Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Промислові інтерфейси CANopen для інтернету-речей в проектах «розумних міст»

Виконав: студент VI курсу групи СНмз-61

спеціальності (напряму підготовки) 122 Комп'ютерні науки
(шифр і назва спеціальності (напряму підготовки))

(підпис) Леськів Р.А. (прізвище та ініціали)

Керівник (підпис) Гром'як Р.С. (прізвище та ініціали)

Нормоконтроль (підпис) Мацюк О.В. (прізвище та ініціали)

Рецензент (підпис) Михалик Д.М. (прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Промислові інтерфейси CANopen для інтернету-речей в проектах «розумних міст» // Дипломна робота освітнього рівня "Магістр" // Леськів Роман Анатолійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кафедра комп’ютерних наук, група СНмз-61 // Тернопіль, 2019 // С. , рис. – , табл. – , кресл. – , додат. – , бібліогр. – .

Ключові слова: CANOPEN, ІНТЕРФЕЙС, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ІНТЕРНЕТ-РЕЧЕЙ, ІНТЕРФЕЙС, МОНТАЖ, СЕРВЕР, УПРАВЛІННЯ.

Дипломна робота присв’ячена дослідженню промислових інтерфейсів CANopen для Інтернету-речей в проектах «розумних міст». В першому розділі дипломної роботи розглянуто описано програмно-алгоритмічні комплекси в сучасних інформаційно-технологічних проектах «розумних міст». Проаналізовано промислові інтерфейси для «IoT»-пристроїв у проектах класу «розумне місто». Досліджено протокол «CANopen».

В другому розділі дипломної роботи розглянуто подано основні поняття «CANopen» для «IoT»-проектів «розумних міст». Описано мережеві сервіси «CANopen». Досліджено процеси, що впливають на роботу CANopen в умовах «розумного міста».

В третьому розділі дипломної роботи розглянута побудова ідеальної моделі «CANopen» в «IoT»-пристроях». Подано рекомендації щодо використання «CANopen» в «IoT»-проектах класу «розумне місто». Описано розроблення програмної частини.

Виконано розділи «Спеціальна частина», «Обґрунтування економічної ефективності», «Охорона праці та безпека в надзвичайних ситуаціях», «Екологія».

ANNOTATION

Industrial interfaces CANopen for Internet of Things in “smart cities” projects // Master's Thesis // Roman Leskiv // Ivan Puliuyi Ternopil National Technical University, Department of Computer Information Systems and Software Engineering, Department of Computer Sciences, SNMz-61 group // Ternopil, 2019 // C. , Fig. - , Table. - , Chair. - , Add. - , Biblio. - .

The thesis is devoted to the research of CANopen industrial interfaces for the Internet of Things in smart cities projects. The first section of the thesis deals with the description of software-algorithmic complexes in modern information and technological projects of "smart cities". Industrial interfaces for IoT devices in smart city projects are analyzed. The CANopen protocol is explored.

The second section of the thesis deals with the basic concepts of "CANopen" for "IoT" projects of "smart cities". The CANopen network services are described. The processes that influence the operation of CANopen in a "smart city" are investigated.

The third section of the thesis deals with the construction of the ideal model "CANopen" in "IoT" devices. Recommendations on the use of "CANopen" in "smart city" IoT projects have been provided. The development of the software part is described.

The sections “Special part”, “Justification of economic efficiency”, “Occupational health and safety”, “Ecology” have been completed.

Keywords: CANOPEN, INTERFACE, INFORMATION TECHNOLOGIES, INTERNET THING, INTERFACE, INSTALLATION, SERVER, MANAGEMENT.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АСУ – Автоматизована система управління.

ПЛК – Програмований логічний контролер.

ACK (англ. Acknowledge) – підтвердження.

CAN (англ. Controller Area Network) – Локальна мережа контролерів.

CRC (англ. Cyclic Redundancy Check) – алгоритм знаходження контрольної суми.

DLC (англ. Data Link Control) – високорівневий протокол каналу передачі даних в ієрархії інформаційної моделі OSI.

IoT (англ. Internet of Things) – Інтернет речей.

OD (англ. Object Dictionary) – Словник Об’єктів.

OSI (англ. Open Systems Interconnection) – Взаємодія відкритих систем.

PDO (англ. Process Data Object) – Опрацювання об'єкта даних.

SCT (англ. Safeguard Cycle Time) – Час циклу захисту.

SDO (англ. Service Data Object) – Сервісний об’єкт даних.

SRDO (англ. Safety-Relevant Data Object) – Об'єкт даних, що стосуються безпеки.

SRVT (англ. Safety-Relevant Validation Time) – Час перевірки, що стосується безпеки.

ЗМІСТ

ВСТУП 8
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ 10
1.1 Програмно-алгоритмічні комплекси в сучасних інформаційно-технологічних проектах «розумних міст» 10
1.2 Промислові інтерфейси для «IoT»-пристроїв у проектах класу «розумне місто» 12
1.3 Протокол «CANopen» 18
1.4 Висновок до першого розділу 25
2 СИСТЕМНИЙ АНАЛІЗ ТА ОБҐРУНТУВАННЯ ПРОБЛЕМИ 26
2.1 Основні поняття «CANopen» для «IoT»-проектів «розумних міст» 26
2.2 Мережеві сервіси «CANopen» 32
2.3 Дослідження процесів, що впливають на роботу CANopen в умовах «розумного міста» 35
2.4 Висновок до другого розділу 40
3 МОДЕЛЮВАННЯ ПРОЦЕСІВ У МІСЬКИХ IOT-МЕРЕЖАХ НА БАЗІ «CANOPEN» 41
3.1 Побудова ідеальної моделі 41
3.2 Рекомендації щодо використання «CANopen» в «IoT»-проектах класу «розумне місто» 47
3.2.1 Підвищення надійності та дублювання муніципальних мереж .. 49
3.3 Розроблення програмної частини 52
3.4 Висновок до третього розділу 54
4 СПЕЦІАЛЬНА ЧАСТИНА 56
4.1 Проектування елементів пристрою для тестового підключення до шини «CAN» 56
4.2 Висновок 60

5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ 61
5.1 Розрахунок норм часу на виконання науково-дослідної роботи..... 61
5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи..... 62
5.3 Розрахунок матеріальних витрат..... 66
5.4 Розрахунок витрат на електроенергію..... 67
5.5 Розрахунок суми амортизаційних відрахувань 67
5.6 Обчислення накладних витрат..... 68
5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи 69
5.8 Розрахунок ціни проведених науково-дослідних робіт..... 70
5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень..... 71
5.10 Висновок..... 72
6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ..... 74
6.1 Організаційно-технічні засоби та санітарно-гігієнічні заходи щодо збереження працездатності працівників, які працюють в галузі ІТ..... 74
6.2 Основні завдання та функції системи управління охороною праці на підприємстві (СУОП) 75
6.3 Забезпечення безпеки життєдіяльності при роботі з ПК..... 77
6.4 Джерела, зони дії та рівні забруднення навколишнього середовища у разі аварій на хімічно і радіаційно небезпечних об’єктах 82
6.5 Висновок..... 91
7 ЕКОЛОГІЯ 92
7.1 Стратегія і тактика збереження й розвитку життя на землі..... 92
7.2 Вимоги до моніторів (ВДТ) і ПЕОМ 96
7.3 Висновок до розділу 98

ВИСНОВКИ..... 99
ПЕРЕЛІК ДЖЕРЕЛ.....101
ДОДАТКИ

ВСТУП

Актуальність теми. У сучасному світі і особливо в інноваційних проектах класу «розумне місто» побудованих на основі інформаційних технологій Інтернету речей (IoT) проектування і впровадження автоматичних систем управління технологічним процесом є одним з основних напрямків при модернізації міських виробництв, служб та сервісів і є на сьогоднішній день актуальним напрямком науково-практичних досліджень. За останні десятиліття зроблено істотний ривок в розмаїтті обладнання, доступного для розроблення IoT-пристроїв, зокрема можна вибрати необхідні програмовані логічні контролери, давачі і зв’язуючі елементи.

