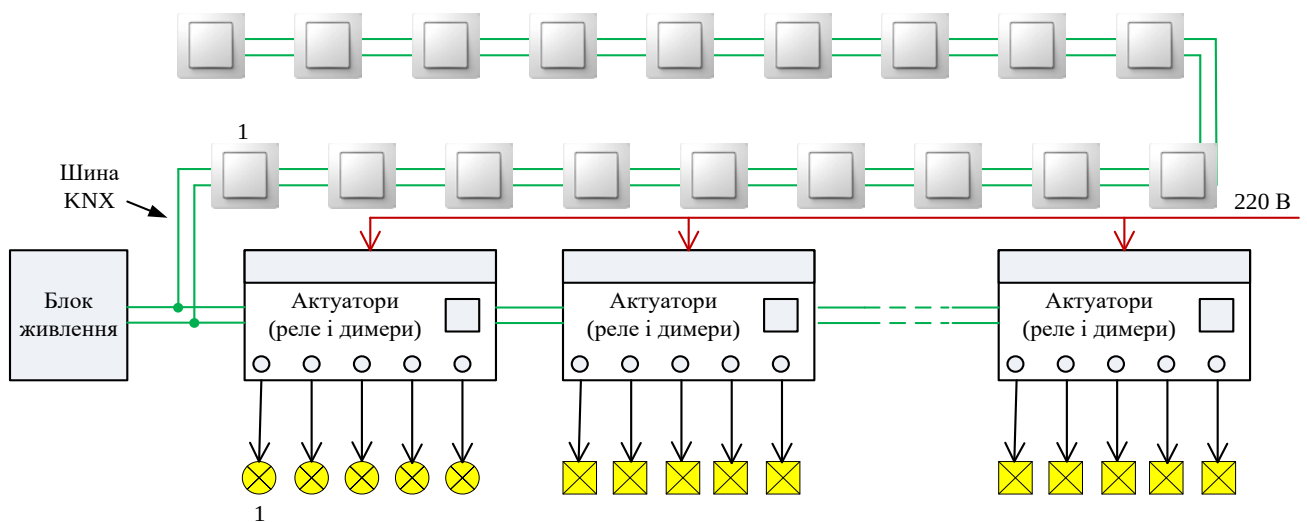


Рисунок 13.25 – Реалізація системи освітлення з використанням шини KNX

Шина KNX це кабель типу крученої пари (рекомендується спеціальний кабель для мереж KNX 2×2×0.8). До кабелю підключаються всі пристрої у кожному з яких вбудований мікроконтролер. Кожен модуль має адресу. Наприклад, ми натискаємо кнопку вимикача 1. У його процесорі запрограмовано, що з натискання на цю кнопку треба відправити в шину сигнал на включення лампочки №1. Вимикач відправляє на адресу актуатора, керуючого лампочкою №1, команду на включення. Команду отримують усі пристрої на шині, але виконує її тільки пристрій, якому вона була адресована.

Актуатор – це пристрій, який виконує конкретну дію. Наприклад, включає лампочку, змінює яскравість свічення, включає двигун керування воротами та ін.

Переваги розподіленої системи:

1. Простота розширення системи.
2. Велика кількість виробників компонентів, можна вибрати зовнішній вигляд на свій смак, всі пристрої мають узгоджені між собою інтерфейси..
3. Висока надійність системи при використанні якісних компонентів. Якщо раптом один актуатор чи вимикач відмовить, решта системи продовжуватиме працювати.

Недоліки розподіленої системи:

1. Найголовніший мінус – вартість системи. У кожному вимикачі знаходиться процесор для спілкування з шиною та передачі/прийому команд, тому коштують вони досить багато.

Вимикачі (звичайні, не сенсорні і без екрану) – від 150 євро, актуатори приблизно від 100 євро за один вихід керування, димери від 200 євро за канал, блоки живлення шини від 350 євро і так далі. Будь-які дрібниці на кшталт накладок, рамок, клавіш – дуже дорогі. Використовувати звичайні "класичні" вимикачі можна через спеціальний KNX-перехідник, який коштуватиме не менше спеціального KNX-вимикача. Наведено ціни на обладнання компанії Jung. Є виробники з меншою вартістю обладнання, наприклад HDL або Zennio.

2. Датчики всіх типів також дуже дорогі. Датчик руху – від 200 євро, температури – від 300 євро, метеостанція – 500 євро. Підключити стандартні аналогові датчики температури або руху можна, але потрібні модулі введення аналогових сигналів.

3. Для програмування системи необхідно придбати досить дороге програмне забезпечення ETS. Окрім того доведеться або кожного разу викликати спеціалістів для налаштування системи, або самому навчитись роботі з програмою ETS.

13.3.1 Централізована система керування

У централізованій системі всім керує центральний контролер (ПЛК), дроти від усіх підключених пристроїв йдуть до контролера або до його модулів розширення (рис. 13.26).

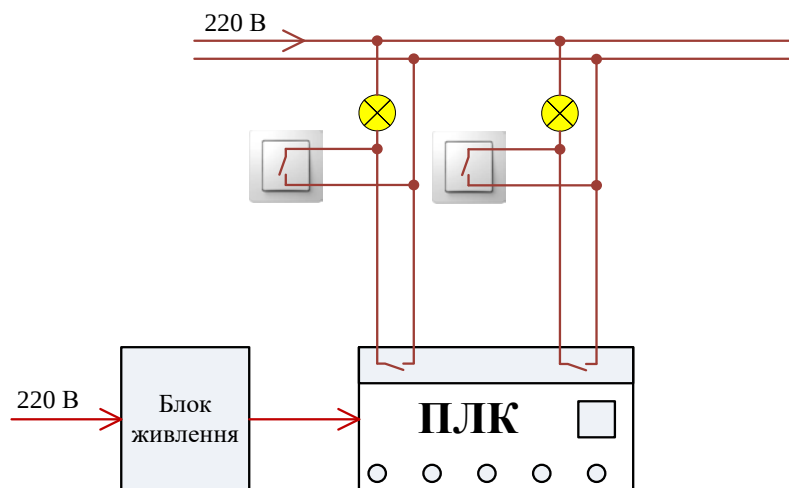


Рисунок 13.26 – Керування освітленням в централізованій системі керування

Система керування на рис. 13.16 передбачає програмне включення освітлювальних приладів командами ПЛК або ручне увімкнення світильників.

Однак можна побудувати систему, в якій сигнали від вимикачів надходитимуть на входи керування ПЛК і включатимуть світильники або за програмою, або від сигналу вимикача (рис. 13.27).

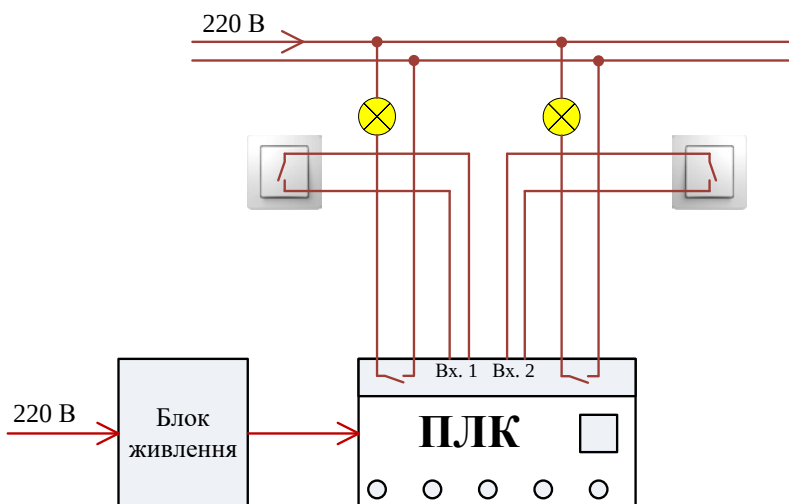


Рисунок 13.27 – Керування освітленням в централізованій системі керування тільки командами ПЛК

Від вимикачів прокладаються слаботочні кабелі в шафу, в якій змонтовані ПЛК, джерело живлення та модулі розширення (зазвичай це кабель FTP 5

категорії), а від лампочок, вентиляторів, розеток, сервоприводів – силові кабелі в шафу. Центральний ПЛК через реле чи димери керує електричними приладами.

Датчики всіх типів підключаються до ПЛК. Від кожного датчика окремий провід.

Переваги централізованої системи:

1. Можливість використовувати будь-які вимикачі, будь-які датчики температури, руху та інших параметрів. Наслідок – значне зниження вартості системи та свобода вибору компонентів.

2. При навичках роботи з ПЛК (програмування) користувач може самостійно все налаштовувати. Не потрібно купувати програмне забезпечення. Ви не залежите від інтегратора, програміста ПЛК знайти простіше, ніж налагоджувача KNX.

3. Майже необмежена інтеграція з різним обладнанням. Можна навіть використовувати гарні настінні панелі KNX за бажанням.

4. ПЛК забезпечує високу надійність системи при належному захисті від замикань та стрибків напруги в мережі, а цей захист забезпечити нескладно.

Недоліки централізованої системи:

Якщо контролер вийде з ладу, то і система в цілому виходить з ладу. Це часто повторюють прихильники шинних систем.

Так як від кожного пристрою керування йде свій кабель у шафу керування, то кабелю буде набагато більше, ніж у шинній системі. Але кабель FTP має невисоку вартість, порівняно з вартістю шинного кабелю для систем KNX. І під час розведення кабелю для централізованої системи ми отримуємо універсальний варіант. Можна за необхідності створити майже класичну систему керування освітленням.

На базі ПЛК можна побудувати таку "центрально-розподілену" систему, в якій буде кілька контролерів в мережі Ethernet, що дозволяє розносити модулі розширення по великій площі. Можна об'єднувати кілька контролерів в одній мережі Ethernet, якщо це дозволяє програмне забезпечення.

13.3.3 Функціональні можливості ПЛК

Програмований логічний контролер це пристрій алгоритм роботи якого програмується користувачем. ПЛК вирізняються дуже високою надійністю. Розглянемо як приклад ПЛК програмований контролер ПЛК200-01-CS. Структура ПЛК200-01-CS наведена на рис. 13.28 [13].

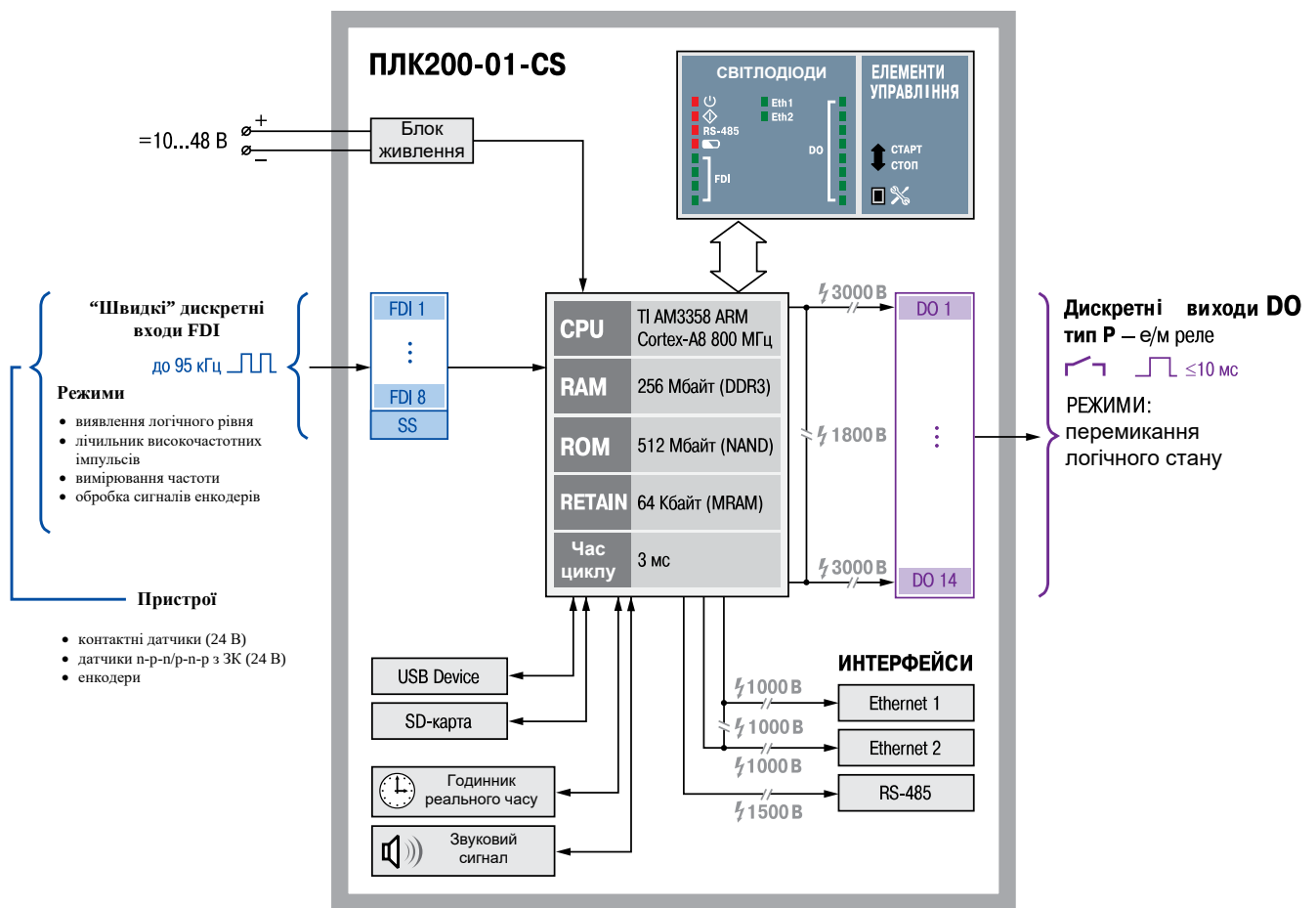


Рисунок 13.28 – Структура ПЛК200-01-CS [13]

У контролера є входи та виходи. Входи для підключення до контролера різних типів датчиків. Виходи змінюють свій стан згідно з програмою контролера. Входи та виходи можуть бути дискретними або аналоговими.

Дискретний вхід – фіксує наявність, або відсутність сигналу. Тобто логічний 0 або 1. Наприклад, датчик руху при спрацьовуванні подає сигнал на дискретний вхід контролера. Контролер подає на виконавчий пристрій дискретний сигнал

увімкнутися або не вмикатися. Якщо дискретні виходи це контакти реле, можна увімкнути або вимкнути пристрій, наприклад, лампочку.

Аналоговий вхід – це вхід, здатний приймати сигнали різного рівня та перетворювати їх у цифровий код. Наприклад, аналоговий сигнал може утворювати напівпровідниковий датчик температури. Аналоговий вихід може формувати сигнали керування різного рівня. Наприклад, для керування димером.

ПЛК має обмежену кількість входів і виходів (досить для багатьох завдань). Якщо їх недостатньо, можна підключати додаткові модулі за інтерфейсом RS-485. Однак при підключенні додаткових модулів реакція системи уповільнюється, оскільки потрібен час на обробку сигналів RS-485.

При кількості керованих електроприладів до 30 ПЛК Овен буде гарним рішенням, при більшому – можна подумати про перехід на ПЛК Beckhoff або Siemens. Beckhoff (Німеччина) – професійні промислові контролери з модулями розширення, які підключаються по внутрішній шині K-Bus та забезпечує високу швидкість передавання даних.

Система є універсальною. За бажання можна буде поміняти центральний контролер на іншу модель, всі датчики та виконавчі пристрої будуть функціонувати. Навіть саму програму, швидше за все, буде перенесено на новий контролер без особливого доопрацювання.

При такій системі керування відсутня прив'язка до жодного виробника. Всі елементи системи можуть бути такими, якими захочеться, аби вони формували універсальний сигнал відомого промислового протоколу, "сухий контакт" або 0-10 мА, 4-20мА. Це можуть бути будь-які датчики, вимикачі, приводи та інші пристрої.

"Сухий контакт" – сленговий термін в галузі промислової автоматики та сигналізації, що позначає дискретний вихідний сигнал приладу. Слово "сухий" означає, що на клемі сухого контакту немає ніякої напруги, якщо клему не підключено до іншого обладнання.

13.3.4 Керування системою на ПЛК

Розрізняють такі способи керування системою автоматики на промисловому контролері:

1. Якщо ми хочемо щоб всі основні функції (світло, штори, вентиляція та ін.) мати можливість керуватися зі звичайних вимикачів, а не з додатків або з панелей, то через входи контролера. Натискаємо на вимикач, контролер сприймає сигнал на своєму дискретному вході та виконує операції відповідно до своєї програми. Вмикає світло, відкриває штору, ставить на охорону або запускає інший сценарій.

2. Через інтерфейси RS-485, RS-232, KNX та інші. Наприклад, ми можемо використовувати настінну сенсорну панель, що працює за RS-485 або ModbusTCP (EasyHomeTPD). Або GSM модем по RS-232 повідомляє про те, що надійшло керуюче SMS-повідомлення.

3. Через Ethernet, тобто комп'ютерну мережу. Робота йде за протоколом ModBusTCP, контролер має певну IP адресу в локальній мережі. Можливий доступ до контролера через інтернет за відповідних налаштувань роутера. У контролерів Beckhoff, Овен, EasyHomePLC та ще багатьох немає web-інтерфейсу, лише передача команд по ModBusTCP. У контролерів WirenBoard та RazumDom є web-інтерфейс для налаштування. У будь-якому випадку, контролер може керуватися з програми на будь-якій системі, яка буде відправляти команди та запити на IP адресу та порт контролера. Безкоштовних програм величезна кількість, платні професійні програми EasyHome (орієнтовану саме під ПЛК, максимально простий у налаштуванні інтерфейсу) та Iridium Mobile (працює з великою кількістю систем, складніше у налаштуванні інтерфейсу).

Контрольні питання

1. Що мається на увазі під терміном "розумний" будинок?
2. Які канали зв'язку використовують в системі "розумного" будинку?
3. Для чого призначена шина KNX?

4. Яку кількість пристроїв можна підключити до шини KNX?
5. Для чого призначені димери в системах освітлення?
6. Яка максимальна довжина лінії зв'язку в системі KNX?
7. Чи можна здійснювати зв'язок по шині KNX на відстані більше ніж 350 м? Якщо так, то що потрібно зробити для цього?
8. Які особливості джерел живлення для пристроїв системи KNX?
9. Як передаються повідомлення та живлення по шині KNX?
10. Як здійснюється живлення виконавчих пристроїв (двигунів, кондиціонерів та інші) при використанні шини KNX?
11. В чому відмінність централізованої системи керування від розподіленої?
12. Вартість якої системи – централізованої чи розподіленої буде вищою?

Перелік посилань

1. Загальна інформація про KNX. Url: <http://knx.com.ua/o-knx/technologija/books> (дата звернення: 3.10.2024).
2. European Installation Bus. Url: http://www.fact-index.com/e/eu/european_installation_bus.html (дата звернення: 13.10.2024).
3. ISO/IEC 14543-3-3:2007. Url: <https://eos.isolutions.iso.org/obp/ui#iso:std:iso-iec:14543:-3-3:ed-1:v1:en> (дата звернення: 13.10.2024).
4. A brief introduction to KNX. Url: <https://www.knx.org/knx-en/for-professionals/What-is-KNX/A-brief-introduction/index.php> (дата звернення: 13.10.2024).
5. KNX Basics. Url: https://knx.fi/doc/esitteet/KNX-Basics_en.pdf (дата звернення: 13.10.2024).
6. Create your digital smart home with KNX Virtual. Url: <https://www.knx.org/knx-en/for-professionals/get-started/knx-virtual/index.php> (дата звернення: 13.10.2024).
7. KAA-8R/KAA-8R-S Universal Actuator 8-fold, 230V AC, 16A. Url: <https://www.meanwell.com/Upload/PDF/KAA-8R-E.pdf> (дата звернення: 13.10.2024).

8. KNX-20E-640. Url: <https://www.meanwell-web.com/en-gb/ac-dc-knx-eib-din-rail-power-supply-with-knx--20e--640> (дата звернення: 13.10.2024).
9. KAA-4R4V-S Dimming Actuator Instruction Manual. Url: <https://www.meanwell.com/Upload/PDF/KAA-4R4V-E.pdf> (дата звернення: 13.10.2024).
10. KDA-64~KNX/DALI Gateway. Url: <https://www.meanwell.com/newsInfo.aspx?c=1&i=497> (дата звернення: 13.10.2024).
11. KSI-01U KNX-USB Interface Instruction manual. Url: <https://www.meanwell.com/Upload/PDF/KSI-01U-E.pdf> (дата звернення: 13.10.2024).
12. KSR-01IP. Url: <https://www.meanwell.com/Upload/PDF/KSR-01IP-E.PDF> (дата звернення: 13.10.2024).
13. ПЛК200. Контролер для малих і середніх систем автоматизації. Url: <https://aqteck.com.ua/ua/programovani-logichni-kontrolery/plk200-programovanyj-logichnyj-kontroler> (дата звернення: 13.10.2024).

14 СТРУКТУРОВАНІ КАБЕЛЬНІ СИСТЕМИ

14.1 Структура СКС

14.1.1 Топологія СКС

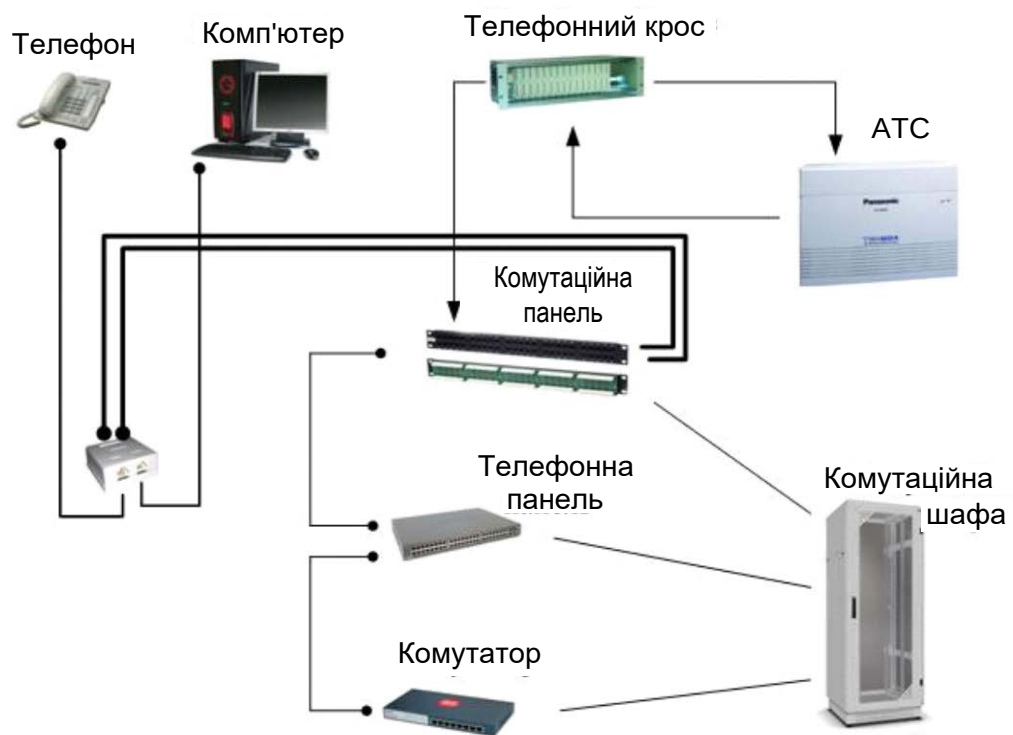
Структурована кабельна мережа – це універсальна телекомунікаційна інфраструктура будівлі чи комплексу будівель, що забезпечує передачу сигналів всіх типів, інформаційні системи (також голосові, відео), охоронні, пожежні, тощо [1]. Це сучасне, високошвидкісне, багатофункціональне мережеве рішення, що відноситься до капітальних комунікаційних утворень, та має довгостроковий час функціонування.

СКС це універсальна система, з можливістю масштабування та модернізації, на існуючих кабельних лініях для всіх потенційних користувачів на протязі всього часу експлуатації будівлі, незалежно від активного обладнання. Основними елементами таких мереж є мідний кабель типу “вита пара” cat. 5e, 6, 6A, 7, а також оптоволоконний кабель.

Структурована кабельна мережа – це також засіб оптимізації ІТ-інфраструктури. Оптимальним рішенням при побудові слугує модульна, ієрархічна структура, що не матиме прив’язки до конкретних мережевих технологій. Компоненти СКС – це обладнання передових технологій, які в цілому утворюють комп’ютерні системи, системи цифрової телефонії, системи сигналізації, контролю доступу та обліку часу, системи відеоспостереження, системи протипожежної охорони та сповіщення, а також всі види диспетчеризації на слабострумних лініях зв’язку.

В основу будь-якої повномасштабної структурованої кабельної системи покладена деревоподібна топологія, що іноді називають також структурою ієрархічної зірки [2]. Функції вузлів структури виконує комутаційне устаткування різного виду, що має два основні різновиди: індивідуальні інформаційні розетки й панелі різних типів, що утворюють групове комутаційне поле, з яким працює обслуговуючий персонал (рис. 14.1). Комутаційне устаткування з’єднується між собою електричними й волоконно-оптичними кабелями різних видів [2].

Всі кабелі, що входять у технічні приміщення, обов'язково заводяться на згадані вище комутаційні панелі [3], на яких за допомогою шнурів здійснюються всі підключення й перемикання в процесі поточної експлуатації кабельної системи. Стандарти дозволяють також організацію резервних трактів передачі сигналів. Все це в сполученні з використаною деревоподібною топологією в частині, що стосується СКС, забезпечує гнучкість і надійність, а також можливість легкої переконфігурації й адаптації кабельної системи під конкретний об'єкт.



а)



б)

Рисунок 14.1 – Структура СКС (а) та комутаційна панель (б) [3]

14.1.2 Комутація в СКС

Інсталяція кабельних мереж великих та малих масштабів була б неможливою без з'єднувальних елементів. Крім того, для організації серйозної СКС просто необхідні комутаційні конструкції та обладнання – вони є обов'язковою структурною ланкою.

Майже для будь-якої СКС характерно те, що комутація, на відміну від електронних АТС і мережевого комп'ютерного обладнання, завжди виконується вручну комутаційними кабелями, і перемичками, що істотно підвищує надійність, і незалежність системи від електроживлення мережі.

Для комутації в СКС застосовується таке монтажне устаткування: монтажна шафа (стійка), комутаційні панелі, комутаційні кабелі, розетки та адаптери, кабельні коробки (рис. 14.2).



Рисунок 14.2 – Монтажне устаткування [4, 5]

Кабельними коробами є порожнисті закриті жолоби різних перетинів, обов'язково мають кришку, що від'єднується або відкидається і призначені для монтажу на будь-якій плоскій капітальній або декоративній вертикальній поверхні. Призначені для захисту від механічних пошкоджень, від попадання бризок води і інших рідин, для забезпечення високих естетичних характеристик.

Телекомунікаційні шафи призначені для установки мережевого і комунікаційного, кросового, активного та пасивного обладнання [2]. Комутаційні шафи – одні з найбільш часто застосовуваних сьогодні конструкцій (якщо мова йде про масштабну СКС), що встановлюються в серверних, в лабораторіях, або на

полігонах випробувань. Дані елементи СКС відрізняються найбільшим ступенем надійності – в них ховають проводку тоді, коли потрібно захистити кабелі від вологи, вогню, випадкових фізичних пошкоджень, агресивних середовищ.

Стійки – без них будівництво СКС також було б неможливим – від комутаційних шаф вони відрізняються своєю відкритістю. У них немає дверцят (рис. 14.3), тому дані конструкції монтуються в приміщеннях з середовищем, сприятливим для встановлення на їх полицях обладнання. Потрібно сказати, що стійки таки можуть інстальоватися в лабораторіях з шкідливими для кабелів умовами, але тільки в тих випадках, коли шафи поставити неможливо.

Полки – конструктивні елементи, на які безпосередньо встановлюють працююче обладнання. Вони можуть бути як висувними, так і стаціонарними, з різною шириною (найчастіше використовуються моделі 15, 17, 19 дюймів). Комутаційні полки встановлюються як в шафи, так і в стійки. Тримачі – з'єднувальні елементи СКС, призначені для фіксації проводки. Їх важливість важко переоцінити: коли проводиться монтаж кабельних мереж, більшість комунікаційних ліній потрібно закріплювати, щоб вони не хиталися. Тримачі якраз допомагають це зробити – без них підключення всіх проводів того ж шафи було б далеко не таким раціональним.



Рисунок 14.3 – Комутаційні стійки [4]

Організатори – найпростіші, але при цьому важливі комутаційні елементи. По суті, кожна така конструкція є кільце, що монтується в стіну, або на стелю. У нього і протягується кабель – практика показує, якщо встановлено достатню кількість утримувачів (на відстані 0,4-0,5 м), комунікаційна лінія зафіксована більш ніж добре, без будь-яких провисань. Всі ці комутаційні конструкції та елементи СКС доводять свою актуальність щодня – вони є тим базисом, на основі якого проводиться з'єднання і будівництво СКС.

Комутаційна панель (крос-панель або патч-панель) – одна зі складових частин СКС. Представляє собою панель із великою кількістю сполучених роз'єднувачів, розташованих на лицьовій стороні панелі. На тильній стороні панелі знаходяться контакти, призначені для фіксованого з'єднання з кабелями. Комутаційна панель відноситься до пасивного мережевого устаткування. Існує два типові способи використання комутаційних панелей. У першому випадку, комутаційна панель використовується як точка, комутації між портами активного мережевого устаткування АМУ (АМУ – активне мережне устаткування) і портами робочих місць, через кабель горизонтальної підсистеми СКС. Комутація здійснюється комутаційними шнурами від панелі до портів АСО. У другому випадку, так зване подвійне представлення порту, комутаційні панелі використовуються попарно, одна з панелей представляє порти АСО, а друга – порти робочих місць. Комутація здійснюється комутаційними шнурами між панелями [5].

1.1.3 Технічні приміщення СКС

Технічні приміщення необхідні для побудови СКС і інформаційної системи в цілому. У загальному випадку вони діляться на **апаратні і кросові**.

Апаратною надалі називається технічне приміщення, у якому поряд із груповим комутаційним устаткуванням СКС розташовується мережне устаткування колективного користування масштабу підприємства (сервери, комутатори). Апаратні обладнуються фальшивою стелею, системами

пожежогасіння, кондиціонування й контролю доступу. Рівень установлюваних в апаратній різних пристроїв і систем інженерного забезпечення повинен відповідати рівню комп'ютерного й телекомунікаційного устаткування, що встановлено в апаратній (рис. 14.4).



Рисунок 14.4 – Обладнання апаратної СКС [6]

Кросова являє собою приміщення, у якому розміщується комутаційне устаткування СКС, мережеве й інше допоміжне устаткування, що обслуговує найчастіше обмежену групу користувачів (рис. 14.5). При цьому рівень оснащення кросової, устаткуванням інженерного забезпечення її функціонування в цілому є більше низьким у порівнянні з апаратною.

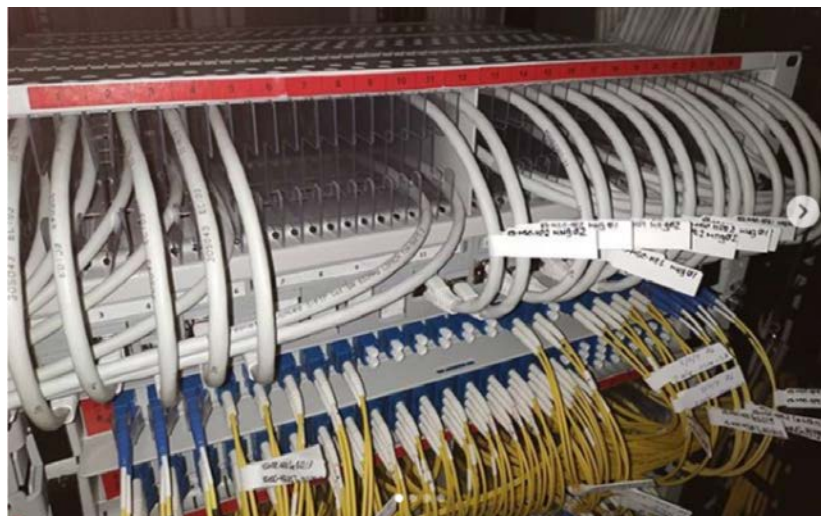


Рисунок 14.5 – Монтаж патч-панелей у кросовій [7]

Апаратна може бути сполученою із кросовою будинку (КБ). У цьому випадку його мережне устаткування може підключатися безпосередньо до комутаційного устаткування СКС. Якщо апаратна розташована окремо, то її мережне устаткування підключається до локального розташованого комутаційного устаткування або до звичайних інформаційних розеток, аналогічним розеткам робочих місць. У кросову зовнішніх магістралей (КЗМ) сходяться кабелі зовнішньої магістралі, що підключають до неї окремі КБ. У КБ заводяться внутрішні магістральні кабелі, що підключають до них кросові поверхів (КП).

До КП, у свою чергу, горизонтальними кабелями підключені розеткові модулі інформаційних розеток робочих місць. Як додаткові зв'язки, що збільшують гнучкість і живучість системи, допускається прокладка зовнішніх магістральних кабелів між КБ і внутрішніх магістральних кабелів – між КП. Прокладки інформаційної кабельної мережі, безперебійна робота якої є однією з умов успішної діяльності. На рис. 14.6 [8] наведений приклад структури СКС із прив'язкою до будинків.

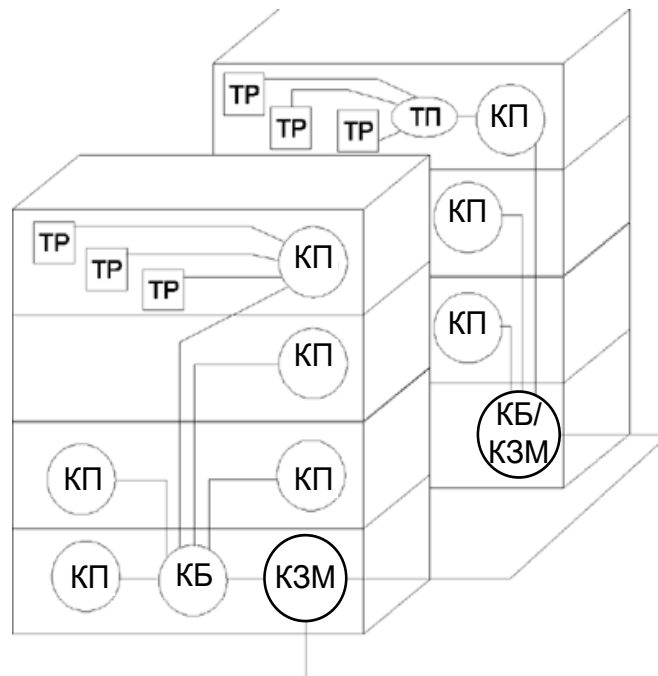


Рисунок 14.6 – Приклад структури СКС із прив'язкою до будинків [8]

На рис. 14.6 прийняті наступні позначення:

- TR – телекомунікаційна розетка;

- КП – кросова поверху;
- КБ – кросова будинку;
- КЗМ – кросова зовнішніх магістралей.

14.1.4 Підсистеми СКС

У загальному випадку СКС містить у собі три підсистеми:

1. **Підсистема зовнішніх магістралей** складається із зовнішніх магістральних кабелів між КЗМ і КБ, комутаційного устаткування в КЗМ і КБ, до якого підключаються зовнішні магістральні кабелі, і комутаційних шнурів, і/або перемичок у КЗМ. Підсистема зовнішніх магістралей є тією основою, що з'єднує в єдину мережу зв'язку, окремо розташовані на одній території будинки. На практиці ця підсистема досить часто має фізичну кільцеву топологію, що додатково забезпечує збільшення надійності за рахунок наявності резервних кабельних трас. Із цих же міркувань підсистема зовнішніх магістралей іноді реалізується по подвійній кільцевій топології. Якщо СКС встановлюється автономно тільки в одному будинку, то підсистема зовнішніх магістралей відсутня.

2. **Підсистема внутрішніх магістралей**, має назву в деяких СКС вертикальної або вторинної підсистеми, містить прокладені між КБ, і КП внутрішні магістральні кабелі, підключене до них комутаційне устаткування в КБ і КП, а також частину комутаційних шнурів і/або перемичок у КБ. Кабелі розглянутої підсистеми фактично зв'язують між собою окремі поверхи будинку і/або просторово рознесені приміщення в межах одного будинку. У даному випадку СКС обслуговує один поверх, тому підсистема внутрішніх магістралей відсутня.

3. **Горизонтальна підсистема** утворена, горизонтальними кабелями між КП і розетковими модулями інформаційних розеток робочих місць, самими інформаційними розетками, а також комутаційним устаткуванням у КП, до якого підключаються горизонтальні кабелі [8]. До складу горизонтальної підсистеми входить більша частина комутаційних шнурів і перемичок у КП. При побудові горизонтальної проводки допускається використання однієї точки переходу на

тракт, у якій відбувається зміна типу кабелю (наприклад, перехід на плоский кабель для прокладки під килимовим покриттям з еквівалентними характеристиками).

На рис. 14.7 наведена структура підсистем СКС.

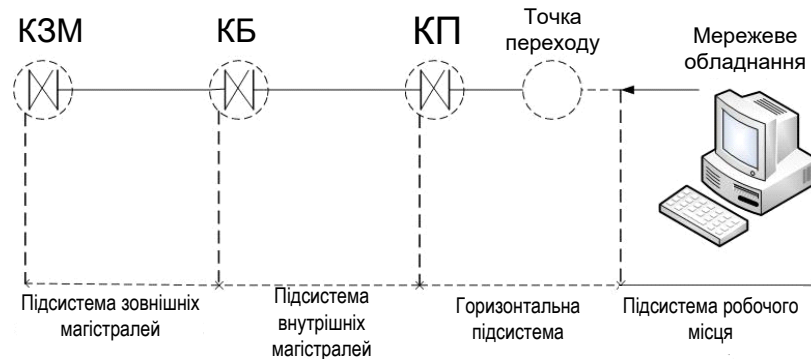


Рисунок 14.7 – Структура підсистем СКС [8]

Розподіл СКС на окремі підсистеми застосовується незалежно від виду або форми реалізації мережі, тобто воно принципово буде однаковим. У загальному випадку СКС відповідно до діючих редакцій міжнародних нормативно-технічних документів містить у собі наступні вісім компонентів:

1. Лінійно-кабельне устаткування підсистеми зовнішніх магістралей.
2. Комутаційне устаткування підсистеми зовнішніх магістралей.
3. Лінійно-кабельне устаткування підсистеми внутрішніх магістралей.
4. Комутаційне устаткування підсистеми внутрішніх магістралей.
5. Лінійно-кабельне устаткування горизонтальної підсистеми.
6. Комутаційне устаткування горизонтальної підсистеми.
7. Точки переходу.
8. Інформаційні розетки.

У переважній більшості випадків підключення до СКС мережного устаткування й комутація окремих портів кабельної системи здійснюється за допомогою шнурових виробів найрізноманітніших видів. Застосування різних перемикачів для рішення завдань комутації, незважаючи на їх очевидні технічні експлуатаційні переваги, не одержало широкого поширення через істотно менші

функціональні можливості. У деяких ситуаціях, обумовлених головним чином, конструктивними особливостями портів активних мережних приладів, крім шнура може знадобитися адаптер, що забезпечує узгодження сигнальних і механічних параметрів оптичних, або електричних інтерфейсів СКС, і мережного устаткування.

14.1.5 Принципи адміністрування СКС

Принцип адміністрування або керування СКС цілком, і повністю визначаються її структурою. Розрізняють одноточкове та багатоточкове адміністрування. Під багатоточковим адмініструванням розуміють керування СКС, що побудоване по класичній архітектурі ієрархічної зірки, тобто містить у собі магістральну підсистему, хоча б одного рівня. Основною ознакою цього варіанту є необхідність використання перемикачів мінімум двох шнурів (або елементів, що їх замінюють) у загальному випадку зміни конфігурації. Використання даного принципу гарантує найбільшу гнучкість керування й більш широкі можливості адаптації СКС для підтримки нових додатків [2, 9].

Архітектура одноточкового адміністрування застосовується в тих ситуаціях, коли потрібно максимально спростити керування кабельною системою. Її основною ознакою є пряме з'єднання всіх інформаційних розеток робочих місць із комутаційним устаткуванням у єдиному технічному приміщенні. Принципово подібна архітектура може використатися тільки для СКС, установлених в одному будинку і не маючих магістральної підсистеми. З викладеного ясно, що структури розглянутого різновиду характерні в першу чергу для СКС із невеликою кількістю портів.

14.2 Класи і категорії кабелів, та їх зв'язок з довжинами кабельних трас

14.2.1 Кабелі СКС

Одним з ефективних способів підвищення техніко-економічної ефективності кабельних систем офісних будинків є мінімізація типів кабелів, застосовуваних для їхньої побудови. У СКС відповідно до міжнародного стандарту ISO/IEC 11801 допускається використання тільки симетричних електричних кабелів на основі витой пари із хвильовим опором 100, 120 і 150 Ом в екранованому й неекранованому виконанні, або одномодових і багатомодових оптичних кабелів [10, 11].

Електричні кабелі із витих пар використовуються в першу чергу для створення горизонтальної проводки. По ним передаються як телефонні сигнали й низькошвидкісна дискретна інформація, так і дані високошвидкісних додатків.

Застосування оптичних рішень у горизонтальній підсистемі в цей час зустрічається досить рідко, хоча їхня частка росте дуже швидкими темпами. У підсистемі внутрішніх магістралей електричні і оптичні кабелі застосовуються однаково часто, причому електричні кабелі призначені для передачі, головним чином, телефонних сигналів, і даних із тактовими частотами до 1 МГц, тоді як оптичні кабелі забезпечують передачу цифрової інформації високошвидкісних додатків. На зовнішніх магістралях оптичні кабелі відіграють домінуючу роль. Для переходу з електричного кабелю на оптичний у процесі передачі даних зі швидкістю 100 Мбіт/с і вище в технічних приміщеннях встановлюється відповідне мережне устаткування (рис. 14.8). Такі пристрої звичайно обслуговують груповий пристрій (звичайний або комутуючий концентратор системи передачі даних, виносний модуль АТС, контролер інженерної системи будинку і т.д.).

Пряме використання волоконно-оптичного кабелю для передачі телефонних сигналів і низькошвидкісних даних етапу розвитку техніки є економічно недоцільним, і застосовується вкрай рідко – у тих ситуаціях, коли інші рішення

неможливі або ж висуваються особливі вимоги відносно захисту інформації від несанкціонованого доступу.

Тому для поліпшення техніко-економічної ефективності мережі в цілому, звичайно, процес перетворення низько швидкісного електричного сигналу в оптичний сполучається з мультиплексуванням [12].

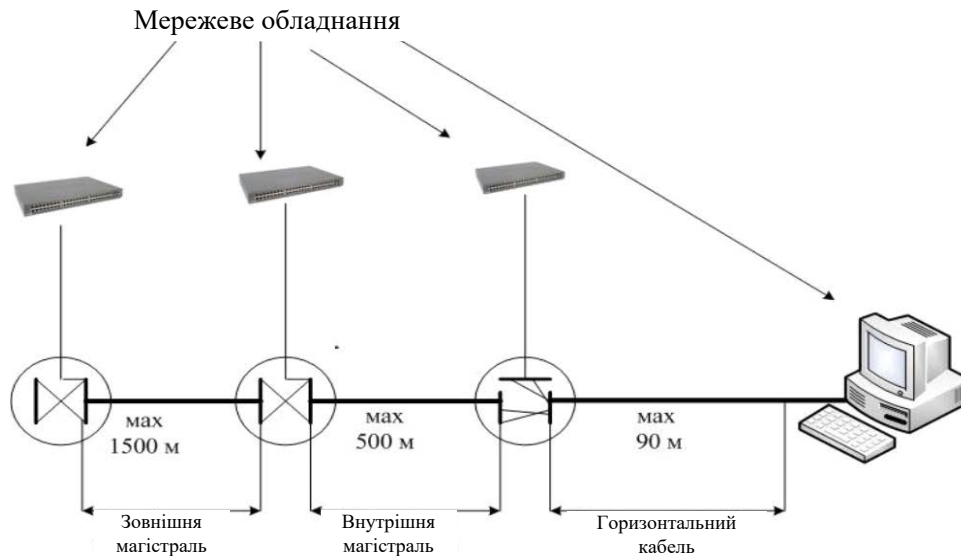


Рисунок 14.8 – Розташування та довжина кабелів при побудові горизонтальної підсистеми СКС [12]

Для побудови горизонтальної підсистеми стандартами допускається застосування екранованого і неекранованого кабелю. Екранований симетричний кабель потенційно має кращі електричні характеристики в порівнянні з неекранованим. Однак кабельні траси на основі його є дуже критичними до якості виконання монтажу й заземлення, а самі кабелі мають помітно більшу вартість і гірші масогабаритні показники.

Стандарти дозволяють будувати СКС на електричних кабелях із витих пар із хвильовим опором 100, 120 і 150 Ом. При цьому два останні різновиди кабелів часто мають помітно кращі характеристики. Однак, у силу цілого ряду причин технічного й економічного плану, вони не мають широкого поширення в нашій країні.

Багатомодові волоконно-оптичні кабелі використовують в основному як основу підсистеми внутрішніх магістралей. Одномодові волоконно-оптичні кабелі рекомендуються застосовувати тільки для побудови довгих зовнішніх магістралей.

Підпільні канали являють собою спеціалізовані металеві або пластикові конструкції переважно із прямокутним поперечним перерізом. Канали встановлюються в структурі міжповерхового перекриття перед заливанням підлоги з переважною орієнтацією паралельно або перпендикулярно капітальними стінами, і перегородками будинку. Їх, застосування дозволяє одержати ефективний захист кабелів від механічних ушкоджень, зменшити рівень зовнішніх наведень і електромагнітного випромінювання. Вони виготовлені з металу, що забезпечує прихованість прокладки. Як недоліки такого рішення відзначимо високу вартість і досить більшу тривалість реалізації, наявність вимоги по завершенню монтажу до закінчення будівельно-монтажних робіт ще й необхідність застосування спеціальних напільних, або підпільних коробок для доступу до електричних, і інформаційних розеток. Одночасний пристрій підпільних каналів супроводжується помітним збільшенням сумарної маси будівельних конструкцій.

14.2.2 Класи додатків, категорії кабелів і роз'єднувачів СКС

Діюча редакція стандарту ISO/IEC 11801 підрозділяє всі види додатків, які можуть обмінюватися даними по витій парі, на 4 класи – А, В, С, D (табл. 14.1). До додатків оптичного класу ставляться ті з них, які використовують як середовище передачі сигналу оптичний кабель. Для таких додатків на момент прийняття стандарту ширина, смуги пропускання не є обмежуючим чинником.

У вересні 1997 року ІЕС почала роботу зі стандартизації двох нових класів додатків Е і F, а також компонентів СКС для категорій 6 і 7.

CAT1 (смуга частот 100 Гц) – телефонний кабель, лише одна пара. Використовується тільки для передачі голосу та даних при допомозі модему.

CAT2 (сму́га частот 1 МГц) – стандартний тип кабелю, 2 пари провідників, підтримує передачу даних на швидкості до 4 Мбіт/с, використовувався в мережах token ring і ARCNet. Зараз зустрічається в телефонних мережах.

CAT3 (сму́га частот 16 МГц) – 4-парний кабель, використовується при побудові мереж 10BASE-T і token ring, підтримує швидкість передачі даних до 100 Мбіт/с. На відміну від двох попередніх відповідає вимогам стандарту IEEE 802.3. Також до цього часу зустрічається в телефонних мережах.

CAT4 (сму́га частот 20 МГц) – кабель складається з 4 скручених пар, використовується в мережах token ring, 10BASE-T, 100BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с по одній парі. Зараз не використовується.

CAT5 (сму́га частот 100 МГц) – 4-парний кабель, використовується при побудові локальних мереж 10BASE-TX підтримує швидкість передачі даних до 100 Мбіт/с при використуванні 2 пар. При прокладці нових мереж використовують покращений кабель CAT5e (сму́га частот 125 МГц), це і є, що зазвичай називають "вита пара", завдяки високій швидкості передавання, до 100 Мбіт/с при використанні 2 пар, і до 1000 Мбіт/с при використанні 4 пар, є **найбільш розповсюдженим мережевим носієм**, що використовується в комп'ютерних мережах до цього часу.

CAT6 (сму́га частот 250 МГц) – використовується в мережах Fast Ethernet і Gigabit Ethernet, складається з 4 пар провідників, і здатен передавати дані на швидкості 1000 Мбіт/с. Доданий у стандарт у червні 2002 року. Існує категорія CAT6a, у якій збільшена частота пропускнуго сигналу до 500 МГц. По даним IEEE, 70% встановлених мереж в 2004 році, використовували кабель категорії CAT6.

CAT7 – специфікація на даний тип кабелю поки, що не затверджена, швидкість даних до 100 Гбіт/с, частота пропускнуго сигналу до 600-700 МГц. Кабель цієї категорії екранований.

Таблиця 14.1 – Класи додатків по ISO/IEC 11801 [13]

Клас лінії	Визначення
A	Телефонні канали й низькочастотний обмін даними. Максимальна частота сигналу 100 Гц.
B	Додатки із середньою швидкістю обміну. Максимальна частота 1МГц. Швидкість передачі до 4 Мбіт/с.
C	Додатки з високою швидкістю обміну. Максимальна частота 16МГц. Швидкість передачі до 100 Мбіт/с.
D	Додатки з дуже високою швидкістю обміну. Максимальна частота 100 МГц. Швидкість передачі до 100 Мбіт/с.
Оптичний	Додатки, що використовують як середовище передачі оптичний кабель. Частоти 100 МГц і вище.

Таблиця 14.2 – Категорії кабелів і роз'єднувачів

Категорія кабелю і роз'єма	Максимальна частота сигналу	Типові додатки
Категорія 3	16 МГц	Локальні мережі token ring і Ethernet 10BASE-T, телефонні канали
Категорія 4	20 МГц	Локальні мережі token ring і Ethernet 10BASE-T
Категорія 5	100 МГц	Локальні мережі зі швидкістю передачі даних до 100 Мбіт/с
Категорія 5e	100 МГц	Локальні мережі зі швидкістю передачі даних до 100 Мбіт/с
Категорія 6	250 МГц	Локальні мережі зі швидкістю передачі даних до 1000 Мбіт/с
Категорія 7	600 МГц	Локальні мережі зі швидкістю передачі даних до 1000 Мбіт/с, сигнали кабельного телебачення
Категорія 8	1200 МГц	Локальні мережі зі швидкістю передачі даних до 1000 Мбіт/с, сигнали кабельного телебачення

Клас А вважається нижчим класом, а клас D вищим. Для додатків кожного класу визначається відповідний клас лінії зв'язку, що задає граничні електричні

характеристики лінії, необхідні для нормальної роботи додатків відповідного й більше низького класу (табл. 14.2).

Додатки класу E і компонента СКС категорії 6 мають нормовані характеристики до частоти 250 МГц. Вибір саме такого частотного діапазону параметрів був обумовлений вимогою забезпечення потенційної можливості підтримки функціонування двопарних варіантів інтерфейсів Gigabit Ethernet. Клас F і компоненти категорії 7 розраховуються на частоти до 600 МГц. Вибір останнього значення в першу чергу обумовлений широким поширенням апаратури АТМ зі швидкістю передачі 622 Мбіт/с, а також необхідністю підтримки передачі сигналів багатоканального аналогового телебачення з верхньою граничною частотою 550 МГц.

Для побудови трактів категорії 6 використовуються кабелі всіх типів (екрановані та неекрановані). Як з'єднувач застосовується в основному модульне рознімання. Лінії категорії 7 при сучасному стані рівня техніки можуть бути реалізовані тільки на кабелі з екранованими парами. Остаточне рішення про вибір типу рознімання трактів категорії 7 комітетами зі стандартизації не прийнято [3].

14.2.3 Обмеження довжини кабелів СКС

Стандарти ISO/IEC 11801 в редакції 2000 року TIA/EIA 568-A установлюють **обмеження максимальної довжини кабелів і з'єднувальних кабелів** горизонтальної, і магістральних підсистем. Довжини кабелів вказані в табл. 14.3 [2, 12].

Довжина кабелю горизонтальної підсистеми встановлена 90 м (плюс 10 см на з'єднувальні шнури). Вибір саме цього значення вибраний, виходячи з можливості витої пари, як направляючої системи електромагнітних коливань передавати сигнали найбільш масових високошвидкісних додатків типу Fast Ethernet.

У випадку реалізації горизонтальної розводки на волоконно-оптичному кабелі довжина, кабельної траси обмежена довжиною 90 м із тих міркувань, що

вона гарантовано дозволяє виконувати обмеження протокольного характеру мереж Fast Ethernet по максимальному діаметру колізійного домену.

Таблиця 14.3 – Максимальні довжини кабельних трактів в залежності від типу кабелю і класу додатку

Клас додатку	A	B	C	D	Оптика
Симетричний кабель категорії 3	2 км	200 м	100 м	–	–
Симетричний кабель категорії 4	3 км	260 м	150 м	–	–
Симетричний кабель категорії 5	3 км	260 м	160 м	100 м	–
Симетричний кабель 150	3 км	400 м	250 м	150 м	–
Багатомодовий оптичний кабель	–	–	–	–	2 км
Одномодовий оптичний кабель	–	–	–	–	3 км

Основним призначенням підсистеми внутрішніх магістралей є об'єднання в одне ціле технічних приміщень у межах однієї будівлі. Виходячи із цього максимальна довжина, такої магістралі встановлюється стандартами рівною 500 м.

Підсистема внутрішніх магістралей довжиною 2 і 3 км у залежності від типу. При сучасному стані рівня волоконно-оптичної техніки ця відстань може бути збільшеною до 100 і більше кілометрів із використанням звичайної серійної апаратури. Але при необхідності забезпечення зв'язку на такі великі відстані стандартами передбачається, що для передачі інформації будуть використовуватися лінії і канали зв'язку загального використання різних телекомунікаційних операторів.

14.3 Методи проектування СКС

Горизонтальна підсистема СКС [2, 12], якщо при її реалізації використовуються кабелі з витой пари, може бути побудована по чотирьох різних варіантах, які в схематичному виді зображені на рис. 14.9.

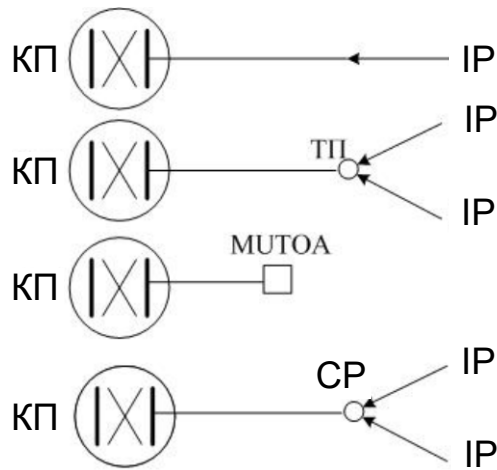


Рисунок 14.9 – Варіанти побудови горизонтальної підсистеми СКС [2]

На рис. 14.9 прийняті такі позначення:

- IP – інформаційна розетка;
- КП – кросова поверху;
- СР – точка консолідації;
- ТП – точка переходу;

На практиці найбільш **часто застосовується перша** з них, що утворена безперервним **кабелем довжиною 90 м**, що з'єднує розетковий модуль інформаційної розетки (IP) і комутаційну панель у кросовій поверху (КП).

У другому варіанті тракт передачі утвориться послідовним з'єднанням кабелів двох різних типів, але з еквівалентними передатними характеристиками. Ці **кабелі з'єднуються між собою в так званій точці переходу**. Точка переходу реалізується на звичайному комутаційному устаткуванні, що відрізняється від комутаційного устаткування технічних приміщень тільки видом конструктивного виконання. Однак це устаткування забороняється використовувати для виконання операцій адміністрування підсистеми кабельної системи й для підключення активних мережевих пристроїв будь-якого призначення. Відповідно до цього в точці переходу ніколи не повинні застосовуватися комутаційні і кінцеві шнури. З визначення точки переходу й вимог до неї, що кількість пар вхідних і вихідних кабелів повинне збігатися, або відрізнятися не більше ніж на одну.

Останні два варіанти побудови горизонтальної підсистеми СКС орієнтовані в першу чергу на застосування в так званих **відкритих офісах** (рис. 14.10). Під цим об'єктом розуміються робочі приміщення великої площі, які не мають некапітальних стін взагалі, або розділені на окремі секції спеціалізованими меблями, або перегородками, що легко демонтуються. Загальною відмітною ознакою таких офісів [13] є часті переміщення співробітників і зміни складів робочих груп, а також наявність явно вираженого зонного угруповування окремих робочих місць.



Рисунок 14.10 – Відкритий офіс [14]

У відкритих офісах можуть застосовуватися телекомунікаційні розетки для багатьох користувачів і консолідаційні точки (КТ). Розетка, що обслуговує декількох користувачів, має назву MUTOA (Multi User Telecommunication Outlet Assemblies). Максимальна кількість розеткових модулів у розетці MUTOA може досягати 12.

Такий елемент виділяється більшістю виробників в окремий вид устаткування, що встановлюється на колонах і стінах будинку, під фальшивою стелею, у коробках встановлених на підлозі, і досить рідко – у просторі між капітальною і підвісною стелями [3]. Консолідаційна точка представляє собою

проміжну точку комутації, яка використовується в горизонтальній підсистемі при умові, що вона не буде являтися точкою адміністрування, і до неї не буде підключатися обладнання, тобто це лише прохідна точка підключення. Крім цього в межах однієї лінії горизонтальної кабельної магістралі вона повинна бути єдиною і розміщатися в обслуговуваній зоні (рис. 14.11).

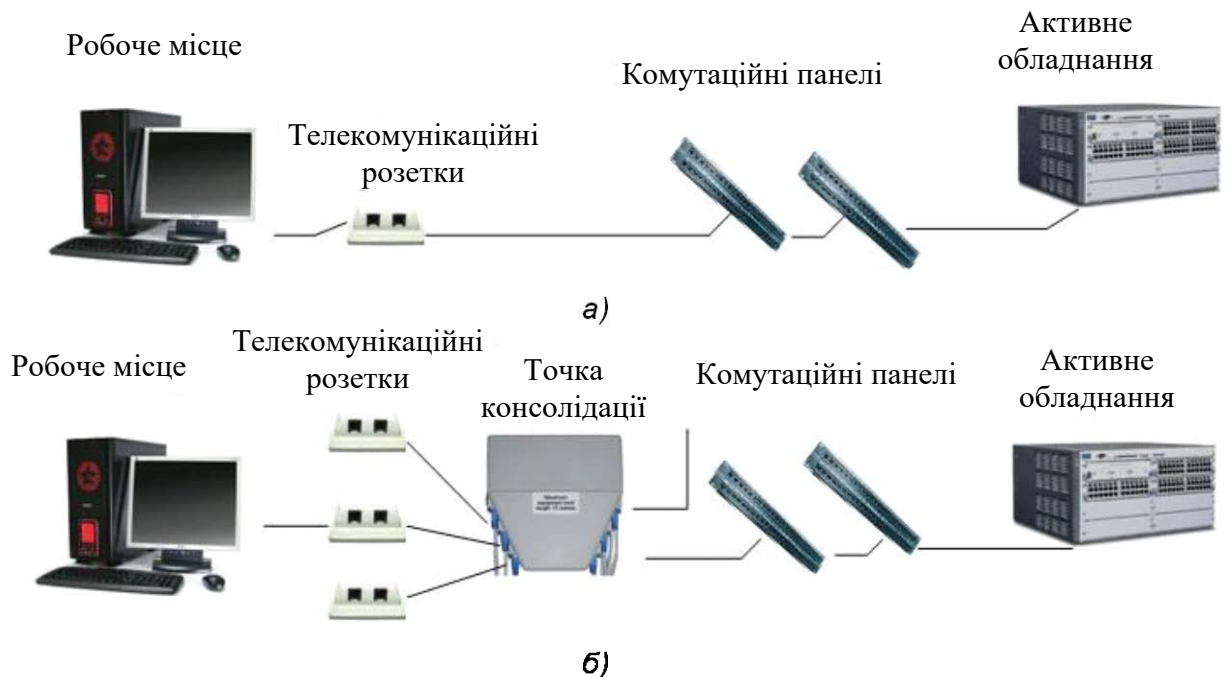


Рисунок 14.11 – Узагальнена модель горизонтальної підсистеми без використання точки консолідації (а) і з використанням точки консолідації (б) [15]

Як випливає з рисунку, радикальних змін традиційна схема (рис. 14.7,а) не зазнала, а просто з'явилася додаткова ланка з'єднання в кабельній магістралі. Але суттєво змінилася гнучкість підключення: тепер до однієї точки консолідації можна підключить декілька телекомунікаційних розеток, що у свою чергу забезпечують більшу свободу розміщення робочих місць в приміщенні [5].

14.4 Організація кабельних трас

Кабельні траси горизонтальній підсистемі призначені для прокладки по них кабелів від КП до робочих місць. Способи прокладання показані на рис. 14.12.

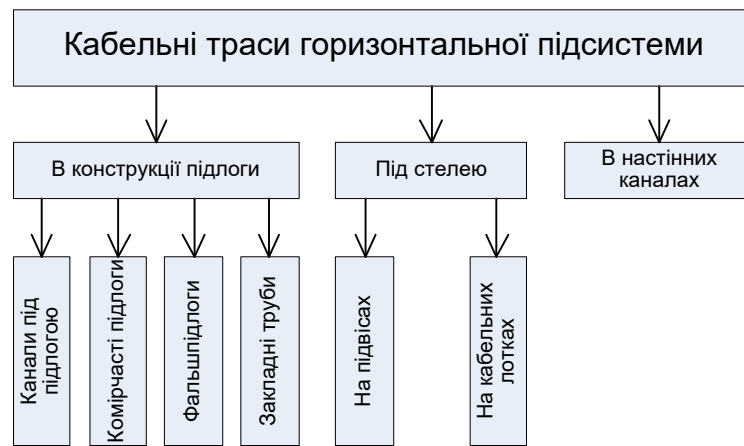


Рисунок 14.12 – Способи прокладання кабелю в горизонтальній підсистемі

Підпільні канали являють собою спеціалізовані металеві або пластикові конструкції в основному з прямокутним перетином, які встановлюються в структурі міжповерхового перекриття перед "чистою заливкою" підлог. Такі канали дозволяють отримати ефективний механічний захист, зменшують рівень зовнішніх наведень і електромагнітного випромінювання, забезпечують прихованість прокладки. Недоліком такого рішення є висока вартість реалізації, необхідність завершення монтажу до закінчення будівельно-монтажних робіт і використання спеціальних підлогових коробок для доступу до електричних і інформаційних розеток, що тягне за собою збільшення маси підлоги.

В системі **однорівневих підпільних каналів**, магістралі й розподільні канали розташовані на одному рівні відносно поверхні міжповерхового перекриття, і відрізняються один від іншого лише площею поперечного перерізу. Це дозволяє установлювати їх в будівлях з товщиною підлоги 63 мм і більше.

В системі дворівневих підпільних каналів, магістральні і розподільні канали розташовуються на різних рівнях. Розподільні канали зазвичай прокладаються вище магістральних. Для організації дворівневих каналів товщина підлоги повинна бути не менше 100 мм.

Закінчення кабельних каналів у приміщенні кросової проектується таким чином, щоб забезпечити зручність виведення кабелів і їх підключення до панелей комутаційного обладнання [16]. На рис. 14.13 наведено два варіанти

конструктивного оформлення кінцевих ділянок, які найчастіше застосовуються на практиці.

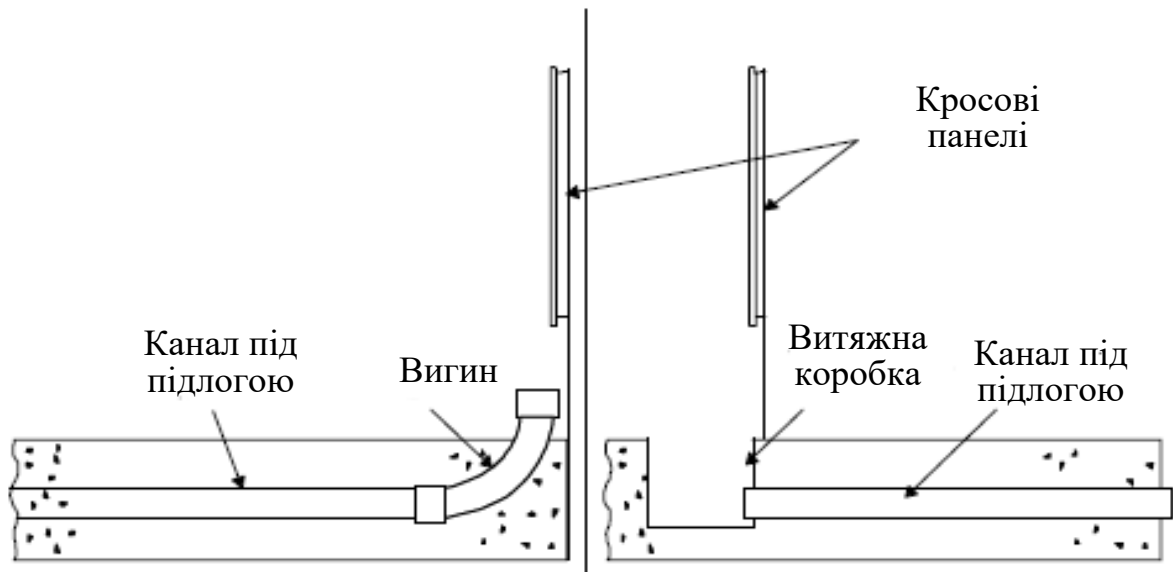


Рисунок 14.13 – Основні варіанти реалізації виведення кабелів з підпільних каналів в приміщення кросової [16]

Комірчасті підлоги (рис. 14.14) можуть розглядатися як один з різновидів підпільних каналів, і являють собою систему безперервних смуг порожнеч в бетонних плитах конструкції підлоги. Ця конструкція має практично такі ж властивості, як і підпільні канали, за винятком ефективності екранування електромагнітного випромінювання. Крім того вони перевершують конструкції з підпільними каналами по ємності кабелів.



Рисунок 14.14 – Конструкції комірчастих підлог [16]

Фальшпідлога традиційної конструкції формується квадратними плитками різного розміру, які встановлюються на металевих стійках (з можливістю регулювання висоти) або на решітці каркасу (рис. 14.15). Плитки зазвичай виготовляються з литого металу, і мають верхнє покриття з лінолеуму.

Для прокладання кабелів під фальшпідлогою досить часто застосовуються канали у вигляді повністю закритих металевих лотків відносно малого поперечного перерізу. Вивід до підлогових і підпільним коробок різного виду для встановлення розеток, в цьому випадку, виконується з використанням металевого рукава. Застосування такого рішення дозволяє істотно знизити вимоги до рівня пожежної безпеки кабельних виробів.

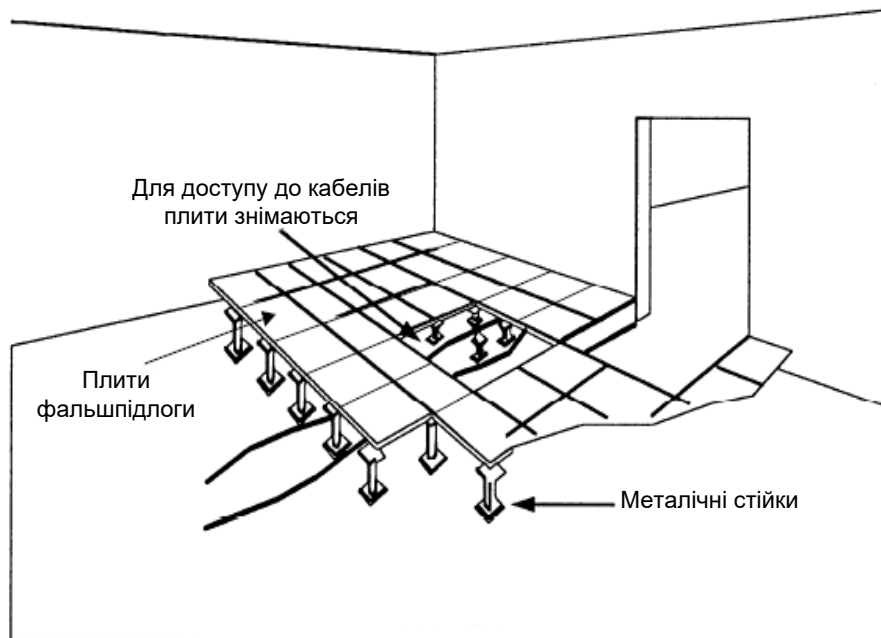


Рисунок 14.15 – Конструкція фальшпідлоги [16]

Мережа *закладних труб* або пластмасових труб різного діаметру аналогічна підпільним каналам і встановлюється в структурі міжповерхового перекриття. Може ділитися на дві підсистеми: магістральну і розподільну. Вигідно відрізняється, від розглянутих вище рішень, своєю низькою вартістю, але має обмежену гнучкість і малу ємність. Мережа закладних труб проектується, таким чином, щоб у ній були відсутні ділянки, які мають більше двох вигинів під прямим кутом між точками витяжки кабелів і проміжними витяжними коробками.

Кабелі можуть прокладатися до робочих місць чотирма основними способами.

Згідно **зонному методу**, обслуговувана площа розбивається на зони площею до 72 м² (рис. 14.16). Інформаційні розетки монтуються по одному із чотирьох способів, із використанням вертикальних коробів чи колон, які верхнім своїм кінцем виводяться в простір над фальшстелею. У кожній зоні організовується точка переходу, до якої прокладається багатопарний кабель. Від точки переходу горизонтальний кабель зазвичай по коротшій відстані доводиться до коробу або колони, і далі до розетки. Перевагою методу є простота його реалізації і достатньо висока гнучкість. Як недолік складність реалізації в тих випадках, коли в просторі над фальшстелею є значний об'єм устаткування інших інженерних систем будівлі і системи освітлення.

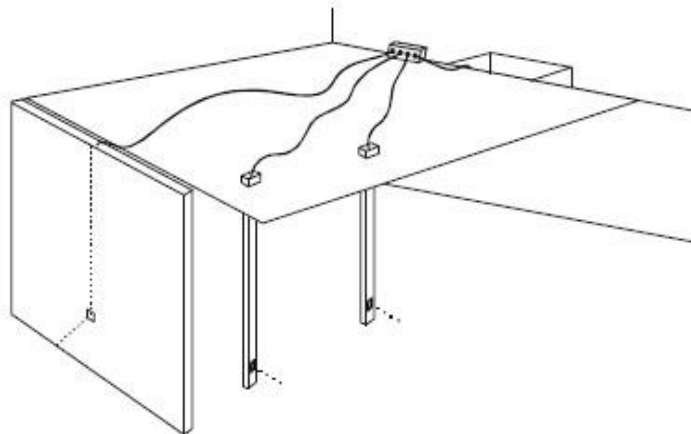


Рисунок 14.16 – Ілюстрація "Зонного" методу прокладання кабелю [16]

Відмінною особливістю **методу прокладки зв'язки кабелів** є формування жмута кабелів, що вводяться в приміщення. Останній укладається вздовж місць установки коробів або колон із кріпленням до стіни, чи стелі. При проході біля коробу чи колони зі зв'язки виймається один, або декілька кабелів, які спускаються до інформаційних розеток (рис. 14.17).

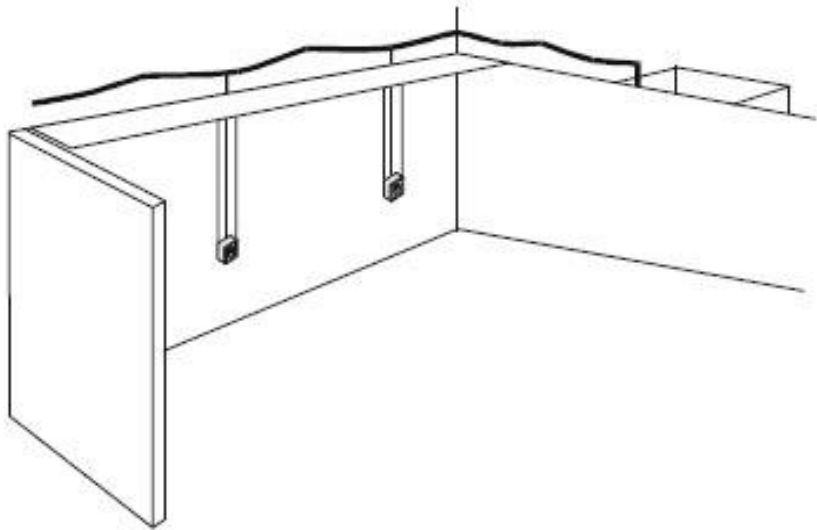


Рисунок 14.17 – Метод прокладки зв'язки кабелів [16]

Перевагою розглянутого методу є його висока гнучкість, простота, реалізації і зменшення наводок від ламп денного світла в тих випадках, коли прокладка виконується вздовж стін. Основним недоліком вважається необхідність використання Plenum-кабелів* і прокладка зв'язків в захисних трубах, так як у іншому випадку не вдасться витримати норми протипожежної безпеки.

Метод прокладки в кабельних лотках передбачає, як це слідує з назви, наявності в приміщенні системи кабельних лотків. Жмут кабелів укладається в лоток і у випадку необхідності, кріпиться до нього пластиковими стяжками. При проході розеток аналогічно попередньому методу, від жмута відділяється один або декілька кабелів. До переваг методу відносяться ефективний захист кабелів від механічних дій, а також простота прокладки додаткових кабелів. Як недолік, складність реалізації і підвищена вага стельових конструкцій, тому даний метод використовується зазвичай у службових приміщеннях, і при прокладці в коридорах.

При використуванні **методу прокладки через перекриття**, кабель на робоче місце прокладається через отвір в міжповерховому перекритті з підвісної стелі нижнього поверху (рис. 14.18). Із-за зменшення вогнестійкості будівлі і зниження механічної міцності перекриттів таке рішення може прийматися в

крайніх випадках, коли прокладка іншими методами неможлива з тих, чи інших причин.

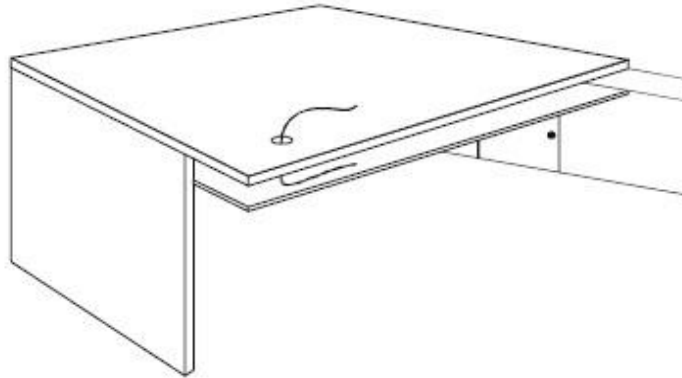


Рисунок 14.18 – Метод прокладки кабелю через перекриття [16]

Настінні кабельні канали призначені для прокладки кабелів до інформаційних розеток, установлених на стіні приміщення на зручній для використання висоті. У деяких випадках накладні настінні кабельні канали використовуються для прокладки джгутів горизонтальних кабелів на проміжках від виходу з кросової до входу в приміщення з інформаційними розетками. Можуть бути використанні наступні різновидності настінних кабельних каналів:

- накладні кабельні канали, декоративні короба або плінтуса;
- скриті кабельні канали, які монтуються в стіні, таким чином, щоб на її поверхню виходили тільки інформаційні чи силові розетки.

Зазвичай заповнення коробів кабелями не перевищує 30-60% площі їх поперечного перерізу, конкретне значення залежить від допустимого мінімального радіуса вигину кабелів, укладених у короб [6].

14.5 Приклад побудови реальної системи СКС

Перш за все, потрібна система, що забезпечує повноцінну роботу ІТ-інфраструктури на весь час існування будівлі (до капітального ремонту або повної реконструкції), а це – десятки років. Тобто витрати на СКС відразу розглядалися як капітальні вкладення.

Настільки довгострокова перспектива вимагає забезпечення пропускної здатності мережі для швидкостей майбутнього. Як відомо, швидкість 10 Гбіт/с вже на підході, і тому популярна сьогодні на ринку п'ята категорія представляється морально застарілою і не зможе підтримувати функціонування додатків, які будуть розповсюджені через 5...7 років. То чи варто сьогодні закладати систему, яка автоматично буде вимагати реконструкції бізнес-центру через якихось сім років і прирече на необхідність використання застарілих інформаційних технологій? Тому було прийнято однозначне рішення: СКС будівлі повинна забезпечувати передачу даних зі швидкістю 10 Гбіт/с до робочого місця.

Для горизонтальної підсистеми було вирішено використовувати екранований кабель PiMF600 (екран як для кабелю в цілому, так і для кожної пари), який забезпечує функціонування більшості відомих слабкострумних додатків, у тому числі Ethernet 10 Гбіт, і має великий запас пропускної здатності. Для вертикальної проводки використовується оптичне волокно.

У комутаційних центрах встановлюються крос-панелі AMPTRAC Ready, що дозволяють надалі встановити систему контролю кабельної системи в реальному часі AMPTRAC. Причому, для одного з поверхів така система інсталується відразу. Група робочих місць проектується за технологією АСО, яка забезпечує високу гнучкість підключень і використання ресурсів СКС. Спочатку передбачено щільне розміщення інформаційних розеток з розрахунку: одна розетка на 6 м² корисної площі.

Загальна схема проекту передбачає наявність поверхових кросів (всього 12 комутаційних кімнат), з'єднаних між собою оптичними лініями зв'язку. Для розміщення "активного" устаткування кросові кімнати оснащуються секційними шафами компанії Rittal, що також поставляються фірмою VD MAIS.

Важливим моментом при інсталяції екранованої системи вважається правильне і якісне заземлення; в проекті застосовується система заземлення та блискавкозахисту компанії OBO Bettermann, яка рекомендується в методичних матеріалах AMP.

14.5.1 Кабельні траси

Як відомо, будівництво СКС починається з прокладки кабельних трас. Саме на цьому етапі реалізується кабельна інфраструктура. Для всіх кабельних підсистем використана єдина система трас, як показано на рис. 14.19. Традиційно кабельні траси інженерних підсистем (СКС, охоронної та пожежної сигналізації, контролю доступу, диспетчеризації, електроживлення тощо) проектуються і монтуються окремо. При цьому перед генеральним проектувальником стоїть складне завдання розподілу простору в коридорах і стояках для ув'язки кабельних трас окремих інженерних підсистем, що вимагає багато часу і має ітераційний і циклічний характер. Проектувальники кожної підсистеми намагаються зайняти найбільш зручні місця, і виходить, що вони претендують на одні й ті ж ділянки простору. До того ж, на розподіл простору між підсистемами в основному впливає суб'єктивний фактор, ступінь "близькості" відносин між головним інженером проекту і проектувальником конкретної підсистеми.



Рисунок 14.19 – Багаторівнева єдина система кабельних трас

На етапі монтажу всі ці проблеми проявляються з новою силою. Найчастіше найбільш зручний простір займає той, хто раніше приступив до робіт. Відхилення від проектної документації призводить до конфліктів, а іноді навіть... до демонтажу

раніше прокладених трас через брак вільного місця. Координація робіт та вирішення протиріч важким тягарем лягає на плечі генпідрядника.

Істотно знизити конкуренцію між інженерними підсистемами дозволяє саме єдина система лотків та кабельростів, дозволяє врахувати і відобразити всі необхідні аксесуари: п'яти, швелери, консолі, редукції, повороти, арки та ін.

14.5.2 Вибір типу кабеля

Для створення своєї IT-інфраструктури керівництво VD MAIS вибрало сучасне рішення з розрахунком на пропускну здатність кабелів для завдань завтрашнього дня. У зв'язку з цим у проекті застосовується кабель PiMF600 виробництва компанії Tyco Electronics AMP (рис. 14.20), який тільки недавно з'явився на нашому ринку. Саме з таким типом кабелю прямо пов'язане забезпечення швидкості передавання даних 10 Гбіт/с. Індивідуальне екранування кожної пари (PiMF – Pairs in Metal Foil) в комплексі з додатковим загальним екраном істотно знижують міжкабельні наведення і забезпечують високі характеристики.



Рисунок 14.20 – Котушки з кабелем PiMF600 (а) та його розмотування і укладання в лотки (б)

Разом з тим, при роботі з кабелем PiMF600 потрібен особливий підхід. Трудомісткість роботи з ним набагато вище, ніж зі звичними коробками кабелю довжиною по 305 м. Кабель PiMF поставляється в котушках по 1000 м, загальною масою – 64 кг (рис. 14.20,а). І розмотати такий кабель без спеціальних пристроїв вельми складно, особливо, якщо, як у цьому проекті, його загальна довжина перевищує 100 км. Компанія "Світ Кабельних Систем" застосувала для розмотування котушок особливі пристосування – піддони з валиками (рис. 14.20,б), які дозволяють одній людині розмотувати кабель відразу з десятка котушок.

У цій операції критичне зусилля, що прикладається до окремого кабелю. За документацією АМР зусилля не повинно перевищувати 110 Н, тобто близько 11 кг. Після вимірювання динамометром було визначено, що зусилля зберігається в межах 1.5...2.5 кг на кабель для окремої котушки, тобто запас цілком достатній.

14.5.3 Технологічні нюанси прокладання кабеля

Основні операції при прокладці кабелю відомі всім інсталяторам: визначення довжини кабельних відрізків, їх маркування, розмотування кабелю з котушок, прокладка по трасах, вхід і прокладка кабелю в кросових кімнатах та в зонах робочих місць. І якщо регламентувати всі ці дії, то вийде більше двох десятків технологічних операцій. І в кожній з них є певні резерви підвищення якості та зниження всіляких ризиків.

Простий приклад: звичайна установка кронштейнів в кімнатах по проектному маршруту кабельних трас може стати елементом системи забезпечення якості, оскільки відстань між двома рядами кронштейнів становить 30 см. Як наслідок, під час монтажу ні інсталяторам СКС, ні електрикам не знадобиться відслідковувати технологічно необхідну відстань між трасами – вони просто не зможуть її змінити.

При прокладанні кабелю особливо дбайливо слід поводитися з ним на поворотах. Зазвичай для цього на кожному повороті ставлять для страховки по одній людині. А на цьому об'єкті використовувалися спеціальні блоки, які

встановлюються на поворотах і забезпечують безпечний прохід кабелю і економію трудових ресурсів (рис. 14.21).



Рисунок 14.21 – Розмотування кабелю і обхід повороту

У міру наближення до кросової кімнати джгути об'єднуються і при вході в неї включають до 24 кабелів. Для кожної крос-панелі, вірніше, її кабельного джгута, закладена окрема труба (до речі, запас по кількості труб забезпечується на рівні 50%). З обох сторін стіни і прохідних отворів встановлюються таблички, на яких вказується, для якого кабельного джгута призначена відповідна труба. Таке, здавалося б, елементарне рішення забезпечує порядок на кабельростах кросових кімнат.

14.6 Система інтелектуального моніторингу кабельної мережі AMPTRAC

Більшість фірм починають свою діяльність з прокладки інформаційної кабельної мережі, безперебійна робота якої є однією з умов успішної діяльності. З розвитком фірми і зростанням кількості обладнання, підключеного до мережі, її обслуговування багаторазово ускладнюється. Збільшується й число простоїв мережі. Нижче наведені деякі відомості про роботу мереж:

- за рік мережа зупиняється в середньому 70 разів
- 70% простоїв мережі обумовлені відмовами в кабельному господарстві, при їх усуненні 80% часу витрачається на діагностику, 20% – на усунення причини
- в середньому більше 270 годин на рік складають плановані простої і більше 175 годин – простої, що виникають через раптові відмови.

Причини планованих простоїв:

- щорічний переїзд близько 30% користувачів
- заміна комп'ютерів за час життя мережі до чотирьох разів, решти устаткування – до трьох разів
- перебудова підрозділів, офісів, виробництва.

Важливість проблем, що виникають при обслуговуванні мережі, важко переоцінити. І якщо в невеликій мережі проблеми можуть вирішуватися порівняно просто, то в мережі з кількома сотнями портів навіть реєстрація всіх змін у паперовому вигляді являє собою досить трудомістку задачу.

Фірма AMP NETCONNECT/TYCO розробила і випускає систему AMPTRAC, призначену для інтелектуального моніторингу кабельних мереж [17]. Ця система забезпечує істотне скорочення витрат на експлуатацію мережі, підтримуючи високий рівень її готовності. Вона дозволяє звести до мінімуму час простою і автоматизувати багато операцій, що виконуються при експлуатації мережі, а саме:

- ведення журналу з'єднань, що відображає реальний стан мережі
- підготовку завдань на проведення змін конфігурації мережі
- отримання інформації про кількість, місце розміщення вільних портів і про можливості організації нових місць підключення до мережі
- повідомлення адміністратора про несанкціоновані перемикання або неполадки в мережі та інші операції.

З впровадженням системи адміністратор отримує єдину базу даних, що дозволяє зберігати інформацію про все обладнання мережі, починаючи від АТС та центральних комутаторів і закінчуючи робочими станціями та IP-адресами, виділеними кожному користувачеві.

14.7 Принцип роботи системи AMPTRAC

Узагальнена структурна схема системи приведена на рис. 14.22 [17].

Принцип роботи системи полягає в наступному. Для автоматичного визначення наявності з'єднання над кожним портом комутаційних панелей розташовується додаткова контактна площадка. Всі майданчики комутаційної панелі з'єднані з окремим роз'ємом, підключеним до аналізатора. Для з'єднання портів використовуються спеціальні кабелі (патчкорди), що закінчуються стандартними вилками, в захисні ковпачки яких вбудовані з'єднані між собою додаткові контакти. При з'єднанні таким кабелем будь-якої пари портів автоматично з'єднуються і відповідні контактні площадки. Аналізатор безперервно опитує всі підключені до нього контактні площадки для визначення наявності з'єднань і передає цю інформацію на сервер, в якому зберігається безперервно оновлювана база даних про поточну конфігурацію всієї мережі і зміни, що відбуваються в ній.

Прийнятий у системі AMPTRAC спосіб визначення конфігурації мережі відрізняється від застосовуваного в інших системах наступними перевагами:

- для відстеження з'єднань в мережі використовуються додаткові електричні ланцюги, які не впливають на обмін даними по мережі
- використання стандартних 8-контактних роз'ємів RJ45 дозволяє значно знизити вартість системи в порівнянні з системами інших виробників, що використовують 10-контактні роз'єми
- з'являється можливість визначення наявності з'єднання не тільки кабелів з мідними жилами, а й оптоволоконних
- додаткові контактні площадки можна встановити не тільки на комутаційних панелях, але і на мережевому обладнанні, включивши його таким чином до бази даних системи.

Склад системи AMPTRAC

::AMPTRAC-аналізатор:
відстежує з'єднання між контактними площадками і відновлює базу даних ІМ

::AMPTRAC-кабелі введення-виведення:
з'єднують контактні площадки панелей і активного обладнання з аналізаторами

::AMPTRAC-комутаційні панелі: панелі з вбудованими контактними площадками

::AMPTRAC-сенсорні наклейки: самоклеючі полоски з контактними площадками

::AMPTRAC-комутаційні шнури: стандартні шнури зі службовим «9-м» провідником для замикання кола між контактними площадками

::IM Software: програмні засоби

::AMPTRAC-сервер: комп'ютер, на якому встановлено ПО ІМ.

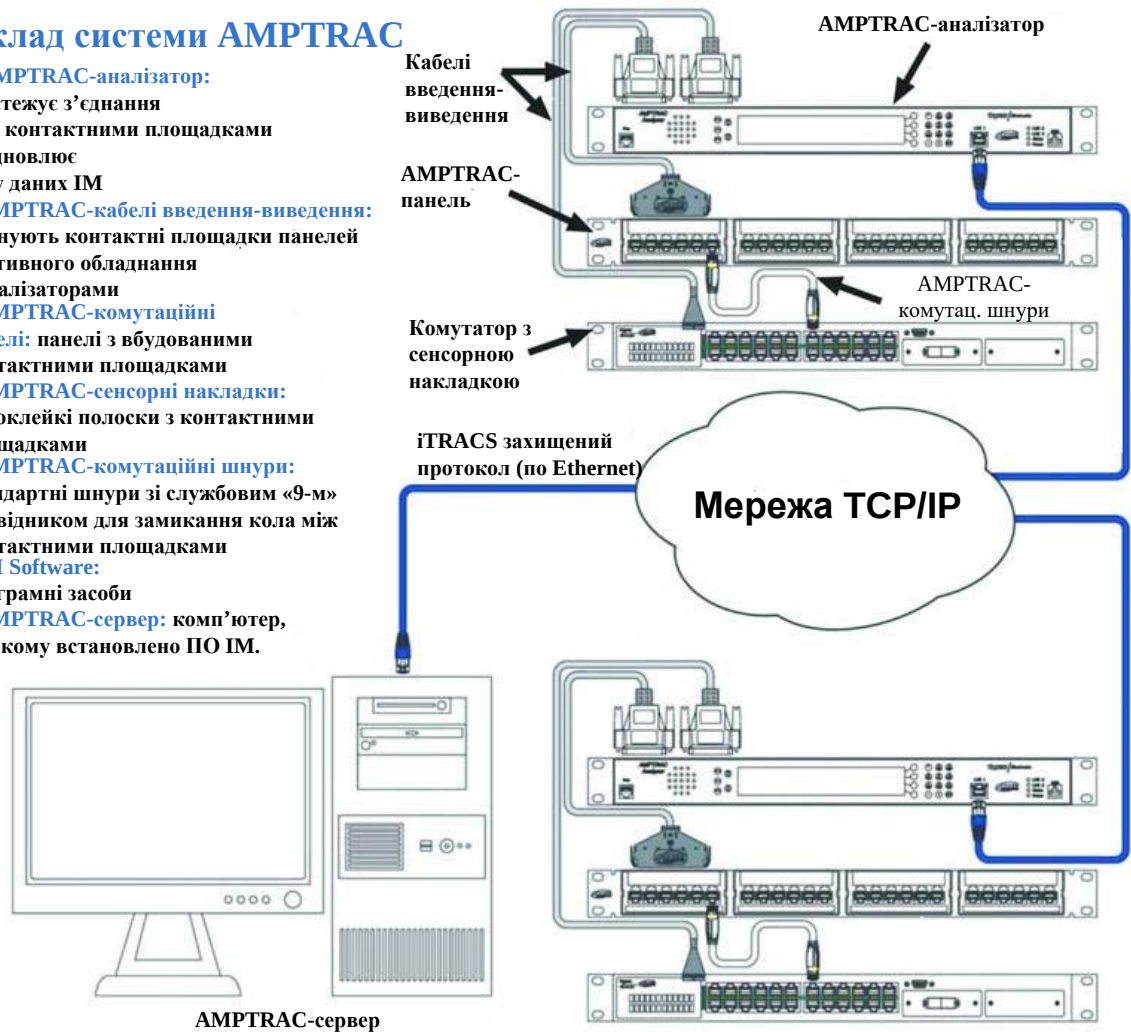


Рисунок 14.22 – Узагальнена структурна схема системи AMPTRAC [17]

Контрольні питання

1. Що таке топологія СКС?
2. Які класи додатків вам відомі?
3. Чим відрізняються параметри кабелів різних категорій?
4. Де розташовуються кросові приміщення?
5. Яка максимальна довжина кабеля від кросової до робочого місця?
6. Для чого використовується система інтелектуального моніторингу СКС?
7. За якими критеріями здійснюється вибір кабеля вертикальної підсистеми?
8. Які технологічні прийоми використовуються при прокладці кабелів у коридорах що мають відгалуження і повороти?