Подібне різноманіття існує і при виборі протоколів зв’язку між елементами системи. З’являються все більше промислових інтерфейсів і протоколів зі своїми особливостями і сферами застосування. При цьому, найчастіше, інженери в сфері автоматизації воліють використовувати зарекомендували себе в минулому, але застарілі на сьогоднішній день технології передачі даних. Цьому є кілька пояснень: тривалий цикл життя, що розробляється, який може досягати декількох десятиліть, з можливістю сполучення до старих підсистем; небажання тестування невідомого протоколу зв'язку в важливих вузлах; використання готових напрацювань і модулів; недостатня обізнаність в існуванні нових рішень.

Мета і задачі дослідження. Метою даної роботи є покращення якості міських мереж IoT-пристроїв, та як наслідок підвищення їх сервісних харктеристик.

Об’єкт дослідження. Протоколу «CANopen»: його можливе застосування при розробленні «IoT»-пристроїв, відмінні риси, існуючі обмеження і методи їх усунення. Розгляд можливостей використання «CANopen» в міських «IoT»-системах дозволить додатково вивчити даний

протокол на предмет застосування в умовах, коли важлива швидкодія і відмовостійкість мережі.

Предмет дослідження. Методи та засоби організації міських «IoT»-мереж з використанням промислового протоколу «CANopen».

Наукова новизна одержаних результатів. Виконана побудова ідеальної моделі «CANopen» в «IoT»-пристроях.

Практичне значення одержаних результатів. Розроблено та запропоновано рекомендації щодо використання «CANopen» в «IoT»-проектах класу «розумне місто».

Апробація результатів магістерської роботи проведена на двох наукових конференціях з публікацією тез доповідей.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Програмно-алгоритмічні комплекси в сучасних інформаційно-технологічних проектах «розумних міст»

Останнім часом деякі розумні міські проекти та ініціативи сприяли стратегічному та технологічному розвитку міст, надаючи підтримку на рівні застосунків для «розумних» міських сервісів. Проект «VITAL» [1] об'єднує гетерогенні «IoT»-платформи (побудовані на основі Інтернету-речей) за допомогою семантичних засобів в хмарному середовищі, призначених для «розумного міста». Цей проект забезпечує рівномірний рівень доступу для різнорідних «IoT»-платформ («X-GSN», «Xively» [2], «FIT», «Hi Reply» [3] та «OpenIoT») для збирання даних про «розумні міста» [4, 5]. У проекті «Vital» доступ до існуючих «IoT»-платформ здійснюється шляхом адаптації до наданих інтерфейсів та абстрактних шарів за допомогою «RESTfull»-платформи. Розробники повинні суворо дотримуватися концепції «HTTP-REST» для створення послуг.

Сучасний стан «розумних міст» акцентує увагу на наявних розумних міських платформах [6]. Існуючі наукові праці в основному включають в себе наступні сфери: збір даних [7]; семантичну сумісність; аналіз даних у режимі реального часу [8], [9], [10], виявлення подій [11], підтримка розробки розумних міських застосунків [12]. В таблиці 1.1 наведено порівняння «розумних» міських платформ та підтримуваних ними функцій.

Як показано в таблиці, додатково до збору даних та семантичної сумісності, система «CityPulse» забезпечує повний набір інструментів аналітичного опрацювання даних в режимі реального часу, таких як консолідація даних, агрегація даних, виявлення подій, аналіз якості та підтримка прийняття рішень. Розробка додатків підтримується через набір «API», наданих «CityPulse», котрі забезпечують відкритий доступ до повної

інтелектуальної системи аналізу даних міст і можуть використовуватись для розробки «розумних» міських додатків.

Таблиця 1.1 – Порівняння «розумних» міських платформ та підтримуваних ними функцій

«IoT Smart City Platforms» та підтримувані функції	«iCity»	«Smart Santan-dler»	«Open IoT»	«iCo-re»	«Spit Fire»	«PL-AY»	«Star City»	«VIT-AL»	«City Pulse»
«IoT» збирання даних	так	так	так	так	так	так	так	так	так
Семантична сумісність	част-ково	част-ково	так	так	так	ні	так	так	так
Виявлення подій і аналіз даних	ні	ні	ні	ні	ні	так	так	ні	так
Пітримка розробки застосунків	так	так	част-ково	част-ково	част-ково	ні	ні	част-ково	так

Підтримка «API»-рівня на основні компоненти системи «CityPulse» сприяє створенню вільно пов'язаної архітектури для розробки «розумних» міських додатків [13]. Розробники додатків можуть використовувати повний конвеєр обробки схеми CityPulse або використовувати лише спеціалізовані компоненти в залежності від вимог їх застосування.

«NYC Open Data» надає різнорідні дані про бізнес, міське самоврядування, освіту, навколишнє середовище, охорону здоров'я, соціальні послуги, транспорт та громадськість. Щорічна акція «BigApps» [14] об'єднує сотні розробників, дизайнерів, виробників та маркетологів у конкурсі для вирішення різних завдань за допомогою технологій. Приклади попередніх завдань включають «Виробництво з нульовими відходами», «Доступне житло для містян» та інші. За винятком доступу до великої кількості наборів даних, «NYC Open Data» не пропонує ніяких наборів аналітичних даних або компонентів для попередньої обробки даних, які спільнота розробників може

використовувати для розробки своїх служб та програм. Тому системи для комплексного збору, зберігання та аналітичного опрацювання даних мають потенціал для полегшення процесів розробки міських застосунків та підтримки прийняття рішень.

Аналогічно Хан і ін. [15] запропонували прототип, розроблений для демонстрації ефективності служб аналітичного опрацювання на основі хмарних сервісів для зведеного відкритого доступу до «Bristol Smart City» для визначення співвідношень між вибраними показниками міського середовища та якості життя [16]. Запропонована система ділиться на три шари для забезпечення процесу створення єдиної бази знань. Нижній рівень в архітектурі складається з розподілених та неоднорідних сховищ даних та різних давачів підключених до системи. Картографічний та зв'язаний шар ресурсів знаходить нові сценарії та підтримує робочі процеси для пошуку кореляцій, котрий неможливий в ізольованих сховищах даних. Аналітичний рушій у верхньому шарі обробляє дані для конкретних задач проекту. Модулі підтримки прийняття рішень, контекстної фільтрації та технічної адаптації, не включені в згадану структуру.

Проект «Амстердам Смарт Сіті» («ASC») [17] включає ряд проектів, що охоплюють декілька областей, для створення «розумного міста». Напрямки реалізації включають «розумну» мобільність [18], «розумне» життя, «розумне» суспільство, «розумну» територію, «розумну» економіку, великі за обсягом та відкриті даних та інфраструктуру [19].

1.2 Промислові інтерфейси для «IoT»-пристроїв у проектах класу «розумне місто»

На сьогоднішній день можна виділити наступні найпопулярніші промислові інтерфейси, котрі можуть бути використані при реалізації «IoT»-

пристроїв інформаційно-технологічних проектів класу «розумне місто», і протоколи на їх основі на польовому рівні в «АСУ»:

– «Industrial Ethernet» [20] («Modbus TCP/IP» [21], «ProfiNet» [22]).

– «RS-485» [23] («Modbus» [24], «Profibus» [25]).

– «CAN» [26] («CANopen» [27], «DeviceNet» [28]).

«RS-485» – послідовний асинхронний інтерфейс, який є одним з найбільш поширених в промислової автоматизації та може ефективно використовуватись при реалізації «IoT»-проектів класу «розумне місто». В основі даного інтерфейсу лежить диференційний спосіб передачі сигналу, зазвичай на базі витої пари. Завдяки цьому вдається знизити вплив перешкод на переданий сигнал, оскільки можна вважати, що вони впливають однаково на сигнальні лінії. Однак, лінії на основі інтерфейсу «RS-485» схильні до ефекту відбиття сигналу. Для мінімізації цього ефекту використовують термінуючі резистори і введена рекомендація щодо використання шинної топології мережі з мінімальним відстанню кінцевих пристроїв від шини.

Переваги:

– Можливість одночасного підключення великої кількості пристроїв в мережу без використання повторювачів, зокрема до «32шт.».

– Передача даних на відстанях до «1200м».