- D1%82%D0%BE%D1%80-
 %D1%88%D0%BD%D1%83%D1%80%D0%BE%D0%B2-48-
 %D1%81%D0%B5%D0%BA%D1%86%D0%B8%D0%B9-spm-
 400%D0%BC%D0%BC/ (дата звернення: 3.11.2024).
8. Експлуатація та ремонт кабельних ліній. Url: <https://kazedu.com/referat/195999/1> (дата звернення: 3.11.2024).
 9. Моделі реалізації горизонтальної підсистеми СКС. Url: <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://learn.ztu.edu.ua/mod/resource/view.php%3Fid%3D178355&ved=2ahUKEwj9r>
 10. Екрановані комутаційні шнури. Url: <https://catalog.vdmais.ua/uk/products/21/2101/210115/21011505/>. (дата звернення: 3.11.2024).
 11. Типи мідних інсталяційних кабелів в СКС. Url: https://www.ivynet.ua/kabel_SKS.php. (дата звернення: 3.11.2024).
 12. Структуровані кабельні системи. Принципи побудови, експлуатація, інсталяція та адміністрування СКС. Url: <https://deps.ua/ua/training/catalog/structured-cabling-systems/10378.html>. (дата звернення: 3.11.2024).
 13. ISO/IEC 11801-1:2017(en) Information technology — Generic cabling for customer premises — Part 1: General requirements. Url: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:11801:-1:ed-1:v1:en> (дата звернення: 13.11.2024).
 14. Переваги та недоліки офісів відкритого типу. Url: <https://prostostroy.com/preimushhestva-i-nedostatki-ofisov-otkrytogo-tipa.html> (дата звернення: 13.11.2024).
 15. Мережі та бізнес. Url: [https://sib.com.ua/arhiv_2005/5\(24\)2005/consolidation_point/consolidation_point.htm](https://sib.com.ua/arhiv_2005/5(24)2005/consolidation_point/consolidation_point.htm) (дата звернення: 13.11.2024).
 16. Кабельні траси горизонтальної підсистеми Url: https://bstudy.net/802530/tehnika/kabelnye_trassy_gorizontальной_podsystemy (дата звернення: 13.11.2024).

17. AMPTRAC – система інтелектуального моніторингу кабельної мережі. Url: http://www.ekis.kiev.ua/UserFiles/Image/pdfArticles/ekis114_p16_19.pdf (дата звернення: 13.11.2024).

15 БЕЗПРОВОДОВІ СИСТЕМИ ЗВ'ЯЗКУ ІНТЕРНЕТУ РЕЧЕЙ

15.1 Загальні зауваження

Для IoT не властиві універсальні рішення. Є безліч шляхів використання з'єднаних пристроїв, тисячі варіантів, кожний з яких висуває свої вимоги. Деяким пристроям потрібна низька пропускна здатність мережі, іншим – висока.

Багатьом технологіям необхідна велика пропускна здатність. Таким, як відеомоніторинг або розважальний контент (онлайн-гри, фільми та ін.). Але умови передавання радіосигналів усередині приміщень зовсім не такі, як зовні. Пристрій може бути стаціонарним (ворота, камери відеоспостереження, машини на заводах) або мобільними (у поїздах або на автомобілях).

Більшість розв'язків вимагають малої пропускної здатності (наприклад, додатки для контролю розумних будинків або здійснення платіжних операцій). Хоча у таких додатках невисокий рівень використання даних і низькі вимоги до пропускної здатності, це не повинно позначатися на користувачах – помилки поставлять під удар фінансову й фізичну безпеку людей. Тому таким технологіям потрібні мережі високої надійності.

Багато IoT-пристроїв вимагають підключення до мобільних мереж. Користувачі міняють смартфони й планшети досить часто – у середньому, кожні 18-24 місяця. Але життєвий цикл "розумних" технологій куди довше – і клієнти, що змінили пристрій, як і раніше розраховують на якість обслуговування.

15.2 Важливість стандартів

Зростаюча частка ринку IoT складають пристрої з низьким енергоспоживанням [1, 2]. Багато "розумних" лічильників контролю води, газу та інших розташовані в місцях, де не так просто підключити їх до електромережі. Наприклад, паркувальні сенсори й додатки для розумних будинків (контроль температури, вологості, ефективності витрати енергії та ін.). IoT у цих випадках вимагає дуже низького енергоспоживання й мереж, що передають дані малого

обсягу. Це робить стандартизацію й функціональну сумісність дуже важливими для технологій інтернету речей.

У цей час для Інтернету речей розробляють як нові стандарти, так і модернізують існуючі мережі мобільного зв'язку для різних сценаріїв використання. Найбільш відомі з таких мереж – стандартизовані LoRa, Sigfox і NB-IoT і в процесі стандартизації – EC-GSM і EMTС. Експерти відзначають, що мережі, що працюють у неліцензуюемому діапазоні частот, будуть більш затребувані в більшості країн. Перші з них на основі стандарту LoRa, уже розгортаються в багатьох країнах.

15.3 Технології, засновані на існуючих стандартах мобільного зв'язку

Технології консорціуму 3GPP (The 3rd Generation Partnership Project) для Інтернету речей засновані на існуючих стандартах мобільного зв'язку. Через невимогливість M2M-устаткування до швидкостей передавання даних стільникові мережі, що існують, прийнято вважати дорогими. Робота сенсорів і пристроїв через надмірне енергоспоживання в мобільних мережах і складних протоколів, приводить до швидкої розрядки батареї M2M-пристроїв [1]. Тому мережі стільникового зв'язку модернізували для роботи IoT-пристроїв (рис. 15.1 та 15.2) [3].



Рисунок 15.1 – Існуючі мобільні технології зв'язку придатні для IoT [3]



Рисунок 15.2 – Стандартизація консорціуму 3GPP для Інтернету речей [3]

До основних модернізованих мереж можна віднести: EC-GSM (також носить назви EC-GPRS, EC-GSM-IoT), eMTC (теж, що й LTE-M, LTE CAT.M1) і NB-IoT [1].

Пристрої Інтернету речей спочатку задовольнялися низькою пропускнуою здатністю, але вимагали широке покриття. Як підсумок, були створені мережі LP-WAN (Low-Power, Wide-Area Networks): SigFox, LoRa і Weightless.

Нові рішення на базі 4G і LTE споживають занадто багато енергії, тому не підходять в стандартних модифікаціях для IoT-рішень (лічильників, датчиків і т. д.). Наведемо коротку характеристику різних модифікацій стільникових мереж [1]:

1. Cat-1

На даний момент це єдиний повністю доступний варіант стільникового Інтернету речей, який дозволяє підключати пристрої до існуючої мережі LTE. Продуктивність поступається мереж 3G, але зате технологія підходить для IoT-систем, що вимагають передачу даних або голосу. Мережа вже стандартизована і вельми проста, тому може використовуватися всюди. Згідно з прогнозами фахівців, коли настане захід 3G і 4G-мереж, Cat-1 (і Cat-M1) буде успішно існувати.

2. Cat-0

Щоб IoT-системи, що базуються на LTE, успішно розвивалися, вони повинні мати наступні характеристики:

- споживати мало енергії;
- мати низьку вартість;
- підтримувати якомога більшу кількість пристроїв;
- забезпечувати хороше проникнення сигналу через стіни.

Cat-0 – забезпечує низьку вартість, так як в обладнанні немає функцій, що вимагають великої швидкості передачі даних, як у випадку з пристроями Cat-1. Якщо Cat-1 покликаний замінити 3G, то Cat-0 є протоколом, прийшли на зміну 2G.

3. Cat-M1 / Cat-M / LTE-M

Cat-M (офіційно відомий як LTE Cat-M1) часто розглядається як друге покоління чіпів LTE, створених для IoT-додатків. Основу технології, яка характеризується низькою вартістю і енергоспоживанням, заклала розробка Cat-0.

У Cat-M може використовуватися смуга частот шириною тільки 1,4 МГц, тоді як в Cat-0 смуга може становити 20 МГц. Технологія створена виключно для LPWAN-мереж, де кількість переданих даних вкрай мала.

Головна перевага Cat-M полягає в сумісності з LTE-мережами. Це означає, що операторам не потрібно витратити гроші на установку обладнання: досить лише оновити програмне забезпечення.

4. NB-IoT / Cat-M2

NB-IoT має багато спільного з Cat-M. Принципова відмінність полягає в тому, що NB-IoT використовує DSSS-модуляцію (Direct Sequence Spread Spectrum – технологія модуляції, що забезпечує більшу продуктивність локальних безпроводових мереж шляхом розширення спектру випромінюваного сигналу). NB-IoT не претендує на діапазони LTE, що означає для операторів вищі витрати на початкових етапах запуску мережі.

Сьогодні технологія NB-IoT розрекламована як найкращий варіант по співвідношенню можливостей та вартості розгортання, оскільки для мережі не потрібен мережевий шлюз. Інші варіанти інфраструктури вимагають наявності шлюзів для збору даних з пристроїв і потім направлення їх до головного сервера. У мережі NB-IoT дані відразу направляються до головного комп'ютера без

посередників. Це пояснює, чому передові оператори світу і в тому числі українські віддають перевагу саме цій технології.

Згідно з прогнозами Sierra Wireless, майбутнє за двома IoT-мережами: NB-IoT і LTE-M.

5. EC-GSM

EC-GSM являє собою оптимізовану для IoT мережу GSM, яка характеризується широким покриттям і підтримкою 80% мобільних пристроїв на світовому ринку.

Як можна зрозуміти з назви, EC-GSM розгортається на існуючій мережі GSM. Вона має величезну перевагу з точки зору практичності та мобільності, оскільки вимагає лише простого програмного забезпечення.

Технологія є основною в малорозвинених регіонах, наприклад, в африканських або малайзійських, так як там 2G-мережа залишається основною. На початку 2020 року випробування EC-GSM завершили такі компанії, як Ericson, Intel і Orange. Однак все-таки мережа EC-GSM не настільки перспективна, як Cat-M або NB-IoT.

6. 5G

Якщо з вищенаведеними технологіями все зрозуміло, то 5G-стандартні були ще офіційно визначені для IoT. За даними Generation Mobile Networks Alliance (NGMN), мережа на основі 5G забезпечує швидкість передавання даних в 40 разів більшу ніж у мережах 4G і може обслуговувати близько одного мільйона пристроїв на квадратний кілометр.

Технологія 5G буде актуальна в тих сферах Інтернету речей, де потрібно передавати 4K- і 8K-відео в реальному часі (системи відеоспостереження, мультимедійний контент), управляти безпілотними автомобілями, а також працювати з VR / AR додатками.

Вибір мережі має значення для економічної ефективності

Провайдери змушені вибирати тільки одну мережу з перерахованих вище для розгортання. Щоб це зробити, потрібно оцінити перспективність кожного варіанта. Іншим же учасникам ринку досить розуміння того, що перераховані технології не

завжди є взаємовиключними. Для різних цілей можуть вимагатися абсолютно різні варіанти. Н рис. 15.3 наведені швидкості передавання даних необхідні для різних додатків Інтернету речей.

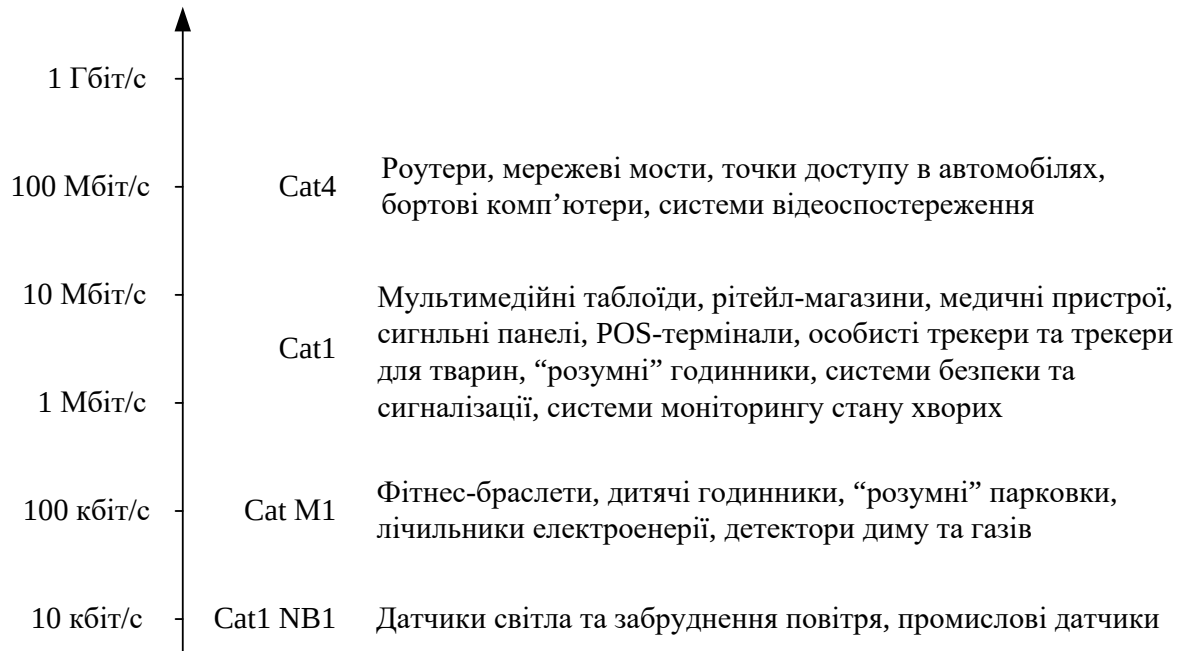


Рисунок 15.3 – Порівняння швидкості передавання даних при використанні різних технологій стільникового зв'язку

Недоліки цих мереж полягають у тому, що для їхнього функціонування необхідний ліцензуємий діапазон частот, тарифи на передачу даних можуть бути високими для невимогливого до швидкостей устаткування, вартість пристроїв, що працюють у стандарті LTE, залишається досить високою, необхідно розробляти устаткування, що підтримує кілька стандартів зв'язку і т.д.

До переваг можна віднести використання інфраструктури існуючих мобільних операторів, підтримка роумінгу, високі швидкості передавання даних для мультимедійного устаткування й пристроїв, яким необхідно функціонувати в режимі реального часу і т.д.

15.4 Характерні особливості безпроводових сенсорних мереж

У цілому безпроводові сенсорні мережі (БСМ) можна описати як мережу вузлів, які спільно здійснюють моніторинг навколишнього середовища й збір даних, забезпечують взаємодію між людьми або комп'ютерами й навколишнім середовищем [2]. У цей час БСМ, як правило, включають сенсорні вузли, вузли приводних пристроїв, шлюзи й клієнтів. Велика кількість сенсорних вузлів, розташованих у випадковому порядку усередині або біля контрольованої області (поле виявлення), формують мережі шляхом самоорганізації (рис. 15.4) [4].

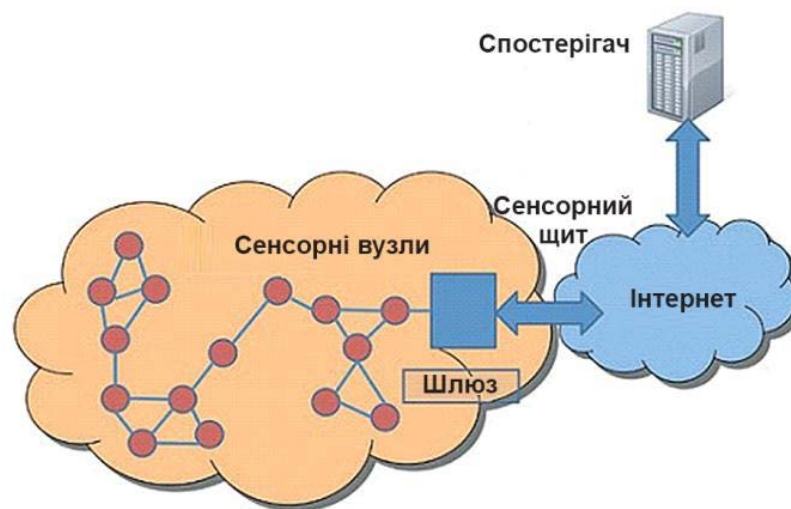


Рисунок 15.4 – Структура безпроводової сенсорної мережі [4]

Сенсорні вузли здійснюють контроль зібраних даних для їхньої передавання на інші сенсорні вузли стрибкоподібним методом. Під час передавання дані, що відслідковуються, можуть оброблятися декількома вузлами для переходу до вузла шлюзу після маршрутизації з декількома переходами, і, в остаточному підсумку, досягти вузла управління у Інтернеті або за допомогою супутника. Користувач здійснює конфігурацію й управління БСМ за допомогою вузла управління, формує завдання по моніторингові й здійснює збір контрольованих даних.

Датчик (сенсорний вузол) є однієї з основних частин БСМ. Апаратне забезпечення сенсорного вузла, як правило, складається із чотирьох частин:

силового модуля, модуля управління енергоспоживанням, сенсора, мікроконтролера й безпроводового прийомопередавача сенсора (рис. 15.5).



Рисунок 15.5 – Типова структура сенсора з безпроводовим зв'язком

Силовий модуль забезпечує електроживлення системи. Сенсор є центральним елементом вузла БСМ, який може одержати інформацію про стан навколишнього середовища й устаткування. Сенсор відповідає за збір і перетворення сигналів, таких як світло, вібрація й хімічні сигнали в електричні сигнали з наступною їхньою передачею на мікроконтролер. Мікроконтролер отримує дані від сенсора й проводить їхню відповідну обробку. Потім безпроводовий прийомопередавач (RF-модуль) здійснює передавання даних для фізичної реалізації процесу зв'язку.

Важливо, щоб конструкція всіх частин вузла БСМ враховувала характеристики вузла БСМ – малий розмір і обмежену споживану потужність.

Ключовою особливістю Інтернету речей є їхня робота з аналоговими інформаційними сигналами, які перетворюються у цифровий код й обробляються наявними в складі Інтернету речей засобами. Структура, що забезпечує проходження сигналу від сенсора в "хмарні" сховища, наведена на рис. 15.6.

Тому перший структурний вузол Інтернету речей включає сенсори для перетворення фізичної величини в аналоговий електричний сигнал, підсилювачі, АЦП, процесор, а також канал передавання даних для їхньої обробки "хмарними" технологіями.

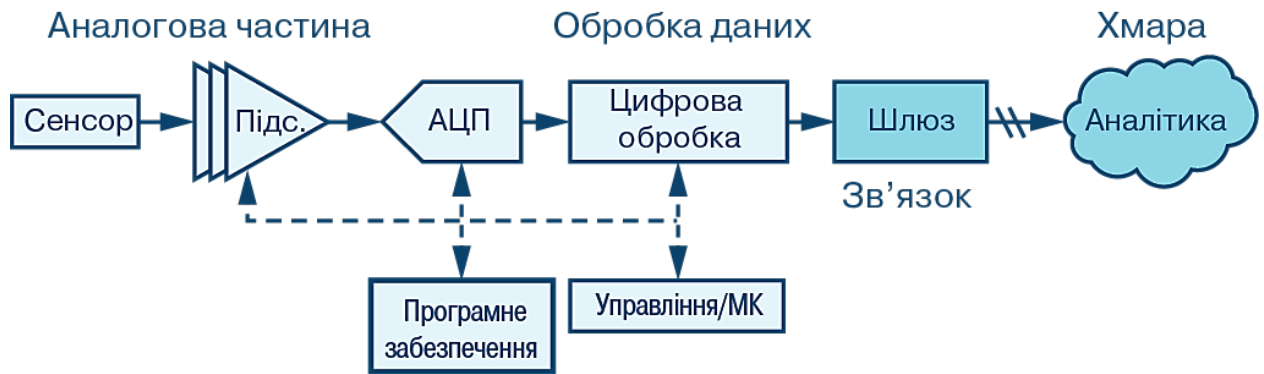


Рисунок 15.6 – Зв'язок сенсора з хмарним сховищем

Оптимальний розв'язок для структури цього вузла полягає в тому, щоб виключити передачу надлишкових даних для наступної обробки в "хмарі" [2]. У свою чергу, хмарні технології призначені для роботи з великими обсягами даних (Big Data). Фахівці вважаються, що в майбутньому тільки 1% даних, що перебувають у хмарах, буде використаний, тому що з метою зниження рівня погроз найбільш важливі дані бажане зберігати в локальних сховищах. Це забезпечується застосуванням смарт-сенсорів із вбудованими алгоритмами обробки даних. Порівняльна оцінка характеристик сьогоdnішнього й завтрашнього поколінь безпроводових сенсорних мереж наведена на рис. 15.7.

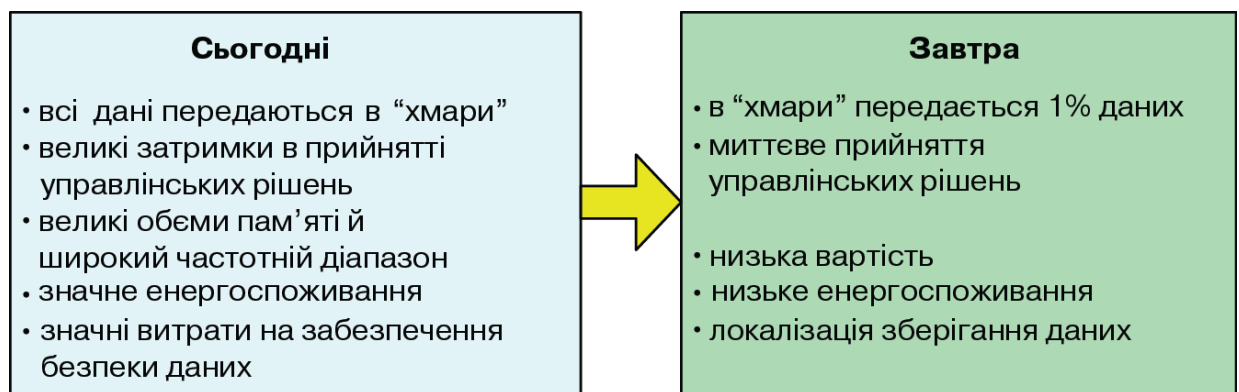


Рисунок 15.7 – Порівняльна оцінка характеристик сьогоdnішнього й завтрашнього поколінь безпроводових сенсорних мереж

15.5 Базова архітектура сенсорної мережі

Мережа доступу, довжина якої коливається від декількох сотень метрів до декількох кілометрів, охоплює всі пристрої між магістральною (базовою) мережею й користувацькими терміналами. Її називають "останньою милею".

Оскільки магістральна мережа, як правило, використовує оптичне волокно з високою швидкістю передавання, мережа доступу стала слабким місцем усієї мережної системи. Через відкритість безпроводових каналів виникають конфлікти в часовому, просторовому або частотному вимірі, коли канал використовується декількома користувачами. Функція технологій мережного доступу полягає в керуванні й координації використання ресурсів каналів для забезпечення взаємозв'язку й комунікації декількох користувачів у загальному каналі зв'язку.

Залежно від відстані й швидкості доступу, що існують технології мережного доступу можна розділити на чотири категорії:

- безпроводова локальна мережа (WLAN);
- безпроводова міська мережа (WMAN);
- безпроводова персональна мережа (WPAN);
- безпроводова глобальна мережа (WWAN).

Вимоги до БСМ

У більшості випадків застосування БСМ для IoT необхідно забезпечити надійний зв'язок у режимі реального часу. З погляду енергоефективності низьке енергоспоживання є запорукою тривалого часу безперервної експлуатації автономних пристроїв з живленням від акумуляторів і зниження витрат на технічне обслуговування. Це також є ще однією вимогою при використанні БСМ для IoT.

Прикладами технологій доступу для БСМ в IoT є Bluetooth 4.0 і Bluetooth LE з орієнтацією на медичні БСМ, IEEE 802.15.4e (ZigBee®, WirelessHART, ISA100.11a і WIA-PA створені на базі стандарту IEEE 802.15.4 [5]) з орієнтацією на промислові БСМ; і WLAN IEEE 802.11™ (Wi-Fi) для IoT [6].

15.6 Типові архітектури та топології БСМ

Як правило, БСМ складається з декількох вузлів мережних сенсорів і шлюзу для підключення до Інтернету. Загальний алгоритм розгортання БСМ виглядає в такий спосіб (рис. 15.8) [2]:

1. Розміщення сенсорів у необхідній для контролю параметрів області.
2. Вузли мережі сенсорів включаються (активуються) і передають свої дані іншим вузлам і одержують дані від інших вузлів для виявлення один одного.
3. Вузли сенсорної мережі організовуються в мережу відповідно до певної топології (лінійна, зірка, дерево, комірчаста і т.д.).
4. Підходящі шляхи обчислюються в побудованій мережі для передавання отриманих сенсорами даних.

Енергоживлення вузлів сенсорної мережі, як правило, забезпечується акумуляторами, тому дальність передавання вузлів БСМ невелика. Дальність передавання може становити від 800 до 1 000 метрів у відкритому середовищі за межами приміщення із прямою видимістю. Вона суттєво зменшується у випадку закритого навколишнього середовища в приміщенні приблизно до декількох метрів.

Мережа сенсорів для розширення охопту мережі використовує режим багатоетапного передавання. Тобто вузли сенсорної мережі є одночасно передавачем і приймачем. Перший мережний вузол сенсора, вузол джерела, відправляє дані в сусідній вузол для передавання даних на шлюз. Найближчий вузол пересилає дані одному зі своїх найближчих вузлів, які перебувають на шляху до шлюзу.

Переадресація повторюється доти, поки дані не надійдуть на шлюз. Особливостями БСМ є самоорганізація, самоадаптація, обмежена енергія вузлів і нестабільні за параметрами лінії передавання даних.

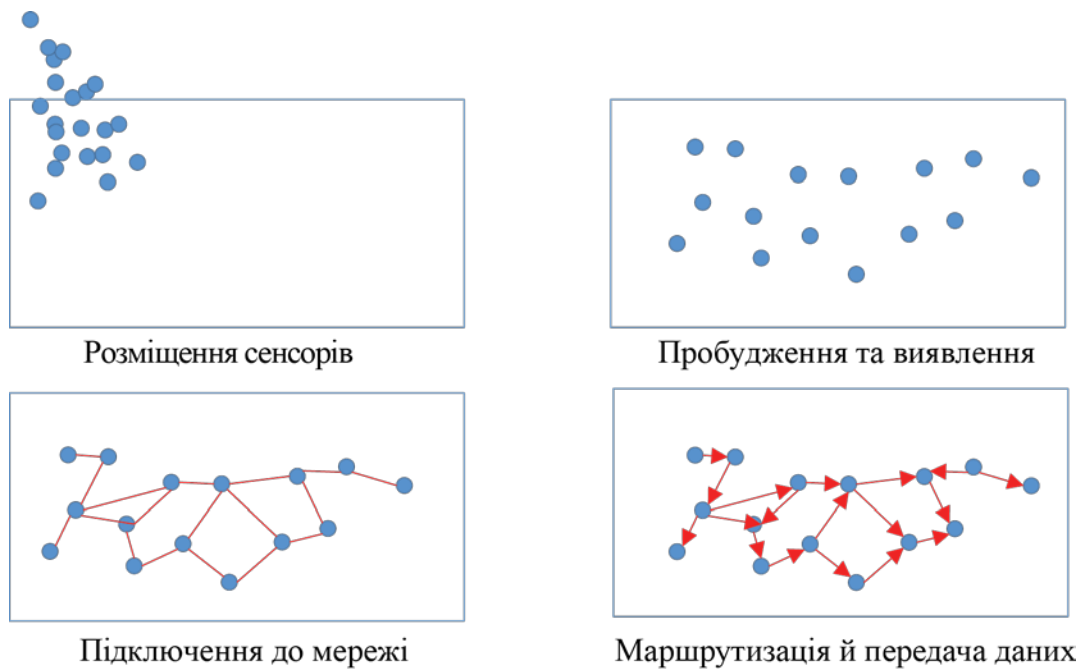


Рисунок 15.8 – Алгоритм розгортання БСМ [2]

На рис. 15.9 наведені приклади побудови топології БСМ з використанням технології передавання даних ZigBee.

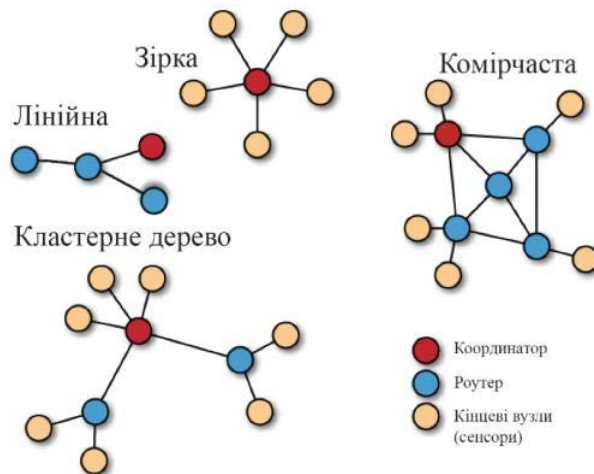


Рисунок 15.9 – Топології, що використовуються у технології ZigBee [2]

У комірчастих мережах вузли БСМ розташовуються у випадковому порядку, а самі вузли можна переміщати і приховувати. Топологія комірчастих мереж має значні переваги по гнучкості й надійності в порівнянні з іншими мережними технологіями. Метод управління мережними вузлами у вигляді самоорганізації

може значно поліпшити надійність мережі, у результаті чого з'явилася розумна технологія комірчастої мережі, як показано на рис. 15.10.

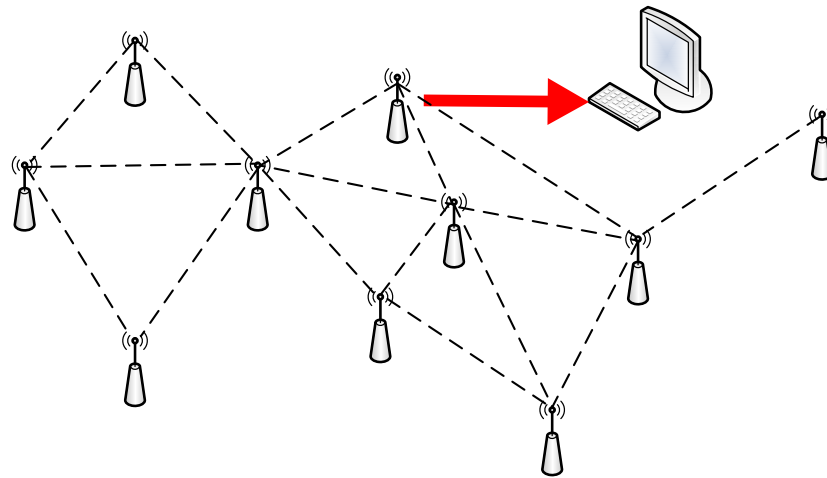


Рисунок 15.10 – Комірчаста мережа, що самоорганізується

У розумних спеціалізованих комірчастих мережах вузол першою справою здійснює моніторинг сусідніх вузлів і вимірює рівень сигналу, а потім вибирає відповідний сусідній вузол для часової синхронізації й відправляє запит з'єднання. Потім сусідній вузол відправляє запит на шлюз. Шлюз приймає запит і виділяє вузлу мережні ресурси. Завдяки комірчастій мережі вузлам мережі сенсорів можуть бути виділено два або більш шляхів передавання сигналів (даних) з метою підвищення надійності мережі. Мереж з синхронізованим за часом комірчастим протоколом (TSMP) мереж сенсорів може надавати підтримку мережі, що самоорганізується, і підтримувати мережу, що складається зі ста вузлів.

15.7 Безпека у безпроводових сенсорних мережах

15.7.1 Загальні зауваження

Питання конфіденційності й безпеки усередині суспільства для кожного індивідуума стає досить складно реалізованими на практиці, оскільки складний ланцюг, у рамках якого були створені умови безпеки, є по суті нескінченним, а сама слабка ланка визначає рівень безпеки всієї системи.

У звичайних мережах TCP/IP система безпеки створюється для захисту конфіденційності, цілісності й доступності мережних даних, забезпечуючи надійність системи і її захист від шкідливих атак, які можуть привести до збоїв у роботі систем і розкриттю інформації.

Безпека БСМ у якості характеристики середовища вузлів і середовища додатків вимагає не тільки традиційного захисту безпеки, але також і наявності особливих вимог відносно захисту, безпеки й конфіденційності (TSP) БСМ-мереж.

Захист, безпека й конфіденційність

Системі TSP БСМ треба здійснювати захист вузлів від несанкціонованого доступу, захист каналів зв'язку й маршрутизації на мережному рівні [6, 7]. Для виявлення атак TSP можуть знадобитися функції реєстрації й перевірки.

Технологія TSP БСМ складається з аутентифікації повідомлень, шифрування, контролю доступу, ідентифікації і т.д. Потреби БСМ у системі TSP повинні бути класифіковані в такий спосіб: безпека вузлів, криптоалгоритми, управління ключами, безпечна маршрутизація, групування даних (рис. 15.11).

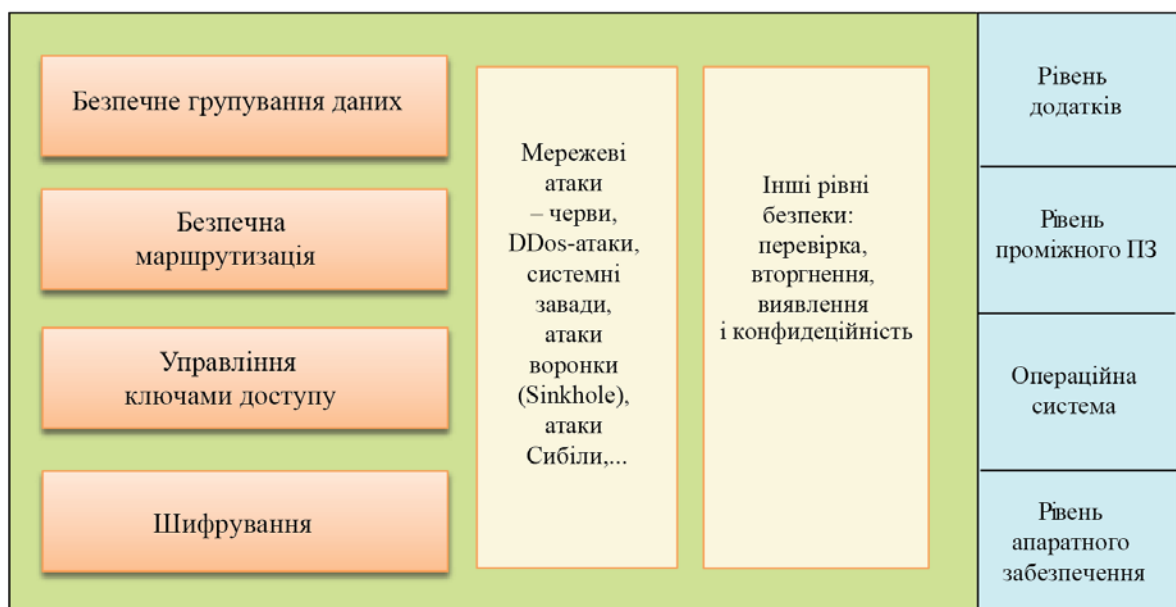


Рисунок 15.11 – TSP-архітектура БСМ-мереж [6]

Безпека вузла й "позбавлення сну"

Вузол БСМ може бути зламаний через його логічні інтерфейси або шляхом прямих фізичних атак. Він може бути переміщений без дозволу або украдений.

Безпека вузла може включати функції безпечного пробудження й безпечного завантаження. Легкий робочий цикл має вирішальне значення для забезпечення тривалого терміну служби вузлів сенсорів з живленням від акумуляторів.

Існують особливі сервісні атаки, так звані "**атаки позбавлення сну**", які перешкоджають переходу вузла сенсора в енергозберігаючий сплячий режим, що, у свою чергу, значно скорочує термін служби вузла, що атакується, сенсора. Стандартні механізми безпеки, такі як коди аутентифікації повідомлень або шифрування груп даних, не можуть запобігти "атакам позбавлення сну": вузол активується, і енергія витрачається на обробку отриманого повідомлення. Атака може бути помічена тільки тоді, коли заряд акумулятора вже був витрачений.

На рис. 15.12 наведено вузол сенсора з радіоприймачем пробудження з низьким енергоспоживанням. Радіоприймач пробудження прослуховує канал, коли вузол сенсора перебуває в сплячому режимі. Він викликає спрацьовування сенсора при одержанні сигналу пробудження. Для підвищення рівня безпеки системи радіо пробудження, сигнал пробудження повинен бути закодованим.

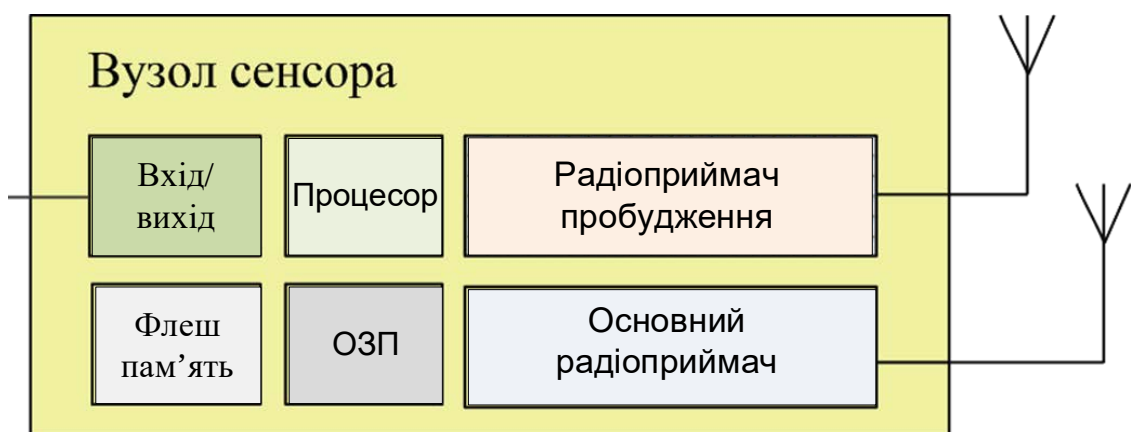


Рисунок 15.12 – Радіоприймач безпечного пробудження

Оскільки код пробудження використовується тільки один раз і, є індивідуальним для кожного вузла, його можна відправляти в незашифрованому виді при пробудженні вузла.

Управління ключами БСМ

У цілому, система управління ключами покликана забезпечити безпеку БСМ. Управління ключами включає генерацію, розподіл, верифікацію, відновлення, зберігання, резервне копіювання, забезпечення дійсності й знищення ключів [6, 8]. Ефективна система управління ключами також є основою інших механізмів безпеки, таких як безпечна маршрутизація, безпечне позиціонування, групування даних. Типові схеми управління ключами в БСМ охоплюють управління ключами загального застосування, управління випадковими ключами, управління ключами місць розташування, управління ключами кластеризації й управління ключами загального користування.

У ході процедури безпечного початкового завантаження створюється безпечна конфігурація вузла сенсора, наприклад, встановлюється ключ з'єднання. Оскільки існує безліч процедур початкового завантаження, і вибір відповідної процедури в значній мірі обумовлений конкретним середовищем, нормальне функціонування мережі сенсорів у значній ступені відділене від початкового завантаження, отже, є можливість змінити процедуру початкового завантаження без яких-небудь змін в архітектурі безпеки для нормальної експлуатації.

Криптографічні алгоритми

Шифрування – це спеціальний алгоритм для зміни вихідної інформації вузла сенсора даних, який не дозволяє неавторизованому користувачеві розпізнати вихідну інформацію при одержанні доступу до зашифрованої інформації [9]. Мережі БСМ державної інфраструктури неминуче зазнають безлічі операцій. Традиційні коди перевірки дійсності повідомлень, симетричне шифрування й шифрування з відкритим ключем показали безліч недоліків. Тому виникла необхідність у новій системі шифрування для БСМ. Іспанська компанія Libelium розробила бібліотеки шифрування **waspmote** для забезпечення безпеки даних БСМ розумного міста в 2010 році. В основному їхні безпроводові сенсорні пристрої

підтримували ці бібліотеки. Бібліотеки призначені для різних механізмів шифрування й механізмів консультацій на рівні каналу передавання даних, рівні мережі й рівні додатка. При цьому, вони розширюють протокол ZigBee®, забезпечуючи його більшу безпеку (рис. 15.13).

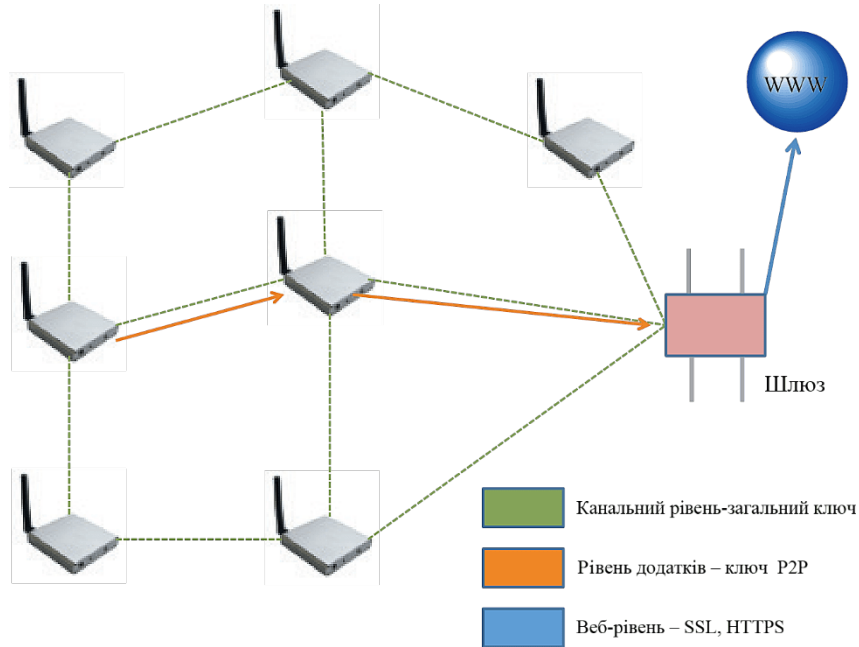


Рисунок 15.13 – Приклади типового використання бібліотек шифрування waspmote [9]

Безпечна маршрутизація БСМ

Оскільки БСМ використовують при передавання даних кілька транзитних шлюзів і самоорганізацію в мережі, кожному вузлу також потрібне виявлення, встановлення та обслуговування маршрутизації. Безпечний протокол маршрутизації являє собою повний розв'язок маршрутизації й може бути необхідною умовою для групування даних і безпечного видалення надмірності від вихідного вузла до сенсора. Захищені маршрутизовані мережі з декількома рівнями захисту були спеціально розроблені для БСМ, їх можна розділити на три групи залежно від структури мережі: лінійна маршрутизація, ієрархічна маршрутизація й географічна маршрутизація.

Управління рівнем доступу до середовища (MAC)

Хоча в рамках цього методу не використовується шифрування, він може забезпечити захист від типових атак, наприклад, неправильної інформації про

маршрутизацію, атаки cesspool і черв'яків (хробаків). Більшість сучасних протоколів безпечної маршрутизації припускають, що мережа сенсорів є стаціонарною, тому є необхідність розробити нові протоколи безпечної маршрутизації для забезпечення мобільності вузлів сенсорів.

Безпечне групування даних БСМ

Безпечне групування даних покликано забезпечити безпеку кожного вузла [9]. Таким чином, загальний алгоритм безпечного групування даних полягає в наступному: перші вузли надають надійні й достовірні дані й передають їх на більші агрегуючі вузли. Більші агрегуючі вузли оцінюють вірогідність даних і проводять розрахунки по групуванню на основі надмірності. Кожний агрегуючий вузол вибирає наступний безпечний і надійний транзитний шлюз і передає дані на центральний вузол. Центральні вузли оцінюють вірогідність даних і здійснюють остаточний розрахунки по групуванню.

Спочатку групування даних використовувалося для економії енергії, а при його здійсненні майже не враховувалися питання безпеки. У цей час безпечне групування даних в основному здійснюється за допомогою аутентифікації й шифрування на основі теорії кластера, кільця й ієрархії. Університет Мюнхена розробив прототип групування даних, який заснований на протоколі DTLS з метою практичного здійснення захищених схем передавання. Жовте коло на рис. 15.14 являє собою їх безпечний прототип групування даних.

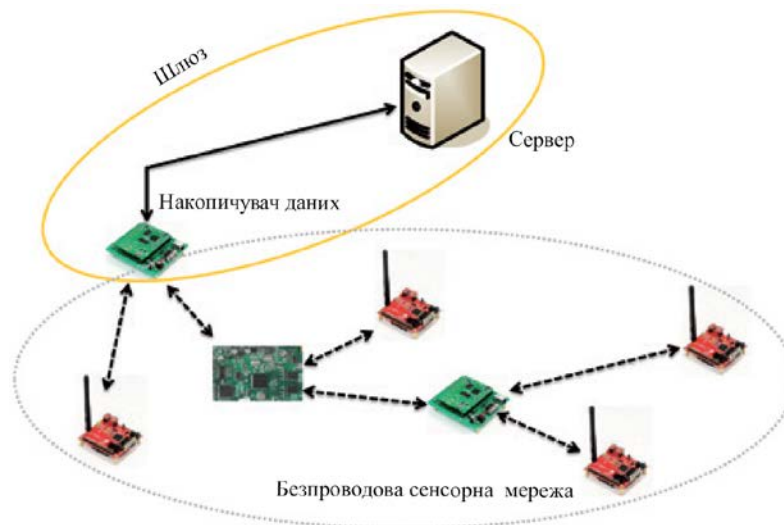


Рисунок 15.14 – Продукти безпечного групування даних [9]

15.7.2 Структура протоколу безпеки

Беручи до уваги обчислювальну здатність, споживання енергії й пропускну здатність каналу зв'язку з вузлами сенсорів, захист конфіденційності й управління ідентифікацією, необхідно провести дослідження в області структури безпеки протоколу, яка буде підходящою й загальною моделлю для кожного рівня БСМ. Оскільки єдиний розв'язок в області безпеки одного рівня не може бути найбільш ефективним розв'язком, цілісний підхід до забезпечення безпеки буде включати всі рівні загальної безпеки в мережі. Його мети спрямовані на підвищення ефективності БСМ у контексті безпеки, довговічності й можливостей підключення. Основний принцип полягає в тому, що витрати на забезпечення безпеки не повинні перевищувати певний рівень ризику для безпеки в певний час.

У цей час є безліч методів забезпечення спеціальної безпеки рівнів в БСМ, таких як безпечне пробудження вузлів, захист від стороннього впливу, аутентифікація й шифрування для мережних рівнів, реєстрація для рівнів додатків [7, 8].

Проте, порядок структурування протоколу інших рівнів і створення загальної інфраструктури протоколу безпеки є серйозною проблемою для досліджень у майбутньому.

У майбутньому буде створена загальна модель, яка може об'єднати всі механізми рівні безпеки разом. Інші механізми дозволять захистити БСМ від атак, навіть якщо на одному якомусь рівні захист буде переборений. Проте, економічна ефективність і енергоефективність можуть як і раніше бути більшими проблемами для розв'язку в рамках досліджень у найближчі роки.

Захист, безпека й конфіденційність

Забезпечення конфіденційності, прав людини на недоторканність приватного життя, безпека даних і цілісність обходиться досить дорого. Питання полягає в наступному: який коефіцієнт витрат і вигід при розгляді переваг, надаваних розв'язком? Чи хоче людина втратити свої права для отримання вигоди.

Компанії Google і Apple змогли одержати більше свободи при роботі з особистими даними в обмін на вигоди, які переважають ризики принаймні, для багатьох споживачів.

Інфраструктура персональних ключів і повноваження компанії, що сертифікує, у рамках необмеженої кількості джерел даних будуть обкладати податком систему, і багато гравців будуть прагнути звести до мінімуму активні заходи безпеки й протидіяти, що винятково фактично мають місце кібератакам таким чином, піддаючи ризику всю систему.

Важливо, щоб максимальна кількість систем функціонували незалежно одна від одної щоб уникнути поразки всіх інших внаслідок уразливості однієї системи. Такий потенційний ефект доміно є найгіршим сценарієм, оскільки погана цілісність даних може привести до помилок, величина яких не була передбачена якою-небудь однієї системою. Ефективність активних систем безпеки буде залежати від розуміння того, що таке "нормальний" кіберфізичний потік даних, однак, це може бути надмірно дорогим заходом, знизивши вигоди або побільшавши витрати на обов'язкові розв'язки IoT.

З метою безпеки структури БСМ мають чотири рівні (рис. 15.15). По-перше, безпека БСМ уразлива для мережних атак через широкомовну природу середовища передавання даних і обмеженості обчислювальних ресурсів вузлів сенсорів, таких як маленька потужність і маленька пропускна здатність. По-друге, управління ідентифікацією й захистом є більш складним і комплексним по своїй суті через глибоку інтеграцію інформаційного простору з фізичним світом і повсюдного доступу до інформаційних технологій. Таким чином, управління ідентифікацією й системи захисти зустрічаються з більшими проблемами. По-третє, динамічні, неоднорідні й масові характеристики моделі сприйняття й обчислення БСМ також є серйозними проблемами для ефективного захисту цілісності системи, цілісності даних, конфіденційності даних, конфіденційності користувачів, таких як ідентифікація, поведінка й навколишнє середовище. Нарешті, оскільки БСМ має велику кількість терміналів, різні типи терміналів і динамічні адаптивні мережні

структури, розмір і складність даних середовища є серйозними проблемами для існуючої системи контролю безпеки [3].

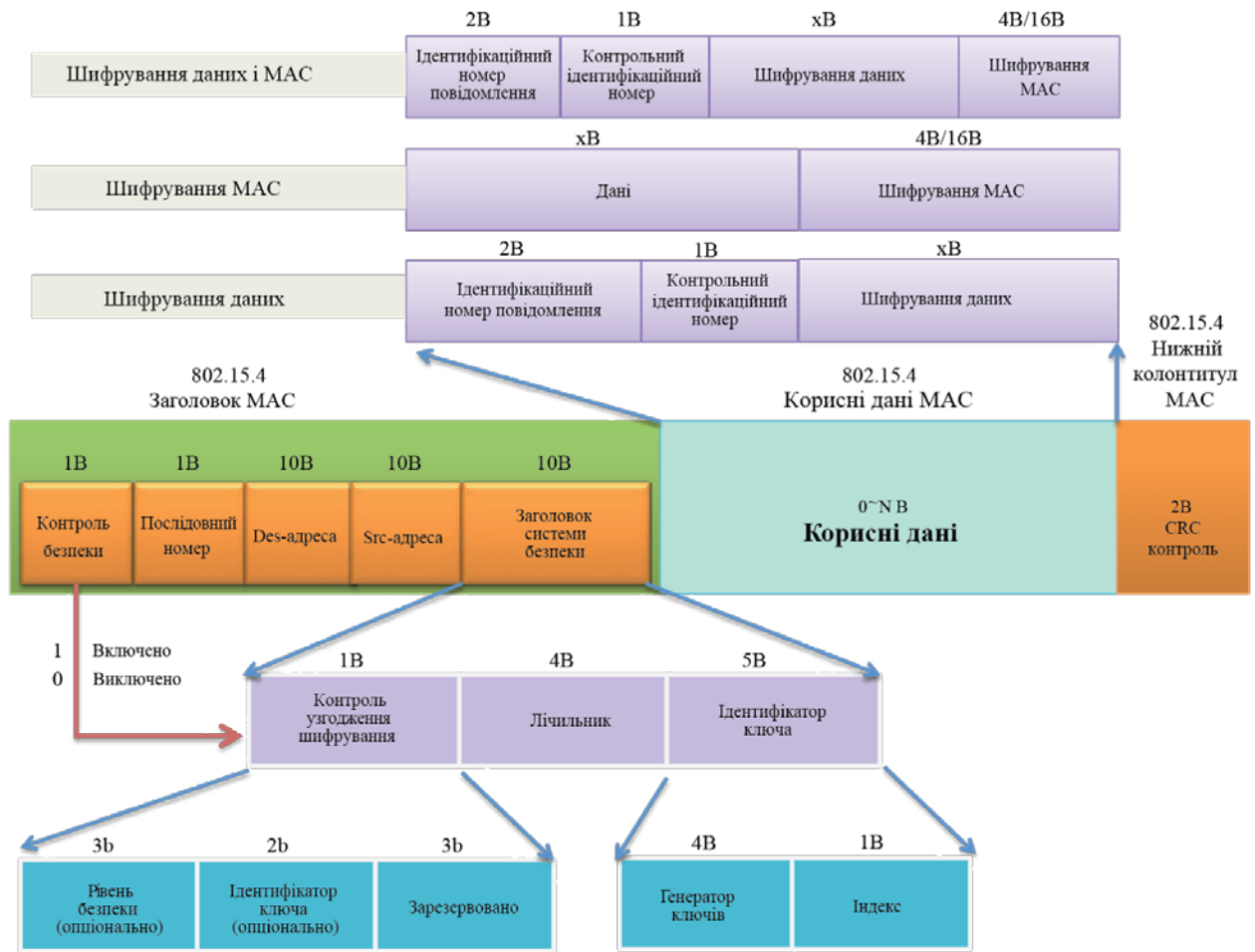


Рисунок 15.15 – Канальний рівень структури протоколу безпеки [3]

15.8 Безпека в мережах Wi-Fi

15.8.1 Загальні зауваження

Для мереж Wi-Fi більшість безпроводових точок доступу постачаються з можливістю ввімкнення одного з чотирьох стандартів шифрування [6]:

- Wired Equivalent Privacy (WEP);
- Wi-Fi Protected Access (WPA);
- WPA2;
- WPA3.

Обираючи між протоколами безпеки безпроводових мереж WEP, WPA, WPA2 і WPA3, експерти сходяться на думці, що WPA3 найкраще підходить для безпеки Wi-Fi. Як найсучасніший протокол шифрування, WPA3 є найбільш безпечним вибором. Однак деякі безпроводові точки доступу не підтримують WPA3. У цьому випадку наступним найкращим варіантом буде WPA2, який сьогодні широко поширений у корпоративному секторі.

Наразі ніхто не повинен використовувати оригінальний протокол безпеки безпроводових мереж WEP або навіть його найближчого наступника WPA, оскільки обидва застаріли і роблять безпроводові мережі вкрай вразливими для зовнішніх загроз.

15.8.2 Протокол безпеки WPA2

Як наступник WPA, стандарт WPA2 був затверджений IEEE у 2004 році як 802.11i [6]. Як і його попередник, WPA2 також пропонує корпоративний і персональний режими. WPA2 замінює RC4 і TKIP двома надійнішими механізмами шифрування та аутентифікації:

1. AES (Advanced Encryption Standard) – механізм шифрування;
2. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) – протокол блочного шифрування з кодом автентичності повідомлення (механізм аутентифікації).

Також для забезпечення зворотної сумісності WPA2 підтримує TKIP як запасний варіант, якщо пристрій не може підтримувати CCMP.

Розроблений урядом США для захисту секретних даних, AES складається з трьох симетричних блокових шифрів. Кожен код шифрує і розшифровує дані блоками по 128 біт, використовуючи 128-, 192- і 256-бітові ключі. Хоча використання AES вимагає більшої обчислювальної потужності від точок доступу і клієнтів, постійне вдосконалення комп'ютерного та мережевого обладнання дало змогу зменшити проблеми з продуктивністю.

CCMP захищає конфіденційність даних, дозволяючи отримувати їх тільки авторизованим користувачам мережі. Для забезпечення цілісності повідомлень використовується код аутентифікації з ланцюжком блоків шифрів.

У WPA2 також реалізовано безперешкодний роумінг, що дає змогу клієнтам переходити від однієї точки доступу до іншої в одній і тій самій мережі Wi-Fi без повторної аутентифікації, використовуючи кешування парних майстер-ключів (PMK) або попередню аутентифікацію.

15.8.3 Протокол безпеки WPA3

У 2018 році Wi-Fi Alliance почав сертифікацію WPA3, найновішого стандарту безпеки безпроводових мереж, який експерти вважають найбезпечнішим [6]. З липня 2020 року Wi-Fi Alliance вимагає, щоб усі пристрої, які бажають отримати сертифікацію Wi-Fi, підтримували WPA3.

Цей протокол практично усунув проблеми атаки KRACK (Key Reinstallation Attacks), які так докучали і докучають протоколу WPA2. Справа в тому, що дані атаки небезпечні тим, що використовують вразливості в самому стандарті Wi-Fi, а не в окремих продуктах чи рішеннях. Це означає, що будь-яка реалізація WPA2 піддається загрозі. Іншими словами, будь-який сучасний пристрій, що підтримує Wi-Fi, є вразливим до атак KRACK, незалежно від виробника або того, якою операційною системою він управляється. А у новому протоколі WPA3 розробникам вдалося усунути вразливість вже на стадії розробки.

Протокол WPA3 Enterprise використовує 192-бітне, а WPA3 Personal 128-бітне шифрування, що підвищує його надійність та стійкість до зломів. Також варто згадати про захист від атак грубої сили – автоматичного блокування при спробі злому пароля за словником та зворотної сумісності з попередніми алгоритмами WPA/WPA2. До того ж, новий WPA3 отримав можливість використовувати більш короткі електронні ключі. Як бачите, змін достатньо, і основний упор зроблений на безпеку шифрування та передачі даних.

Разом із WPA3 Wi-Fi Alliance також представила новий протокол під назвою Wi-Fi Easy Connect, який спрощує процес під'єднання IoT-пристроїв, що не мають візуальних інтерфейсів налаштування, за допомогою такого механізму, як сканування QR-коду.

Нарешті, додаткова функція під назвою Wi-Fi Enhanced Open робить підключення до публічних мереж Wi-Fi безпечнішим, автоматично шифруючи інформацію між кожним клієнтом і точкою доступу за допомогою нового унікального ключа.

На практиці WPA3 є вразливим для загроз. Ванхоеф, експерт із безпеки, який виявив KRACK, і Еяль Ронен, дослідник із Тель-Авівського університету, опублікували кілька нових вразливостей у WPA3 у 2019 році [6]. Так звані вразливості Dragonblood охоплювали дві атаки на пониження класу, під час яких зловмисник змушує пристрій повернутися до WPA2, і дві атаки по побічних каналах, що дають змогу проводити атаки за словником в автономному режимі. Однак Wi-Fi Alliance применшив ризики, заявивши, що виробники можуть легко усунути їх за допомогою оновлення програмного забезпечення. Незважаючи на потенційні вразливості, експерти вважають WPA3 найбезпечнішим протоколом на сьогодні.

Контрольні питання

1. Яка пропускна здатність потрібна для безпроводових сенсорних мереж?
2. Чи залежить пропускна здатність безпроводової сенсорної мережі від призначення сенсорів?
3. Яка швидкість передавання даних потрібна для систем відеоспостереження?
4. Яка швидкість передавання даних потрібна для систем збору даних від датчиків температури, тиску та інших?
5. Для чого потрібна стандартизація в системах безпроводової передачі даних?
6. Чи можна використовувати стільникові мережі для організації сенсорних мереж?

7. У чому полягають недоліки використання стільникових мереж для організації сенсорних мереж?
8. Які основні вимоги до сенсорів безпроводових сенсорних мереж?
9. Для чого будуються самоорганізовані безпроводові сенсорні мережі?
10. Із яких апаратних частин складається сенсорний вузол?
11. Чи залежить дальність зв'язку від розташування сенсорів?
12. Якими методами забезпечують безпеку передавання даних у безпроводових сенсорних мережах?

Перелік посилань

1. NB-IoT vs. LTE-M vs. 5G: порівнюємо популярні технології зв'язку для Інтернету речей. Url: <https://shop-gsm.ua/blog/nb-iot-vs-lte-m-vs-5g-sravniyaem-populyarnye-tehnologii-svyazi-dlya-interneta-veschej/> (дата звернення: 4.07.2024).
2. Christopher Siu IoT and Low-Power Wireless: Circuits, Architectures, and Techniques. – CRC Press, Taylor & Francis Group, 2018. pp. 427.
3. Understanding IoT Networks: A Beginner's Guide. Url: <https://deviceauthority.com/understanding-iot-networks-a-beginners-guide/> (дата звернення: 4.07.2024).
4. Design and Implementation of AquoSense – a Water Quality Sensor System. Url: <https://www.semanticscholar.org/paper/Design-and-Implementation-of-AquoSense-%E2%80%93-a-Water-Monje-Guico/7f3703538530352da93a4e4d9070a8875168205a> (дата звернення: 4.07.2024).
5. IEEE 802.15.4 стандарт. Url: <https://oxorona.com/ieee-802-15-4/> (дата звернення: 4.07.2024).
6. Безпека WiFi: історія небезпеки WEP, WPA і WPA2. Url: <https://e-server.com.ua/uk/poradi/bezpeka-wifi-istoriia-nebezpeki-wep-wpa-i-wpa2> (дата звернення: 4.07.2024).

7. Системи захисту від несанкціонованого доступу. Url: <https://sva.ua/sistemi-zakhistu-vid-nesanktsionovanogo-dostupu/> (дата звернення: 4.07.2024).
8. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Тадждіні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с. DOI: 10.5281/zenodo.2671768
9. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? URL: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms> (дата звернення: 14.10.2024).

16 ТЕХНОЛОГІЇ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ

16.1 Технології мереж з низьким енергоспоживанням

16.1.1 Технологія LORA

16.1.1.1 Загальна характеристика мережі LORA

Однією з важливих характеристик Інтернету речей є тривала робота пристроїв без додаткового обслуговування й заміни джерел живлення. Для ефективного розв'язку завдань, пов'язаних з енергоспоживанням, з'явилися нові типи мереж LPWAN (Low Power Wide Area Networks) [1...5]. Технології, які дозволяють підключати автономні пристрої до глобальної мережі, з'явилися в 2015-2016 рр. і поступово набирають популярність. Найбільш полярними серед таких технологій є LoRa, SIGFOX, NB-IoT, Weightless P та ін. Їхня поява обумовлена необхідністю підключення великої кількості пристроїв обліку й телеметрії для централізованого збору даних.

Розроблювачі LoRa Alliance вважають, що технологія LoRa має значні переваги перед Wi-Fi і стільниковими мережами, завдяки можливості розгортання міжмашинних з'єднань (Machine-to-Machine – M2M) на відстань до 20 км при швидкості до 50 кбіт/с, а також має мінімальне споживання електроенергії, що забезпечує кілька років автономної роботи на одному акумуляторі типу АА. Масштаб застосувань даної технології великий – від домашньої автоматизації й інтернету речей до промисловості й розумних міст.

Суть технології LoRa зводиться до варіації лінійної частотної модуляції (Chirp Spread Spectrum – CSS). Технологія використовує кодування даних широкосмуговими імпульсами із частотами, які зменшуються або збільшуються на деякому часовому інтервалі. Такий розв'язок дозволяє приймачу бути стійким до відхилень частоти від номінального значення й спрощує вимоги до системи.

Система використовує пряму корекцію помилок (Forward Error Correction – FEC) і працює в субгігагерцовому діапазоні частот: 169, 433 і 915 МГц у США, а в Європі – у діапазоні 868 МГц. Найчастіше застосовуються частоти 868 і 915 МГц. Також обмежено використовується робочий діапазон 2,4 МГц.

Швидкість передавання даних у системі LoRa може змінюватись в діапазоні від 0,3 до 50 кбіт/с. Щоб максимізувати час автономної роботи кінцевого пристрою і загальну пропускну здатність мережі, мережна інфраструктура LoRa може управляти швидкістю передавання даних для кожного пристрою індивідуально, використовуючи адаптивну зміну швидкості передавання даних.

У той час як реалізація LoRa є закритою, інша частина стека протоколів, відома як LoRaWAN, залишається відкритою, і її розвиток здійснюється організацією LoRa Alliance, очолюваного IBM.

На рис. 16.1 наведена архітектура LoRaWAN мереж [4]. Класична мережа LoRaWAN складається з наступних елементів: кінцеві вузли (сенсори), шлюзи, сервер мережі й сервер додатків.

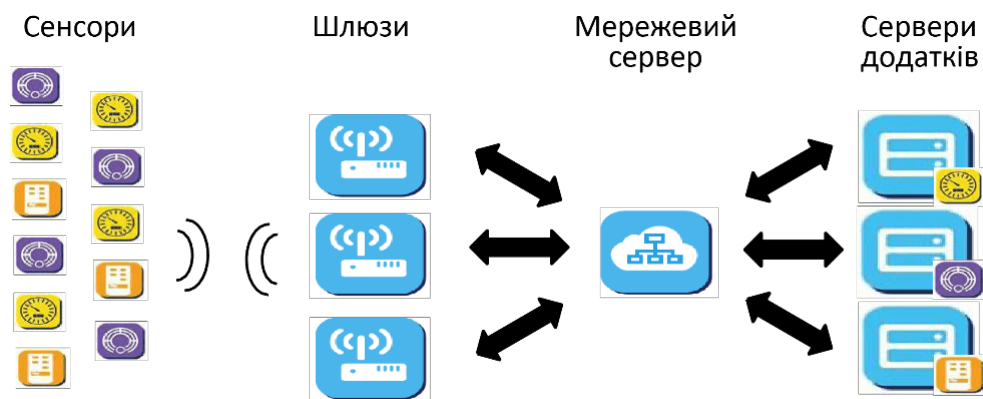


Рисунок 16.1 – Архітектура мережі LoRa [4]

Кінцевий вузол (End-Node) призначений для здійснення керуючих, контролюючих і вимірювальних функцій. Він містить набір необхідних сенсорів і керуючих елементів. Мають, як правило, батарейне живлення. Вузли включають передачу даних лише на деякий проміжок часу (звичайно на 1...5 секунд), по закінченню якого відкривається два часові вікна для приймання даних. Решту часу прийомопередавачі кінцевих вузлів перебувають або в неактивному стані, або в стані приймання, залежно від класу пристрою (A, B або C).

Пристрій, що отримує дані від кінцевого пристрою за допомогою радіоканалу й передає їх у транзитну мережу – шлюз LoRa (Gateway/Concentrator). Транзитними

мережами можуть виступати Ethernet, Wi-Fi, стільникові мережі й будь-які інші телекомунікаційні канали. Шлюз і кінцеві пристрої утворюють мережну топологію типу "зірка". Часто даний пристрій містить багатоканальні прийомопередавачі для обробки сигналів у декількох каналах одночасно або навіть, декількох сигналів в одному каналі. Відповідно, кілька таких пристроїв забезпечують зону покриття мережі й прозору двонаправлену передачу даних між кінцевими вузлами й сервером.

Сервер мережі (Network Server) призначений для управління мережею: завданням розкладу, адаптацією швидкості, зберіганням і обробкою прийнятих даних.

Сервер додатків (Application Server) може віддалено контролювати роботу кінцевих вузлів і збирати з них необхідні дані.

Мережа LoRa звичайно має топологію "зірка", у якій пристрій підключається через шлюзи LoRa, які, у свою чергу, підключені до загального мережевого серверу (Netserver) через стандартні протоколи IP (рис. 16.2) [4].

Технологія LoRa краще підходить для додатків, що вимагають високу швидкість передавання даних (передавання даних на основі розширення спектру). Розвиток технології LoRa підтримується декількома операторами зв'язку.

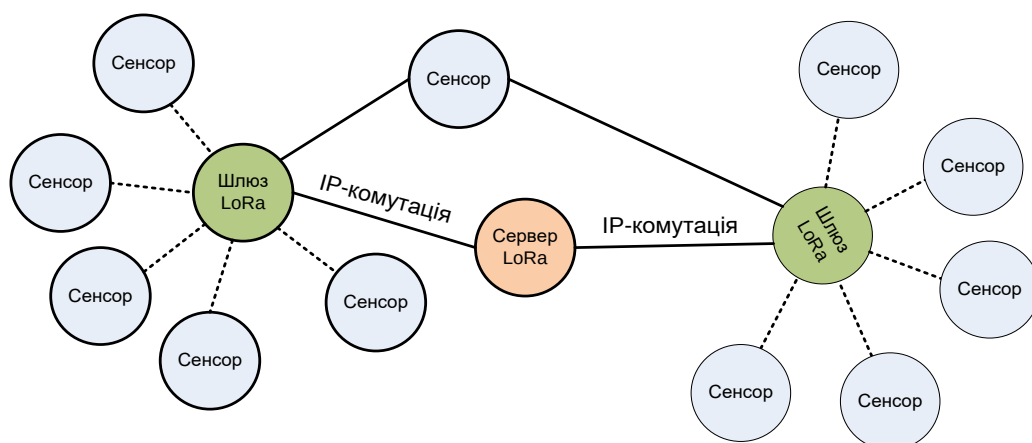


Рисунок 16.2 – Архітектура системи LoRa [4]

В LoRaWAN мережах стандартом передбачене обов'язкове дворівневе шифрування даних двома різними AES-64 і 128 ключами для захисту від

несанкціонованого доступу й спотворення, або перехоплення даних, переданих кінцевими пристроями.

16.1.1.2 Пристрої системи LoRa

Розглянемо параметри головної базової станції (шлюзу) на прикладі LoRaWAN Conduit [6] від компанії Multi-Tech (рис. 16.3).

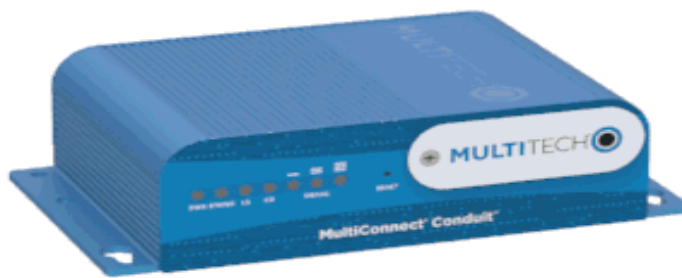


Рисунок 16.3 – Шлюз LoRaWAN Conduit [6]

Основні параметри LoRaWAN Condu наведені у табл. 16.1.

Таблиця 16.1 – Основні параметри шлюзу LoRaWAN Conduit

Параметр	Значення
Процесор	RM9, 400 МГц
Підтримка мереж	3G/LTE
Живлення	9...32 В
Ethernet	Ethernet 10/100 (RJ-45)
USB Host	USB Host (Type A), Micro USB D
Габаритні розміри	161×107×43 мм
Діапазон робочих температур	-30...70 °C
Вартість	14325 грн

Антенa W1063 рекомендована компанією MultiTech для використання з модулями LoRa MTDOT-868 і шлюзами LoRaWAN. Антенa діапазону 868 МГц з

круговою діаграмою спрямованості і посиленням 5 дБ використовується в якості "базової" в системах збору даних при невеликій дальності зв'язку (рис. 16.4) [7].



Рисунок 16.4 – Антена W1063 [7]

Антенa – чвертьхвильовий вібратор з хвильовим опором 50 Ом. Стійка до впливу атмосферних явищ і УФ випромінювання, що забезпечує тривалий термін експлуатації і надійність в роботі. Довжина антени 198,6 мм.

У якості універсального модему розглянемо Вега SH-2 від компанії "Вега-Абсолют", призначений для збору, накопичення і передавання даних в мережу LoRaWAN або LTE NB-IoT [8, 9]. Зовнішній вигляд модема зі знятою кришкою наведено на рис. 16.5 [8].



Рисунок 16.5 – Зовнішній вигляд модема Вега SH-2 зі знятою кришкою і підключеними антенами [8]

Для підключення зовнішніх датчиків в модемі передбачено 2 аналогових і два цифрових входи. Дані, що надходять від зовнішніх пристроїв, зчитуються періодично з налаштованим інтервалом часу 5, 15, 30 хвилин, 1, 6, 12 або 24 години. Отримані дані зберігаються в пам'яті модема у вигляді пакету з зазначенням часу збереження даних і передаються при черговому сеансі зв'язку з мережею LoRaWAN. Інтервал часу між сеансами зв'язку для передавання даних також налаштовується і може мати такі ж значення, як і період зчитування даних. Пам'ять модема розрахована на збереження 100 пакетів даних. У режимі передавання даних спочатку відправляються пакети з найбільш ранніми даними, а потім більш пізні.

Живлення модема здійснюється від вбудованої батареї ємністю 6,4 А·годин. Передбачена можливість підключення двох батарей ємністю 6,4 А·годин або зовнішнього джерела живлення напругою 4,5...55 В.

Час внутрішнього годинника встановлюється автоматично при підключенні до "Vega LoRaWAN Configurator" через інтерфейс USB, а також може бути скориговано через мережу LoRaWAN.

16.1.2 Технологія SIGFOX

SIGFOX є приватною компанією, діяльність якої спрямована на створення всесвітньої мережі, спеціально розробленої для пристроїв IoT [9]. Технологія дозволяє здійснювати передавання даних на великі відстані при малій потужності передавального пристрою й малій ємності батареї. Мережа відмінно підходить для простого і автономного пристрою, який пересилає через мережу обмежений об'єм даних. Мережа SIGFOX схожа на стільникову інфраструктуру (GSM і GPRS-3G-4G), але є більш енергоефективною і в той час менш дорогою. SIGFOX використовує ультра-вузьку смугу частот (Ultra Narrow Band – UNB) на основі радіотехнології для підключення пристроїв до глобальної мережі. Використання UNB – ключовий фактор у забезпеченні дуже низького рівня потужності передавача сенсора, який буде використовуватися [10, 11].

Мережа працює в існуючих неліцензованих діапазонах (ISM – Industrial, Scientific, Medical) у глобальному масштабі й співіснує в цих діапазонах з іншими радіотехнологіями без конфліктів з іншими системами зв'язку. У Європі широко використовується діапазон 868,8 МГц (у відповідності ETSI і CEPT), а в США 915 МГц (як визначено FCC).

Зона охоплення мережі SIGFOX становить близько 30...50 км у сільській місцевості й у міських районах. При зростанні в навколишньому середовищі рівня завад (шуму) зона покриття зменшується до 3...10 км.

На рис. 16.6 представлена топологія мережі SIGFOX. Загальна топологія мережі була розроблена для забезпечення масштабованої, високопродуктивної мережі з дуже низькою витратою енергії, при цьому зберігаючи просту й легку топологію "зірка" на основі комірчастої інфраструктури.



Рисунок 16.6 – Топологія мережі SIGFOX [10]

В SIGFOX вузли можуть використовуватися у двох конфігураціях:

- режим P2P – прямі зв'язки між вузлами (інтерфейс LAN);
- гібридний режим – SIGFOX/P2P (P2P + GW у мережі SIGFOX).

У режимі P2P, вузли можуть з'єднуватися безпосередньо між собою й відразу відправляти повідомлення. При цьому відправлення буде безкоштовне, тому що передавання даних відбувається без транзитного каналу, за який треба платити. Це корисно, тому що можна створити вторинні мережі в будь-який час і немає необхідності міняти прошивання, досить тільки використовувати спеціальні команди поточної бібліотеки.

У гібридному режимі використовується комбінація SIGFOX і P2P режимів, що дозволяє відправляти тільки певні повідомлення через мережу. У цьому випадку використовується один вузол як шлюз мережі (режим P2P + SIGFOX), а інші вузли в режимі P2P.

SIGFOX з ETSI (European Telecommunications Standards Institute – Європейський інститут стандартизації електрозв'язку) визначили, що один пристрій може в день відправити до 140 повідомлень, при цьому одне повідомлення повинне містити максимально 12 байт корисної інформації [12]. Було встановлено, що ці 12 байт покривають потреби пристроїв, які передають такі дані, як інформацію про споживання енергії, місце розташування пристрій, сигнал тривоги й інші основні типи інформації від сенсорів [9].

Також можливо передавати до 4 повідомлень, що складаються із 8 байт корисної інформації в добу убік кожного пристрою. Ці 8 байт дозволяють відправити дані конфігурації, а також оптимізувати термін служби акумулятора. Цього буває досить у випадку, якщо не потрібно повноцінний двосторонній зв'язок. Пристрій, щоб одержати повідомлення, повинен запросити дані із сервера, на якому завчасно повинен бути запрограмований певний час, або конкретна подія.

Технологія використовує шифрування AES з HMACs із закритим ключем, який вбудований у пристрій, плюс деякий порядковий номер.

Технологія SIGFOX спрямована на низьку вартість пристроїв, де потрібна широка зона покриття. Є цілий ряд додатків, які потребують цієї технології безпроводового зв'язку. Області, у яких можуть бути використані мережі SIGFOX включають:

- домашні й споживчі товари;

- енергетичні комунікації, зокрема, інтелектуальний облік;
- охорону здоров'я;
- транспорт, включаючи управління;
- вибірковий моніторинг і контроль;
- роздрібні точки продажу, зберігання і т.д.;
- системи безпеки.

Стандарт має ряд переваг у порівнянні з іншими базовими технологіями LPWAN-мереж. Це більша зона покриття; висока проникаюча здатність; до 20 років роботи сенсора від 2-х батарей АА, тобто наднизьке енергоспоживання; низька вартість.

Як і всі технології сучасного світу, енергоефективна технологія SIGFOX також має й негативні характеристики:

- низька швидкість передавання даних;
- залежність від стільникової інфраструктури;
- обмежена завадостійкість;
- потрібна наявність мереж SIGFOX у регіоні.

У цей час технологія охоплює Францію, Іспанію, багато міст Великобританії, Нідерландів, Бельгії, Португалії, Ірландії, Люксембургу, багато великі європейські міста, і деякі міста в США, Австралії та Новій Зеландії. SIGFOX мережі планується впроваджувати в 60 країнах.

В Україні, як і в усіх інших країнах, SIGFOX працює через ліцензованих партнерів – операторів національних мереж. Компанія UTILIX.ONE [13], яка працює під брендом Sigfox Ukraine розпочала розвиток української мережі Sigfox наприкінці 2020 року.

Всі 75 операторів, як наприклад Sigfox Ukraine – незалежні від Sigfox SA і є власниками своїх національних мереж у власних країнах.

Спільнота операторів об'єдналась в асоціацію 0G United Nations, яка продовжує надавати локальні послуги в глобальному масштабі своїм клієнтам та партнерам.

16.1.3 Технологія NB-IoT

NB-IoT (Narrow Band IoT – "вузькосмуговий Інтернет речей"), він же стандарт LTE-Cat.M2, має ряд достоїнств: широка зона охоплення, швидка модернізація існуючої мережі, низьке енергоспоживання, що гарантує термін служби батареї 10 років, низьку вартість термінала, просте підключення, підвищену надійність і високу безпеку мережі.

NB-IoT дозволяє сучасним операторам працювати із традиційними напрямками IoT, такими як інтелектуальні системи обліку, системи відеоспостереження, завдяки ультранизькій вартості, а також відкриває більше можливостей для використання IoT в промисловості, в "розумному місті", в системах електронної охорони здоров'я [3, 14].

Технологія NB-IoT в першу чергу призначена для додатків M2M. Стандарт NB-IoT був специфікований угодою 3GPP в Release 13 (LTE Advanced Pro) і з 2016 р. по теперішній час він проходить тестування.

На рис. 16.7, наведено дев'ять галузей, у яких існує великий потенціал ринку для використання технології NB-IoT.

Сільське господарство	Торгівля	Системи безпека та охорони
Автомобільний транспорт та логістика	Енергетика та ЖКХ	"Розумне місто"
Медицина	Промисловість	"Розумний будинок"

Рисунок 16.7 – Перспективні галузі для використання технології NB-IoT

Приклади використання технології NB-IoT:

- інтелектуальний облік (електрика, газ і вода);

- охоронно-пожежна сигналізація для будинків і комерційних об'єктів;
- прилади для виміру параметрів здоров'я;
- відстеження людей, тварин або предметів;
- розумні міські інфраструктури, такі як вуличне освітлення або система контролю й обліку транспортних засобів;
- підключення промислових приладів, таких як зварювальні апарати або повітряні компресори.

На рис. 16.8 схематично показані функціональні можливості та основні достоїнства технології NB-IoT.



Рисунок 16.8 – Функціональні можливості та основні достоїнства технології NB-IoT

У порівнянні з іншими технологіями LPWAN такими, як E-MTC, SIGFOX, LoRa, технологія NB-IoT забезпечує більш високу продуктивність. Крім того, з погляду мережних інвестицій, сценаріїв покриття, трафіка вхідної й вихідної ліній зв'язку й надійності мережі, можна зробити висновок, що NB-IoT є найбільш підходящою технологією.

Відомо, що оператори мобільного зв'язку по усьому світу використовують смугу частот 900 МГц для GSM через велику зону покриття. Це пояснюється тим, що сигнали у цій смузі частот мають більший радіус поширення, і це, як правило, поліпшує проникнення і в приміщенні. Існує значне число комерційних мереж UMTS і LTE, які в цей час працюють у діапазоні частот 900 МГц.

В 3GPP були запропоновано 3 сценарії для розгортання LPWAN NB-IoT: Guard Band (захисна смуга), In Band (у смузі частот) і Standalone (автономний), що наведені на рис. 16.9.

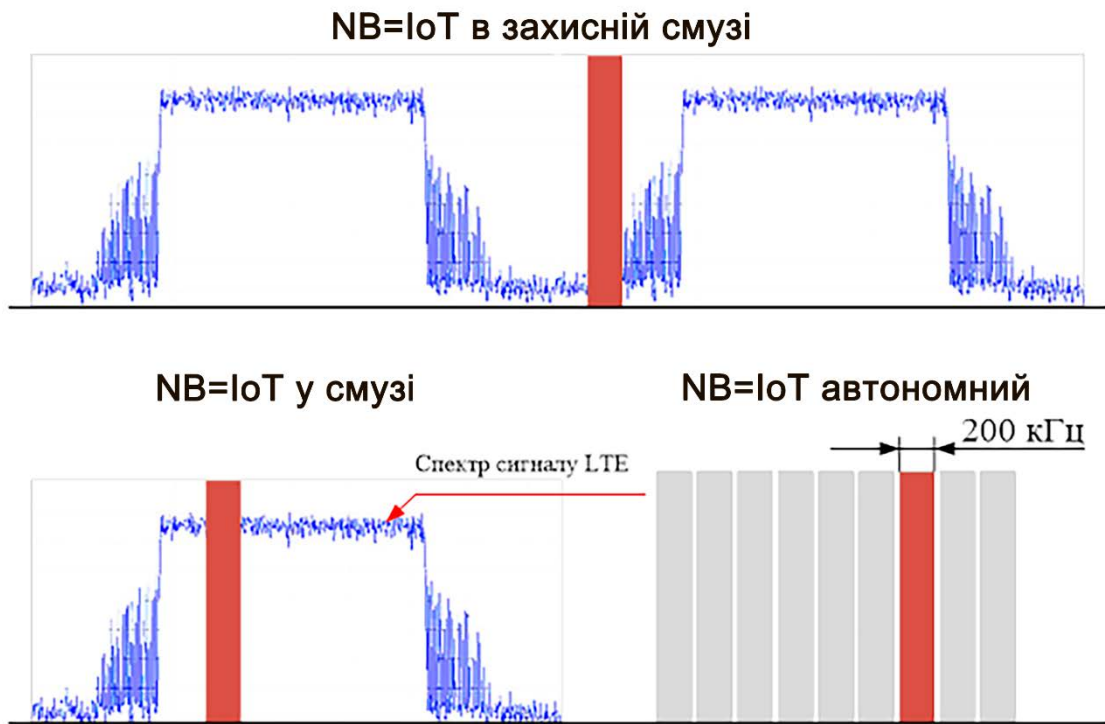


Рисунок 16.9 – Сценарії розгортання мереж NB-IoT

Таким чином, мережу NB-IoT можна розгорнути в частотних діапазонах, у яких функціонують мережі стандарту GSM або в "захисних" інтервалах між сигналами мереж GSM і LTE. Швидкість передавання даних в NB-IoT досягає 200 кбіт/с, що є достатнім для пристроїв, що періодично передають одностипні дані невеликого обсягу.

16.1.4 Технологія Weightless P

Розробку стандарту Weightless просуває компанія Ubiik. Weightless – являє собою відкритий стандарт для мереж LPWAN підвищеної потужності, призначеної для підвищення продуктивності сенсорної мережі [15]. У спеціальній групі інтересів Weightless (Special Interest Group – SIG) пропонується три різні

протоколи: Weightless-H, Weightless-W і Weightless-P, які підтримують різні форми й варіанти використання [15].

Weightless-W це відкритий стандарт призначений для роботи в частотах телевізійного діапазону (TV White Space – TVWS). Weightless-W добре підходить для використання в нафтовій і газовій галузі.

Weightless-N забезпечує надзвичайно широку зону покриття але меншу швидкість передавання інформації та зв'язок тільки в одному напрямку. Weightless-N зумовлює низьке енергоспоживання пристроїв мережі. Підходить для сенсорних мереж сенсорів контролю температури, рівня рідини в резервуарах, вимірів параметрів, що змінюються з малою швидкістю.

Weightless-P це вузькосмугова технологія LPWAN для IoT з високою щільністю кінцевих пристроїв, з довгостроковою службою батарей і двонаправленим зв'язком. Особливостями цієї технології є масштабованість, оптимізація висхідної й низхідної ліній зв'язку, широка зона покриття, тривалий термін служби батарей й висока безпека мережі. Weightless-p є найбільш масштабованою технологією LPWAN. Одна базова станція Weightless-P підтримує більше пристроїв, чим будь-яка інша технології LPWAN. Висока ємність базових станцій мінімізує витрати на розгортання.

Можна виділити десять основних характеристик Weightless-P [15]:

- технологія вузькосмугова (12,5 кГц на канал);
- оптимізація підтримки планового і позапланового трафіку (у стандарті TDMA/FDMA);
- спектрально-ефективна модуляція OQPSK;
- працює у всіх діапазонах звільнених від ліцензування ISM діапазонах частот для глобального розгортання: 169 / 433 / 470 / 780 / 868 / 915 / 923 МГц;
- можливість роумінгу;
- зона покриття до 2 км у міському середовищі;
- малий час-синхронізації базових станцій для ефективного планування ресурсів і використання радіоефіру;
- можливість спільного використання інфраструктури;

- адаптивна швидкість передавання даних від 200 біт/с до 100 кбіт/с;
- контроль потужності передавача сенсора для зменшення перешкод й збільшення пропускної здатності мережі.

Ресурси в субгігагерцовому неліцензуємому діапазоні частот обмежені й трафік від інших технологій неухильно росте. Тому Weightless-P використовує вузькосмуговий 12,5 кГц канали, що дає можливість передавати в 7 раз більше даних, чим SIGFOX, і в 98 раз більше даних, чим LoRaWAN у міських умовах. Синхронні мережі означають, що кожен пристрій й базова станція точно знає, коли говорити, а коли слухати.

Низька затримка, двонаправлений зв'язок між кінцевими пристроями й базовою станцією забезпечує високу надійність мережі і її продуктивність.

16.2 Порівняння технологій мереж далекого радіуса дії LPWAN

Порівняння основних характеристик технологій мереж далекого радіуса дії наведено в табл. 16.2 [16]. Як випливає з таблиці, технології забезпечують високу дальність зв'язку, підвищену перешкодозахищеність, низьку швидкість передавання даних, низьке енергоспоживання і, як наслідок, високий ступінь автономності кінцевих пристроїв.

По незалежній оцінці стану й перспективного розвитку глобальних мереж з низьким енергоспоживанням для ринку Інтернету речей на найближчі 1...2 роки найбільш затребуваною технологією буде LoRaWAN і, ймовірно, SIGFOX. Надалі можна буде очікувати спільне використання пристосованих для IoT технологій 3GPP (наприклад, LTE-M) і діючих технологій LPWAN.