– Високі швидкості передачі даних, до «10 Мбіт/с».

Недоліки:

– Відсутність сервісних сигналів.

– Велике енергоспоживання.

На основі цього інтерфейсу створено багато популярних протоколів передавання даних.

«Modbus RTU» [29] є одним з найпоширеніших комунікаційних протоколів на основі інтерфейсу «RS-485». Даний протокол побудовано на архітектурі «master-slave», коли в мережі є один головний пристрій («master») та множина дочірніх пристроїв («slave»).

Головними перевагами даного протоколу є простота програмної реалізації і відсутність необхідності в спеціальних мікроконтролерах для реалізації. Однак, структура «master-slave» вимагає постійного активного опитування всіх відомих пристроїв, що може призводити до підвищених навантажень на лінії передачі даних, особливо у міських програмно-апаратних рішеннях.

В рамках протоколу є деякі інструменти контролю помилок, а саме обчислюється контрольна сума кожного кадру і можливість застосування біта паритету при передачі кожного байта повідомлення.

«Profibus DP» [30] – інший протокол на основі «RS-485» [31], який набув широкого застосування в контролерах фірми «Siemens» [32]. Головною його особливістю можна назвати багатомайстерність мережі, де дочірніми пристроями є різноманітні давачі. Таким чином можна об’єднувати декілька контролерів в єдину мережу з дочірніми пристроями і кожен з цих контролерів зможе ініціювати обмін даними.

Щоб уникнути конфліктних ситуацій між провідними пристроями застосовується спеціальний метод арбітражу на основі маркера. Кожен провідний пристрій отримує право на доступ до мережі тільки при наявності у нього маркера, який, в свою чергу, періодично передається між усіма провідними пристроями. Тим самим гарантується, що в будь-який момент часу тільки один провідний пристрій зможе ініціювати обмін даними по шині з дочірніми пристроями або з іншими провідними (комунікація типу «ведучий-ведучий»).

В даному протоколі передбачена підтримка віддаленого налаштування пристроїв та присутні засоби контролю помилок, як наприклад переведення виходів ведених пристроїв в заздалегідь налаштований «безпечний стан» при пропажі зв’язку з ведучим. Також необхідно згадати про програмну підтримку апаратного резервування з низьким часом відновлення.

«Industrial Ethernet». В останні роки спостерігається тенденція до повсюдного використання «Industrial Ethernet», особливо для програмно-апаратних застосувань «IoT»-пристроїв в проектах класу «розумне місто». У 2011 році більше 50% відсотків пристроїв, що випускаються підтримувало даний стандарт і з тих пір їх кількість тільки зростає. Навіть найбільші виробники обладнання підтримують цю технологію, відмовляючись від власних напрацювань в даній області. Так, наприклад, «Schneider Electric» [33] випустив власний ПЛК, повністю орієнтований на використання в «Ethernet»-мережах, а компанія «Siemens» поступово відмовляється від стандартного використання «Profibus» на користь «Industrial Ethernet».

Переваги даного інтерфейсу складно переоцінити:

– Висока швидкість передачі даних.

– Відома технологія «Ethernet» в основі, що спрощує обслуговування мереж та підготована велика кількість фахівців.

– Можливість прямої інтеграції з «Ethernet»-мережами верхнього рівня, аж до глобальної мережі Інтернет, включно, з можливим застосуванням її протоколів, як наприклад «SNMP». [34]

– Можливість передачі даних на великі відстані із застосуванням оптичних кабелів.

Як недоліки можна виділити:

– Відсутність стандартизованих методів захисту інформації. У сукупності з легкістю інтеграції промислових мереж на основі «Industrial Ethernet» в інші «Ethernet»-мережі, обладнання може стати вразливим для зловмисників. Необхідно закладати різні заходи захисту, наприклад, брандмауери між підмережами, і використовувати спеціальні програмні розширення протоколів для забезпечення безпеки.

– Можливість перевантаження каналу, при обміні великої кількості інформації. Сюди ж можна включити вразливість до спланованим «DDoS»-атакам. [35]

– Нестандартизованого обладнання під використання в різних топологіях мережі. Так, наприклад, не радиться використовувати деяке обладнання в складі шинної топології мережі, коли відключення такого обладнання (наприклад, для ремонту), призведе до зникнення з мережі вузлів наступного за ним.

– Викока вартість. Сюди ж можна включити необхідність використання додаткових перетворювачів при підключенні пристроїв, що не підтримують «Industrial Ethernet».

«Modbus TCP/IP» – цей протокол використовує «Ethernet» в якості транспорту для передачі кадру «Modbus RTU» на прикладному рівні. Основні відмінності в кадрі: відсутність контрольної суми, використовується контрольна сума «Ethernet TCP/IP» і поля адреси, що полегшує інтеграцію «IoT»-пристроїв у повсюдні мережі «розумних міст». [36] Структура даних для пристрою при цьому залишається аналогічною «Modbus RTU», що призвело до популяризації даного протоколу, оскільки відсутня необхідність в програмних зміни на пристроях. Також можливе об’єднання пристроїв на «Modbus TCP/IP» з пристроями на «Modbus RTU» за допомогою спеціальних перетворювачів.

За аналогією з «Modbus TCP/IP», «Profinet» був створений як перекладення прикладного рівня «Profibus» на транспортну основу «Ethernet». Основною відмінною рисою при цьому є виділення спеціальних вікон для передачі трафіку даних в реальному часі («RT» та «IRT»). Під час передачі цих даних ніякий інший пакет не може перервати його, чим досягається більша швидкодія при використанні з польовим обладнанням.

«CAN» – послідовний інтерфейс передачі даних з дуже великим ступенем надійності і захищеності. Спочатку він використовувався в автомобільній промисловості, але з часом знайшов своє застосування і в промисловій автоматизації.

Даний інтерфейс вирішує завдання двох нижніх рівнів моделі «OSI»: фізичного та канального. На фізичному рівні – це вита пара зі специфічними приймально-передавачами.

Основна особливість канального рівня полягає в тому, що спочатку все вузли мережі «CAN» рівноправні, а ідентифікатори присвоюються повідомленнями, які надсилаються на лінію відповідно до пріоритету, а приймати це повідомлення чи ні вирішують приймач в залежності від ідентифікатора.

Головна перевага такого підходу: відсутність конкретного ведучого пристрою в загальному випадку і можливість у будь-який момент підключити новий пристрій в мережу без попереднього налаштування.

Основними недоліками інтерфейсу є його складність, в тому числі через відсутність стандартизованого протоколу високого рівня моделі «OSI» і відносно висока вартість, через наявність специфічних приймачів для кожного пристрою на шині. Проте зазначені недоліки не заваджають використання зазначеного протоколу при реалізації окремих архітектурних рішень для інформаційно-технологічних платформ «IoT»-проектів класу «розумне місто».

«CANopen» є відкритим протоколом, підтримуваним організацією «CiA» («CAN in Automation»). [37] Даний протокол спирається на інтерфейс «CAN», при цьому стандартизована тільки основна функціональність. Тим самим у розробників залишається великий простір по розширенню функціональності. Додатково, «CANopen» дозволяє проводити підключення до «CAN»-мереж без втрати функціональності існуючих «CAN»-пристроїв в цій мережі, до тих пір, поки у них не перетинаються ідентифікатори повідомлень. Що добре підходить для організації міських спецалізованих мереж виконавчих пристроїв.

«DeviceNet» [38] як і «CANopen» даний протокол описує верхні рівні моделі «OSI», спираючись на «CAN». Даний протокол спочатку розроблявся

під використання в промисловості, він є відкритим і, в основному, просувається компанією «Allen Bradley». [39]

Основні відмінності від «CANopen»:

– Менша максимальна швидкість передачі даних «500 Кбіт/с», замість «1 Мбіт/с».

– Менше максимальну кількість пристроїв на шині «64» проти «127».

– Багатомастерність мережі, коли певні пристрої призначаються провідними зі своїм набором ведених пристроїв.