Таблиця 16.2 – Порівняння технічних характеристик мереж далекого радіуса дії LPWAN

Технічні характеристики	LoRa	SIGFOX	NB-IoT	Weightless P
Метод модуляції	CSS	–	OFDMA/DSSS	FDMA / TDMA
Діапазон частот	ISM	ISM	Ліцензований	ISM
Швидкість	0,3...50 кбіт/с	100 біт/с	UL: 1...144 кбіт/с DL: 1...200 кбіт/с	0,2...100 кбіт/с (адаптивна)
Ширина смуги частот, кГц	Широка, до 500	Вузька, 100	Вузька, 200	Вузька, 12,5
Час автономної роботи	> 10 років	–	До 10 років	3...5 років
Діапазон частот, МГц	868,8 (Європа), 915 (США), 433 (Азія)	868,8 (Європа) 915 (США)	700/800/900	169/433/470/ 780/868/915/923
Шифрування	AES-64 і 128 біт	AES з HMACs	–	AES-128/256
Дальність зв'язку, км	До 2,5 у місті, до 45 поза містом	До 10 у місті, до 50 поза містом	–	До 2 у місті
Підтримка	LoRa Alliance, IBM, Cisco, Actility, Semtech та ін.	Sigfox, Samsung	3GPP, Ericson, Nokia, Huawei, Intel та ін.	Ubiik Weightless SIG

16.3 Мережа на основі HART-протоколу

Обмін інформацією між двома пристроями (типу "точка-точка") є найбільш типовим застосуванням HART-протоколу [17]. Однак HART-пристрої можуть бути об'єднані в мережу. Для цього використовують тільки цифрову частину HART-протоколу, без аналогової, а інформація передається у формі напруги, що дозволяє з'єднувати HART-пристрої паралельно. Максимальна кількість пристроїв у мережі може становити 15, якщо не використовувати HART-повторювачі (ретранслятори). HART-мережа може мати довільну топологію, оскільки при малих швидкостях передавання (1200 біт/с) ефектів, характерних для довгих ліній, не виникає. Цим же пояснюються вкрай низькі вимоги до смуги пропускання кабелю (2,5 кГц за рівнем -3 дБ). Такій смузі відповідає постійна часу лінії передавання 65 мкс, тобто при опорі лінії 250 Ом її ємність може досягати 0,26 мкФ, що відповідає довжині кабелю близько 2...3 км (табл. 16.3).

Таблиця 16.3 – Залежність довжини кабелю від погонної ємності

Кількість пристроїв у мережі	Довжина кабелю при погонній ємності			
	65 пФ/м	95 пФ/м	160 пФ/м	225 пФ/м
1	2800 м	2000 м	1300 м	1000 м
5	2500 м	1800 м	1150 м	900 м
10	2100 м	1600 м	1000 м	750 м
15	1800 м	1400 м	900 м	700 м

У мережі можуть бути два ведучих пристрої, одним з яких є контролер, другим ручний комунікатор, використовуваний для зчитування показань і установки параметрів HART-пристроїв. Комунікатор може бути підключений у будь-якому місці мережі, але звичайно доступними є тільки клеми сенсорів або комутаційні клеми в монтажній шафі. На рис. 16.10 наведено приклад підключення HART-пристроїв.

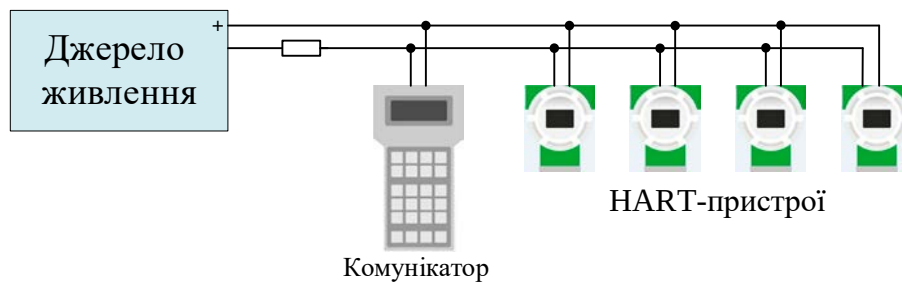


Рисунок 16.10 – Приклад підключення HART-пристроїв

Мережа допускає гарячу заміну або додавання нових пристроїв (тобто без відключення живлення). У випадку збою, наприклад, при випадковому короткому замиканні, мережа повторює невиконані операції обміну.

В HART-мережі тільки один вузол може посилати сигнал, у цей час інші "слухають" лінію. Ініціює процедуру обміну ведуче обладнання (контролер або ручний комунікатор). Відомі одержують команду й посилають відповідь на неї. Кожне ведене обладнання має персональну мережну адресу, яка включається в повідомлення ведучого пристрою. Адреса має довжину 4 біта ("коротка адреса")

або 38 біт ("довга адреса"). Є також другий спосіб адресації за допомогою тегів (ідентифікаторів, призначуваних користувачем).

16.4 Безпроводова технологія WirelessHART™

Безпроводова технологія HART (WirelessHART™) перший безпроводовий стандарт, найбільше широко розповсюджений і використовуваний в області автоматизації технологічних процесів [18, 19]. Розроблений фондом HART COMMUNICATION FOUNDATION (фонд HART-комунікації – HCF) і підтримуваний багатьма членами фонду HART-комунікації, включаючи компанію Pepperl+Fuchs, стандарт опубліковано у вересні 2007 р. Перші прототипи продукції були представлені на виставках ISA Show 2006 у Х'юстоні.

Поширенню і розвитку протоколу WirelessHART сприяють дві причини.

Перша – ринку потрібна безпроводова альтернатива проводовому HART, здатна забезпечити функції виміру, контролю, управління технологічним процесом і передавати всю необхідну інформацію надійно й безпечно.

Друга причина – необхідність забезпечити доступ до додаткової діагностичної й вимірювальної інформації, яка присутня в більш ніж 32 млн. HART-пристроїв, установлених по усьому світу, але залишається недоступною.

За основу безпроводових розв'язків, побудованих на базі відкритого протоколу WirelessHART, взяті технології мереж, що самоорганізуються (mesh). Тобто налаштування параметрів передавання відбувається автоматично з мінімальною участю користувача (рис. 16.11) [14].

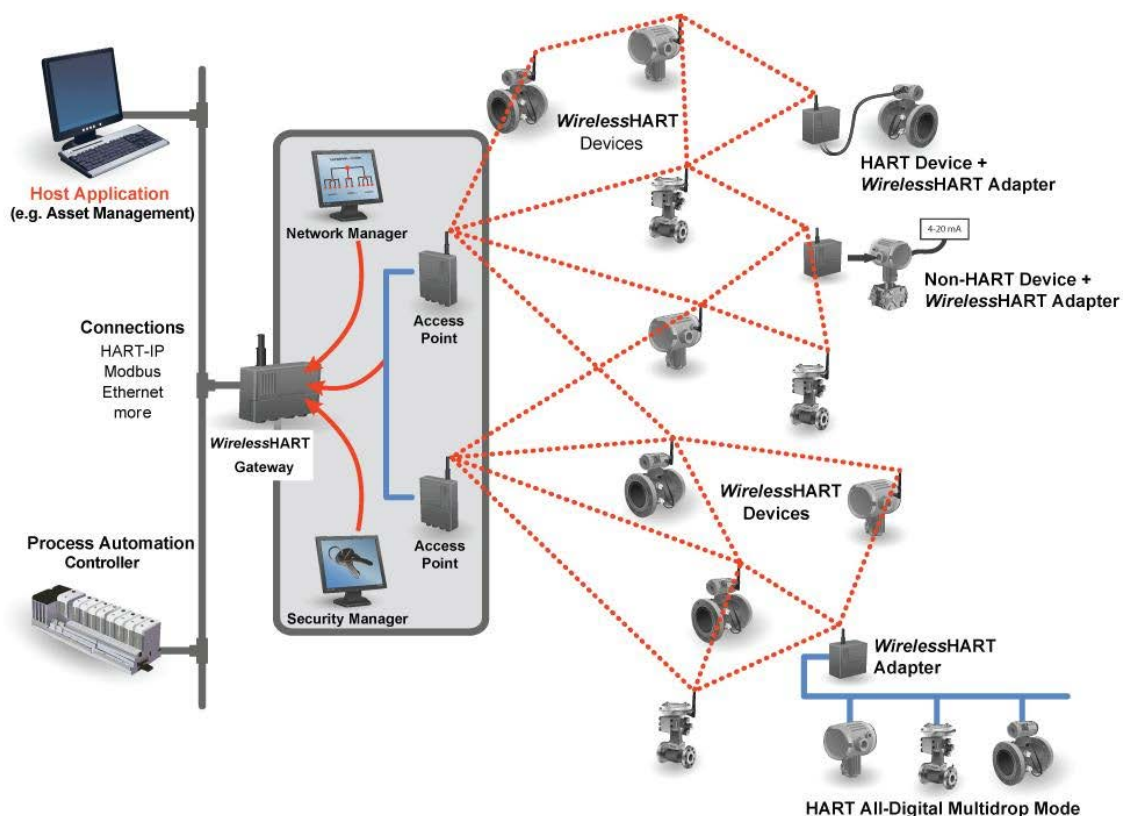


Рисунок 16.11 – Безпроводова мережа WirelessHART пропонує більш високу безпеку передавання даних внаслідок використання альтернативних і резервованих каналів передавання [14]

HART-пристрої працюють у неліцензуюемому діапазоні 2,4 ГГц.

На рис. 16.12 і 16.13 [21] показані приклади сенсорів з безпроводовими адаптерами, а на рис. 16.14 – адаптер безпроводового зв'язку для мереж HART.



Рисунок 16.12 – Ультразвуковий сенсор рівня із встановленим адаптером WirelessHART [22]



Рисунок 16.13 – Сенсори витрати з безпроводовими адаптерами [22]



Рисунок 16.14 – Безпроводовий адаптер Siemens [22]

16.5. Технологія безпроводового зв'язку ZigBee

Розглянемо WPAN-мережі, зокрема, мережі ZigBee та стандарт IEEE 802.15.4. Безпроводова персональна обчислювальна мережа WPAN являє собою локальну мережу з невеликим радіусом дії 15...20 м, і призначена для заміни кабельних з'єднань між персональними комп'ютерами, а також для зв'язку з різноманітною периферією та мультимедіа-системами (КПК, принтери, факси, сканери стереосистеми і т. д.) [23]. Відповідно для обміну інформацією між такими системами необхідна висока швидкість передавання даних, що й забезпечують стандарти специфікацій Wi-Fi і Bluetooth.

Але існує велика кількість систем (різноманітні сенсори, системи збору інформації і т.д.), які мають специфіку, внаслідок якої в такого роду додатках

неможливо ефективно використовувати згадані вище технології. Для реалізації подібних задач був розроблений стандарт IEEE 802.15.4 (ZigBee) для низькошвидкісних WPAN-мереж (рис. 16.15).

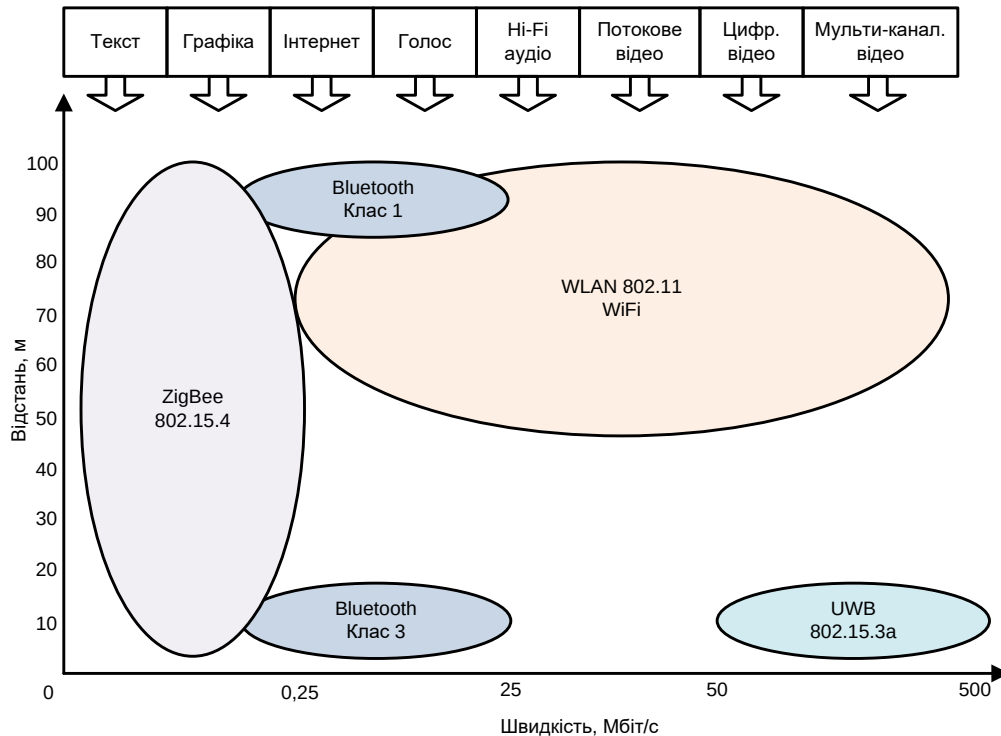


Рисунок 16.15 – Класифікація основних безпроводових стандартів [24]

Технологія ZigBee займає раніше відсутній тип радіоінтерфейсів, замість якого використовували системи і технології з більш високими технічними характеристиками і, відповідно, більш дорогі, або рішення, які ґрунтуються на окремих мікросхемах радіотрансиверів різних виробників електронних компонентів, що не мають під собою жорстко стандартизованої бази.

Розробники вимушені були йти на підвищення витрат при розв’язанні простих задач або створювати свої протоколи передавання та програмні стеки для організації персональних безпроводових мереж, що також відображалось на вартості кінцевого виробу і строках виходу готового продукту на ринок. В результаті часто втрачалась новизна та інтерес ринку до продукції.

В табл. 16.4 наведені порівняльні характеристики деяких безпроводових мереж [25].

Таблиця 16.4 – Порівняння стандартів сімейства 802.15 та 802.11b

Стандарт	802.15.4 ZigBee			802.15.1 Bluetooth	802.15.3 High Rate WPAN, WiMedia	802.15.3a UWB	802.11b Wi-Fi
Додатки	Моніторинг, управління, мережі сенсорів, автоматика			Голос, дані, заміна кабелю	Потокове мультимедіа, заміна кабелів аудіо/відеосистем		Дані, відео, ЛВС
Переваги	Ціна, енергозбереження, розміри мережі		+	Ціна, енергозбереження, передавання голосу, перескоки частоти	Висока швидкість, енергозбереження		Швидкість, гнучкість
Частота, ГГц	0,868	0,915	2,4			3,1...10,6	2,4
Макс. швидкість	20 кбіт/с	40 кбіт/с	250 кбіт/с	1...24 Мбіт/с (в залежності від версії)	22 Мбіт/с	110, 200, 480 Мбіт/с (в залежності від відстані)	11 Мбіт/с
Вих. потуж., дБп	0			0 (клас 1) 4 (клас 2) 20 (клас 3)	0	< 20 (110 Мбіт/с) < 22 (200 Мбіт/с)	20
Відстань, м	10 - 100			10 (клас 3) 100 (клас 1)	5 - 50	10 (110 Мбіт/с) 4 (200 Мбіт/с)	100
Чутливість, дБп	- 92		-85	-70	-75	–	-76
Розмір стека, КБ	4...32			>250	–		>1000
Строк служби батареї, днів	100...1000+			1...7	теоретично більше 1000		0,5...5
Розмір мережі	216 або 264			майстер +7	до 127 на хост		32

Стандарт 802.15.4 дозволяє створювати мережі з багатокомірковою технологією, таким чином обслуговуючи надзвичайно велику кількість вузлів і збільшуючи відстань зв'язку без додаткових витрат на підсилювачі потужності.

Технологія ZigBee не призначена для передавання великих об'ємів інформації, як Wi-Fi чи Bluetooth. Але для передавання, наприклад, показів лічильників, сенсорів, об'єм яких рідко перевищує десятки байт, не потрібно великих швидкостей – в цьому випадку обов'язкові високі показники по енергозбереженню, ціні та надійності. Більшість пристроїв ZigBee працюють за наступним алгоритмом: пристрій знаходиться в режимі очікування майже весь час, забезпечуючи оптимальний режим енергозбереження; при надходженні нової інформації або під час чергового сеансу зв'язку пристрій активується, швидко передає інформацію і знову переходить в режим енергозбереження.

Типові часові затримки при цьому складають 30 мс для підключення нового пристрою до мережі, 15 мс для переходу з режиму очікування в активний стан і стільки ж часу для доступу до каналу. Так вдається збільшити строк служби батарей до 10 років і більше в залежності від типу додатка і тривалості робочого циклу, при цьому струм при передаванні може складати 15-30 мА, а в режимі очікування – менше 2 мкА.

В результаті, затримки по виклику настільки малі, що людина, яка, наприклад, заходить в кімнату і натискає на вимикач безпроводового зв'язку ZigBee, навіть не помітить, що світло з'являється майже миттєво, в той час як затримки при підключенні пристроїв до мережі Bluetooth складають близько 3 с.

Технологія ZigBee повністю задовольняє всім вимогам для систем дистанційного контролю та управління промисловими і побутовими об'єктами:

- стабільний надійний двосторонній зв'язок;
- відстань роботи: від 10 м і більше;
- робоча частота в неліцензійному діапазоні;
- малі фізичні розміри;
- виконання на одному кристалі;
- низьке енергоспоживання;
- низька вартість.

Крім цього, як впливає з табл. 16.4 пристрої ZigBee поєднують найменшу потужність передавачів з найбільшою чутливістю приймачів в порівнянні з іншими конкурентами. Така комбінація дає очевидний позитивний ефект – мінімальне опромінення людей, що знаходяться в зоні обслуговування мережі. Таким чином, ZigBee можна вважати одним з найбільш безпечних та екологічних на сьогодні безпроводових стандартів.

Перспективною сферою застосування стандарту є безпроводові системи зчитування показів різних лічильників, оскільки відпадає необхідність щомісяця перевіряти їх. Також технологія надає великі можливості для промислових систем контролю різних процесів. Наприклад, в сфері добування та транспортування нафти використовуються тисячі сенсорів. Надзвичайно дорого вести сигнальний

провід від кожного з них окремо. Ціна одного сенсора з кабелем може досягти 150\$, в той час як ціна недорогого безпроводового рішення складає близько 5\$.

Прикладом інформаційної системи на базі безпроводової технології може бути система обліку показань лічильників води та електроенергії в багатоповерховому будинку. Система складається з кінцевих автономних пристроїв (мікроконтролер та модем ZigBee підключаються до лічильників води у кожній квартирі), поверхових маршрутизаторів з мережевим живленням, які також мають входи для лічильників електроенергії, а в підвалі знаходиться будинковий контролер, який збирає інформацію з усіх маршрутизаторів та передає інформацію в диспетчерський пункт по каналу Ethernet.

Встановлення на кожному поверсі свого маршрутизатора дозволяє системі обрати оптимальний шлях передавання повідомлень, а також обійти несправну ділянку мережі.

Простою системою автоматизації можна обладнати звичайну квартиру. Навіть невеликі можливості у вигляді індикації, яка повідомляє про ввімкнене світло, відкриті вікна при виході з будинку, автоматичне ввімкнення світла при вході в приміщення, сенсори води на підлозі у ванній чи туалеті. Приклад такої системи наведено на рис. 16.16.

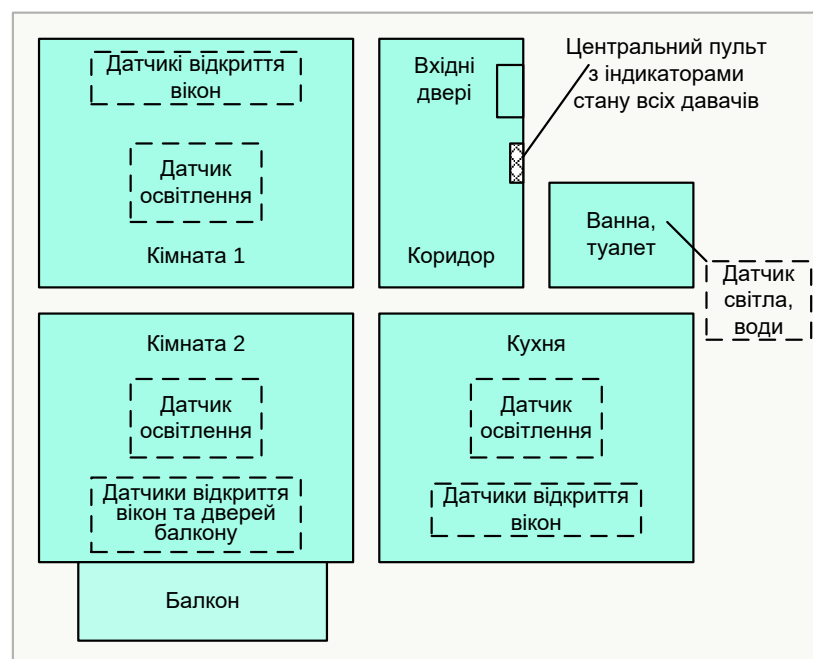


Рисунок 16.16 – Приклад автоматизованої квартири на базі технології ZigBee

Приклад мережі ZigBee наведено на рис. 16.17 [25].

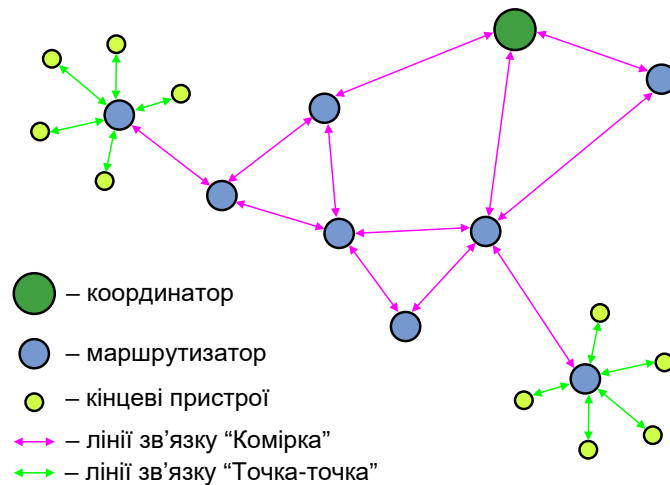


Рисунок 16.17 – Приклад мережі ZigBee з використанням пристроїв 3 класів [25]

Головним завданням мережі ZigBee є мінімізація енергоспоживання. Одним з розв'язків цього завдання є стратегія зв'язку, яка ґрунтується на передаванні даних лише при їх надходженні і наступного очікування підтвердження у випадку успішного прийому пакету з боку адресата. При цьому кожен пристрій може ініціювати передачу в будь-який момент.

Пропускна здатність системи залежить від обраного частотного діапазону. Максимальна швидкість передавання, рівна 250 кбіт/с, можлива в діапазоні 2,4 ГГц (16 каналів з кроком по частоті 5 МГц). Для частот 868 МГц (1 канал) та 902...928 МГц (10 каналів з кроком 2 МГц) швидкості дорівнюють відповідно 20 кбіт/с та 40 кбіт/с (рис. 16.18).

Основним діапазонами для європейських країн є неліцензовані діапазони частот 2,4 ГГц та 868 МГц, оскільки діапазон 915 МГц заборонений для використання в даному регіоні.

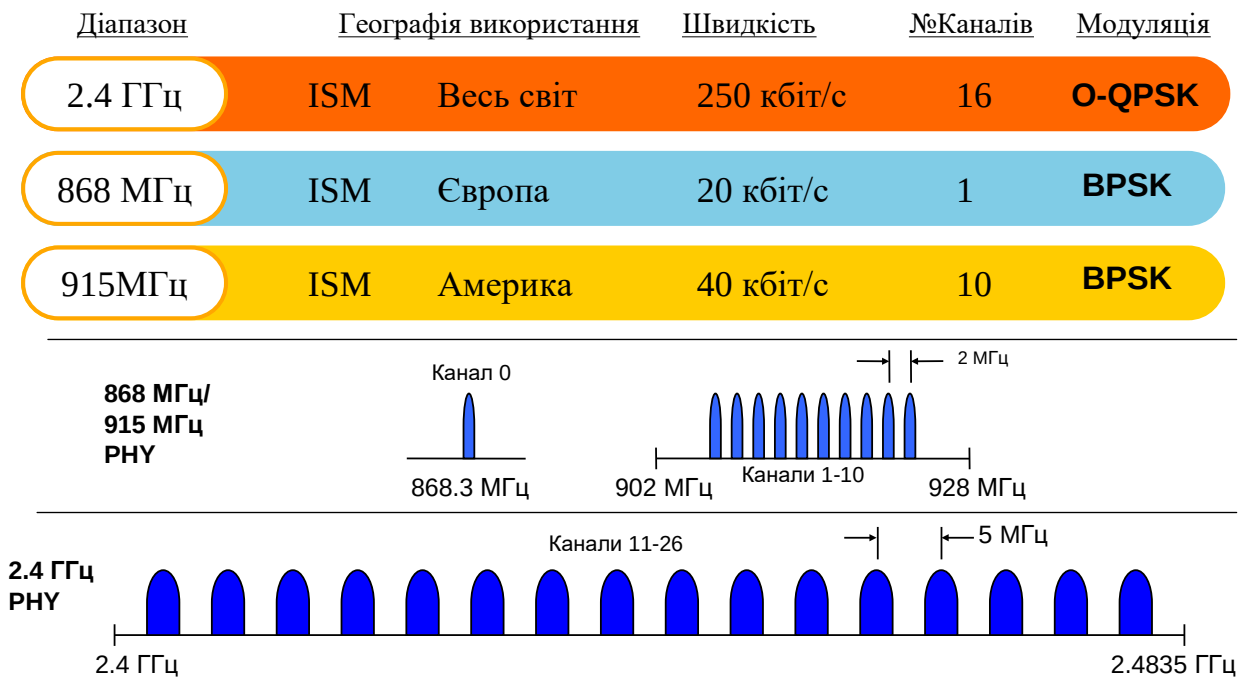


Рисунок 16.18 – Розподіл частотного ресурсу для стандарту ZigBee [26]

На рис. 16.19 наведено приклад побудови системи управління інфраструктурою будинку з використанням пристроїв ZigBee.

Система керування інженерними системами будинку складається з наступних вузлів (рис. 16.19):

- 5 модулів для керування мікрокліматом теплиці;
- 8 модулів для керування вуличним освітленням;
- модулів для пожежної, охоронної сигналізації, контролю показів лічильників;
- координатора мережі, узгоджуючих шлюзів та каналів передавання даних до диспетчерської служби.

Керування мікрокліматом передбачає регулювання температури, вологості повітря та ґрунту, освітленості. Освітленість та вологість ґрунту визначається окремо для кожного сорту рослин відповідним модулем. Окреме регулювання вологості повітря та температури є проблематичним для невеликої теплиці, а тому дані параметри встановлюються загальними для всіх сортів рослин. Всі модулі мають давачі руху та диму.

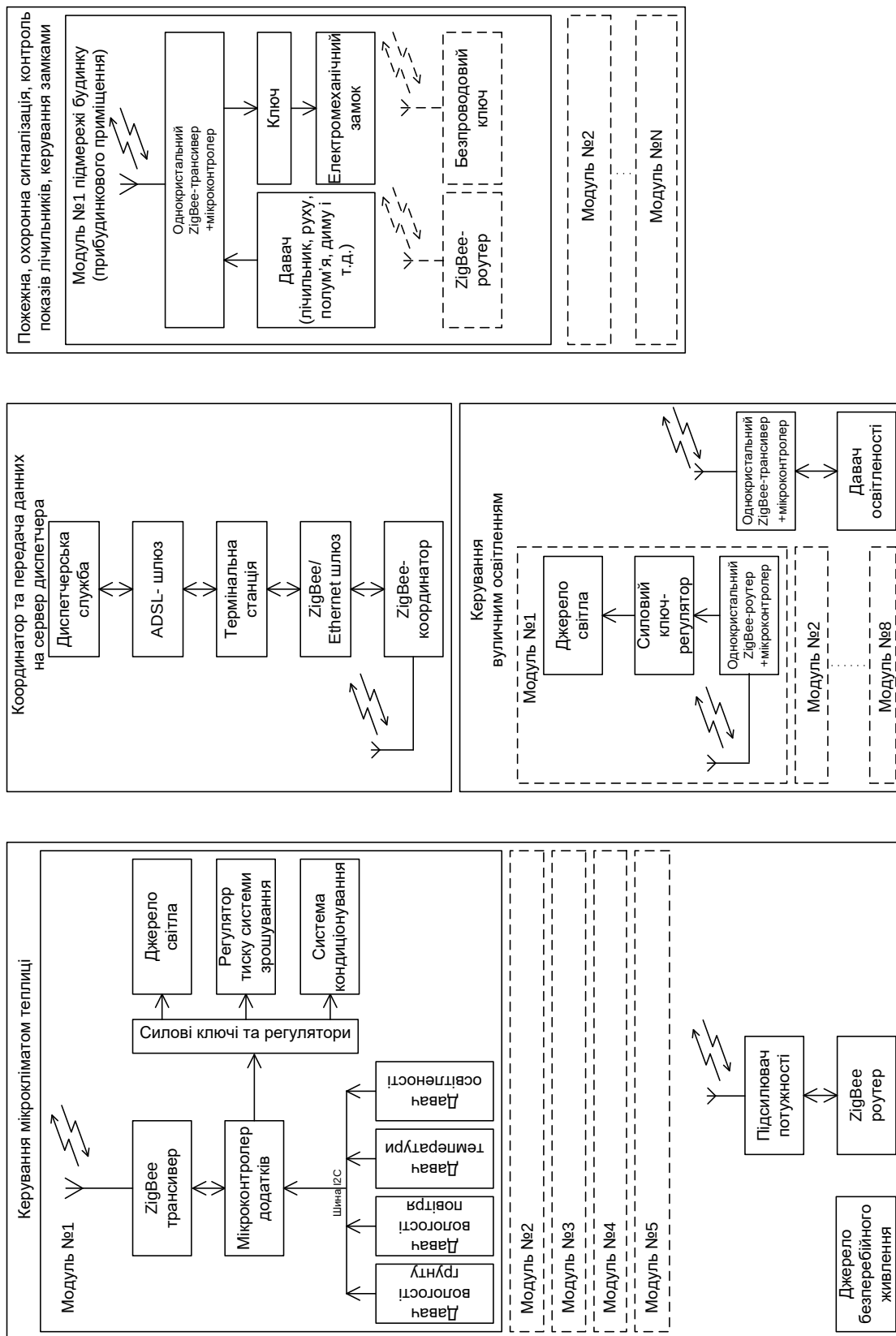


Рисунок 16.19 – Структурна схема системи управління інфраструктурою будинку

З 5 модулів один є головним. Він включає в себе, крім вище зазначених функцій, також функції маршрутизації, регулювання температури, вологості повітря, відкриття/закриття електромеханічного замка. Він має підсилювач потужності сигналу, оскільки передбачається, що теплиця може знаходитись на відстані більшій, ніж 100 м.

Керування мікрокліматом здійснюється наступним чином: спочатку давачі всіх модулів вимірюють параметри та передають їх на координатор. Термінальний ПК обчислює параметри оптимальні для рослин відповідно до пори року, часу доби тощо. Якщо необхідно, передається інформація змінити той чи інший параметр для окремого або всіх модулів. Мікроклімат регулюється системою зрошування, кондиціонування та освітлення через силові регулятори. Загалом система живиться від мережі змінного струму, однак для давачів охорони та протипожежної безпеки передбачено джерело безперебійного живлення. Оскільки кожен модуль обробляє інформацію з декількох давачів, то використовується окремий мікроконтролер додатків.

В інших приміщеннях будинку та прибудинкової ділянки модулі ZigBee використовуються для охорони та протипожежної безпеки, керування відкриттям та закриттям дверей. Принцип роботи даних систем було розглянуто вище. Всі давачі працюють на основі однокристального трансивера та мікроконтролера, оскільки кожен модуль має всього 1-2 давачі.

Система освітлення, крім регулювання, виконує також функції маршрутизації пакетів даних від інших модулів, оскільки опори ліхтарів розміщені по периметру ділянку, що є вдалим розташуванням для маршрутизаторів.

Інформація з усіх модулів збирається координатором мережі та обробляється термінальним ПК. Сигнал пожежі чи охорони через телефонні лінії зв'язку надходить до відповідних диспетчерів.

Контрольні питання

1. В яких випадках доцільно використовувати безпроводові мережі для підключення сенсорів (датчиків)?
2. Чи потребує технологія LORA наявності мережі базових станцій?
3. Яку швидкість передавання даних забезпечує технологія LORA?
4. Чи потрібно оплачувати послуги в мережі LORA?
5. Чи потребує технологія SIGFOX наявності мережі базових станцій?
6. Яку швидкість передавання даних забезпечує технологія SIGFOX?
7. Чи потрібно оплачувати послуги в мережі SIGFOX?
8. Чи потребує технологія NB-IoT наявності мережі базових станцій?
9. Яку швидкість передавання даних забезпечує технологія NB-IoT?
10. Чи потрібно оплачувати послуги в мережі NB-IoT?
11. Яка з технологій LORA, SIGFOX або NB-IoT забезпечує найбільший строк служби без заміни джерела живлення сенсорного вузла?
12. Яка з технологій LORA, SIGFOX або NB-IoT забезпечує найбільший радіус дії?
13. В чому переваги мереж ZigBee у порівнянні з мережами LORA, SIGFOX та NB-IoT?
14. Сенсори якого стандарту мають найнижче енергоспоживання?

Перелік посилань

1. LoRa® and LoRaWAN®: A Technical Overview. Url: https://loradevelopers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf. (дата звернення: 16.05.2024).
2. Як працює технологія LoRa та як її застосовують у розумних містах. Url: <https://jooby.eu/uk/blog/yak-pracyuye-tehnologiya-lora-ta-yak-yiyi-zastosovuyut-u-rozumnih-mistah/>. (дата звернення: 16.05.2024).

3. S. R. Sharan, W. Y. Qiao, and H. Seung-Hoon, "A survey on LPWAN technology: LoRa and NB-IoT," *ICT Express*, vol. 3, no. 1, 2017. [Online]. Available: 10.1016/j.icte.2017.03.004. (дата звернення: 16.05.2024).
4. What is LoRaWAN® Specification. Url: <https://loro-alliance.org/about-lorawan/>. (дата звернення: 16.05.2024).
5. A. Zourmand, C. W. Hung, A. L. K. Hing, and M. AbdulRehman, "Internet of Things (IoT) using LoRa technology" in *International Conference on Automatic Control and Intelligent Systems IEEE*, June 2019, Selangor, Malaysia. Url: <https://scihub.se/10.1109/i2cacis.2019.8825008>. (дата звернення: 16.05.2024).
6. MultiTech Conduit®. URL: <https://multitech.com/all-products/cellular/cellular-gateways/multitech-conduit/>. (дата звернення: 16.05.2024).
10. Антена для роутера. Url: <https://tehbezpeka.ua/ua/p1435163405-antenna-dlya-routera.html> (дата звернення: 4.07.2024).
7. Вега SH-2 – Універсальний модем LoRaWAN®/Nb-IoT. <http://iotvega.com/product/sh2>. (дата звернення: 4.07.2024).
8. Універсальний модем ВЕГА SH-2. Інструкція з експлуатації. http://iotvega.com/content/ru/si/sh2/01-%D0%92%D0%95%D0%93%D0%90%20SH-2%20%D0%A0%D0%9F_rev%2004.pdf. (дата звернення: 4.07.2024).
9. Технологія SIGFOX. Url: <https://sigfox.ua/technology/>. (дата звернення: 4.07.2024).
10. Мережі IoT: порівняння 4 типів і приклади використання. Url: <https://e-server.com.ua/uk/poradi/merezi-iot-porivniannia-4-tipiv-i-prikladi-vikoristannia>. (дата звернення: 4.07.2024).
11. Nokia: LTE evolution for IoT connectivity | Open Ecosystem Network, Available at: <http://bit.ly/Nokia2DsnEj6> [Accessed 23 Apr. 2019]. (дата звернення: 4.07.2024).
12. SIGFOX device. ETSI mode white paper. Url: https://storage.googleapis.com/public-assets-xd-support-sigfox-production-338901379285/att38407169-sigfox%20device%20ETSI%20mode%20whitepaper_v5.pdf (дата звернення: 24.11.2024).

13. Utilix.One. Url: <https://utilix.one/> (дата звернення: 24.11.2024).
14. Narrow Band Internet of Things (NB-IoT). Url: <https://business.vodafone.ua/produkty/iot/nb-iot>. (дата звернення: 4.07.2024).
15. Weightless-P System specification. Url: https://pro-bee-user-content-eu-west-1.s3.amazonaws.com/public/users/Integrators/929cb090-e779-401a-b06c-c629ff6b0fea/ap-cambridgestartuplimi/Weightless-P_v1.03.pdf (дата звернення: 24.11.2024).
16. Мережі IoT: порівняння 4 типів і приклади використання. Url: <https://e-server.com.ua/uk/poradi/merezi-iot-porivniannia-4-tipiv-i-prikladi-vikoristannia>. (дата звернення: 4.07.2024).
17. Посібник для початківців із комунікаторів HART-протоколу. Url: <https://www.drurylandetheatre.com/uk/beginners-guide-to-hart-communicators-hart-protocol/>. (дата звернення: 4.07.2024).
18. Hart комунікатор, як користуватися. Url: <https://ktitor.com.ua/poradi-dlya-domu/hart-komunikator-yak-koristuvatisya.html> (дата звернення: 4.07.2024).
19. Wireless HART Communication Protocol Overview. Url: <https://instrumentationtools.com/wireless-hart-communication-protocol-overview/>. (дата звернення: 4.07.2024).
20. The underlying technologies in WSNs: ZigBee vs. wireless HART. Url: <https://www.semanticscholar.org/paper/The-underlying-technologies-in-WSNs%3A-ZigBee-vs.-Jindal-Verma/2a72863191de2f9ba35a19b8e84e6696a2f1d559> (дата звернення: 4.07.2024).
21. Шлюз WirelessHART SWG70. Url: https://portal.endress.com/wa001/dla/5000586/7174/000/00/BA064SRU_0610.pdf (дата звернення: 4.07.2024).
22. SITRANS AW210 - HART V7 - SIMATIC PDM V6.0. Url: <https://support.industry.siemens.com/cs/document/66807785/edd-sitrans-aw210-hart-v7-simatic-pdm-v6-0?dti=0&lc=en-LT> (дата звернення: 4.11.2024).
23. Що таке ZigBee в IoT? Url: <https://www.dusuniot.com/uk/blog/the-definitive-guide-for-zigbee-gateway-for-solution-vendors/>. (дата звернення: 4.07.2024).

24. Порівняння стандартів IEEE 802.15.2 та 802.15.4. Url: https://ozlib.com/984061/tehnika/sravnenie_standartov_ieee_80215. (дата звернення: 4.11.2024).
25. Palagin O.V., Romanov V.O., Galelyka I.B., Voronenko O.V., Brayko Yu.O., Imamutdinova R.G. Wireless sensor network for precision farming and environmental protection//Information theories and applications. - Vol.24, Number 1. - 2017. p. 19-34.
26. Апаратне та програмне забезпечення сенсорних мереж. Url: https://learn.ztu.edu.ua/pluginfile.php/206253/mod_resource/content/0/%D0%9B5-6__%D0%A1%D0%B5%D0%BD%D1%81%D0%BE%D1%80%D0%BD%D1%96%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96.pdf (дата звернення: 4.11.2024).

17 БЕЗПРОВОДОВІ НАТІЛЬНІ ТА ДВОПРОТОКОЛЬНІ СЕНСОРНІ МЕРЕЖІ

17.1 Загальні зауваження

Безпроводова натільна комп'ютерна мережа БНМ (WBAN – Wireless Body Area Network) – безпроводова мережа сенсорів, закріплених на тілі або в тілі пацієнта [1, 2]. Пристрої БНМ можуть бути вбудовані в тіло (рис. 17.1), імплантовані, прикріплені до поверхні тіла у фіксованому положенні або сполучені із пристроями, які люди носять у різних місцях (у кишенях, на тілі й у сумках).

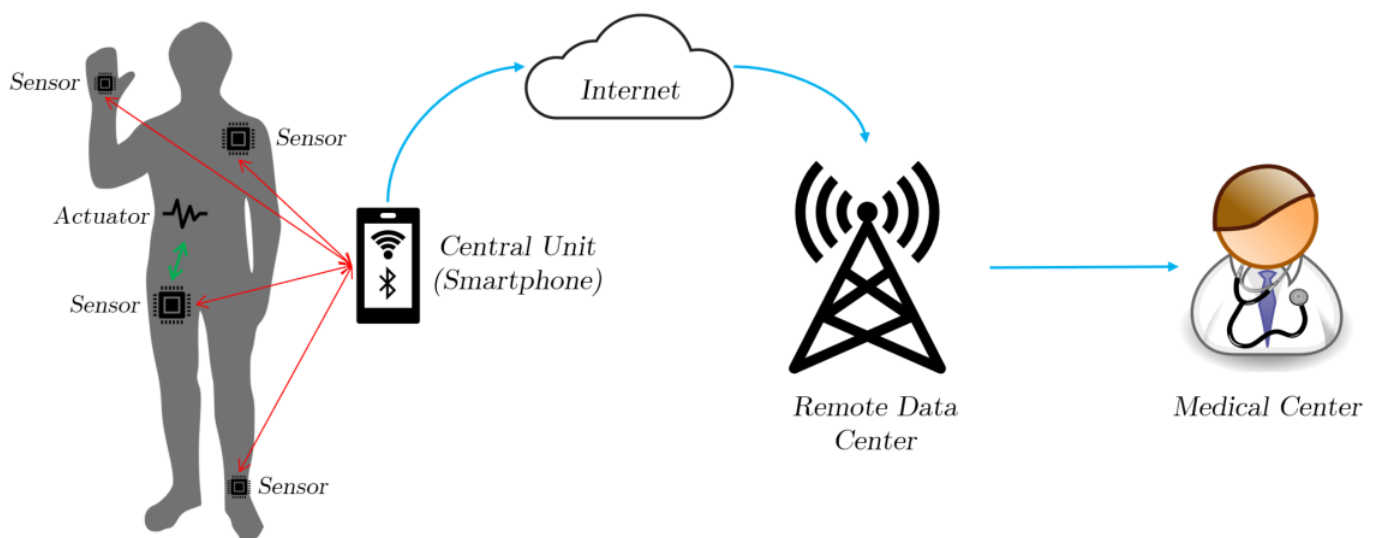


Рисунок 17.1 – Віддалений моніторинг параметрів організму людини за допомогою БСМ [1]

Розробка технології БНМ почалася близько 1995 року на основі ідеї використання безпроводових персональних мереж для реалізації зв'язку "на", "поруч", і "навколо" людського тіла. Близько 6 років через термін БНМ став позначати системи, де зв'язок повністю "у межах", "на" або "у безпосередній близькості" від людського тіла. Система БНМ може використовувати безпроводові технології для передавання даних від сенсорів через Інтернет у медичні установи. Таким чином, медичні працівники зможуть одержувати доступ до даних про

пацієнта онлайн, використовуючи Інтернет (незалежно від місця розташування пацієнта).

Безпроводові натільні мережі мають величезний потенціал для революційного перетворення майбутніх оздоровчих технологій [2]. БНМ підтримує велику область додатків медичної й споживчої електроніки. Наприклад, БНМ дозволяють робити віддалений моніторинг стану здоров'я пацієнтів протягом тривалого часу без обмежень його/її нормальної активності. Для успішного впровадження БНМ потрібна стандартна модель, яка буде призначена як для медичних, так і для споживчих додатків. В 2007 році Комітет IEEE 802 утворив цільову групу, названу IEEE 802.15.6 для стандартизації БНМ [1]. Завдання групи полягало у визначенні нових фізичних рівнів і рівнів доступу до середовища для БНМ. Вибір фізичного рівня (частотних діапазонів був одним з основних питань). Доступні для БНМ частоти визначаються в різних країнах відповідними органами [1].

Діапазон частот комунікаційної служби медичних імплантів (MICS – Medical Implant Communication Service) є ліцензуємим, використовується для зв'язку з імплантами й має смугу частот 402...405 МГц у більшості країн. Служба безпроводової медичної телеметрії (WMTS – Wireless Medical Telemetry Services) являє собою ліцензуєму смугу частот для медичних телеметричних систем. Як MICS, так і WMTS не підтримують додатка з високою швидкістю передавання даних. Неліцензуєма смуга частот для промисловості, науки й медицини ISM (Industrial, Scientific and Medical) підтримує високошвидкісні додатки. Однак при цьому виникає небезпека інтерференції з іншими радіозасобами, включаючи пристрою стандартів IEEE 802.1, IEEE 802.11 і IEEE 802.15.4.

17.2 Стандарт IEEE 802.15.6

17.2.1 Загальні зауваження

Стандарту IEEE 802.15.6 передувала розробка цілого ряду стандартів, що існують у цей час і широко використовуються [3]. Найбільш значимими з них є

IEEE 802.11 (WLAN), IEEE 802.15 (WPAN), що включає стандарти IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee) та інші [3].

Перший, чорновий варіант стандарту IEEE 802.15.6 був опублікований дослідницькою групою в травні 2010 року. Остаточна версія стандарту була опубліковано 29 лютого 2012 року.

17.2.2 Причини стандартизації БНМ

Незважаючи на наявність ряду попередніх стандартів персональному безпроводовому зв'язку, була виявлена необхідність у спеціальному новому стандарті для натільних безпроводових мереж. Розглянемо деякі порівняльні дані для безпроводових стандартів зв'язки загального застосування й БНМ нового стандарту.

IEEE 802.11 являє собою групу стандартів для локальних безпроводових мереж – ЛБМ (Wireless Local Area Networks – WLAN або Wi-Fi). Вона включає різні версії стандарту, такі як IEEE 802.11/a/b/g/n/ac/ah. ЛБМ головним чином використовуються комп'ютерами або портативними пристроями й з'єднують їх з безпроводовим комунікаційним середовищем [4, 5]. Але очевидно, що цей стандарт, у відповідності зі своїм застосуванням, не приділяє великого значення енергозбереженню й складності пристроїв.

Стандарт IEEE 802.15 орієнтований для зв'язку на малих відстанях, невисокій складності пристроїв, низькій вартості й малій споживаній потужності. Він головним чином призначений для безпроводових персональних мереж – БПМ (Wireless Personal Area Networks – WPAN). До цієї групи стандартів входять IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee) і новий стандарт IEEE 802.15.6.

Для порівняння, як приклад розглянемо стандарт IEEE 802.15.4. Цей стандарт широко відомий як ZigBee, хоча насправді ZigBee це – система, побудована на стандарті IEEE 802.15.4. Пристрої ZigBee мають більш тривалий час автономної роботи з порівняння із пристроями Bluetooth, оскільки вони мають більш низьке споживання енергії. ZigBee додатки вимагають менших швидкостей передавання,

тоді як Bluetooth призначений, в основному, для передавання даних на відносно високих швидкостях. Крім того, пристрої ZigBee мають значно менший час з'єднання в мережі.

Таким чином, вони мають ряд властивостей, необхідних для БНМ, але, незважаючи на це, при порівнянні їх характеристик з вимогами для безпроводових натільних мереж видна їхня функціональна недостатність (табл. 17.1).

Порівняння стандартів IEEE 802.15.4 і IEEE 802.15.6 показує, що вони використовуються в різному середовищі. Безпроводові натільні мережі призначені для передавання інформації на малі відстані, але на високих швидкостях. Що стосується енергоспоживання, то БНМ повинні мати надзвичайно мале споживання в сплячому режимі (stand-by mode). і меншу потужність випромінювання в активному режимі, у порівнянні з ZigBee. Це забезпечує пристроям тривалий строк автономної роботи. Області застосування БНМ визначають малі розміри мережі, але повинні відповідати вимогам безпеки й бути дружніми по біологічних параметрах, оскільки робоче середовище пов'язане з тілом людини.

У цілому, БНМ являють собою стандарт для безпроводових комунікаційних систем малого радіуса дії, призначених для роботи в околиці, або усередині тіла людини (але не обмежувані цим). Вони використовують існуючі ISM-діапазони, а також смуги частот прийняті національними медичними й/або регулювальними органами. Підтримка якості сервісів (Quality of Service – QoS), надзвичайно мале споживання й швидкості передавання до 10 Мбіт/с необхідні в них, щоб забезпечити відсутність інтерференції із пристроями інших типів.

БНМ мережі в загальному випадку мають дуже складний різномірний трафік. Існуючі протоколи доступу до середовища, розроблені для WLAN, Bluetooth, ZigBee не задовольняють вимогам низького рівня випромінювання при передаванні. Такі характеристики тіла людини, як втрати поширення не дають можливості використовувати мережі ZigBee для роботи в додатках усередині тіла через необхідний рівень потужності. Медичні додатки повинні мати високий пріоритет і якість обслуговування.

Мережі ZigBee не можуть забезпечити необхідних розв'язків для всіх медичних і немедичних додатків. Внаслідок цього стандарт IEEE 802.15.6 пропонує новий MAC-рівень із трьома різними опціями, а саме: моду з пілот сигналом і границями суперфрейму, моду без пілот-сигналу із границями суперфрейму й моду без пілот-сигналу й границь суперфрейму.

Таблиця 17.1 – Порівняльні характеристики різних стандартів зв'язку

Параметр	Вимоги стандарту		
	IEEE 802.15.6	IEEE 802.15.4 ZigBee – 2,4 ГГц	ППС *
Підтримувані додатки	Медичні, ігрові, розважальні, спортивні і ін.	Домашні, освітлення, промислова автоматизація, і ін.	Домашні, освітлення, промислова автоматизація, медичні й ін.
Дальність зв'язку	2...5 м у приміщенні	10...100 м у вільному просторі 5...30 м у приміщенні	5...30 м у приміщенні
Швидкість передавання даних	1 кбіт/с...10 Мбіт/с	20, 40, 250 кбіт/с	1 кбіт/с...6 Мбіт/с
Споживана потужність	0,01 мВт – сплячий режим 40 мВт – активний (швидкість не зазначена)	135...150 мВт швидкість 250 біт/с. (модулі Xbee)	0,09 мВт – сплячий режим (100%); 27 мВт – 256 кбіт/с; 70 мВт – 1024 кбіт/с
Випромінювана потужність	25 мкВт (-16 дБм)	1 мВт (0 дБм)	200 мкВт (-7 дБм) – 256 кбіт/с 800 мкВт (-1 дБм) – 1024 кбіт/с
Розмір мережі	Помірний, до 256 вузлів	Великий, до 65 тис. вузлів	Великий, до 65 тис. вузлів
Безпека, дружність по біологічних параметрах	Так	Відсутня	Так, при зниженому рівні потужності (дальність до 5 метрів)

* ППС – зверхширокосмуговий прямохаотичний прийомопередавач сигналів

Безпека. Для безпеки зв'язку IEEE 802.15.6 визначає три рівні:

1. Рівень 0 – незахищений зв'язок.
2. Рівень 1 – тільки аутентифікація.

3. Рівень 3 – спільна аутентифікація й шифрування.

17.2.3 Прийомопередавачі на основі хаотичних радіоімпульсів

У стандарті IEEE 802.15.6 у якості носіїв інформації пропонується використовувати імпульсні сигнали трьох типів: імпульси з лінійною частотною модуляцією (Chirp Pulses), хаотичні імпульси (Chaotic Pulses) короткі імпульси (Short Pulses Shape) [3]. У табл. 17.1 проводиться порівняння вимог до прийомопередавачів у стандарті IEEE 802.15.6 з характеристиками типового приймально-передавального модуля ZigBee і зверхширокосмугового прямохаотичного прийомопередавача ППС-43. Прийомопередавач ППС-43 використовує в якості носія інформації хаотичні радіоімпульси. Його програмне забезпечення забезпечувало створення й роботу у режимі мереж, що самоорганізуються.

З табл. 17.1 випливає ряд відмінностей вимог нового стандарту від типових характеристик пристроїв ZigBee, що працює в ISM-діапазоні частот 2,4 ГГц. У той же час характеристики прийомопередавача ППС-43, який створювався для безпроводових зверхширокосмугових сенсорних мереж у діапазоні частот 3...5 ГГц, і використовує в якості носія інформації хаотичні радіоімпульси, рекомендовані стандартом, значно ближче до необхідних параметрів. Зниження потужності випромінювання пристрою на 17...20 дБ, відповідно до необхідної стандарту дальністю передавання не представляє технічної проблеми. У цьому випадку характеристики ППС-43 будуть повністю відповідати стандарту IEEE 802.15.6.

17.2.4 Інфраструктура БНМ

БНМ складається з вузлів, які здійснюють постійний моніторинг життєво важливої інформації пацієнта для діагностики й рекомендацій [2, 5]. Трафік БНМ підрозділяється по категоріях на трафіки по запиту, аварійний і нормальний.

Трафік по запиту ініціюється координатором або лікарем для одержання інформації, в основному для цілей діагностичних рекомендацій. Він у свою чергу ділиться на безперервний (у випадку хірургічних подій) і дискретний (коли інформація потрібно час від часу).

Аварійний трафік ініціюється вузлами, коли вони долають певний поріг і потрібне прийняття рішення менше, чим за секунду. Цей вид трафіка не генерується через регулярні інтервали й у загальному випадку непередбачений.

Нормальний трафік представляє трафік у нормальних умовах при відсутності критичних подій і подій запитів. Він містить у собі ненав'язливий рутинний моніторинг здоров'я пацієнта й спостереження багатьох хвороб, таких як хвороби шлунково-кишкового тракту, неврологічні порушення, виявлення раку, період реабілітації й найнебезпечніші хвороби серця. Нормальні дані збираються й обробляються координатором. Координатор містить у собі пробуджуючий ланцюг, основний радіоканал, функцію мосту, усе з яких пов'язані з інтерфейсом даних. Пробуджуючий ланцюг використовується для адаптації до аварійного трафіка й трафіку по запитах. Функція мосту використовується для встановлення логічного зв'язку між різними вузлами, що працюють у різних частотних діапазонах.

17.2.4 Фізичний рівень БНМ

У БНМ розрізняють три типи вузлів [5, 6]:

1. **Імплантовані вузли** – вузли, які поміщені усередині тіла людини. Вони можуть бути розміщені безпосередньо під шкірою або значно глибше усередині тіла.

2. **Поверхневі вузли** – вузли, які розташовані на поверхні тіла, або на відстані від нього до 2 сантиметрів.

3. **Зовнішні вузли** – вузли, які не контактують зі шкірою людини й розташовані поза тілом на відстанях від декількох сантиметрів до 5 метрів.

При комунікаціях по поверхні тіла, відстань між передавальним і прийомним вузлом визначається як відстань по дузі мінімальної довжини, що проходить по

поверхні тіла й з'єднуючий передавач і приймач, а не як безпосередня відстань між цими пристроями. Це дозволяє розглядати для зв'язку поверхневі хвилі, що огинають тіло. Для зовнішнього комунікаційного вузла відстань між передавачем і приймачем розглядається як довжина прямої лінії, що з'єднує поверхневий вузол із зовнішнім вузлом. Ця відстань може досягати 3...5 метрів.

Обмеження по максимуму випромінюваної потужності для медичних приладів, розташовуваних на тілі, визначається національним і міжнародним регулюванням.

Обмеження по максимальній потужності для MICS становить у Європі (розв'язок ETSI – European Telecommunication Standards Institutes) 25 мкВт ERP, у США (розв'язок FCC & ITU – R) 25 мкВт EIRP, що на 2,2 дБ нижче, чим ERP рівень.

Граничне значення потужності в 25 мкВт відноситься до рівня сигналу поза тілом людини (загальної випромінюючої системи), що допускає для рівня потужності імплантованих вузлів трохи більше значення з урахуванням втрат у тілі.

При побудові БНМ на основі зверхширокосмугових сигналів розглядається чотири сценарії роботи: "поверхня тіла – поверхня тіла" при наявності прямого променю "поверхня тіла – поверхня тіла" при відсутності прямого променю, "поверхня тіла – зовнішній вузол" при наявності прямого променю, "поверхня тіла – зовнішній вузол" при відсутності прямого променю. У перших двох випадках використовується модель каналу CM3, у третьому й четвертому випадках модель каналу CM4.

Зверхширокосмугові сигнали формуються у двох смугах частот: нижній й верхній. Смуги діляться на канали, із шириною кожного 499,2 МГц. Нижня смуга містить у собі три канали (1...3). Другий канал має центральну частоту 3999,3 МГц і розглядається як основний канал. Верхня смуга містить у собі вісім каналів (4...11), де канал 7 із центральною частотою 7987,2 МГц розглядається як основний, а інші як опціональні. Типовий ЗШС-пристрій повинен підтримувати як мінімум один з основних каналів. Фізичний рівень ЗШС прийомопередавача повинен мати невисоку складність реалізації й генерувати сигнал того ж рівня потужності, як і використовуваний у смузі MICS.

17.2.5 Додатки БНМ

БНМ мають великий потенціал для декількох застосувань, включаючи віддалену медичну діагностику, інтерактивні ігри й військові застосування [5].

Додатки усередині тіла включають моніторинг і програму змін для пейсмейкерів і імплантуємих серцевих дефібриляторів, контроль функцій сечового міхура й реабілітацію руху кінцівок. Медичні застосування на тілі людини містять у собі моніторинг ЕКГ, тиску крові, температури й подиху [5]. До немедичних застосувань відносяться: моніторинг забутих речей, створення соціальних мереж, зниження втоми солдат і підвищення їх боєздатності.

Розглянемо деякі із цих застосувань докладніше.

17.2.5.1 Серцево судинні хвороби

Традиційно холтерівські монітори використовувалися для збору порушень серцевого ритму в режимі “off line” без зворотного зв’язку. Однак, у такому режимі використання іноді важко виявити перехідні аномалії. Наприклад, багато серцевих захворювань асоціюються з епізодичними, а не з безперервними аномаліями, такими як хвилі переходу в кров’яному тиску, миготлива аритмія або індуковані епізоди ішемії міокарда, і час їх настання не може бути точно передвіщеним. БНМ є ключовою технологією попередження настання інфаркту міокарда, моніторингу епізодичних подій і інших аномальних умов і може бути використана для амбулаторного спостереження за здоров’ям (рис. 17.2) [3, 5].

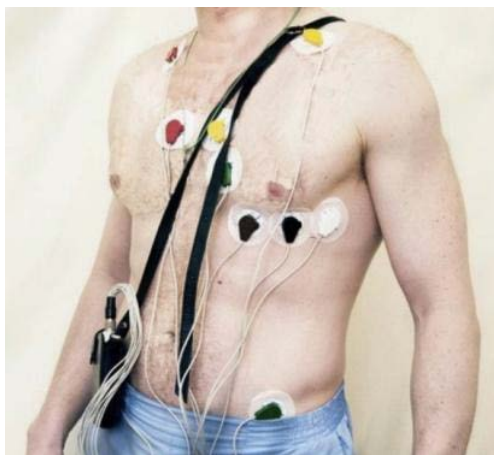


Рисунок 17.2 – Холтерівський монітор для використання у БНМ [5]

17.2.5.2 Виявлення раку а ранній стадії хвороби

Рак залишається однією із самих найбільших небезпек для життя людини. Згідно з Національним центром статистики здоров'я, в 1999 році 9 мільйонів жителів США мали діагноз ракового захворювання. Безліч мініатюрних сенсорів, здатних виявити ракові клітини можуть бути рівномірно інтегровані в БНМ. Це дозволить медикам діагностувати новотвору без біопсії.

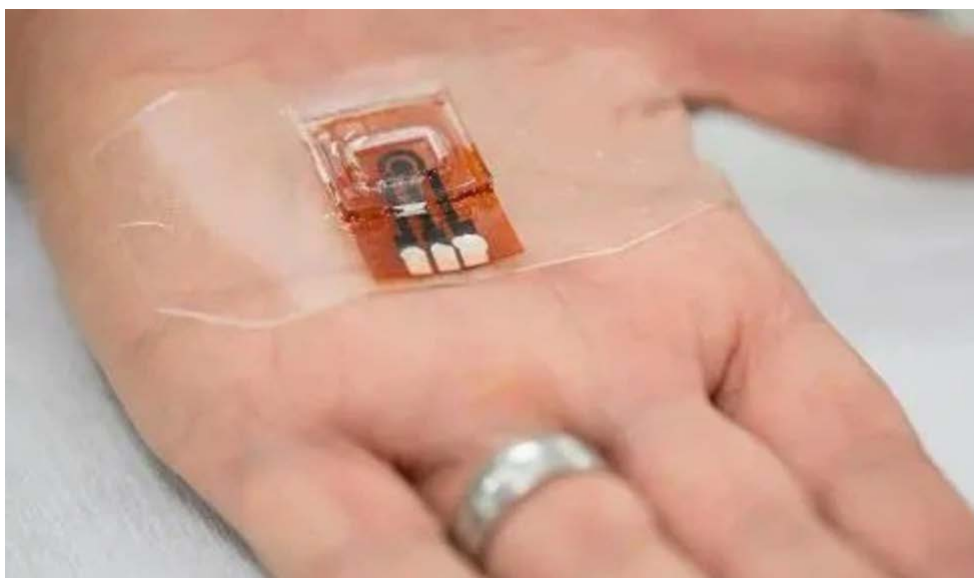


Рисунок 17.3 – Сенсор для виявлення ракових клітин [7]

17.2.5.3 Попередження хворих астмою

БНМ можуть допомогти мільйонам людей страждаючих від астми шляхом моніторингу алергенів у повітрі й надання медикам зворотного зв'язку у режимі реального часу (рис. 17.4). Запропонований прилад на основі GPS-технології, який здійснює моніторинг факторів навколишнього середовища й включає сигнал тривоги при виявленні інформації про алергени для пацієнта.



Рисунок 17.4 – Моніторинг алергенів у повітрі й надання медикам зворотного зв'язку у режимі реального часу [8]

17.2.5.4 Монітори стану здоров'я людей похилого віку

На сьогодні для багатьох сімей немає можливості взяти батьків похилого віку у свій власний дім, щоб пильніше стежити за ними, оскільки більшості людей не вистачає фінансових ресурсів, медичних знань або часу, щоб присвятити своїм

близьким повний або навіть частковий догляд. Проте багато хто вважає, що не добре поміщати близьку людину у заклад для догляду за пацієнтами похилого віку чи будинок престарілих, коли вона ще майже здатна жити самотійно. Носимі цифрові засоби охорони здоров'я, такі як пристрої моніторингу стану здоров'я компанії CarePredict Tempo™, можуть стати рішенням для догляду за близькими літніми людьми [2].

- населення Землі старше 60 років у 2030 досягне 17%;
- кількість людей у США, яким щодня виповнюється 65 років, становить 10 тисяч осіб;
- носимі монітори збирають дані про стан здоров'я літньої людини в режимі реального часу, що дає змогу членам сім'ї чи опікунам отримувати оперативну інформацію про стан здоров'я своїх підопічних.

Розглянемо для прикладу носимий пристрій для моніторингу стану здоров'я Tempo компанії CarePredict, який може спостерігати за пацієнтом незалежно від його місцезнаходження: спальня, кухня чи ванна кімната [4]. Завдяки обробці даних штучним інтелектом, пристрій Tempo (рис. 17.5) допомагає сім'ям або опікунам літніх пацієнтів виявляти незначні зміни у їх поведінці, такі як менше споживання їжі, поганий сон або малорухливий спосіб життя. Таким чином, платформа Tempo, яка доступна на настільних комп'ютерах і мобільних пристроях, відображає поведінкові тенденції, які можуть допомогти виявити проблеми зі здоров'ям, перш ніж вони стануть серйознішими.

Цифрова платформа охорони здоров'я компанії CarePredict використовує носимі сенсори, які відстежують поведінку та відхилення фізіологічних показників літнього пацієнта. Система, яка використовується в закладах для проживання людей похилого віку та приватних будинках, спирається на сенсори, алгоритми глибокого навчання та прогнозу аналітику, щоб надати опікунам або лікарям практичну інформацію. Ці дані можуть допомогти їм заздалегідь передбачити серйозні захворювання, такі як інфекційні хвороби, депресію або ризик падіння.

Носимий пристрій Tempo додатково може розпізнавати жести для дистанційної ідентифікації різних дій літнього пацієнта, наприклад, коли він

підносить виделку до рота. Більше того, вивчаючи щоденний ритм дій такого пацієнта, пристрій може виявляти та повідомляти лікаря про зміни в його поведінці для забезпечення своєчасного медичного втручання. Пацієнт, крім того, має можливість натиснути кнопку на пристрої, щоб зв'язатися з лікарем або членом сім'ї.

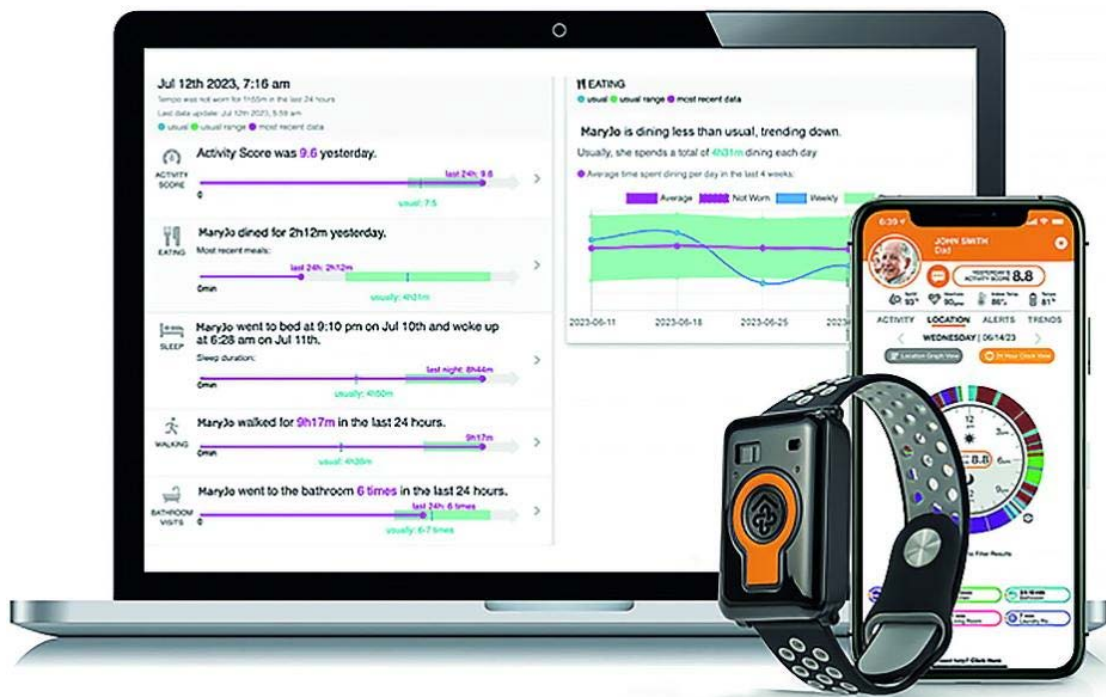


Рисунок 17.5 – Платформа Tempo, яка відображає поведінкові тенденції літньої людини [2]

Основні параметри та особливості монітору стану здоров'я CarePredict Tempo Series 3

Носимий монітор стану здоров'я CarePredict Tempo Series 3 відстежує щоденні дії людини похилого віку за допомогою сенсорів, розміщених у будинку. Якщо щось у розпорядку літньої людини змінюється, близькі отримують практично у реальному часі відповідне повідомлення. Це дає можливість визначити ризики для здоров'я включно падіння чи серцевий напад. Так, наприклад якщо людина похилого віку проводить більше часу в ліжку, вона зазвичай страждає від

депресії, якщо уникає кухні, вона може потребувати допомоги в приготуванні їжі або нагадуванні часу для її прийому.

Носимий пристрій Tempo Series 3 компанії CarePredict включає традиційні функції, які часто зустрічаються в сучасних медичних системах оповіщення, такі, наприклад, як виявлення падіння (рис. 17.6).



Рисунок 17.6 – Монітор Tempo Series 3 та відображення інформації носимого пристрою на смартфоні [2]

Для цього у будинку розміщують відповідні сенсори, так звані маяки, для того, щоб відстежувати переміщення літньої людини у приміщенні. Ці сенсори, крім того, відстежують поведінку та активність людини похилого віку. Tempo Series 3 сумісний з мережею Wi-Fi і його можна використовувати з пристроями на основі ОС типу iOS або Android. Пристрій також відстежує частоту серцевих скорочень за допомогою пульсоксиметра. Крім того, Tempo Series 3 визначає звички літньої людини, а саме коли вона, наприклад, їсть, спить, готує їжу або приймає ванну. Також можна дистанційно спостерігати за допомогою ультрафіолетового сенсора скільки часу літня людина проводить, наприклад, на сонці. Це допомагає відстежувати різні типи поведінки літньої людини та визначити потенційні медичні проблеми, такі як депресія чи недоїдання. Таким чином, цей монітор стану здоров'я, виконаний у вигляді медичного браслету, який має автономне живлення, забезпечує двосторонній зв'язок, оцінює активність, має сумісність з Wi-Fi, виявляє падіння, забезпечує сумісність з приладами на базі ОС

iOS і Android, вимірює частоту серцевих скорочень. Вбудована у монітор система штучного інтелекту робить прогнози щодо потенційних ризиків для здоров'я на основі відповідного алгоритму. На відміну від аналогів Tempo Series 3 допомагає близьким літньої людини виявляти потенційні медичні проблеми, а не просто попереджає про екстремальні ситуації, такі як падіння чи серцевий напад. Крім того, пристрій забезпечує двосторонній зв'язок, що дає можливість літнім людям постійно залишатися під наглядом близьких чи опікунів.

17.2.5.5 Штучна сітківка

Чипи із протезом сітківки можуть бути імплантовані в око людини, що допомагає пацієнтові з ослабленим зором, або невидючому бачити на адекватному рівні (рис. 17.7).

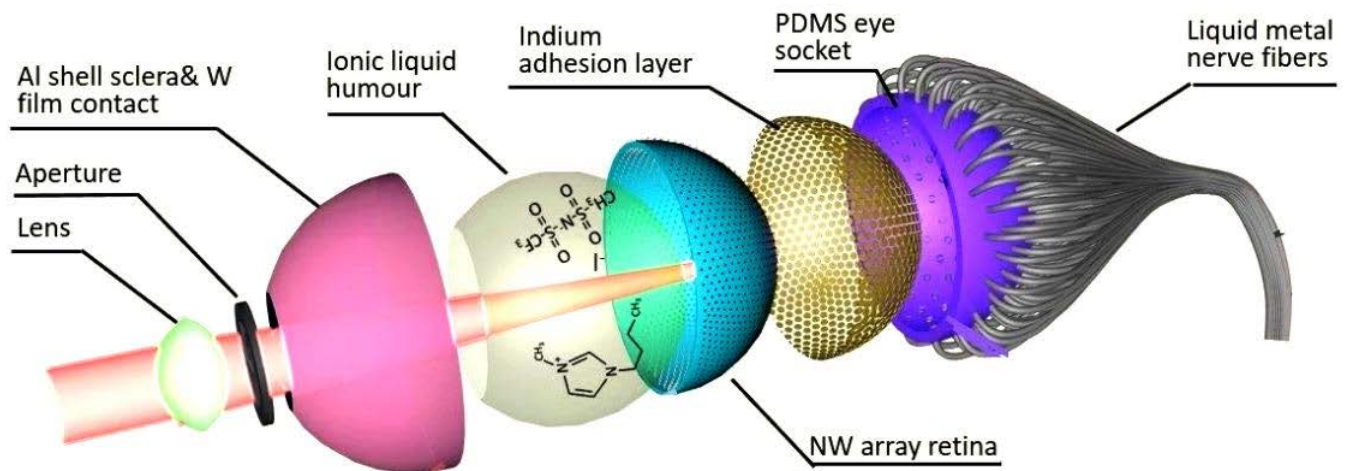


Рисунок 17.7 – Штучна сітківка для імплантації в око [9]

17.2.5.6 Контроль стану діабетиків за допомогою носимих пристроїв безперервного моніторингу глюкози

Носимі пристрої безперервного моніторингу рівня глюкози в крові мають суттєвий вплив на життя мільйонів діабетиків у всьому світі. Для діабетиків першого типу пальцеві тестові смужки є зараз найпоширенішим способом

індивідуального тестування рівня глюкози в крові. Їх застосовують до 7 разів на день у залежності від стану пацієнта-діабетика. Це необхідно для того, щоб отримати значення рівня цукру в крові в реальному часі.

На жаль, цей показник не визначає динаміки зміни рівня цукру в крові діабетика протягом певного часу (в інтервалах між вимірами). Таким чином, пацієнт не усвідомлює, зростає цукор чи знижується в інтервалі між вимірами, тобто не має дієвого розуміння, необхідного для належного вирішення проблеми. Але тепер у діабетиків з'явилася можливість позбавитися від незручностей, пов'язаних з багаторазовими пальцевими тестами за допомогою одноразових тест-смужок. Мінімально інвазивний безперервний моніторинг рівня цукру в крові є зручнішим, ефективнішим і доступнішим способом активного контролю рівня цукру в крові і дозволяє здійснювати контроль цукру у крові (рис. 17.8).



Рисунок 17.8 – Безперервний моніторинг рівня глюкози у крові [10]

Пристрій містить мініатюрний сенсор, введений під шкіру пацієнта-діабетика для безперервного вимірювання рівня цукру в крові протягом дня, якій надсилає результати вимірів на смартфон або розумний годинник для подальшої передачі їх у хмару. Ця інформація в реальному часі допомагає діабетикам швидко регулювати свою фізичну активність, споживання їжі або рівень інсуліну, а також допомагає запобігти виникненню важкої гіперглікемії або епізодів низького рівня

цукру в крові, що може призвести до швидких фатальних наслідків. Економічні переваги пристрою також цілком реальні. Крім економії на голках і тест-смужках, яка є значною протягом життя пацієнта, безперервні дані, отримані від такого монітору, допомагають пацієнтам успішно контролювати небажані симптоми та уникнути додаткових витрат на медичні процедури або відвідування лікаря.

17.2.5.7 Використання БНМ на полі бою

БНМ можуть бути використані для зв'язку між солдатами на полі бою й передавання даних про їхню активність та стан здоров'я командирів та медикам. Тобто, біжить солдат, стріляє або повзе. Солдати повинні мати секретний канал зв'язку, щоб запобігти засідкам [5].

Армії, які воювали на полях битв в XIX і XX столітті, давно залишилися в минулому, багато в чому завдяки розвитку науки і техніки. Сьогодні військові сили НАТО (США і Європи), Ізраїлю та інших країн приступили до реалізації програм, спрямованих на зменшення персоналу, модернізацію і реструктуризацію оперативних можливостей. В рамках даних програм в перерахованих країнах виконуються проекти під назвою "Солдат майбутнього", які об'єднують в собі напрацювання в області збільшення ефективності окремо взятого бійця на основі досягнень XXI століття, в тому числі в області інформаційних технологій і медицини. Ця концепція передбачає використання бійцем систем нічного бачення, позиціонування та навігації, покращених систем ціленаведення, систем контролю фізіологічних параметрів бійця, систем контролю параметрів довкілля, комунікацій та нових динамічних засобів захисту.

У світі існує не так багато сучасних екіпіровок (рис. 17.9). Перелік основних екіпіровок для сучасного солдата наведено нижче [5]:

- Land Warrior і Mounted Warrior, США;
- FELIN (Fantassin a Equipements et Liaisons Integres), Франція;
- IdZ (Infanterist der Zukunft), Німеччина;
- FIST (Future Integrated Soldier Technology), Великобританія;

- COMFUT (COMbatiente FUTuro or Future Warfighter), Іспанія;
- ISSP (Integrated Soldier System Project), Канада;
- ANOG, Ізраїль.



Рисунок 17.9 – Приклад екіпіровки бійця XXI століття [5]

Необхідно відзначити, що навіть легке поранення солдата при великій крововтраті може привести до летального результату. А якщо солдат крім поранення був ще контужений і не може надати собі допомогу самостійно, то наявність в його екіпіровці автоматичних засобів оцінки його фізичного стану, засобів передачі цієї інформації на відстань, а також вбудованого в уніформу навігатора (що є обов'язковим для сучасної екіпіровки) дозволить надати такому бійцеві своєчасну допомогу. Крім того, інформація про боєздатність солдатів дасть можливість командирів ввіреного йому підрозділу ефективно виконати поставлене перед ним бойове завдання.

Слід зазначити, що такі екіпіровки в українській армії відсутні. На рис. 17.10 наведено структуру сучасної екіпіровки для солдатів України, проектне рішення якої запропоновано Інститутом Кібернетики ім. В.М. Глушкова НАН України.

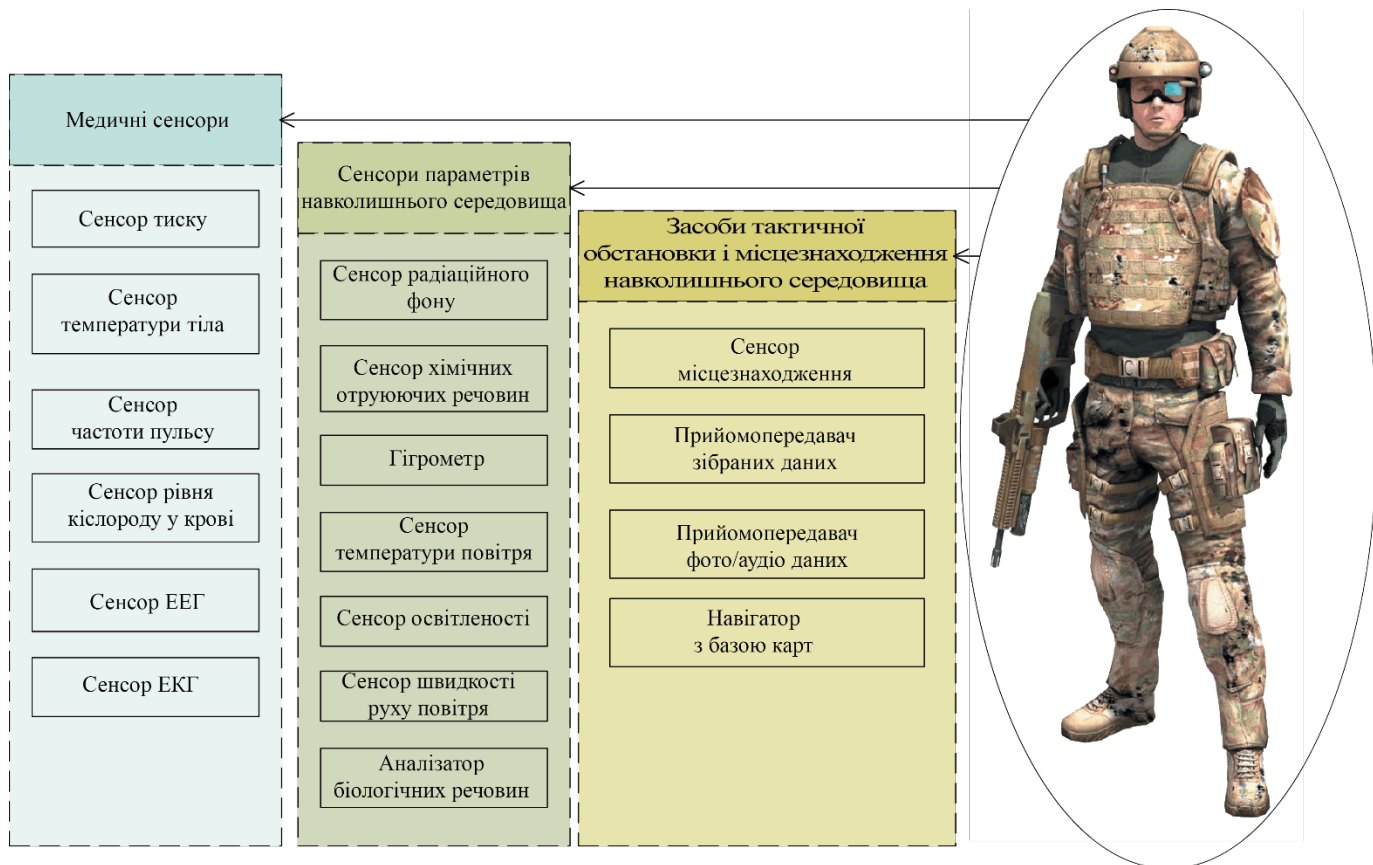


Рисунок 17.10 – Структура сучасної екіпіровки для солдатів України [5]

Для вимірювання фізіологічних параметрів солдата і оцінки його боєздатності в його екіпіровку вбудовані наступні медичні сенсори:

- сенсор частоти пульсу;
- сенсор частоти дихання;
- сенсор температури тіла;
- оксигемометр;
- сенсори кардіосигналів;
- сенсор тиску;
- акселерометр;
- навігаційний сенсор.

Сенсори мають вбудовані прийомопередавачі для передачі даних фізіологічних параметрів солдата у віддалений комп'ютер, в якому експертна система визначає стан солдата за критерієм "боєздатний/небоєздатний". Якщо

солдат втратив боєздатність і йому необхідна медична допомога, в медичну службу з вбудованого в уніформу навігатора передають його координати.

Слід зазначити, що організація збору даних про біологічний і фізіологічний стан військовослужбовців здійснюватиметься шляхом самоорганізації модулів безпроводового зв'язку, вбудованих в екіпіровку кожного бійця, в безпроводову сенсорну мережу.

17.2.5.7 Смарт-сенсори для оцінки крововтрати при пораненнях або травмах

У ряді випадків для комплексної оцінки стану пацієнта синхронно вимірюється кілька медичних параметрів, наприклад, частота серцевого ритму і параметри руху, або частота серцевого ритму і імпедансу шкірного покриву [5]. Слід зазначити, що якщо моніторинг медичних параметрів і їх передача в діагностичний центр виконуються автоматично за заданим алгоритмом, то постановка діагнозу в цих центрах все ще залишається прерогативою лікаря.

Це обмежує застосування дистанційних систем медичного моніторингу при необхідності діагностувати стан пацієнта в реальному часі. Затримка в постановці діагнозу і, як наслідок, в наданні необхідної лікарської допомоги особливо в надзвичайних ситуаціях може призвести до незворотних наслідків, включаючи загибель пацієнта. До подібних ситуацій відносяться важкі травми або поранення, що супроводжуються кровотечами з великою втратою крові, що може викликати важкий геморагічний шок і привести до летального результату. Рівень крововтрати, як правило, виражається через об'єм циркулюючої крові (ОЦК). Виходячи з цього показника, Класифікація крововтрат може бути представлена в наступному вигляді:

1. Легка ступінь крововтрати до 1 л становить 10 – 20% ОЦК.
2. Середня ступінь крововтрати до 1.5 л становить 20 – 30% ОЦК.
3. Важка ступінь крововтрати до 2 л становить 40% ОЦК.
4. Масивна крововтрата-більше 2 л становить понад 40% ОЦК.

Слід звернути увагу на досить великий розкид діапазону показників при оцінці тяжкості крововтрати, при цьому важливо знати ще й швидкість крововтрати. Відзначимо, що для більш точної оцінки крововтрат необхідно мати дані про первісний об'єм циркулюючої крові потерпілого (до отримання ним травми або поранення).

Відомо, що ОЦК залежить від таких параметрів, як вага, зріст, стать, вік і ін. Якщо величина вихідного ОЦК потерпілого невідома, то використовують, як правило, середньостатистичний показник, згідно з яким ОЦК у дорослої здорової людини становить 6-8% від маси тіла. Таким чином, якщо керуватися наведеними вище допусками в показниках, то похибка в оцінці тяжкості крововтрати може коливатися в межах 10% і більше.

У медицині існує досить багато методів оцінки крововтрат в реальному часі. Їх можна умовно розділити на дві великі групи: прямі і непрямі. До прямої оцінки в основному відносяться різні біохімічні методи, які застосовуються при проведенні хірургічних операцій. Поза клінікою використовують непрямі методи, як правило, під наглядом медичного персоналу.

В медичній практиці використовується такий досить точний непрямий показник оцінки крововтрати, як індекс Альговера-Брубера (ІАБ):

$$I_{AB} = ЧСС / АС_C,$$

де ЧСС – частота серцевих скорочень; АС_С – артеріальний або систолічний тиск.

Рівень крововтрати, виражений через індекс Альговера-Брубера, може бути представлений в наступному вигляді:

1. $I_{AB} = 0.8$ і менше – крововтрати становлять 10 – 15% ОЦК.
2. $I_{AB} = 0.9 – 1.2$ -крововтрати становлять 20-25% ОЦК.
3. $I_{AB} = 1.3-1.5$ -крововтрати складають 30% ОЦК.
4. $I_{AB} = 2$ -крововтрати становлять 40% ОЦК.

Для обчислення цього індексу можуть бути використані вже наявні в системі медичного моніторингу сенсори частоти серцевих скорочень і артеріального тиску (рис. 17.11).



Рисунок 17.11 – Сенсор частоти серцевих скорочень і артеріального тиску [11]

17.3 Компоненти безпроводових натільних сенсорних мереж

17.3.1 Вимоги до функціональних можливостей БНС-систем

Типова БНС-система містить у собі сенсори контролю життєво важливих функцій: руху (за допомогою акселерометрів), контролю артеріального тиску, пульсу й багатьох інших параметрів.

БНС-системи повинні забезпечувати безперешкодну передачу даних через мережі, відповідні до стандартів Bluetooth, ZigBee і ін., щоб сприяти обміну інформацією між взаємодіючими пристроями. Крім того, ці системи повинні бути масштабованими, забезпечувати ефективна взаємодія між мережами різних стандартів.

Сенсори, використовувані в БНМ, повинні бути мініатюрними, простими в експлуатації, надійними й недорогими. БНС-системи повинні забезпечити безпека передавання даних, захист конфіденційних даних про здоров'я пацієнтів.

Користувачам можуть знадобитися різні рівні моніторингу, наприклад, тим, хто підданий ризику ішемічної хвороби, необхідно, щоб система БНМ працювала постійно, у той час як іншим групам ризику може знадобитися контроль параметрів тільки тоді, коли вони рухаються. Рівень моніторингу впливає на енергоспоживання БНС-систем.

Розміщення пристроїв БНМ повинне бути зручним для пацієнта, не повинне обтяжувати його. Технологія повинна в остаточному підсумку бути зручної для користувача, виконувати свої завдання моніторингу без його участі.

17.3.2 Фізичні рівні стандарту IEEE 802.15.6 і технології зв'язку

У рамках IEEE 802.15, робоча група TG6 розробила стандарт зв'язку, орієнтований на зв'язок між енергозберігаючими пристроями, які працюють поруч або усередині тіла людини. Стандарт підтримує три фізичні рівні:

- вузькосмуговий (Narrow Band) NB-PHY;
- зверхширокосмуговий (Ultra-Wide Band) UWB-PHY;
- зв'язок по тілу людини (Human Body Communication) HBC-PHY.

17.3.2.1 Технологія зв'язку по тілу

Технологія зв'язку по тілу (Intrabody Communication – IBC) уперше була запропонована Циммерманом в 1996 році в якості нової технології зв'язку для обміну даними між електронними пристроями в натільних мережах [2, 6]. Її застосування не обмежується передачею даних. Одночасно здійснюється передавання енергії для живлення сенсорів. Сенсори отримують енергію, необхідну для роботи одночасно з даними. Також вона може бути використана для зв'язку між предметами одягу й пристроями в навколишньому середовищі. Зв'язок по тілу є новим методом для підключення мобільних пристроїв зовні й усередині тіла людини. Даний метод, що використовує тіло людини як середовища

передавання сигналу, має багато переваг у порівнянні із традиційними підходами радіозв'язку.

У табл. 17.2 наведені порівняльні характеристики систем зв'язку, використовуваних у БНМ. Система IBC забезпечує:

1. Безпеку. Система IBC являє собою захищену й конфіденційну мережу зв'язку, який забезпечує природню безпеку й завадостійкий зв'язок.

2. Енергоефективність. Результати досліджень показали, що IBC споживає на порядок менше енергії при максимальній швидкості передавання даних, що робить її привабливим методом зв'язку для застосування в БНМ.

3. Повторне використання частотного спектра. IBC утворює мережі зв'язку малого радіуса дії усередині й навколо тіла людини. Отже, той же частотний діапазон можна використовувати для БНМ інших користувачів.

Таблиця 17.2 – Порівняння специфікацій IBC з NB і UWB в IEEE 802.15.6

Параметр	IBC	NB, UWB
Середовище передавання	Тіло людини	Повітря
Частота носійного колювання	21 МГц ($\Delta f = 5,25$ МГц)	402 МГц...10 ГГц
Швидкість передавання даних	менше 2 Мбіт/с	менше 13 Мбіт/с
Дальність зв'язку	менш 2 м	до 10 м
Загасання сигналу	слабке	сильне
Натільна антена	немає	так
Енергоефективність при передавання енергії	висока (висока провідність тіла людини)	низька (низька провідність повітря)

Основні схеми модуляції для вузькосмугового фізичного рівня (NB-PHY): DBPSK, $\pi/4$ -DQPSK, $\pi/8$ -D8PSK і GMSK, з діапазоном зміни швидкості передавання даних 75,9...971,4 кбіт/с. Для зверхширокосмугового фізичного рівня (UWB) використовуються два типи схем модуляції/демодуляції: імпульсне радіо (IR-UWB) і зверхширокосмугова частотна модуляція (FM-UWB) з

недиференціальним когерентним детектуванням. Швидкість передавання даних варіюється від 0,2 до 12 Мбіт/с. Фізичний рівень зв'язку людини з тілом (НВС) заснований на стандарті Near Field Communication (NFC) [2] і використовує смугу частот 5,25 МГц із центральною частотою 21 МГц для передавання цифрових сигналів основної смуги частот на поверхні тіла. Швидкість передавання даних варіюється від 164 до 13125 кбіт/с. Для виконання системи вилученого моніторингу пацієнта очевидно, що необхідно додатково впровадити протокол зв'язку на більші відстані (наприклад, 3G або 4G).

Людське тіло може використовуватися для передавання сигналів з біомедицинськими даними на основі технології передавання даних в електричному полі EFC (рис. 17.12). EFC (Electrical Field Communication) забезпечує просту конструкцію й надійну роботу для НВС, тому що:

- передавач використовує тільки цифрові схеми й електрод (замість антени);
- діелектрична проникність тіла людини приблизно в 300...500 раз вище, чим у повітря;
- приймач не вимагає змішувачів, ГКН, АЦП, ЦАП, детекторів і т.д.;
- спрощується реалізація пристроїв і забезпечується низьке енергоспоживання.