1.3 Протокол «CANopen»

Протокол «CANopen» описує тільки верхні рівні моделі «OSI», тому неможливо вивчати «CANopen» без загальних знань щодо інтерфейсу «CAN», на основі якого він побудований. «CAN» охоплює собою нижні два рівня моделі «OSI». На фізичному рівні – це вита пара зі специфічними прийомо-передавачами, які виконані на основі окремих мікросхемах.

Спочатку «CAN» був розроблений для опитування множини давачів з великою частотою, що спричинило за собою обмеження розміром у «8 байт» даних для одного повідомлення. Це дозволило збільшити пропускну здатність лінії, що на максимальних швидкостях до «1 Мбіт/с», коли можуть передаватися тисячі повідомлень в секунду.

Крім даних, кожне повідомлення складається з «11-бітного» ідентифікатора повідомлення і «15-бітної» контрольної суми. Існує розширена версія стандарту «CAN 2.0B», що передбачає використання додаткових «18 бітів» ідентифікатора, але використовувати її в «CANopen» для «IoT»-проектів класу «розумне місто» не рекомендується. Загальна структура кадру «CAN 2.0A» [40] показана на рисунку 1.1. Як видно, контрольна сума і ідентифікатор становить значну частину посилки, що додає надійності при передачі інформації. Більш того, контрольна сума

вираховується кожним вузлом в мережі і, при виникненні хоча б одного розбіжності, кожен вузол ігнорує отримані дані і відбувається перевідправка повідомлення.

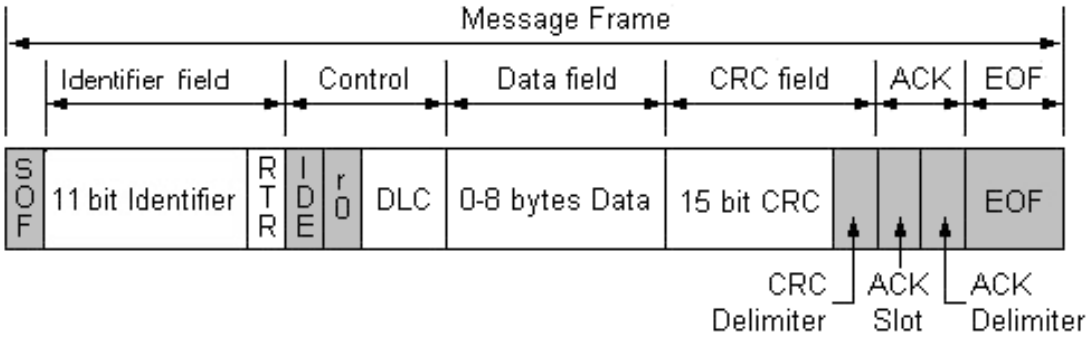


Рисунок 1.1 – Формат кадру CAN 2.0A

Побудована на основі «CAN» мережа є багатомастерною. Основна ідеологія полягає в тому, що вузол приймає потрібне йому повідомлення за ідентифікатором цього повідомлення. Якщо в інших мережах вказується унікальний номер одержувача (веденого) пристрою, то у випадку «CAN» всі пристрої приймають повідомлення, обробляючи тільки необхідні. Арбітраж проводиться за допомогою пріоритетності повідомлень, де повідомлення з меншим номером ідентифікатора вважається більш пріоритетним.

Фізичний рівень «CAN». В якості основних станів для передачі інформації були введені поняття домінантного і рецесивного стану лінії. Під рецесивним станом розуміється режим, коли по витій парі передається однакове значення. Домінантний стан – різниця напруг на витій парі в «2В». При цьому рецесивний стан вважається логічною одиницею, а домінантний – логічним нулем.

При цьому «CAN»-контролер видає по лініях «Tx» і «Rx» сигнали «5 В» для рецесивного і «0 В» для домінантного. Рівні сигналів представлені на рисунку 1.2. Для безпосереднього підключення до лінії використовується спеціальний «CAN»-приймач (трансивер), який перетворює сигнали з

«CAN»-контролера в диференційний сигнал, а також служить для захисту контролера від короткочасного імпульсного напруги до «100 В». Домінантний стан лінії пріоритетніший за рецесивний.

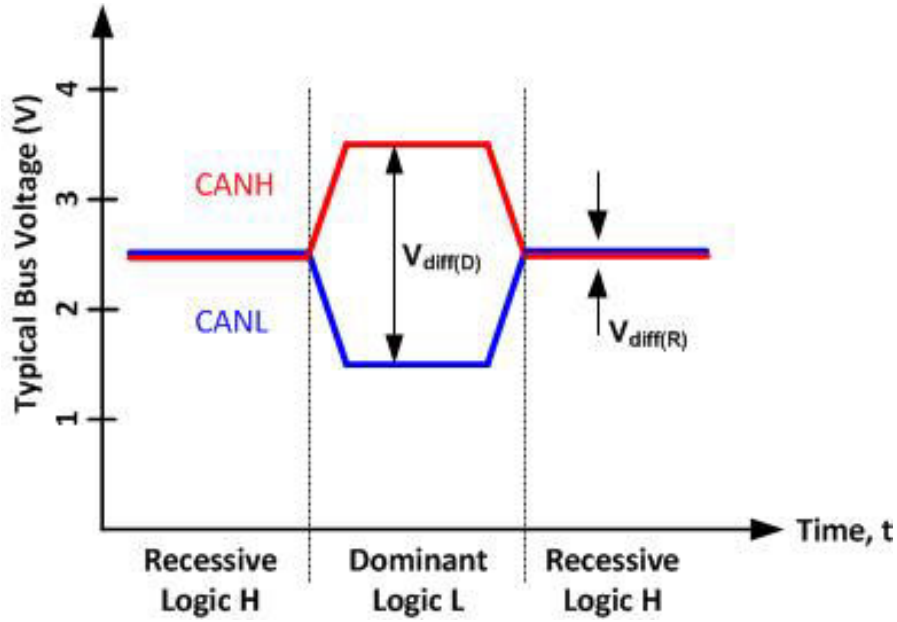


Рисунок 1.2 – Рівні сигналів «CAN»

Це означає, що якщо кілька вузлів починають одночасно посилати на лінію сигнал, то лінія піде в домінантний стан, якщо хоч один вузол його пошле. Дана особливість використовується для додаткового арбітражу на лінії, якщо вузол посилав рецесивний стан, а на лінії виявився домінантний, то вузол відразу розуміє, що на лінії зараз є хтось ще, хто пише домінантний стан. Тим самим рецесивний стан лінії може бути досягнуто тільки в одному випадку, коли всі вузли мережі на даний момент часу оголошують рецесивний стан.

Безсумнівна перевага використання витої пари з диференціальним сигналом – це стійкість до перешкод, коли перешкоди однаково впливають на обидва сигналу лінії, не спотворюючи результуюче значення. Що забезпечує ефективність використання прокладених в міському середовищі ліній. Перелік сигнали для протоколу «CAN».

Таблиця 2.1 – Сигнали, які використовуються в протоколі «CAN»

Сигнал	Опис
«CAN_L»	Лінія з меншою напругою при домінантному стані.
«CAN_H»	Лінія з великою напругою при домінантному стані.
«CAN GND»	Земля для вузлів.
«CAN Shield»	Додаткове екранування сигналів.
«V+»	Додатковий сигнал харчування (вузла).
«GND»	Додаткова земля.

Для коректної роботи обов'язковими є тільки сигнали «CAN_L» і «CAN_H». Роз'єми для підключення вузлів не регламентовані і можуть бути, як і 9-контактними «D-Sub», так і «RJ45» або іншими. [41]

Налаштування бітового інтервалу. Швидкість передачі даних по лінії задається фіксована рівна «1 – 10Мбіт/с», в залежності від призначеного бітового інтервалу. Чим менше час кожного біта, тим швидше можна передати повідомлення, але при занадто маленькому бітовому інтервалі інший пристрій на шині може не встигнути прочитати надіслане повідомлення. Час бітового інтервалу складається з чотирьох полів: «SYNS» – буде синхронізований, що складається з 1 тимчасового такту, «PRS» – Час втрат в лінії «1..8 тактів»> «SYNS», «PHS1» – час затримки, після якого відбувається зняття значення з лінії «1..8 тактів»> «PRS», «PHS2» – невелика затримка після зняття значення з лінії «1..8 тактів» < «PHS1».