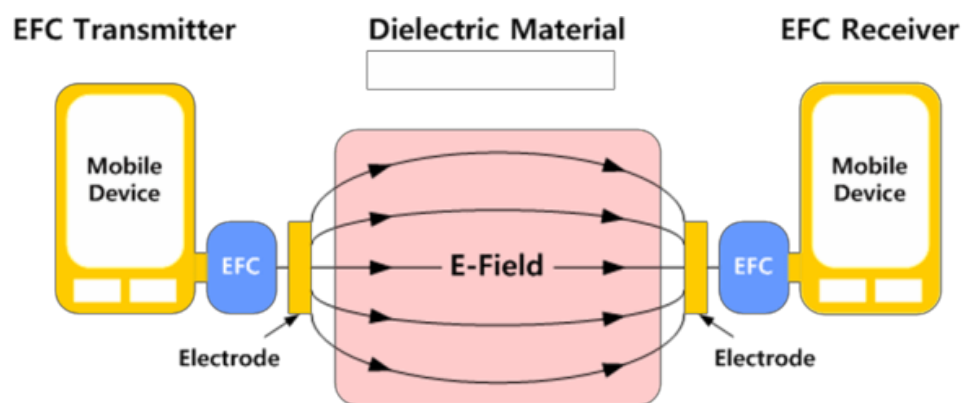


Рисунок 17.12 – Пояснення принципу дії системи зв'язку на основі технології EFC [12]

Пакет EFC складається із преамбули, SFD (початкового обмежника кадра), заголовка й корисного навантаження (Payload) PHY (PSDU). Корисне навантаження PHY складається із заголовка MAC, корисного навантаження MAC і FCS (послідовність перевірки кадра). Структура пакета з полями PHY Header показана на рис. 17.13 [12].

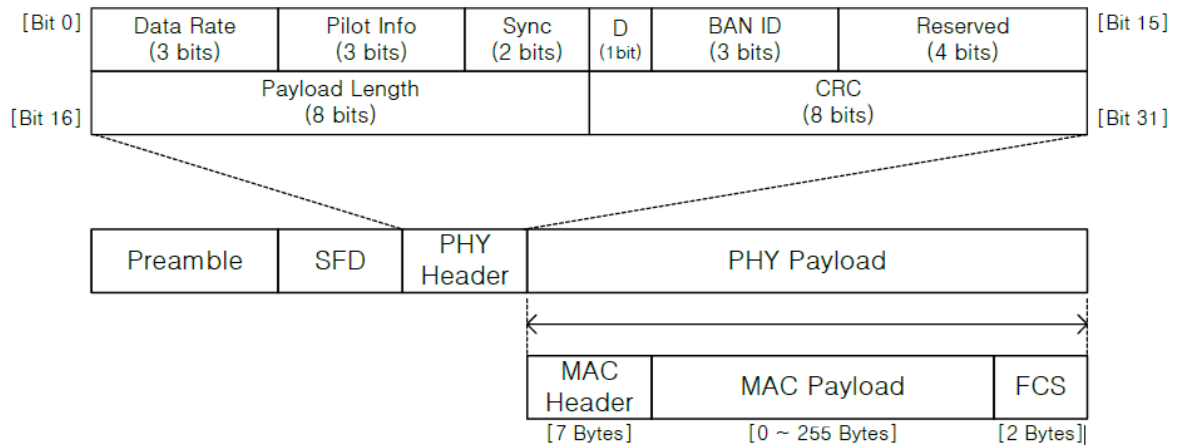


Рисунок 17.13 – Структура кадру EFC [12]

Пакет формується в передавачі (рис. 17.14) і відправляється одержувачеві через електрод. На прийомному кінці здійснюється зворотна процедура.

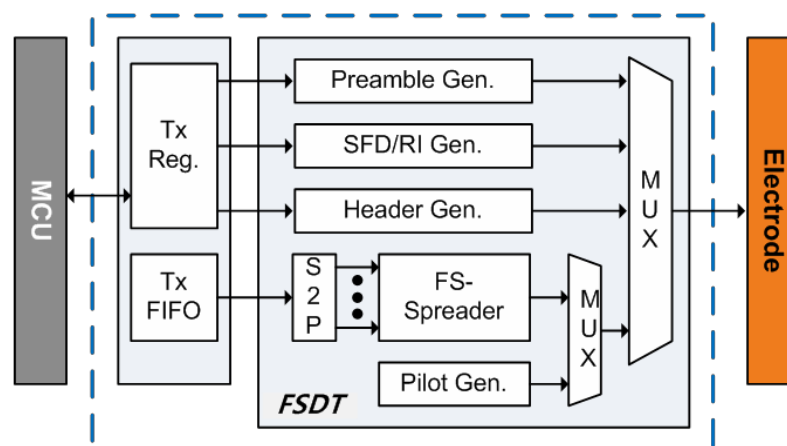


Рисунок 17.14 – Структура передавача системи EFC [13]

Передавач містить три генератори: преамбули (Preamble Generation), обмежника кадра (SFD/RI Generation) і генератора заголовка (Header Generator). Дані з буфера FIFO через перетворювач послідовного коду в паралельний (S2P – Serial-to-Parallel) подаються в блок вибору частоти (Fs-spreader). Сигнали четвертого генератора пілот-сигналу (Pilot Gen.), FS-spreader і генераторів сигналів кадра по черзі підключаються до електрода, закріпленої на тілі людини) за допомогою двох мультиплексорів (MUX).

Послідовність преамбули використовується для синхронізації, а стартовий роздільник кадрів (SFD) вказує початок пакета. SFD також може вказувати швидкість передавання переданих пакетів. У цьому випадку (з наявністю "індикатору швидкості" RI) приймачу не потрібно звертатися до заголовка PHY для визначення швидкості передавання даних вхідного пакета. Це дозволяє передавати заголовки разом з корисною інформацією з однаковою швидкістю, що підвищує ефективність роботи.

Щоб запобігти втраті синхронізації через зміну тактової частоти, в PSDU може бути вставлена послідовність "Pilot". Така ж послідовність, використовувана для SFD, застосовується й для пілота-сигналу. Інтервал вставки пілот-сигналу вказується в полі "Pilot Info" у заголовку PHY.

Докладніше про формування пакета даних можна довідатися в [2].

17.3.2.2 Технологія Bodycom

Bodycom – нова технологія безпроводового зв'язку, який використовує тіло людини для передавання даних [1, 6]. Технологія Bodycom розроблялася з урахуванням наступних пріоритетів:

- дуже низьке енергоспоживання елементів системи;
- швидка реакція системи;
- відносно стабільний і надійний зв'язок;
- обмежене поле дії (кілька сантиметрів), щоб ідентифікувати дотик того, хто носить мобільний модуль;

- низька вартість і складність реалізації.
- Дані передаються між базовим і мобільним модулями через тіло користувача, коли користувач і базовий модуль вступають у контакт один з одним.

Основні відмінності цієї технології:

- передача здійснюється тільки в момент торкання;
- потенційна можливість використання унікальних характеристик тіла людини.

Для передачі сигналу використовується ємнісний зв'язок між тілом людини, базовим модулем і мобільним модулем (рис. 17.15). Частота 128 кГц була обрана для каналу передавання від базового модуля до мобільного модуля. Частота 8 МГц була обрана для каналу передавання від мобільного модуля до базового модуля.

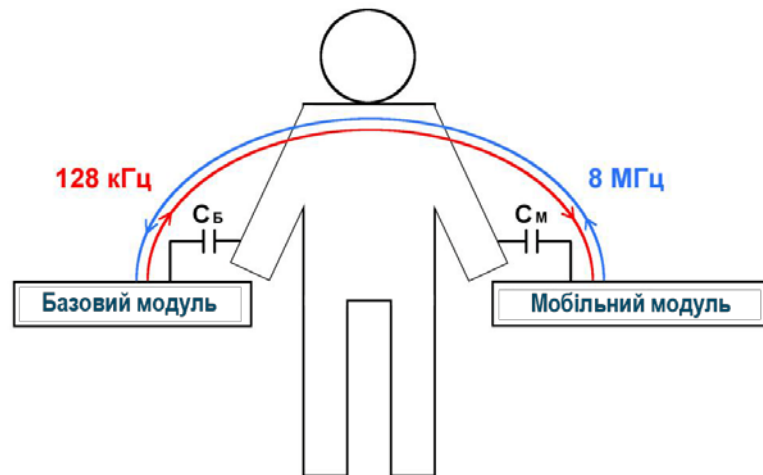


Рисунок 17.15 – Ілюстрація принципу роботи пристроїв Bodysom [6]

Пристрої, розроблені на базі технології Bodysom можуть бути використані в системах (рис. 17.16):

- пасивного входу без ключа (PKE);
- безпеки;
- відмикання домашніх і виробничих дверних замків;
- відмикання дверей для тварин;
- доступу до устаткування або його відключення;
- управління електроінструментом;
- управління зброєю;

- моніторингу пацієнтів у лікарні.



Рисунок 17.16 – Области застосування технології Bodycom [14]

Приклад використання технології Bodycom – система контролю й управління доступом, яка включає:

- комплект для розробки пристроїв на базі технології Bodycom (Bodycom Development Kit) компанії Microchip (рис. 17.17);
- блок управління електромеханічним замком;
- електромеханічний замок.

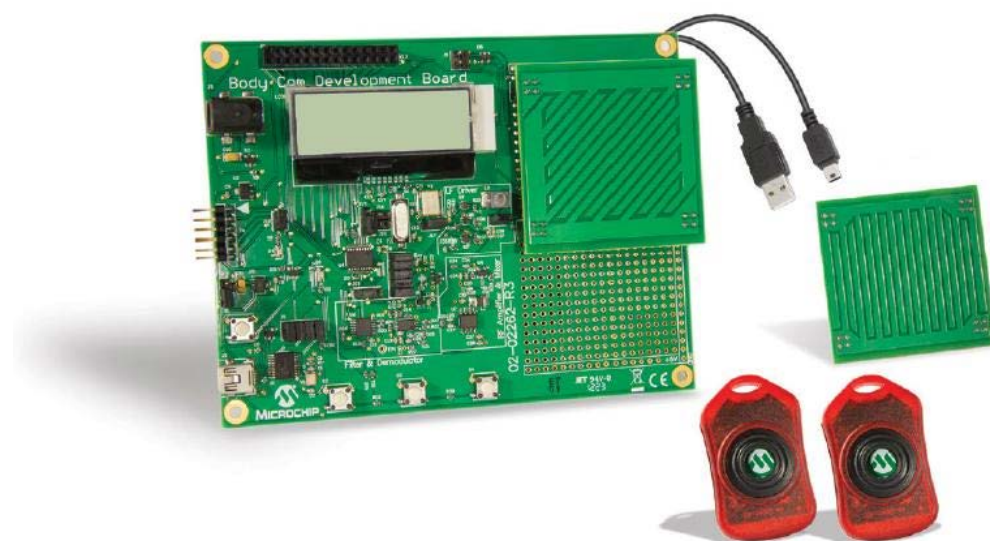


Рисунок 17.17 – Комплект для розробки пристроїв на базі технології Bodycom компанії Microchip [15]

17.4 Оцінка вимог безпеки БСН

Безпека й конфіденційність фізіологічних і неврологічних даних пацієнтів, генеруємих БНМ, є двома незамінними компонентами БНМ. Ці вимоги разом гарантують, що дані надійно зберігаються, передаються й доступні уповноваженим особам. Із цією метою конфіденційність, цілісність і доступність даних є ключовими вимогами. Ці властивості повинні зберігатися протягом усього життєвого циклу пристроїв IMD і БНМ, включаючи належну утилізацію встановлених у тілі людини пристроїв.

Конфіденційність. Дані, інформація про пристрої і структуру системи повинні бути доступні тільки уповноваженим організаціям (тобто відповідним до об'єктів), і ці об'єкти повинні бути аутентифіковані (тобто ідентифікація об'єктів, взаємодіючих із пристроями, повинна піддаватися перевірці). Зокрема, дані повинні залишатися конфіденційними як при зберіганні, так і при їхньому передаванні.

Дані повинні зберігатися в надійному місці під час зберігання на центральному сервері. Навіть якщо зламаний вузол або сервер, зловмисник не повинен мати можливість одержати яку-небудь інформацію.

Цілісність. Дані, інформація про пристрої й структуру системи не повинні модифікуватися несанкціонованими особами. Система повинна також задовольняти аутентифікації джерела даних; джерело будь-яких отриманих даних повинне піддаватися перевірці.

Цілісність даних відноситься до забезпечення того, що несанкціоновані зміни даних не можуть бути зроблені під час зберігання або передавання. Будь-які шкідливі зміни повинні бути виявлені перед використанням і відповідні особи повинні бути попереджені. Це може бути досягнуте за допомогою протоколів аутентифікації даних. Аутентифікація даних дозволяє одержувачеві переконатися, що заявлений відправник відправив повідомлення. Дуже важливо перевірити, що дані були відправлені довіреним сенсором, а не зловмисником, який зламав вузол

або контролер, щоб прийняти неправильні дані. У БНМ аутентифікація даних може бути виконана з використанням симетричних методів.

Доступність. Дані, інформація про пристрої й пристрою системи повинні бути доступні по запиту уповноважених осіб.

Доступність даних означає, що справжнім користувачам доступні правильні дані. Неможливість одержати правильні дані може стати погрозою для життя. Також необхідно аутентифікувати будь-який обмін даними з іншими машинами або людьми. Якщо зловмисники зможуть захопити важливі вузли, здоров'я пацієнтів буде зазнавати ризику.

Таким чином, дані, що зберігаються в різних вузлах БНМ, повинні відповідати, іноді суперечливим вимогам. Вони повинні бути безпечними, безпечно передаватися дані на центральний сервер через Інтернет, коли пацієнт прибуває в лікарню або в інше місце; слід контролювати латентність (скритність); також і для своєчасної діагностики, і для лікування, нові дані завжди повинні бути доступні для лікаря. Крім перерахованих вище основних вимог безпеки й конфіденційності, БНМ повинні також задовольняти наступним вимогам:

1. Особиста конфіденційність пристрою. Неавторизовані особи не повинні мати можливість визначити, що в пацієнта є IMD (Implantable medical devices – імплантуємі медичні пристрої) або БНМ.

2. Конфіденційність пристрою. Якщо конфіденційність існування пристрою неможлива, неавторизовані особи не повинні мати здатність визначити, який тип IMD або БНМ використовується.

3. Індивідуальна ідентифікація конкретного пристрою. Неавторизовані особи не повинні мати можливість визначати унікальний ідентифікатор сенсора IMD або БНМ.

4. Конфіденційність і журнал захисту. Неавторизовані особи не повинні мати можливість визначати приватну телеметрію або доступ до збережених даних про пацієнта.

5. Особиста конфіденційність користувача. Неавторизовані особи не повинні використовувати властивості IMD або БНМ для ідентифікації пацієнта.

6. Відстеження. Несанкціоновані об'єкти не повинні використовувати фізичний рівень (наприклад, контролювати аналогові сенсори або зіставляти дані). Контролер повинен мати можливість виконувати безпечну асоціацію й дисоціацію вузлів.

7. Контроль доступу. Тип і обсяг даних, доступних для різних зацікавлених сторін, таких як лікарі, допоміжний персонал, аптеки й страхові агентства, повинні бути чітко контрольованими. Система повинна надавати різні права доступу для різних користувачів.

8. Актуальність даних. Зловмисник може відтворювати старі дані. Поряд з конфіденційністю й цілісністю важливо забезпечити відправлення даних у тому порядку, у якому вони були створені. Існує два типи актуальності даних: слабка актуальність, яка гарантує впорядкування часткових даних, але не гарантує повну актуальність. Деякі додатки, такі як моніторинг артеріального тиску, можуть добре працювати й при слабкій актуальності.

9. Масштабованість. У міру росту мережі й збільшення числа користувачів система повинна масштабуватися без надмірної затримки. Потрібно контролювати обчислювальні й накладні витрати сховища.

10. Гнучкість. Пацієнт може поміняти лікарню або лікаря, і необхідно забезпечити нескладне підключення до інших центральних серверів і засобам контролю доступу. У випадку виникнення надзвичайних ситуацій лікарі, які раніше не бачили пацієнта, повинні одержати дозвіл негайно. Система повинна також обробляти непередбачені обставини, пов'язані з тим, що пацієнт перебуває в несвідомому стані або психічно нездатний контролювати роботу БНМ.

11. Підзвітність. Факт відправлення повідомлення (якщо він заперечується відправником) повинен піддаватися перевірці незалежною третьою особою, без здійснення контролю змісту, що оскаржується повідомлення.

12. Використання ключів безпеки. Необхідно для досягнення бажаної безпеки й конфіденційності при шифруванні й дешифруванні повідомлень.

17.5 Двопротокольні сенсорні мережі

17.5.1 Загальні зауваження

Сенсорні смарт-мережі на основі сучасних інформаційно-комунікаційних технологій дають можливість істотно поліпшити параметри систем тестування біологічно активних, хімічних і токсичних речовин, біологічних або біохімічних об'єктів, підвищити якість контролю параметрів, обробки й аналізу даних у багатьох областях [16].

Ці засоби нового покоління поєднують біологічні чутливі елементи (біосенсори) з перетворювачами біофізичних або біохімічних сигналів в електричні сигнали. Найважливішими з характерних ознак біосенсорів є висока чутливість і селективність, простота у використанні й швидкість аналізу концентрації речовин, а також широкий діапазон параметрів, які можуть бути обмірювані з їхньою допомогою.

Все це визначає необхідність їхнього застосування в багатьох областях, включаючи фармацевтичну, харчову, біологічну й хімічну промисловість, сільське господарство, медицину й охорону навколишнього середовища [3].

Ринок smart-сенсорів щорічно збільшується, і цей ріст прогнозується ще надовго. Цей ринок включає smart-сенсори й smart-пристрої, які можуть працювати як автономно, так і в складі безпроводових сенсорних мереж, вимірюючи параметри водного й газового середовища.

Високі темпи росту використання сенсорів обумовлені не тільки вимогами ринку, але й досягненнями як інформаційно-комунікаційних технологій, так і мікроелектроніки. Відомі світові виробники мікроелектронної елементної бази, такі як Analog Devices, Texas Instruments, Maxim і інші розробляють нові інтегральні схеми для роботи з біосенсорами, електрохімічними сенсорами, сенсорами фізичних величин і ін. Удосконалюються параметри мереж smart-сенсорів, підвищується їх енергоефективність і надійність.

17.5.2 Структура сенсорної смарт-мережі

У [6] наведені приклади використання **сенсорної смарт-мережі** для експрес-діагностики стану виноградних і плодово-ягідних культур, а також контролю процесу виробництва вина в Україні.

Для цього використана сенсорна мережа, структура якої наведена на рис. 17.18 [16]. Мережа складається з безпроводових сенсорних вузлів (смарт-мультисенсорів), кожен з яких включає набір біосенсорів, координатор сенсорної мережі й робоче місце технолога.

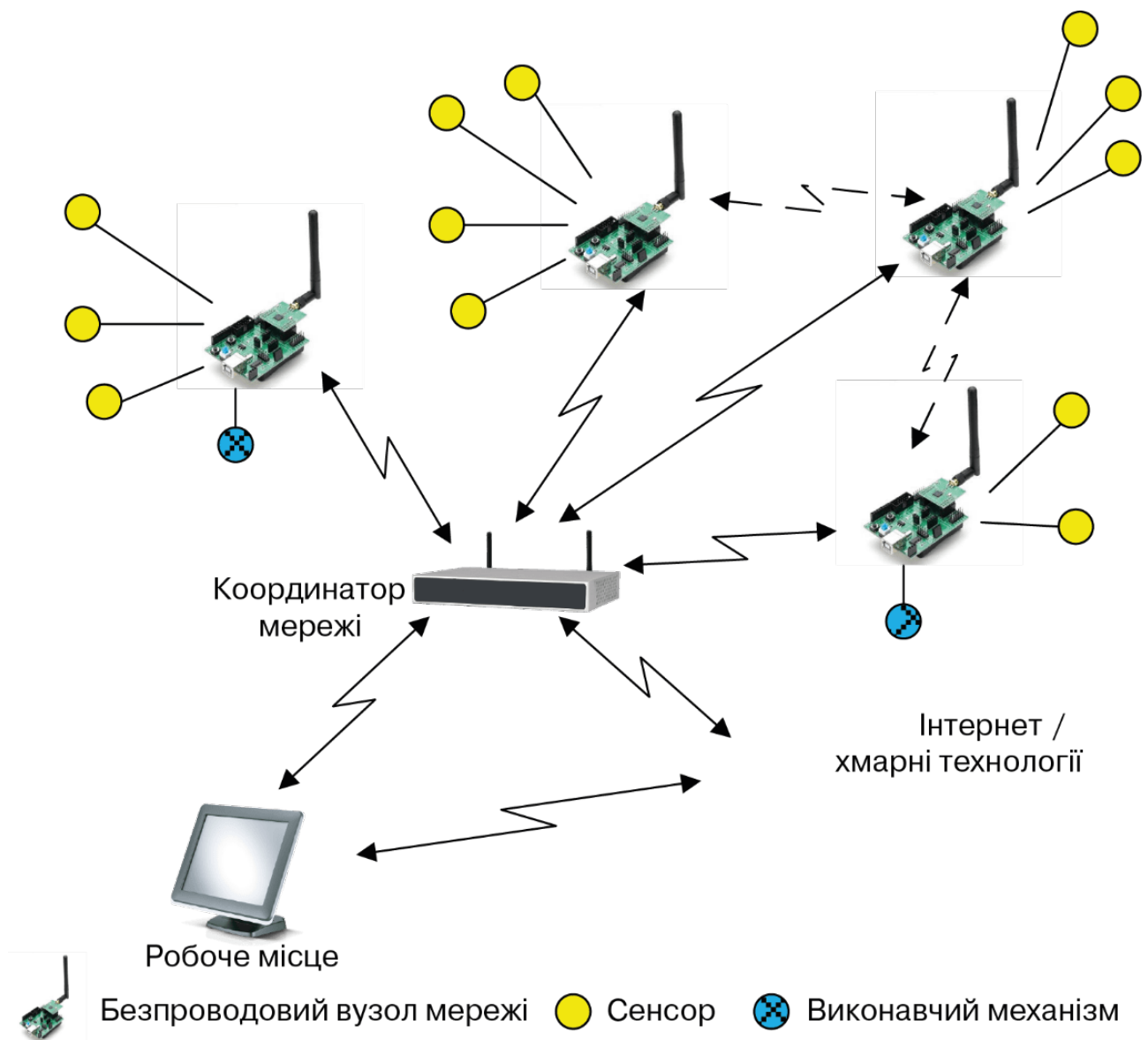


Рисунок 17.18 – Структура сенсорної мережі [16]

Керуючим вузлом мережі є координатор, основна функція якого полягає в організації мережі й підтримці роботи елементів мережі й мережі в цілому. Якщо який-небудь сенсор виходить із ладу, координатор мережі інформує про це користувача й автоматично міняє структуру мережі для забезпечення стабільності її роботи й запобігання втрати даних.

Ще одна функція координатора мережі полягає в зборі й попередній обробці обмірюваних сенсорами даних і передачі їх на робоче місце технолога. Крім того, координатор якщо буде потреба має можливість передавати дані в мережу Інтернет або хмарне середовище. Безпроводові сенсорні вузли після розгортання підключаються до координатора й утворюють мережа smart-сенсорів відповідно до заданої програми топологією. Безпроводові smart-сенсори розміщуються на технологічному устаткуванні й здійснюють вимір робочих параметрів відповідно до технологічного процесу й сертифікованою методикою.

Робоче місце технолога призначається для зберігання (архівації), обробки й візуалізації даних, які отримані від мережі smart-сенсорів, відображення стану мережі й параметрів її вузлів. За допомогою органів керування на робочому місці технолога (клавіатура або сенсорний екран монітора) передбачена можливість вилученого керування технологічним процесом через виконавчі механізми, які можуть бути включені до складу мережі. Архітектура смарт-мережі безпроводових сенсорів для застосування в промисловому виноробстві (із прив'язкою до технологічного процесу виробництва вина) наведена на рис. 17.19 [16].

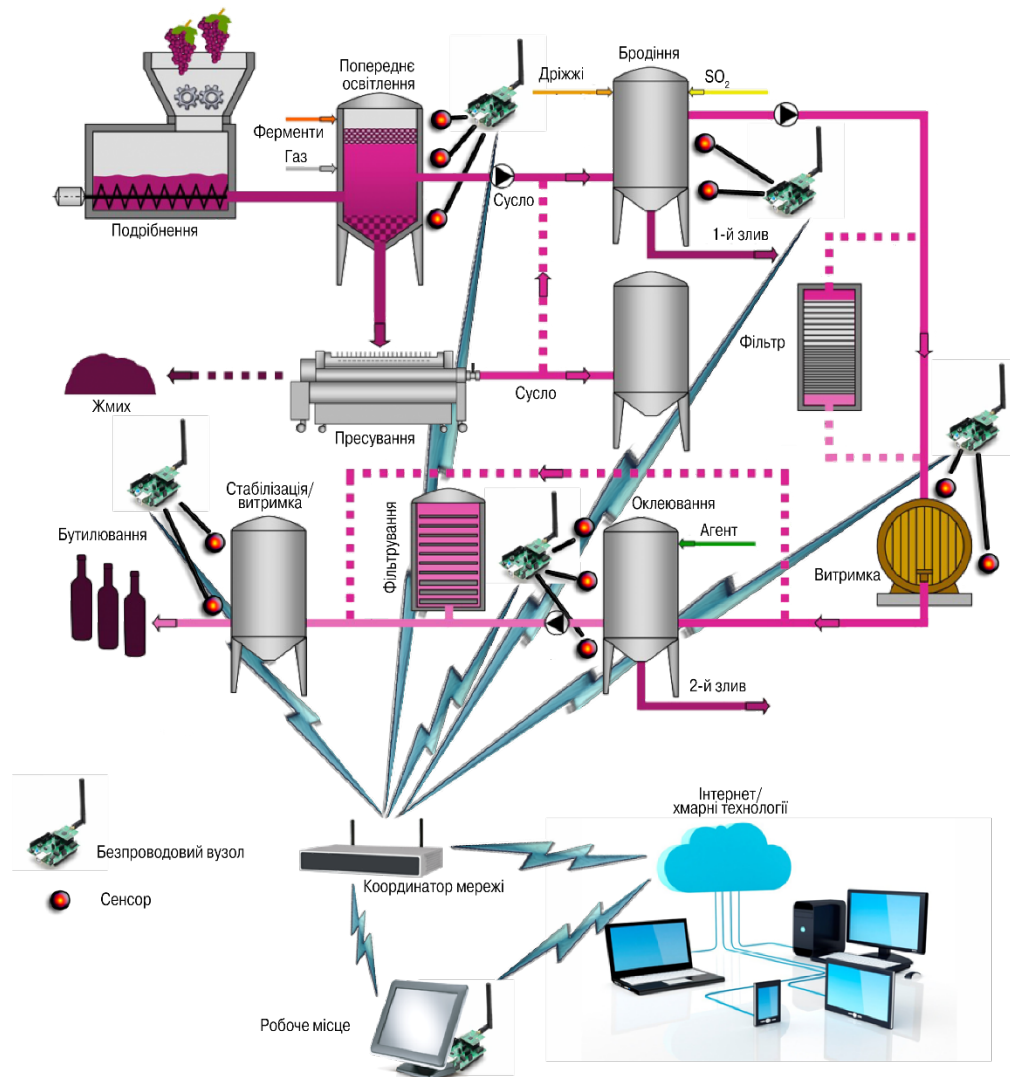


Рисунок 17.19 – Архітектура смарт-мережі безпроводових сенсорних вузлів для промислового виноробства [16]

17.5.3 Алгоритмічне й програмне забезпечення смарт-мережі

Алгоритм роботи смарт-мережі складається з наступних кроків [6]. Спочатку виконується ініціалізація сенсорів і їхнє налаштування. Після ініціалізації сенсори направляють запит координаторові на підключення до мережі. Після підключення сенсорів до мережі координатор направляє їм пакет налаштувань для роботи в мережі, після чого сенсори готові до переходу в робочий режим. У цьому режимі сенсори отримують команди керування від координатора й виконують їх. Після організації мережі координатор передає у вилучений комп'ютер запит на одержання необхідних для керування мережею команд. Потім координатор формує

стек з отриманих команд і передає їхнім сенсорам для виконання. При цьому алгоритм роботи мережі в цілому повинен відповідати технологічній карті виробництва провина.

Вимірювальний блок мультисенсора виконаний на основі прецизійного мікроконтролера ADuCM350 компанії Analog Devices. Безпроводові вузли базового варіанта мережі smart-сенсорів побудовані на базі безпроводового мікроконтролера JN5168 фірми NXP, що містить 32-разрядний RISC-процесор з тактовою частотою 32 МГц і безпроводовий прийомопередавач, що підтримує стандарт IEEE802.15.4 на основі протоколу ZigBee.

Однак, використання протоколу ZigBee у ряді додатків обмежує можливості мережних мультисенсорних вузлів. Це пояснюється тим, що реалізація цього протоколу передбачає використання проміжних перетворювачів ZigBee/USB. У той же час у мережах, у яких, наприклад, використані планшетні комп'ютери або мобільні телефони, USB-порт може бути взагалі відсутнім, а перераховані засоби підтримують стандартну мережу типу Wi-Fi або Bluetooth.

Це дозволяє в деяких додатках замінити спеціалізований координатор планшетним комп'ютером або мобільним телефоном. Для цього варіанта розроблена ще одна версія безпроводової сенсорної мережі з використання протоколів ZigBee і Bluetooth 5.

Відзначимо, що протокол Bluetooth 5 орієнтований на роботу із засобами з низьким енергоспоживанням. Це важливо для мережі з батарейним джерелом живлення. До основних переваг протоколу Bluetooth 5 (і більше пізніх його версій) відносяться наступні:

- обмін даних підтримується на відстані до 150 м (у відкритому середовищі), що практично збігається з можливостями промислового протоколу ZigBee;
- у виробничому приміщенні дальність роботи мережі Bluetooth 5 становить не менш 30-35 м.

Для підтримки роботи протоколу Bluetooth 5 у координаторі й сенсорних вузлах використаний безпроводовий мікроконтролер nRF52840 фірми Nordic Semiconductor, що наведений на рис. 17.20.



Рисунок 17.20 – Безпроводовий мікроконтролер nRF52840 [17]

Мікроконтролер nRF52840 являє собою багатопроTOCOLЬНИЙ пристрій, що підтримує роботу мереж із протоколами Bluetooth, Thread, ZigBee, 802.15.4 і іншими. Він виконаний на основі 32-розрядного процесора ARM Cortex-M4 із плаваючою комою й має тактову частоту 64 МГц. Перемикання протоколів виконується автоматично без перезавантаження програмного забезпечення. Використання протоколу Bluetooth на додаток до ZigBee значно розширює можливості розробленої мережі безпроводових сенсорів. Архітектура двопроTOCOLЬНОЇ сенсорної мережі наведена на рис. 17.21.

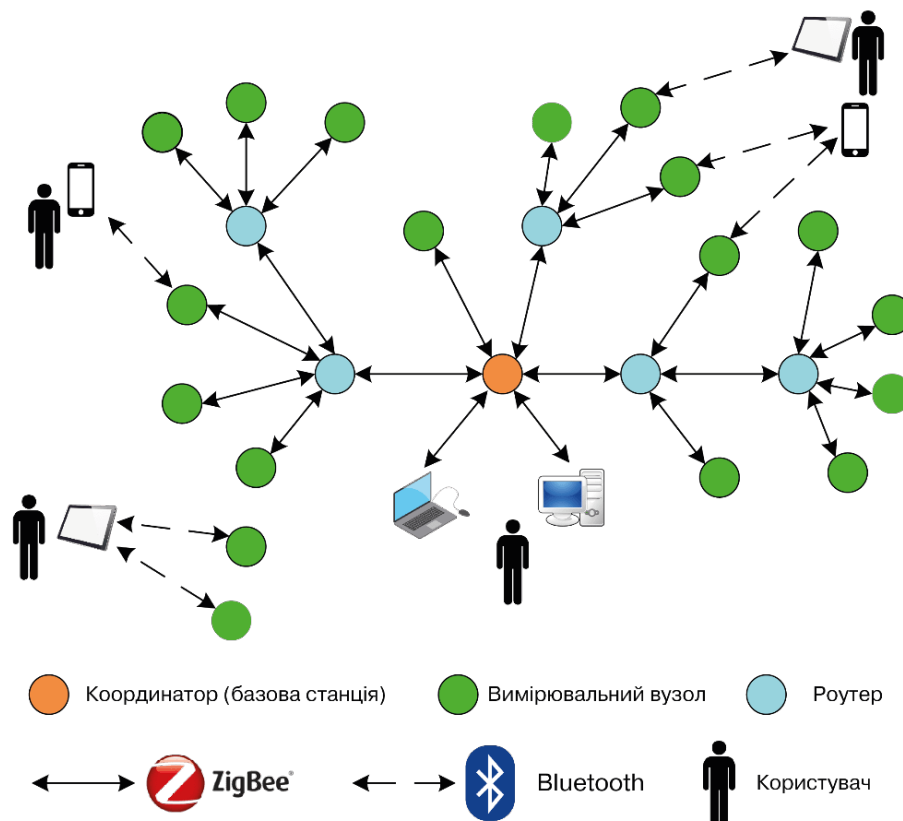


Рисунок 17.21 – Архітектура двопроTOCOLЬНОЇ безпроводової сенсорної мережі [16]

Таким чином, безпроводові сенсорні вузли мають можливість роботи як із протоколом ZigBee, так і із протоколом Bluetooth. Крім того, безпроводові сенсори такої мережі можуть працювати в автономному режимі під керуванням мобільного телефону або планшетного комп'ютера. Координатор, що підтримує роботу двопротокольної сенсорної мережі, показаний на рис. 17.22.



Рисунок 17.22 – Зовнішній вигляд координатора (без корпусу) для мережі безпроводових мультисенсоров [16]

Контрольні питання

1. Що означає термін безпроводова натільна комп'ютерна мережа?
2. Де розташовані сенсори безпроводових натільних комп'ютерних мереж?
3. Який частотний діапазон використовується комунікаційною службою медичних імплантів?
4. Чому потрібна була розробка стандарту БНМ?
5. Які параметри можуть контролювати сенсори усередині тіла?
6. Які параметри можуть контролювати сенсори на поверхні тіла?
7. Для чого призначений холтерівський монітор?
8. Яким шляхом можна попередити хворих астмою?
9. Чи існують пристрої здатні дистанційно контролювати жести людини?
10. Яким чином можна здійснювати неперервний моніторинг рівня цукру у крові людини?

11. Яким чином можна використати технології БНМ для підвищення безпеки солдатів на полі бою?
12. Чи можна дистанційно оцінити крововтрати від травм або поранень?
13. Які компоненти можуть входити до складу безпроводових натільних сенсорних мереж?
14. Яку швидкість передавання даних повинні забезпечувати БНМ?
15. Яка технологія забезпечує передавання даних по тілу людини?
16. Які вимоги висуваються до безпеки в мережах БНМ?
17. Що означає термін двопротокольні сенсорні мережі?
18. Де використовуються двопротокольні сенсорні мережі?

Перелік посилань

1. Mohamed Eddabbah, Charaf Eddine Ait Zaouiat, Mohamed Moussaoui, Yassin Laaziz Body Area Networks IEEE802.15.6 HBC Physical Layer Performances: Bit Error Rate and Message Integrity/International Journal of Computer Networks and Communications Security. vol. 4, No. 7, July 2016, pp. 207–212.
2. В. Романов Як піклуватися про літніх близьких. Електронні компоненти і системи, №3, 2024. с. 37-38.
3. IEEE 802.15 WPAN. Body Area Networks. Url: <http://www.ieee802.org>. (дата звернення: 10.07.2024).
4. IEEE 802.11, The Working Group Setting the Standards. Url: <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.ieee802.org/11/&ved=2ahUKEwj1rr39mfKJAxXYFhAIHVHILHwQFnoECBwQAQ&usg=AOvVaw2cwrIcl2oJhZSffVruVSRI> (дата звернення: 10.07.2024).
5. І. Галелюка, В. Романов Інформаційні технології в екіпіровці бійця XXI століття. Електронні компоненти і системи, №1, 2015. с. 35-40.
6. BodyCom™ Technology. Url: <http://ww1.microchip.com/downloads/en/DeviceDoc/30685a.pdf>. (дата звернення: 10.07.2024).

7. Високотехнологічний датчик. Url: <https://ua.gmleds.com/news/sports-hi-tech-wearable-lactate-sensor-54746696.html> (дата звернення: 10.07.2024).
8. Smart inhalers for asthma management: Revolutionizing Treatment Options. Url: <https://medicallprofessionals.info/smart-inhalers-for-asthma-management/> (дата звернення: 10.07.2024).
9. Liquid-based electronic materials for bioelectronics: current trends and challenges. Url: <https://pubs.rsc.org/en/content/articlehtml/2024/im/d3im00122a> (дата звернення: 10.07.2024).
10. Global China Continuous Glucose Monitoring Devices Market Is Estimated To Propelled By Continuous Technological Advancements. Url: <https://medium.com/@sneha.cmi01/global-china-continuous-glucose-monitoring-devices-market-is-estimated-to-propelled-by-continuous-a20a04d705a1> (дата звернення: 10.07.2024).
11. Поліграф SOMNOtouch NIBP – альтернативний пристрій для вимірювання артеріального тиску без манжети. Url: <https://sleeplab.com.ua/uk/poligraf-somnotouch-nibp-alternativnij-pristrij-dlya-vimiryuvannya-arterialnogo-tisku-bez-manzheti/> (дата звернення: 10.07.2024).
12. Circuitos Integrados de RF para redes sensoriaispara redes sensoriais corporais (WBAN)corporais (WBAN). Url: https://rfic.paginas.ufsc.br/files/2012/06/WBAN_UDESC.pdf (дата звернення: 10.07.2024).
13. Wireless Body Area Network Standard IEEE 802.15.4. Url: <https://ieeewban.wordpress.com/2010/06/21/efc-phy-for-human-body-communication/> (дата звернення: 10.07.2024).
14. MC1139 - BodyCom Technology. Url: <https://www.flickr.com/photos/napierrpr/8510033046> (дата звернення: 10.11.2024).
15. Microchip Technology Engineering Development Tools. Url: <https://www.mouser.do/new/microchip/microchip-development-tools/> (дата звернення: 10.11.2024).
16. В. Романов, І. Галелюка Бездротові сенсорні мережі для сільського

господарства та захисту навколишнього середовища. Електронні компоненти і системи, №2, 2017. с. 13-18.

17. Nordic nRF52840 Dongle. Url: <https://evo.net.ua/nrf52840-dongle/> (дата звернення: 10.11.2024).

18 СМАРТ-ТЕХНОЛОГІЇ В ІОТ

18.1 Інтелектуальний будинок

18.1.1 Загальні зауваження

Поняття "інтелектуальний будинок" означає будинок, "який здатний пристосовуватися до змін навколишнього середовища" [1-3]. Інакше кажучи, цей будинок, інженерні системи якого здатні забезпечити адаптацію до можливих змін у майбутньому.

Сьогодні вже можна говорити про "стандарт" поняття "інтелектуальний будинок". Під цим мається на увазі стійка сукупність характерних рис, властивих такому будинку:

- надання певного набору послуг мешканцям будинку;
- наявність здатності оптимально реагувати на зміни в процесах, що відбуваються в будинку;
- сполучення "децентралізованих" (розподілених) принципів побудови систем з "централізацією" функції моніторингу;
- структурований підхід до побудови інженерних систем будинку; можливість внесення змін з мінімальними витратами.

"Інтелектуальний будинок" – складне поняття. Це й "будинок", і "комплекс систем", і "технологія" і т.д. Інтелектуальний будинок можна визначити і як сучасну технологію автоматизованих комплексів систем інженерного устаткування будинку з певним ступенем їхньої інтеграції на основі структурованих кабельних систем і стандартів відкритих систем.

Термін "інтелектуальний будинок" узагальнює:

- житловий будинок/готель;
- будинки загального користування (офіси, дитячі, навчальні, медичні, культурно-просвітні заклади, адміністративні будинки, місця торгівлі й ін.);
- приміщення й спорудження виробничого (цех, ділянка...) і невиробничого (склад, стоянка...) призначення.

"Інтелектуальний будинок" є продуктом сучасного розвитку існуючих систем автоматики в будинках у напрямку:

- комплексної оптимізації використання ресурсів; підвищення гнучкості конфігурування й зниження загальної вартості володіння;
- інтеграції із широким спектром технологічного й телекомунікаційного устаткування;
- спрощення взаємодії з користувачем.

На рис. 18.1 [4] наведені компоненти інтелектуального будинку.



Рисунок 18.1 – Компоненти інтелектуального будинку [4]

Принципово важливим є розуміння того, що кожний елемент інтелектуального будинку повинен бути інтелектуальним елементом, тобто при його проектуванні використана методологія, що буде змушувати цей елемент прагнути до вибору оптимального рішення в експлуатації, але, звичайно, з урахуванням впливу інших елементів на нього і його впливу на інші елементи. Наслідком цього є можливість створення інтелектуальних елементів

інтелектуального будинку по різних напрямках, а потім їхнього об'єднання на основі системного аналізу.

18.1.2 Комплекс систем безпеки, життєзабезпечення та інформатизації

Інженерне устаткування сучасного будинку являє собою комплекс складних інженерно-технічних систем безпеки, життєзабезпечення, інформатизації з відповідними системами керування [3]. До складу такої системи інтелектуального будинку входять:

1. Інтегрований комплекс технічних засобів безпеки:

- система керування доступом;
- система охоронно-тривожної сигналізації; система відеоспостереження; система збору й обробки інформації;
- система пожежної сигналізації й оповіщення про пожежу; система автоматичного пожежогасіння.

2. Комплекс систем життєзабезпечення:

- системи опалення, вентиляції й кондиціонування повітря; система керування мікрокліматом;
- система гарантованого безперебійного електропостачання; система вилученого моніторингу й керування електропостачанням; системи висвітлення й керування висвітленням;
- система обліку енергоносіїв і інші системи;
- системи контролю й керування ліфтами, ескалаторами та ін.

3. Комплекс систем інформатизації:

- локальна обчислювальна мережа (ЛОМ);
- система прийому ефірного й супутникового телебачення; система радіофікації;
- система телефонної мережі;
- система проведення конференцій із синхронним перекладом;

- засоби оперативного радіозв'язку персоналу й інші системи.
- 4. Структурована кабельна система (СКС);
- 5. Єдиний центр диспетчеризації.

Важливою частиною є автоматизовані системи керування, які й становлять суть інтелектуального будинку. Всі слабкострумові системи контролю поєднуються на основі СКС у систему диспетчеризації інженерного устаткування будинку з єдиним центром моніторингу систем.

18.1.3 Інтеграція й керування

Інтеграція систем забезпечує:

- підвищений рівень безпеки будинку в цілому (запобігання аварій, забезпечення безперервності процесів та ін.);
- чітка взаємодія роботи всіх інженерних систем із пріоритетом системи пожежної безпеки;
- організацію мережної структури керування з реалізацією функцій автоматичного контролю, обробки й зберігання інформації про стан систем з єдиного диспетчерського пульта керування;
- сполучення автоматичного й ручного режимів керування, що забезпечує оперативний контроль чергового персоналу за станом кожного елемента інженерних систем з диспетчерського пульта;
- високий рівень керування середовищем перебування.

Розглянемо приклад взаємодії систем у інтелектуальному будинку при виникненні надзвичайної ситуації. Так, при виникненні пожежі (вогнища загоряння) "спрацьовують" сповіщувачі системи пожежної сигналізації (СПС). Сигнал від них передається на пожежну панель, що формує команду включення світлових, звукових і мовних сповіщувачів. При цьому СПС також формує сигнали для виконання іншими системами інтегрованого комплексу по заданих алгоритмах:

1. Система відеоспостереження "направляє" найближчу відеокамеру на вогнище загоряння й привласнює цій відеокамері вищий пріоритет. На моніторі

спостереження формується повноекранне зображення із цієї відеокамери, і відеореєстратор переходить у режим пріоритетного запису "картинки" із тривожної відеокамери.

2. Система керування мікрокліматом виключає приточну систему вентиляції, що обслуговує дану зону, щоб запобігти надходженню свіжого повітря до вогнища загоряння. Для видалення диму з коридорів, холів, сходів (уздовж маршрутів евакуації) включається відповідна підсистема димовидалення (відкриваються заслінки, включаються вентилятори).

3. Система керування електропостачанням відключає кола електроживлення поблизу зони пожежі.

4. Система керування освітленням включає аварійне освітлення.

5. Система керування доступом розблокує двері для безперешкодної евакуації людей.

6. Система керування ліфтами спустить їх на перший поверх і т.д.

Одночасно сигнал надходить у єдиний диспетчерський центр на автоматизоване робоче місце (АРМ) оператора. На моніторі АРМ з'являється графічна й текстова інформація про пожежу й місце його виникнення. Оператор має можливість проконтролювати роботу системи автоматики й при необхідності продублювати її. Ці дії можуть бути забезпечені тільки за рахунок взаємодії окремих систем комплексу будинку, таких як СПС, системи керування освітленням, мікрокліматом, доступом, електропостачанням і ліфтами.

Саме наявність таких взаємозв'язків між окремими системами комплексу дозволяє говорити про дійсно інтелектуальний будинок, коли комплекс здобуває нову якість – інтегрованість. Інтегрований комплекс не є простою сумою окремих систем, а на основі єдиної платформи керування здобуває нові властивості, відсутні в складових.