Для завдання найшвидшої з можливих швидкостей передавання даних («BRP = 0»), час генерації такту буде:

$$T_{scl} = \frac{BRP + 1}{clk_{IO}} = \frac{1}{clk_{IO}} \quad (1.1)$$

Тоді значенням бітового інтервалу буде стан:

$$SYNS = T_{scl}; \quad PRS = 2T_{scl}; \quad PHS1 = 3T_{scl}; \quad PHS2 = 2T_{scl} \tag{1.2}$$

Повний бітовий інтервал:

$$Tbit = 8T_{scl} \tag{1.3}$$

Рекомендовані бітові інтервали для використання в мережі «CANopen» для «IoT»-проектів класу «розумне місто».

Формат кадру «CAN» показаний на рис. 3.1. Один кадр складається з:

1. Домінантний стартовий біт. Перехід лінії з рецесивного стану в домінантне розглядається, як стартовий біт кадру.

2. «11-бітний» ідентифікатор повідомлення. У «CANopen» даний ідентифікатор використовується як складова частина «COB-ID». За цим ідентифікатором відбувається арбітраж повідомлень на лінії, тому необхідно упевниться, що у кожної посилки унікальний ідентифікатор.

3. Поле віддаленого доступу «RTR». Для використання в «CANopen» ці «3 біти» приймаються зарезервованими, оскільки використання бітів віддаленого доступу заборонено в рамках «CANopen».

4. Поле «DLC», яке описує кількість байтів даних в кадрі, містить число від «1 до 8».

5. Поле даних, довжиною «DLC».

6. «15-бітна» контрольна сума «CRC».

7. Біт «CRC»-роздільник, біт квайтирування «ACK», і «ACK»-роздільник. Роздільники потрібні для того, щоб дати деякий час усім вузлам в технологічній «IoT»-підмережі «розумного міста» для розрахунку «CRC» і порівняння його з отриманою контрольною сумою в кадрі. Біт квайтирування потрібен для підтвердження отримання повідомлення. Якщо «ACK»-

роздільник рецесивний, то це означає, що всі вузли отримали повідомлення з правильною контрольною сумою.

8. Кадр закінчується послідовністю з «7» рецесивних бітів. Для можливості відправки нового кадру має пройти ще «2-3» рецесивного стану лінії.

Арбітраж передбачає методику, при якій гарантується, що на лінії не відбуватиметься колізій, тобто, передача повідомлень декількома вузлами одночасно. Арбітраж здійснюється за рахунок пріоритетності повідомлень на основі технології «CSMA/CD» («Carrier Sense Multiple Access with Collision Detection»). Дана технологія передбачає виявлення поточного стану лінії і застосовується, наприклад, в «Ethernet». Однак в разі «CAN» пропускна здатність каналу залишається незмінною, оскільки при виявленні можливої колізії відбувається негайне порівняння пріоритету повідомлення. Більш того, порівняння пріоритетів відбувається циклічно, так що після закінчення передачі самого пріоритетного повідомлення, негайно почнеться відправка наступного за пріоритетністю. Арбітраж реалізований на фізичному рівні в «CAN»-контролері.

Виявлення та оброблення помилок. На фізичному рівні контроль помилок відбувається за допомогою вираховування контрольної суми «CRC». Кожен вузол мережі порівнює контрольну суму повідомлення на лінії з вираховується значенням на конкретному вузлі. Більш того, приймає повідомлення вузол ще і виставляє біт квайтирування «ACK», при співпадінні контрольних сум, тим самим сигналізуючи іншим вузлам, що повідомлення успішно отримано.

При розбіжності контрольних сум хоча б на одному вузлі повідомлення «знищується» для всіх вузлів: виставляється сигнал помилки, всі вузли ігнорують отримане повідомлення, спроба відправки повідомлення повторюється. Тим самим знищення повідомлення відбувається з ініціативи хоча б одного вузла для всієї мережі. У теорії, будь-який бракований «CAN»-

контроллер, у якого неправильно вираховується контрольна сума, може привести до неможливості обміну інформацією по всій мережі. Для запобігання таких ситуацій були введені кілька станів помилок, які спираються на «2 лічильника»: «REC» – лічильник помилок прийому і «TEC» – лічильник помилок передачі. Вузол переходить в стан ігнорування помилок («Passive error») після досягнення одного з цих лічильників значення «127». У даному стані вузол може приймати і відправляти повідомлення, але позбавляється права знищувати повідомлення на лінії. При перевищенні значення лічильника до «255» відбувається повне відключення вузла від лінії (Bus off). Діаграма станів вузла показана на рисунку 1.3.

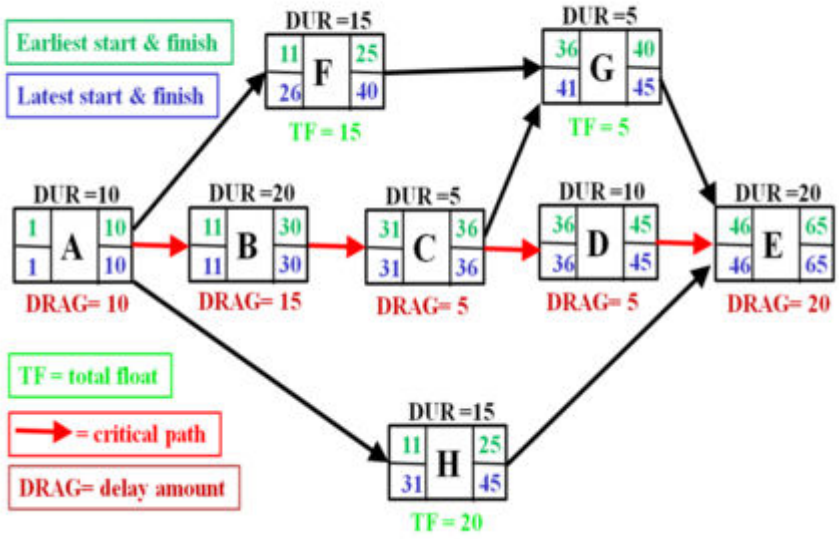


Рисунок 1.3 – Діаграма станів помилок вузла

В цілому, дослідження показують, що «CAN» є вкрай надійним інтерфейсом та має високий потенціал для використання в «IoT»-проектах класу «розумне місто». Не в останню чергу це досягається великий контрольною сумою, «15-бітна» контрольна сума на «8 байт» даних, наприклад, в «Ethernet» це значення «16 біт» контрольної суми на «1500 байт» даних, і можливістю знищення помилкового повідомлення будь-яким вузлом на лінії. Так, наприклад, при швидкості передачі даних в «250

кбіт/сек» і роботі мережі «2000 годин» на рік, помилкові дані пройдуть тільки раз на тисячу років [42].

1.4 Висновок до першого розділу

В першому розділі дипломної роботи досліджено програмно-алгоритмічні комплекси в сучасних інформаційно-технологічних «IoT»-проектах «розумних міст». Описано та подано вичерпні характеристики промислових інтерфейсів для проектів класу «розумне місто». Проаналізовано протокол «CANopen» в контексті його інтеграції в проекти класу «розумне місто».

2 СИСТЕМНИЙ АНАЛІЗ ТА ОБҐРУНТУВАННЯ ПРОБЛЕМИ

2.1 Основні поняття «CANopen» для «IoT»-проектів «розумних міст»

Основні маніпуляції з даними в «CANopen» відбуваються за допомогою об’єктів. При цьому бувають об'єкти різних типів:

– «OD» використовується для зберігання даних (як поточних даних процесу, так і конфігураційних) в форматі таблиці.

– «PDO»– це повідомлення, які передають поточні дані процесу.

– «SDO» – це повідомлення, які містять інформацію по конфігурації вузла або сервісну інформацію.

Також виділяють «3» типи ідентифікаторів в «CANopen»:

– Ідентифікатор вузла, «Node ID» – присвоюється кожному вузлу в мережі і є числом в проміжку «1-127».

– Індекс та підіндекс словника об’єктів («Object Dictionary Index/Subindex») – відповідно «16-бітний» і «8-бітний» ідентифікатор знаходження конкретної змінної в словнику об'єктів. Фактично, це номер комірки таблиці, в якій знаходиться потрібні дані.

– «COB ID» («Connection Object ID») – ідентифікатор повідомлення в мережі. Даний ідентифікатор фактично є ідентифікатором повідомлення «CAN» і є унікальним для кожного з'єднання між вузлами.

Словник об’єктів «OD». Як уже було згадано в попередньому розділі, словник об’єктів («OD») – це таблиця параметрів, до якої мають доступ усі члени мережі. Кожен вузол в мережі «CANopen» має власний словник об’єктів. При запису значення в словник об’єктів з мережі, даний вузол може зробити деяку операцію, а при читанні значення можна отримати інформацію про ці вузли, або процеси, якими він керує.

Кожен елемент словника об'єктів має свою адресу – «16-бітний» індекс і «8-бітний» підіндекс. При цьому, якщо за адресою індексу зберігається кілька значень, то в підіндексі «00h» вказується їх кількість.

Наповнення словника об'єктів – завдання розробника устаткування. Зазвичай кожне обладнання супроводжується спеціальним «EDS/DCF» файлом, в якому описаний словник об'єктів конкретного вузла. При цьому стандартом задано поділ словника на «6» секцій поданих в таблиці 2.1.

Таблиці 2.1 – Поділ словника на секції

Діапазон індексів	Опис
0000h	Резерв
0001h – 0FFFh	Типи даних
1000h – 1FFFh	Дані комунікації
2000h – 5FFFh	Дані виробника обладнання
6000h – 9FFFh	Параметри пристрою
A000h – FFFFh	Резерв

Типи даних. Дана область словника об'єктів не містить змінних, там тільки описуються використовувані типи даних. При читанні елементів з даної області вузла повернеться розмір даного типу в байтах. Це дозволяє встановити ззовні, якими типами даних вміє оперувати конкретний вузол в мережі. Типи даних розділені на кілька категорій:

1. Стандартні типи даних. Наприклад, «BOOLEAN» для позначення булевих змінних або «INTEGER32» для «32-бітних» цілих значень зі знаком.

2. Складовий тип даних. Аналог структур, де кожен тип даних складається з групи стандартних типів даних. Важливим складовим типом даних може вважатися «PDO_MAPPING», який використовується для передачі необхідних даних за допомогою «PDO».

3. Також є окремі індекси, на яких розташовуються складові типи даних конкретного обладнання, які водять розробники цього обладнання.

Дані комунікації. Ця секція словника описує основні параметри для комунікації вузла з іншими пристроями в мережі. При цьому існує список обов'язкових компонентів, без яких комунікація вузлів буде неможлива:

– Тип пристрою («1000h»). «32-бітний» ідентифікатор, який описує основний клас пристрою наприклад, модуль вводу-виводу.

– Регістр помилок («1001h»). «8-бітове» значення поточних помилок вузла. При цьому стандартом заданий тільки «1 біт» – глобальна помилка, інші можуть бути описані розробником.

– «Guard Time» («100Ch»). «16-бітове» значення часу, з яким вузол приймає спеціальне «охоронне» повідомлення від ведучого для позначення своєї присутності в мережі. Дане значення повинно бути вказано, якщо не використовується сигнал серцебиття.

– Час життя вузла («100Dh») – визначає кількість пропущених «охоронних» повідомлень до появи помилки зв'язку.

– Час серцебиття («1017h») – вказує час, з яким вузол повинен передавати повідомлення серцебиття.

– Ідентифікатор обладнання («1080h») – ідентифікує вузол інформація, така як унікальний номер сертифікованого виробника, серійний номер обладнання та ін.

Об’єкт сервісних даних «SDO». Доступ до словника даних з віддаленого вузла можна отримати за допомогою об'єкта сервісних даних («SDO»). Даний механізм використовує клієнт-серверну архітектуру, де ведучий пристрій виступає клієнтом до веденого. При цьому клієнт може посилати запити на запис/читання даних зі словника сервера.

Оскільки ідентифікатори повідомлень унікальні, то для запуску такого клієнт/серверного обміну зарезервовані окремі номери повідомлень. За замовчуванням для відправки вузла сполучення з сервісними даними використовується наступна формула для вираховування ідентифікатора повідомлення:

$$Rx\ SDO = 600h + NodeID;\ Tx\ SDO = 580h + NodeID; \quad (2.1)$$

З такої ідеології виникає одна з головних особливостей «CANopen» – одномайстерності мережі (на відміну від «CAN», де немає єдиного головного пристрою). Ідентифікатори повідомлень повинні бути унікальними, а значить, не повинно бути такої ситуації, коли 2 пристрої мають право посилати «SDO»-повідомлення на один вузол одночасно.

Кожне «SDO» повідомлення містить «8 байт» даних, стандартний розмір даних одного кадру «CAN»:

1. Специфікатор – один байт даних, що містить інформацію про те, команда чи це на читання, запис або скасування операції. Також в цьому байті міститься інформація про те, чи всі дані будуть передані цим повідомленням або ж будуть дописи з даними.

2. Далі йдуть «2-4 байта», що позначають необхідний індекс і підіндекс словника об’єктів на доступ.

3. «5-8 байт» даних.

Потрібно відзначити, що коли дані не поміщаються в одне повідомлення, то виставляється спеціальний біт в специфікаторами і надсилається окреме повідомлення, де вже все «8 байтів» даних заповнені даними. У будь-який момент часу клієнт або сервер інтегрований в міське середовище може перервати передачу повідомлення за допомогою відправки повідомлення скасування операції.

Об’єкт даних процесу «PDO». Хоча «SDO» і дозволяють звернутися до будь-якого елементу словника даних вузла, але їх використання для постійної передачі даних недоцільно. Для цих завдань служать повідомлення «PDO», які були введені саме в якості основного транспорту для передачі даних процесу в реальному часі. «PDO» використовують переваги мережі «CAN», які дозволяють будь-якому вузлу відправляти повідомлення на лінію в кожен момент часу, підкоряючись арбітражу. Кожне «PDO» може містити одну або

кілька змінних зі словника даних, аж до стандартних «8 байт», передбачених полем даних одного повідомлення. Вміст кожного «PDO» заздалегідь налаштовується мапуруется за допомогою «SDO».

Для кожного вузла існують 2 типу «PDO»:

– «TPDO» – виходять з даного вузла повідомлення «PDO».

– «RPDO» – вхідні повідомлення «PDO» для даного вузла.

При цьому вся інформація про налаштування конкретних «PDO», зберігається в певних областях словника даних. Ці настройки різняться у «RPDO» і «TPDO», в загальному випадку, приймати дані легше, ніж їх відправляти.

Режими відправки «TPDO». Основне питання при відправці повідомлення і його основна відмінність від вхідного повідомлення полягає в тому, яким чином виявляти необхідність цієї посилки. Стандартом описано 4 режими відправлення повідомлення на лінію (тригера):

– Відправка повідомлення зі зміни значення.

Даний режим роботи має на увазі, що повідомлення відправляється на лінію в разі зміни даних, які прив'язані до даного «PDO». В даному режимі додатково може здаватися зона нечутливості, яка може бути важлива при передачі аналогового сигналу з високою частотою зміни. У гіршому випадку, при швидкій зміні сигналу, може статися повна забивання лінії одним повідомленням. Щоб уникнути цієї ситуації додатково вводять таймер затримки між відправленням двох однотипних «PDO» (див. рисунок 2.1).

Рисунок 2.1 – Використання таймера затримки

Використання даного режиму може бути важким для повідомлень, що містять одночасно аналогові й дискретні сигнали. У таких випадках, при частій зміні аналогового сигналу, частота посилок постійно буде впиратися в межу таймера затримки, хоча дискретні сигнали можуть і не змінюватися в даний момент. Тому, при використанні даного режиму, важливо заздалегідь продумати структуру повідомлень, що відправляються в середовищі для «IoT»-пристроїв «розумного міста».

– Відправка по таймеру.