18.1.4 Об'єднана кабельна система (СКС + силова мережа)

Структурована кабельна система (СКС) призначена для організації фізичного рівня системи передавання інформації в локальних обчислювальних і телекомунікаційних мережах. СКС забезпечує швидку й легку зміну конфігурації кабельної системи за допомогою комутації на кросових панелях. СКС, що поєднує всі слаботочні системи (ЛОМ, телефонію й т.д.), створює єдину інформаційну кабельну мережу будинку. Єдина інформаційна інфраструктура забезпечує необхідну взаємодію систем і служб будинку, його цілісність як єдиного організму [5, 6].

СКС створюється на основі стандартів і задовольняє вимогам, пропонованим до відкритих систем. Конфігурація СКС і застосовуване устаткування забезпечують можливість нарощування системи без порушення працездатності змонтованої частини системи. При розробці робочої документації передбачається можливість прокладки кабелів всіх вищевказаних систем і 30% резерв для забезпечення подальшого розвитку.

Кабельна система є компонентом інтелектуального будинку із самим тривалим часом життя, довше якого існує тільки каркас будинку. Вважається, що недосконалі кабельні системи є причиною до 70% всіх простоїв інформаційно-обчислювальних мереж. Тому правильна організація кабельних систем, що визначають надійність функціонування всіх служб будинку, є однією із ключових завдань при створенні інтелектуальних будинків.

Об'єднана кабельна система (СКС + силова електромережа) будинку – це багатофункціональне фізичне середовище, що забезпечує передавання й розподіл електроенергії й інформації, а також моніторинг і керування системами будинку [3].

18.1.5 Стандарти об'єднання систем інтелектуального будинку

При оснащенні будинку різними системами й устаткуванням від різних виробників важливо, щоб технічні пристрої не "конфліктували" між собою, а були б сумісні й представляли єдине ціле. Проблема сумісності була вирішена через розробку "стандартів відкритих систем". В основі побудови інтелектуального будинку саме й лежать принципи "відкритої архітектури". Під "відкритістю" ми будемо розуміти наявність єдиного мережного протоколу в устаткування різних виробників, що забезпечує "правильне" взаємодію всіх інженерних систем будинку. Можливість обміну даними забезпечує мережну сумісність систем і можливість інтеграції систем у єдиний комплекс, "працюючий як годинники".

У цей час широке поширення в області систем керування будинками одержали стандарти BACnet, LonWorks, EIB і ін. Стандарт BACnet (Building Automation Control Network – мережний протокол для автоматизації будинків) був розроблений американським суспільством інженерів по опаленню й кондиціонуванню повітря (ASHRAE). Стандарт EIB (European Installation Bus) – європейська інсталяційна шина – призначений для керування енергоспоживанням, освітленням, жалюзі, мікрокліматом і для контролю доступом. У цей час практично скрізь замінюється стандартом KNX, розробленим на основі стандарту EIB.

У травні 1999 відбулося об'єднання трьох європейських асоціацій автоматизації будинків EIBA (European Installation Bus Association), EHSA (European Home Systems Association) і BCI (BatiBUS Club International) в одну, котра згодом одержала остаточну назву "Асоціація KNX" – Konnex. Відбулося й злиття трьох технологій: EIB, EHS і Batibus. Наприкінці 2003 року технологія була затверджена як європейські стандарти EN 50090 і EN 13321-1, а потім як міжнародний стандарт ISO/IEC 145433-3, американський стандарт ANSI/ASHRAE 135 і китайський стандарт GB/Z 20965

18.1.5 Переваги комплексу систем інтелектуального будинку

У цілому концепція інтелектуального будинку спрямована на задоволення індивідуальних вимог замовника в керуванні будинком. Комплексні системи керування забезпечують мешканцям будинку безпеку й комфорт, одержання інформації про стан систем будинку в зручній формі, ефективне використання устаткування. У підсумку – зниження експлуатаційних витрат і споживання енергоресурсів і води [8].

В інтелектуальному будинку оптимізовані основні елементи "середовища перебування" (структура, системи, служби, керування) і взаємини між ними. Експерти вважають, що застосування комплексних інтегрованих систем заощаджує не менш 15% витрат власника на установку за рахунок усунення надлишкових зв'язків в інфраструктурі. Менше витрат потрібно й на навчання персоналу об'єкта керуванню комплексом. Власник одержує можливість управляти всіма системами об'єкта з однієї робочої станції.

У порівнянні з автономними системами комплексна система має наступні переваги:

- істотна економія на кабельних мережах і мережному встаткуванні; зниження енергоспоживання й підвищення надійності всієї системи; підвищення оперативності керування об'єктом;
- графічне подання інформації про стан систем і устаткування на різних рівнях (об'єктовому, зональному, адресному);
- зниження трудовитрат експлуатаційних і диспетчерських служб;
- забезпечення необхідної взаємодії систем;
- зниження ймовірності виникнення страхових випадків;
- "відкритість" комплексу, що забезпечує можливість його нарощування й використання устаткування різних виробників.

Витрати на будівництво таких будинків, звичайно, вище, ніж на будівництво будинків із традиційним складом інженерного устаткування. Однак не слід забувати, що сукупна вартість будинку являє собою суму витрат на будівництво й

експлуатаційні витрати протягом всього "життя" будинку. За деякими оцінками вартість експлуатації "усередненого" будинку перевищує вартість будівництва в десятки разів! Всі гроші ми витрачаємо на експлуатацію. У Європі все навпаки – більше "вкладають" у будівництво, щоб істотно заощаджувати в період експлуатації будинку.

18.1.6 Енергоефективні будинки

Energy-efficiency Building (енергоефективний будинок), Intelligent Building (інтелектуальний будинок), Bioclimatic Architecture (біокліматична архітектура), Healthy Building (здоровий будинок) – це напрямки в архітектурі й інженерії будинків, які дотепер не мають строгих визначень, наукові основи тільки створюються, але самі напрямки реалізовані у великій кількості будівельних об'єктів, у забудовах районів міст і сільських об'єктів [9, 10].

Реалізовані в розвинених країнах. Однак, навіть у розвинених країнах будівництво таких будинків усе ще залишається заняттям елітним. Поясненням цьому може бути наступне:

- низька вартість традиційних джерел енергії без врахування інтересів наступних поколінь і турботи про навколишнє природне середовище сприяє марнотратності її використання (хоча останнім часом ця ситуація змінюється на краще);
- споживачі не готові до значного підвищення оплати за якість комфорту середовища перебування, включаючи в це поняття комплекс сучасних технічних засобів керування, контролю й зв'язків (системи життєзабезпечення й керування будинком);
- не сформувалася наука про мікроклімат приміщень.

На сьогоднішній день енергоефективні будинки (рис. 18.2) містять у собі складовими частинами всі інші типи перерахованих вище будинків. Тут важливим є встановлення ідеології взаємопроникнення й взаємозв'язки між різними типами будинків, наприклад, між енергоефективними й інтелектуальними будинками.

енергоефективний будинок не є просте підсумовування енергозберігаючих рішень в одному об'єкті, а є результат вибору за допомогою системного аналізу на основі математичного моделювання сукупності взаємозалежних технічних рішень, що щонайкраще відповідає мети енергозбереження. З іншого боку, математичні моделі, використовувані при проектуванні будинки, можуть і повинні стати основою функціонування систем керування й контролю інтелектуального будинку.

Буде корисним привести тут визначення інтелектуального будинку, дані різними фірмами, тому що вони доповнюють і розвивають один одного, розглядають об'єкт із різних позицій і в результаті створюють досить закінчену картину для зацікавленого фахівця.

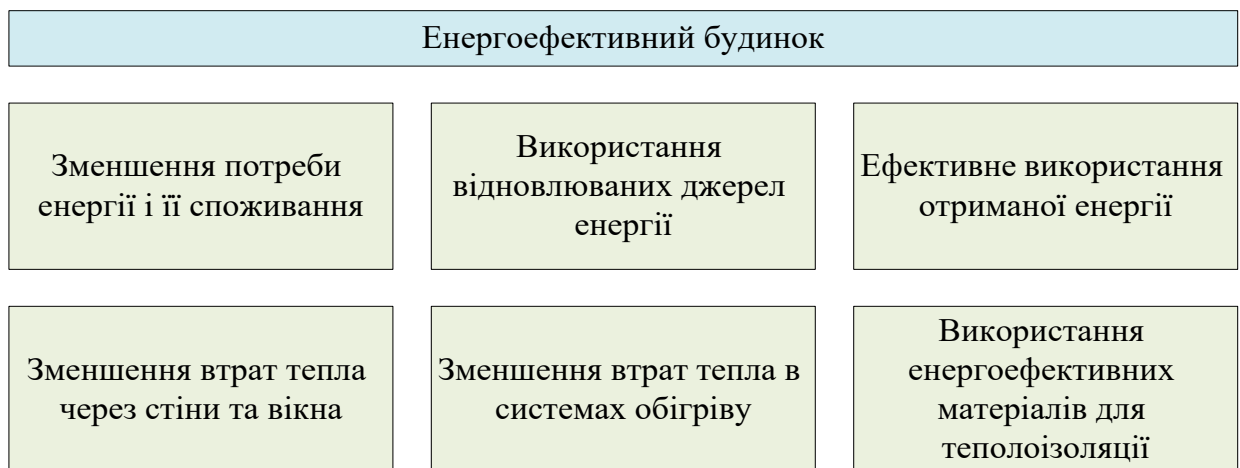


Рисунок 18.2 – Вимоги до енергоефективної будинку

Одним з компонентів інтелектуального будинку є керування системами опалення вентиляції й кондиціонування повітря. У світовій практиці накопичений значний досвід проектування таких систем як елемента інтелектуального будинку.

Основними завданнями системи теплопостачання є:

- забезпечення істотної економії енергії, затрачуваної на опалення й вентиляцію виробничих приміщень;
- підвищення якості теплового комфорту;
- підвищення якості контролю технічного стану встаткування системи;

- створення банку можливих аварійних ситуацій, їхньої діагностики й рекомендацій з ведення технологічного процесу – теплопостачання будинку й роботі обслуговуючого персоналу в цих умовах, тобто розробка інтелектуального елемента системи експлуатованого будинку.

Керування такою системою здійснюється пакетом спеціалізованих програм, якому можна умовно розділити на три групи:

- оптимізуючі;
- основні робочі;
- допоміжні, обслуговуючі системи.

Програма оптимізації витрати теплоти на опалення виконує дві основні функції: періодично обчислює витрату теплоти, необхідної для підтримки заданого мікроклімату в окремих місцях будинку в робочий час, і визначає режим зниження температури в неробочі годинники й підвищення її до заданого значення в робочі годинники.

Програма-спостерігач дозволяє стежити за розвитком процесу протягом тривалого часу, видає повідомлення про відхилення за верхню або нижню границі заданих параметрів. Одержувана інформація необхідна для контролю й оцінки роботи системи.

Програма тривоги реагує на різні аварійні ситуації (вихід з ладу опалювально-вентиляційного устаткування й автоматики, розбиті стекла й т.д.) і діагностує їх.

Програма пуску й включення регулювальних опалювальних пристроїв працює разом із програмою оптимізації й використовує відомості про конкретні регулювальні виконавчі механізми.

Робоча програма здійснює зв'язок оператора із системою у формі діалогу. За допомогою цієї програми можна змінити режим роботи системи, а також одержати різну інформацію про її роботу.

Програми обліку роботи виконавчих механізмів накопичують відомості про годинники їхньої роботи й повідомляють про несправності, а також про строки профілактичних робіт.

Програми обчислення загальної витрати енергії й нагромадження цієї витрати в часі одержують і накопичують відомості за день, за тиждень, за місяць і т.д.

Програма складання звіту веде статистику даних вимірів і обчислень, а також стану встаткування опалення й вентиляції, друкує звіти щодня, щотижня, щомісяця про середні, мінімальні й максимальні значення, аварійні сигнали, витратах, економії енергії та ін.

18.2 Розумний офіс

18.2.1 Особливості БЦ

За деяким даними, якщо оцінювати вартість володіння будинком при середньому строку експлуатації 40 років, то вартість будівництва становить тільки близько 10%, вартість експлуатації – 90% за цей період. Оцінки окупності бізнес центрів (БЦ) в Україні різні – від 2 до 5 років [9].

Припустимо, що стратегія інвестора не перепродаж БЦ, а одержання прибутку за рахунок експлуатації. Ціль власника бізнес центра – найбільший гарантований прибуток від експлуатації, що буде визначатися максимальними ціною оренди площі й завантаженням і мінімальними експлуатаційними витратами.

Критерій оцінки ефективності системи керування – мінімізація експлуатаційних витрат при підвищенні якості середовища й технічного комфорту. Видимо, кожний власник бізнес центру погодиться з визначенням "інтелектуальне" для будинку з такою системою керування.

Склад інженерних систем бізнес центра в принципі практично не відрізняється від складу інженерних систем будь-якого сучасного будинку.

Особливості БЦ, які істотно відрізняють його від інших будинків [10]:

1. Приміщення БЦ можуть належати окремим власникам або експлуатуватися на умовах оренди.
2. Приміщення або цілі поверхи можуть бути вільні досить тривалий час.

3. Режим роботи з 9:00 до 18:00. При цьому окремі орендарі можуть перебувати в приміщеннях до або після робочого часу.

4. Змінна кількість людей.

5. Орендарям необхідне якісне середовище: оптимальна температура повітря, вологість і якість повітря, оскільки ці фактори істотно впливають на ефективність роботи персоналу.

6. Орендарі зацікавлені в об'єктивному контролі наданих послуг, у тому числі тепла, енергопостачання й ін.

Отже, для ефективної експлуатації інженерних систем будинку важливими вимогами є:

1. Планування режимів роботи устаткування відповідно до розкладу.

2. Можливість консервування окремих приміщень на тривалий період з мінімальними витратами на енергопостачання.

3. Керування енергоємними системами "по запиту" – залежно від присутності людей і їхніх кількостей.

4. Технологічний облік енергоресурсів для розрахунків з орендарями, інтеграція з фінансовими системами.

5. Можливість контролю й зміни орендарем параметрів планувальників, уставок температур для своїх приміщень на основі простого, зрозумілого інтерфейсу.

Ці вимоги прямо пов'язані із проектами по різних інженерних системах. Отже, для погоджених проектних рішень по різних системах необхідні грамотна загальна концепція й технічне завдання.

Істотне значення в експлуатаційних витратах мають дві групи витрат:

1. Витрати на експлуатацію й ремонтно-технічне обслуговування інженерного устаткування, у тому числі послуги сторонніх сервісних організацій і заробітна плата персоналу.

2. Витрати на енергоспоживання будинку – оплата за спожите тепло, газ, електроенергію.

У країнах з розвитий економікою будинки споживають близько 40% енергії.

Найбільш енергоємними є системи опалення, вентиляції й кондиціювання повітря будинків. Велике енергоспоживання систем будинків є причиною значних перевантажень і серйозних аварій у системах електропостачання міст і цілих регіонів, у тому числі й у Києві.

18.2.2 Особливості інженерних систем БЦ

Очевидно, що витрати на енергоспоживання будуть істотно нижче для БЦ, у яких застосовуються системи з рекуперацією тепла й енергоефективні локальні котельні.

Традиційно для систем кондиціювання повітря в БЦ, що будуються в Україні, широко застосовується схема чиллер/фанкойл, як система з низькими початковими інвестиціями. Вона забезпечує зміну температури повітря по сигналу датчика температури в приміщенні при постійному обсязі приточного повітря. У системах із централізованим контролем температура повітря в кожному із приміщень відображається на диспетчерському терміналі.

На рис. 18.3 наведений приклад системи чиллер/фанкойл у БЦ.



Рисунок 18.3 – Приклад системи чиллер/фанкойл у БЦ [11]

Критерієм оцінки ефективності системи керування можна вважати мінімізацію експлуатаційних витрат при підвищенні якості середовища й комфорту.

Наприклад, якщо прийняти за комфортне значення зміст CO_2 не більше 800 ppm, то перевищення його змісту над комфортним простежується на інтервалі 85% робочого часу. При цьому 16% робочого часу зміст CO_2 перевищує верхнє граничне значення в 1400 ppm. Надлишковий обсяг повітря, що подається системою вентиляції (виділений зеленими кольорами), залежно від часу й кількості людей у будинку становить більше 50%. Керування вентиляцією "по запиту" на основі змісту CO_2 дасть істотну економію ресурсів.

Досконалі платформи керування забезпечують диспетчеризацію всіх основних систем будинку: керування освітленням, енергообліку, систем охорони й контролю доступу, систем відеоспостереження, контролю складу повітря, температури й інших.

На рис. 18.4 наведений приклад системи диспетчеризації офісного будинку [12].

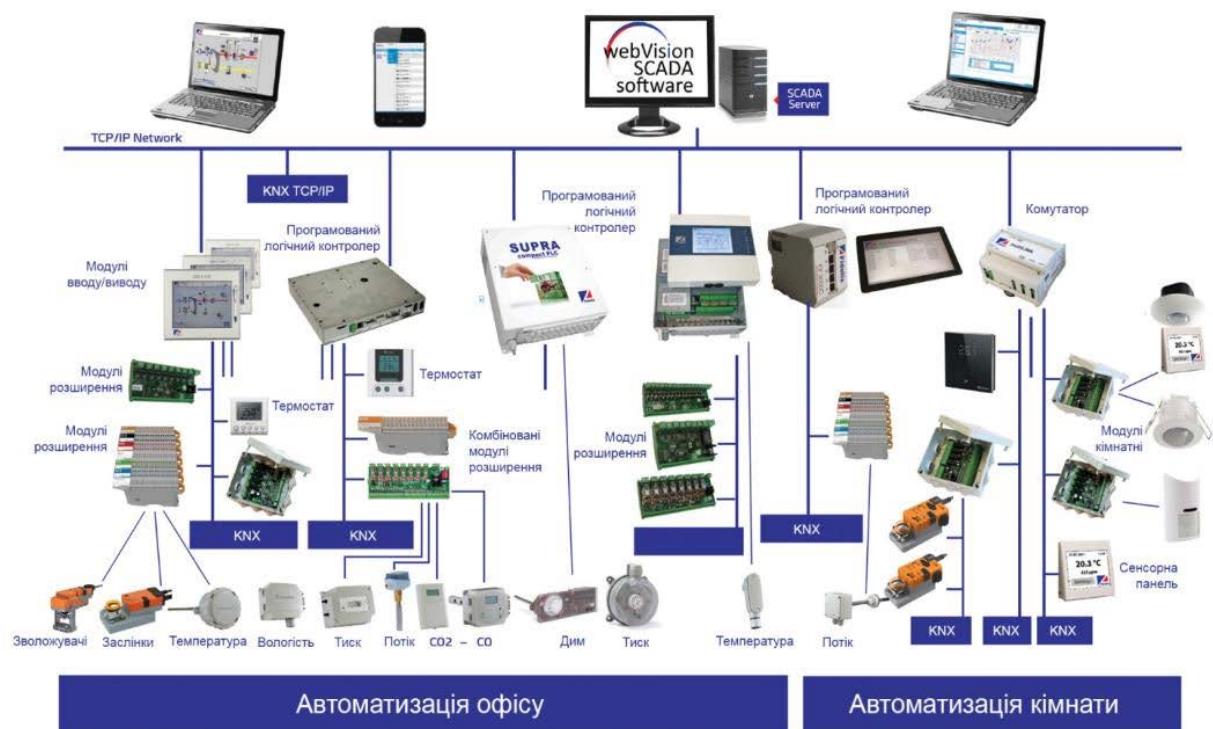


Рисунок 18.4 – Приклад системи диспетчеризації офісного будинку [12]

За межами нашої країни переважно використовується більш енергоефективна схема на основі систем зі змінною витратою повітря. Система може контролювати температуру, а також контролювати й змінювати витрату повітря як по окремих приміщеннях, так і центральними припливно-витяжними установками. Важливою перевагою таких систем є низький рівень шуму.

Можна простежити залежність параметрів мікроклімату для приміщення офісного центру із ціною оренди біля \$20 без системи припливно-витяжної вентиляції. Площа приміщення 50 м², у ньому постійно перебувають 4-5 співробітників.

У робочий час зміст вуглекислого газу (CO₂) перевищує 1700 ppm при підвищенні чутливості до заходів від 800 ppm і граничних значеннях до 1000...1400 ppm. Для провітрювання потрібно періодично відкривати вікна, але якщо офіс у центрі міста, із за шуму й вихлопних газів автомобілів це приносить тільки додатковий дискомфорт.

Системи примусової вентиляції розраховуються на основі кратності повітрообміну. Оскільки при проектуванні БЦ розрахунок виконується на базі усереднених показників, то при реальній експлуатації це приводить або до істотної перевитрати енергоносіїв (із за надлишкової вентиляції), або до зниження якості повітря.

При зниженні якості повітря (підвищенні змісту CO₂) різко погіршується самопочуття й знижується ефективність роботи співробітників, що можуть підтвердити орендарі багатьох БЦ. А, відкриваючи вікна для провітрювання, марно витрачаються енергоносії на нагрівання/охолодження атмосфери.

Таким чином, якісна енергоефективна система повинна мати можливість регулювання кількості припливу свіжого повітря залежно від змісту вуглекислого газу CO₂.

Для керування системами як холодо- так і тепlopостачання застосовується так називане каскадне керування декількома нагрівачами, частотне керування насосами. При цьому досягається істотна економія енергоносіїв.

Системи технологічного енергообліку важливі при зацікавленості орендарів

у зниженні своїх витрат шляхом контролю й оптимізації енергоспоживання (платимо тільки за надані послуги).

18.2.3 Система керування БЦ

Чого очікує замовник від системи керування будинком [13]:

1. Повний контроль інженерних систем одним диспетчером.
2. Надійну систему для роботи в цілодобовому режимі.
3. Можливість вилученого контролю.
4. Контроль і оптимізація енергоспоживання.
5. Можливість аналізу й оптимізації параметрів.
6. Можливість інтеграції із системами безпеки: контролю доступу, охорони, відеоспостереження.
7. Ефективність інвестицій і можливість розширення в майбутньому.

Системи керування будинками (СКБ) базуються на основі систем збору даних і оперативного диспетчерського керування (SCADA), які в нас прийнято називати системами диспетчеризації.

Основні функції систем диспетчеризації (рис. 18.5):

1. Відображення стану устаткування будинку на інтуїтивно зрозумілих графічних мнемосхемах.
2. Об'єктивний контроль параметрів, їхня реєстрація в БД.
3. Налаштування параметрів систем керування відповідно до заданих критеріїв.
4. Реєстрація тривог.
5. Реєстрація дій персоналу.
6. Вилучений контроль устаткування по різних каналах зв'язку.



Рисунок 18.5 – Диспетчерський центр інтелектуального будинку [14]

Багато виробників для відображення й реєстрації параметрів випускають мережні дисплеї й апаратні веб шлюзи, які також застосовуються в невеликих будинках БЦ, де не потрібне інтегроване керування й більші архіви даних.

Для автоматизації інженерних систем БЦ використовуються вільно програмовані мережні контролери, які дозволяють реалізувати практично будь-які алгоритми керування.

Широко застосовуються як стандартні для СКБ логічні протоколи – KNX, LonWorks, BACnet, так і багато інших – Modbus, NCP, Arcnet, SNMP. Як мережа передачі даних всі частіше використовується мережа Ethernet, що легко інтегрується в СКС будинків.

18.3 Розумне місто

18.3.1 Поняття "розумного" міста

"Розумне" місто – це інтеграція багатьох інформаційних та комунікаційних технологій (ІКТ) та Інтернету речей (IoT-рішень) для управління міським господарством. Побудова будь-якого "розумного" міста призводить до розвитку всієї країни. Розумне місто об'єднує інформаційно-комунікаційні технології за допомогою IoT [15, 16]. Вони використовуються для підтримки міських ресурсів, таких як управління містом, інформаційні системи, бібліотеки, школи, лікарні, системи переробки відходів, транспортні системи, тощо (рис. 18.6).

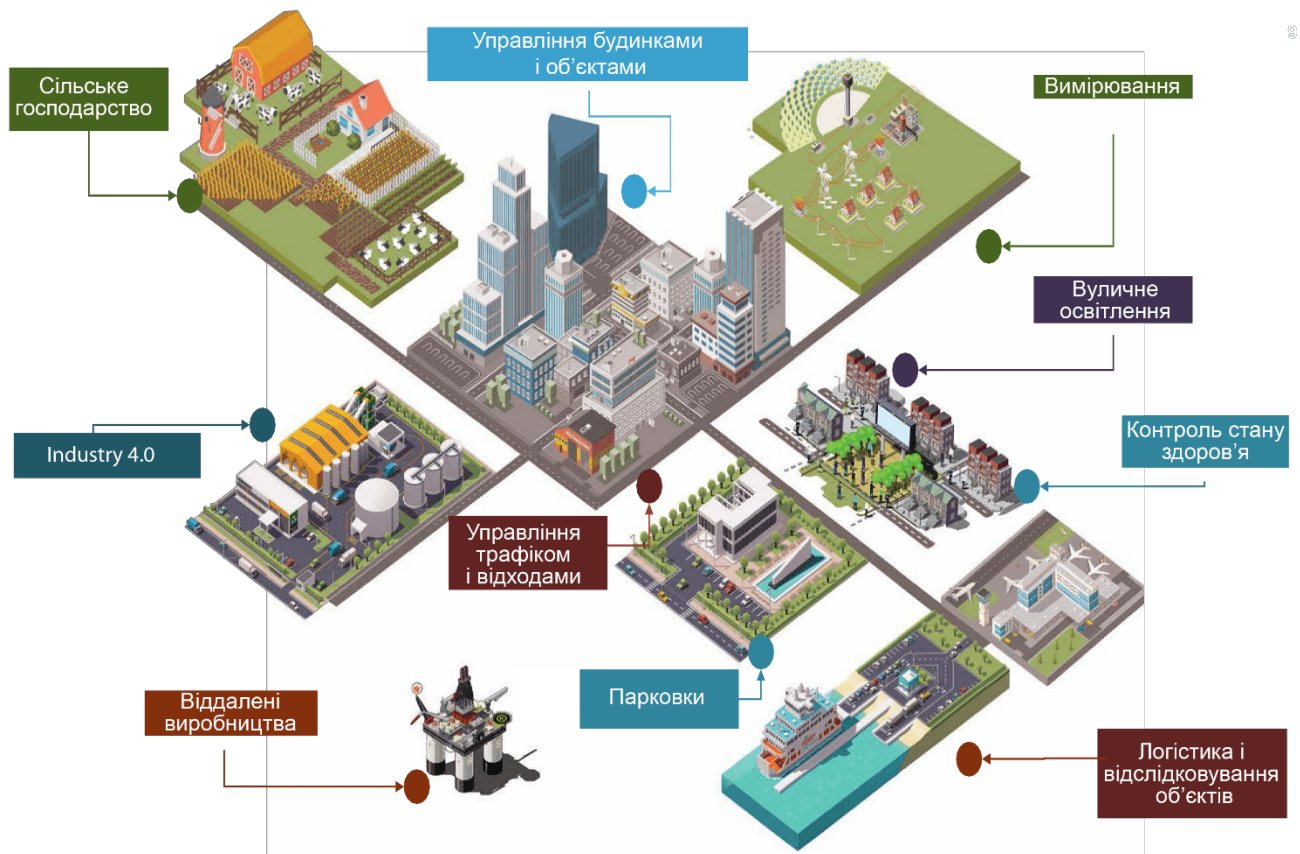


Рисунок 18.6 – Інформаційно-комунікаційні технології "розумного" міста [17]

Мета "розумних" міст – робити життя місцян зручнішим та безпечнішим, а також економія міських коштів та простору. Наприклад, з розумними ліхтарями на

вулицях міста так же безпечно вночі, як і з звичайними, але при цьому кошти на електроенергію тратяться мінімально (світло не горить впусту, поки не стемніло). В ідеальному розумному місті майбутнього технології зустрічають жителів на кожному кроці, формуючи єдину екосистему і відповідаючи за всі аспекти життя людини: від перевищення швидкості до переробки сміття. Розглянемо деякі з систем розумного міста.

18.3.2 Система моніторингу вивозу сміття

В [18, 19] запропоновано систему для контролю очищення смітєвих баків. Оскільки необхідно підтримувати рівень чистоти в місті, тому дуже важливо очищати смітєві баки, як тільки вони заповнюються. В такій системі ультразвуковий датчик використовується для виявлення рівня сміття (рис. 18.7).

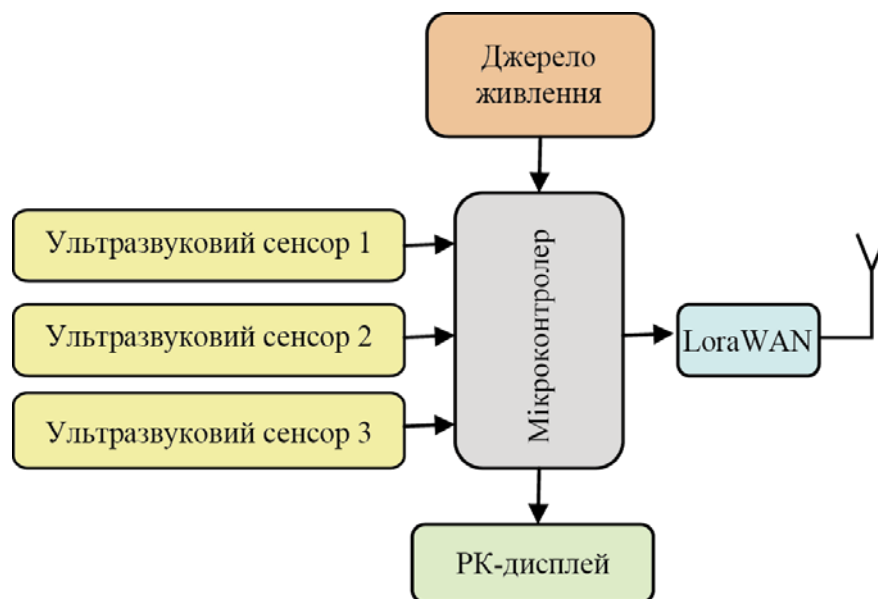


Рисунок 18.7 – Сенсорний вузол для збору інформації про наповнення смітєвих баків

Датчик рівня сміття складається з ультразвукового датчика (від одного до трьох) і мікроконтролера. Датчик, розміщений всередині смітника, визначає рівень сміття. Модуль LoRa передає повідомлення в центр управління через міську мережу LoRaWAN. З центру інформація щодо вивезення сміття надсилається відповідній

службі району, і вона відображається на РК-дисплеї. Інформація про заповнення містить номер вантажівки та точне місце розташування сміттового бака. Якщо сміттовий бак не замінюється протягом певної тривалості часу, мікроконтролер надсилає повторне повідомлення. Розумний сміттовий бак є кращим способом підтримувати довкілля в чистоті та здоров'ї.

18.3.3 Система виявлення витоків газу

Ця система призначена для екстреного інформування відповідні служби при виявленні витоків газу для попередження аварій [20, 21]. На рис. 18.8 наведено модуль контролю витоку побутового газу що складається з газового сенсора, мікроконтролера та модуля зв'язку LoraWAN. Коли сенсор, розміщений в модулі, виявляє витік газу, мікроконтролер через міську мережу LoraWAN надсилає тривожне повідомлення в центр моніторингу і регулярно повторює його, поки відповідні служби не усунуть аварію.

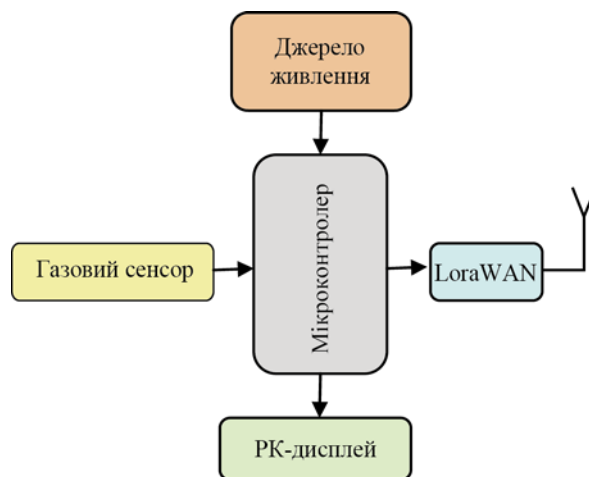


Рисунок 18.8 – Модуль контролю витоку побутового газу

Система моніторингу витоків газу виявляється економічно вигідною та кращим способом забезпечення довкілля в безпеці без будь-яких аварій, викликаних витоками газу.

18.3.4 Система виявлення аварій на транспорті

Ця система призначена про швидке інформування поліції та медиків про виникнення аварій внаслідок зіткнення транспортних засобів [23]. Модулі встановлюються на кожному транспортному засобі (рис. 18.9).

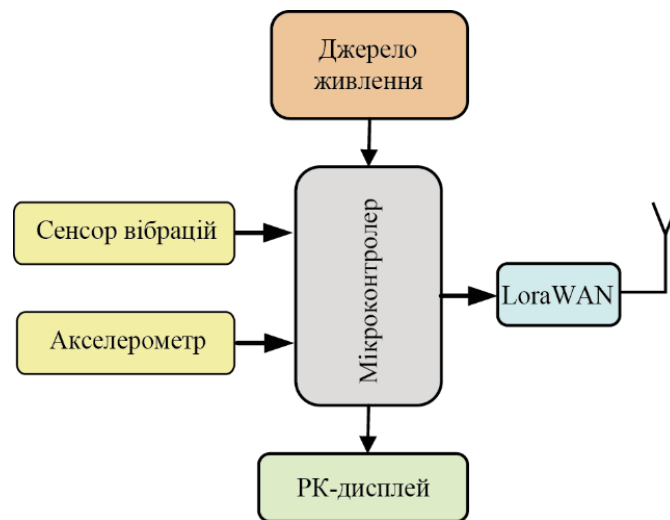


Рисунок 18.9 – Структура модуля реєстрації аварій на транспорті

Модуль складається з двох датчиків, а саме акселерометра та датчика вібрації. Датчики, розміщені в модулі, реєструють виникнення аварії і надсилають повідомлення в центр управління і моніторингу, а також у поліцію та швидку допомогу.

Використання такої системи дозволяє швидко усунути наслідки аварій та зберегти життя багатьох людей, що попали в аварію.

Замість мережі LoraWAN можна використовувати і інші канали зв'язку, як це показано на рис. 18.10.

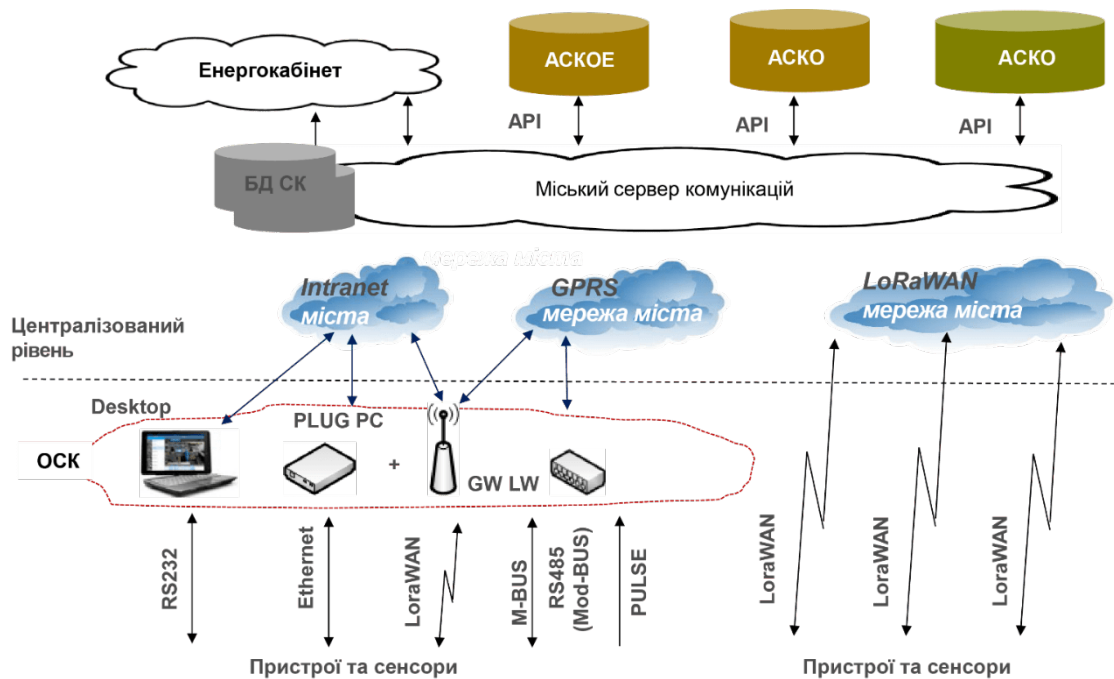


Рисунок 18.10 – Структура систем зв'язку "розумного" міста [23]

Оскільки система LoRaWAN має багато переваг, то при підтримці її операторами зв'язку вона забезпечує охоплення надійним зв'язком всієї території міста (рис. 18.11).

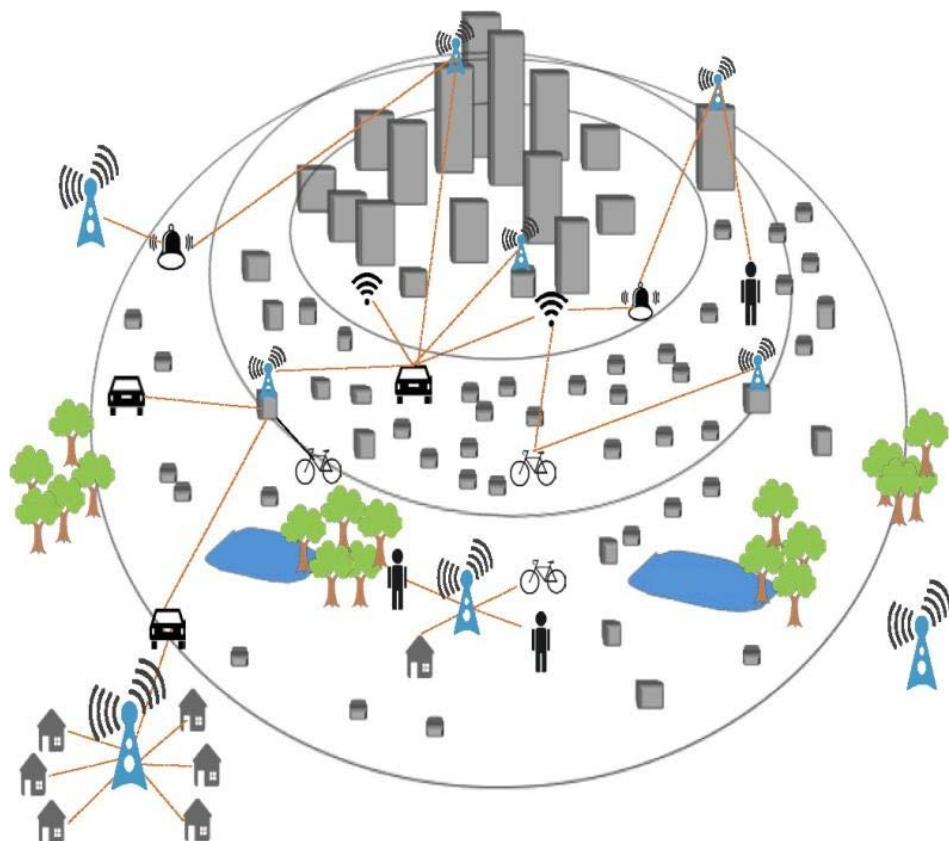


Рисунок 18.11 – Система зв'язку LoRaWAN у місті [17]

18.3.5 Інші системи "розумного" міста

Окрім перелічених вище, ще багато систем можуть використовуватись в "розумному" місті. На рис. 18.12 та 18.13 наведено ще декілька таких систем [24].



Рисунок 18.12 – Системи безпроводового обліку ресурсів [24]



Рисунок 18.13 – Системи відслідковування майна та людей в "розумному" місті [24]

Окрім наведених систем у розумному місті можуть формуватися глобальні мережі відеоспостереження, контролю паркувань, моніторингу водопостачання та аварій на мережах водопостачання, вуличного освітлення, несанкціонованого підключення та багато інших.

Контрольні питання

1. Які системи можна передбачити у "розумному" будинку?
2. Яка різниця між "розумним" будинком та "розумною" будівлею?
3. Які особливості "розумного" офісу у порівнянні з "розумною" будівлею?
4. Які системи "розумного" міста вам відомі?
5. Для чого призначені "розумні" системи?
6. В чому полягають особливості бізнес-центрів?
7. Які системи керування необхідні у бізнес-центрах?
8. Для чого потрібен моніторинг вивозу сміття?
9. Для чого потрібен моніторинг витоку газу?
10. Як система виявлення аварій на транспорті допомагає зберегти життя людей?

Перелік посилань

1. S. Iesanansi, P. Santhiyaa, M. Vidhya Smart city using IoT/ International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04, Apr 2019. pp. 2619-2622.
2. Що таке Розумний будинок і яким він може бути. Url: <https://www.smarthouse.ua/ua/chto-takoe-umnyj-dom-i-kakim-on-mozhet-byt.html> (дата звернення: 14.07.2024).

3. Розумний будинок VS інтелектуальний будинок. Розбираємось, у кого вище IQ. Url: <https://btr.org.ua/rozumniy-budinok-vs-ntelektualniy-budinok-rozbirayemos-u-kogo-vishche-iq>. (дата звернення: 14.07.2024).
4. Akıllı Binalar ve Enerji Yönetimi Uygulamaları. Url: <https://www.vowfashion.com/2024/10/16/akilli-binalar-ve-enerji-yonetimi-uygulamalari-2/> (дата звернення: 14.07.2024).
5. Структуровані кабельні системи – що таке? Url: <https://vse-e.com/ua/novosti/strukturirovannye-kabelnye-sistemy-chto-eto-takoe>. (дата звернення: 14.07.2024).
6. Які бувають системи структурованих кабельних мереж? Url: <https://klaster.ua/ua/stati-i-obzory/kakie-byvayut-sistemy-strukturirovannyh-kabelnyh-setey/>. (дата звернення: 14.07.2024).
7. Що таке KNX. Url: <https://knx24.com/news/basics/knx/>. (дата звернення: 14.07.2024).
8. KNX / EIB. Url: <https://mardalcables.tilda.ws/tpost/ep2mjzunev-knx-eib> (дата звернення: 14.07.2024).
9. Перспективи інвестування: класичні або гнучкі офіси. Url: <https://interfax.com.ua/news/blog/709291.html> (дата звернення: 14.07.2024).
10. Класифікація бізнес центрів та офісів. Url: <https://a-office.com.ua/uk/blog/klassifikatsiya-biznes-tsentrov/> (дата звернення: 14.07.2024).
11. Вентиляція та кондиціонування. Url: <https://www.greenenergycompany.kiev.ua/service/%D0%B2%D0%B5%D0%BD%D1%82%D0%B8%D0%BB%D1%8F%D1%86%D1%96%D1%8F-%D1%82%D0%B0-%D0%BA%D0%BE%D0%BD%D0%B4%D0%B8%D1%86%D1%96%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D0%BD%D1%8F/> (дата звернення: 14.07.2024).
12. An Overview Of Building Management System Bms. Url: https://jethrojeff.com/#google_vignette (дата звернення: 14.11.2024).

13. Автоматизація інженерних систем і мереж. Url: <https://avr.com.ua/avtomatyzacziya-inzhenernih-system/>. (дата звернення: 14.07.2024).
14. Система управління будівлею BMS. Інтелектуальні будівлі і споруди. Url: <https://gpg-group.com.ua/index.php/uk/blog-ua/32-sistema-upravlinnya-budivleyu-bms-intelektualni-budivli-i-sporudi> (дата звернення: 14.11.2024).
15. Розумне місто - що це таке, визначення та концепція. Url: <https://uk.economy-pedia.com/11036003-smart-city>. (дата звернення: 14.07.2024).
16. Що таке розумне місто? Url: <https://uk.history-hub.com/sho-take-rozumne-misto>. (дата звернення: 14.07.2024).
17. Розумне місто майбутнього: 5 ключових технологій. Url: <https://futurenow.com.ua/rozumne-misto-majbutnogo-5-klyuchovyh-tehnologij/> (дата звернення: 14.11.2024).
18. SmartGarbage - пристрій, призначений для моніторингу сміття. Url: <https://vseprezentacii.com/algebra/smartgarbage-pristrij-priznachenij-dlya-monitoringu-smittyu>. (дата звернення: 14.07.2024).
19. Вивіз сміття контролюватимуть через систему GPS-моніторингу. Url: <https://kyiv.ridna.ua/2014/09/vyviz-smittyu-kontrolyuvatymut-cherez-systemu-gps-monitorynhu/>. (дата звернення: 14.07.2024).
20. Виявлення і локалізація витоків газу. Url: <https://temio.com.ua/poslугy/vyyavlennya-i-lokalizacziya-vytokiv-gazu-2/>. (дата звернення: 14.07.2024).
21. Детектори витоку газу. Url: <https://www.carel.ua/gas-leakage-detectors>. (дата звернення: 14.07.2024).
22. Як використовувати функцію Crash Detection. Url: <https://support.apple.com/uk-ua/104959>. (дата звернення: 14.07.2024).
23. Розумні міста світу: приклади. Url: <https://uk.green-ecolog.com/15339143-smart-cities-in-the-world-examples>. (дата звернення: 14.07.2024).