Найпростіший спосіб, коли відбувається відправка повідомлення з заданим таймерним циклом. При цьому потрібно розуміти, що дані таймерні цикли у кількох вузлів не синхронізовані, тому може статися ситуація накладення. У якийсь момент часу лінія буде простоювати, цикл на вузлах ще не пройшов, а в інший момент часу кожен вузол буде намагатися відправити повідомлення на лінію, що призведе до затримок через виконання процедур арбітражу. У порівнянні з минулим способом, даний спосіб виграє в простоті, але при цьому відбувається відправка надлишкової інформації, коли дані не змінюються.

– Груповий синхронізований опитування.

Основна ідея даного режиму полягає в тому, що бувають ситуації, коли необхідно надати вхідні значення одночасно з декількох вузлів, наприклад, при опрацюванні руху робота в міськомі середовищі. Для цього використовується додаткові синхронізаційні повідомлення «SYNC», які не містить даних і відправляється на лінію з певною частотою.

У кожен момент часу вузли зчитують дані і оновлюють свої виходи. У момент отримання сигналу «SYNC» вони фіксують дані і починають пересилання повідомлення «PDO». Незважаючи на те, що повідомлення з усіх вузлів прийдуть послідовно через процедуру арбітражу, але буде відомо, що всі, хто прийняв дані були зафіксовані на одному «часовому зрізі». Зворотний порядок дій відбувається на приймаючому вузлі: йде приймання

всіх повідомлень, але реальний запис на входи відбувається тільки по сигналу «SYNC».

При реалізації інноваційних інформаційно-технологічних «IoT»-проектів класу «розумне місто» описані вище режими можуть використовуватися спільно, наприклад синхронізація повідомлень по сигналу «SYNC» з відправкою тільки по зміні значення. Хорошою практикою є об'єднання режиму 1 і 2 з метою уникнення проблем додавання нових вузлів при робочому режимі 1. Дана проблема може виникнути при режимі зі зміни значення, коли є параметри, які довгий час не змінюються. Тоді при гарячому підключенні нового вузла йому можуть бути невідомі параметри деяких вузлів, бо вони не передалися, через те, що вони не часто змінюються.

2.2 Мережеві сервіси «CANopen»

«NMT» – сервіс мережевого управління («Network Management»), який використовується в кожному інтегрованому в міське середовище вузлі «CANopen». Кожен вузол в будь-який момент часу знаходиться в одному з станів «NMT». Граф переходу цих станів поданий на рисунку 2.2.

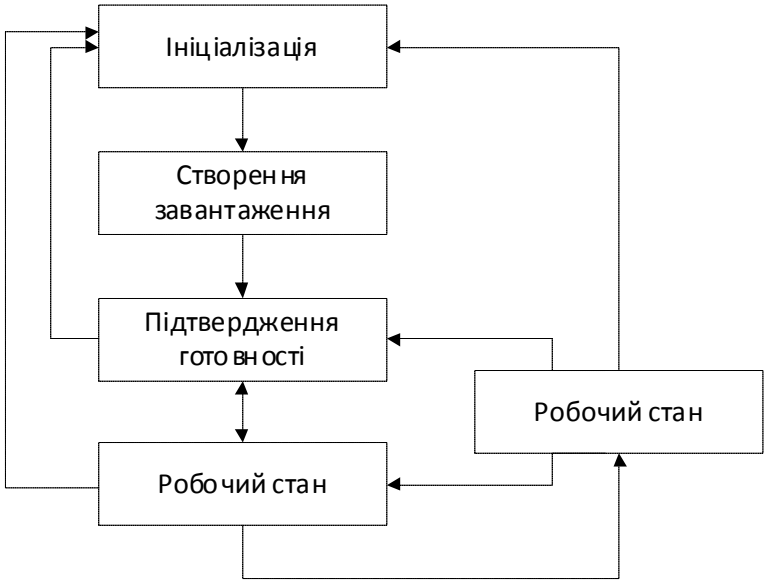


Рисунок 2.2 – Граф станів «NMT»

При перезавантаженні вузла він входить в стан ініціалізації, в якому відбувається первісне налаштування «CAN»/«CANopen» і зв'язку. Після успішної ініціалізації вузол переходить в стан попередньої готовності («Pre-Operational»), в якому можлива настройка вузла, але не передаються повідомлення «PDO». Надсилаючи звіт про проблеми «NMT»-вузол переходить в робочий стан. У таблиці 2.2 подано повідомлення, які може опрацьовувати вузол в різних станах.

Таблиця 2.2 – Повідомлення, які може опрацьовувати вузол

	Ініціалізація	Попередня готовність	Робочий стан	Зупинений стан
Повідомлення завантаження	+			
«SDO»		+	+	
«Emergency»		+	+	
«SYNC»		+	+	
«Heartbeat/Nodeguard»		+	+	+
«PDO»				

Під повідомленням завантаження розуміється спеціальне повідомлення, яке надсилається на лінію для позначення того, що в мережі з'явився новий вузол. Прийом будь-яких повідомлень при ініціалізації неможливий.

Для контролю стану вузла використовується одна з двох технологій: захисту вузла («Node Guarding») або синхронізуюча частота повідомлення («Heartbeat»).

Метод «Node Guarding» полягає в тому, що сервіс «NMT» майстра постійно опитує всі вузли про їх поточний стан «NMT». Якщо вузол не відповідає за встановлений час, то майстер вважає даний вузол відключити і може зробити будь-які дії. При цьому, реакція на відключення вузла не регламентована і має бути введена розробником, наприклад, це може бути як спроба перезавантаження вузла, так і виключення всіх інших вузлів

муніципальної мережі. При цьому ведені вузли муніципальної мережі теж можуть читати опитувальний повідомлення від ведучого, іншого вузла і своєчасно виявляти відключення вузлів. Однак даний метод завантажує лінію постійними повідомленнями до вузлів і не рекомендований до використання.

Метод синхронізуючої частоти повідомлень («Heartbeat») полягає у періодичних посилках самих вузлів свого стану. Тим самим виключається важливість центрального пристрою, який опитує інші, а також збільшується пропускна здатність лінії. При використанні даного методу, час, з яким відбувається посилка синхронізуючого повідомлення на лінію, налаштовується в кожному вузлі окремо. При цьому всі інші вузли знають цей час і тим самим можуть орієнтуватися, коли варто почати вважати вузол таким що втратив зв'язок. Тимчасова діаграма синхронізуючих повідомлень показана на рисунку 2.3.

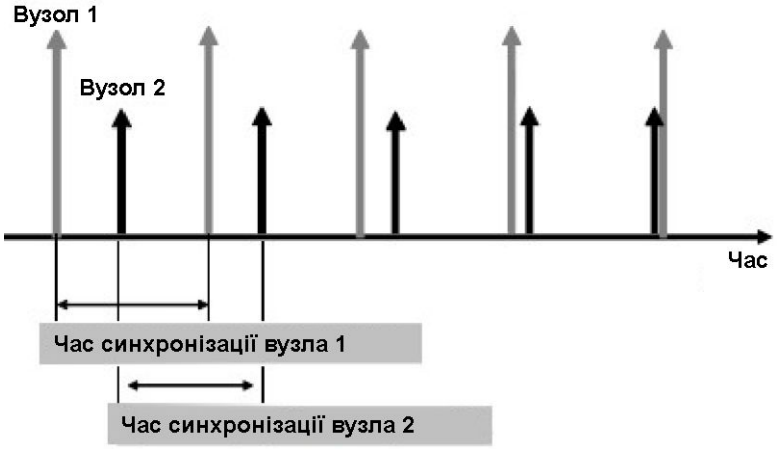


Рисунок 2.3 – Часова діаграма повідомлень «CANopen»

Аварійні повідомлення «EMCY» в міських повсюдних мережах на базі «CANopen». Кожному вузлу в мережі «CANopen» може бути поставлено у відповідність одне аварійне повідомлення («EMCY»). Номер ідентифікатора даного повідомлення зарезервований і вираховується наступним чином:

$$EMCY = 80h + NodeID \tag{2.2}$$

Аварійне повідомлення містить стандартні «8 байт» даних, з яких перші «2 байта» позначають код помилки «CANopen», наприклад, код «1000h» – загальний збій вузла, «3 байти» містить значення регістра помилок даного вузла, а решта «5 байт» доступні для формування виробником обладнання.

У загальному випадку аварійне повідомлення надсилається тільки один раз. Вважається, що помилка залишається, поки не прийде інше аварійне повідомлення, що оповіщає про пропажу даної помилки. Для такого підтвердження про «звільнення» помилки використовується код 00h в старшому байті коду помилки «CANopen». Наприклад, на помилку «8130h – помилка сервісів контролю вузла» скиданням буде повідомлення «0030h».

2.3 Дослідження процесів, що впливають на роботу CANopen в умовах «розумного міста»

При побудові реальних «IoT»-систем регулювання інтегрованих в середовище проектів класу «розумне місто» на основі програмованих логічних контролерів необхідно враховувати обширну множину чинників, які погіршують якість системи. Одним з таких факторів є продуктивність каналів передачі даних в замкнутих системах регулювання. Мета даної розділу – розгляд основних обмежень, які стосуються можливості функціонування пристроїв в міських повсюдних мережах, при заданих швидкостях передавання даних, заданих кількостях вузлів і допустимих довжинах ліній.

Обмеження фізичного рівня. Як відомо, стандарти протоколу «CANopen» описують тільки верхні рівні моделі «OSI», «3-7» – в основному описуючи останній, прикладної, рівень. Фізичний рівень («1 рівень» моделі «OSI») підпорядковується стандартам інтерфейсу «CAN».

У наступній таблиці 2.3 подано рекомендований час одного біта, який обробляється «CAN»-контролером.

Таблиця 2.3 – Рекомендований час одного біта

Швидкість	Час біта
«1 Мбит/с»	«1 μс»
«800 кбит/с»	«1,25 μс»
«500 кбит/с»	«2 μс»
«250 кбит/с»	«4 μс»
«125 кбит/с»	«8 μс»
«50 кбит/с»	«20 μс»
«20 кбит/с»	«50 μс»
«10 кбит/с»	«100 μс»

Структура мережі «CANopen» така, що всі вузли мережі повинні обмінюватися даними з однаковою швидкістю. Максимальна довжина ліній в мережі інтегрованій в міське середовище не повинна перевищувати «1000м».

Таблиця 2.4 містить опис стандартних параметрів кабелів при підключенні менше ніж «64 вузлів» в міській мережу «CANopen».

Таблиця 2.4 – Опис стандартних параметрів кабелів

Довжина лінії («м»)	Січення («мм^2»)	Термінатор («Ом»)	Скорость (кбит/с)
«0 – 40»	«0,25 – 0,34»	«124»	«1000» на «40м»
«40 – 300»	«0,34 – 0,6»	«150 – 300»	«≤500» на «100м»
«300 – 600»	«0,5 – 0,6»	«150 – 300»	«>100» на «500м»
«600 – 1000»	«0,75 – 0,8»	«150 – 300»	«>50» на «1 км»

Стандартні мідні кабелі передбачають затримку «5 нс/м». Розрахунок максимальної довжини ліній в міському середовищі, в залежності від кількості вузлів подано в таблиці 2.5.

Таблиця 2.5 – Розрахунок максимальної довжини ліній в міському середовищі

Січення («мм^2»)	«N = 32»	«N = 64»	«N = 100»
«0.25»	«200»	«170»	«170»
«0.5»	«420»	«360»	«320»
«0.75»	«640»	«550»	«480»

Довжина підвідних ліній до шини розраховується по формулі:

$$L_u < t_{PROPSEG} / (50t_p) \quad (2.3)$$

де, «tp = 5нс/м» – затримка в проводах лінії, а:

$$t_{PROPSEG} = TSEG1 - SJW \quad . \quad (2.4)$$

Виводяться з бітових складових, налаштованих в «CAN»-контролері, «SJW» – точка синхронізації, «TSEG1» – точка до фіксації значення. Рекомендації щодо довжини ліній, по відношенню до швидкості передачі даних подані в таблиці 2.6.

Таблиця 2.6 – Рекомендації щодо довжини ліній

Швидкість передачі даних	Довжина лінії
«1 Мбит/сек»	«25 м»
«800 кбит/сек»	«50 м»
«500 кбит/сек»	«100 м»
«250 кбит/сек»	«250 м»
«125 кбит/сек»	«500 м»
«50 кбит/сек»	«1000 м»
«20 кбит/сек»	«2500 м»
«10 кбит/сек»	«5000 м»

Крім того, при розрахунку реальних затримок «IoT»-мереж інтегрованих в фізичне середовище «розумних міст», варто також враховувати затримки в «CAN»-контролерах і прийомопередавачах.

Розглянемо обмеження на прикладному рівні. Прикладний рівень протоколу «CANopen» складається з:

– Передача оперативних повідомлень «PDO».

– Передача повідомлень настройки «SDO».

– Сигнали перекладу стану вузлів «NMT».

– Сигнали синхронізації «SYNC» або «heartbeat».

– Опрацювання помилок.

У найпростішому випадку, коли інтегрований в муніципальну мережу вузол справно налаштований і працює, тобто відбувається тільки обмін даними за допомогою «PDO», програмної затримкою можна вважати час циклу опрацювання даних, що прийшли вузлом, що показано на рисунку 2.4.

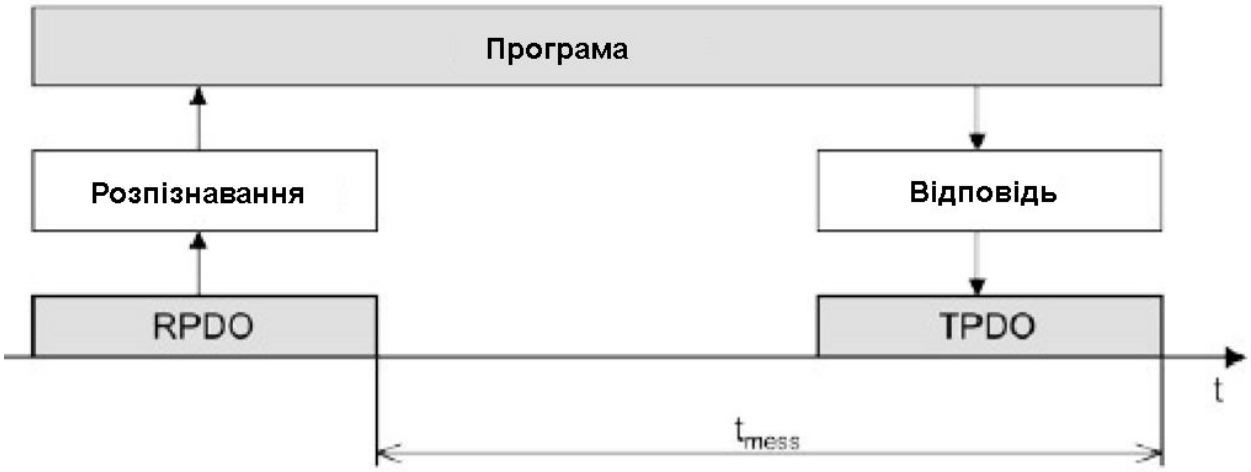


Рисунок 2.4 – Діаграма прийому і відправки повідомлень «PDO»

Затримки на лінії прикладного рівня. Крім фізичних затримок на лінії, розглянутих раніше, існують також і затримки, пов’язані з передачею даних по лінії кількома вузлами.

В інтегрованій в міське середовище мережі «CAN» і, відповідно «CANopen», в кожен момент часу по лінії може передаватися тільки одне повідомлення. Арбітражем на лінії займаються «CAN»-контролери, які визначають, за допомогою домінантного рівня лінії, можливість посилки свого повідомлення. З цього виникає затримка на лінії прикладного рівня.

Організацією «CiA» проведені відповідні експерименти для вимірювання навантаження лінії для «10 вузлів» для різних швидкостей

передачі даних [43]. В таблиці зведені в загальну форму дані цих вимірів для передачі даних по «PDO».

Таблиця 2.6 – Рекомендації щодо довжини ліній

Швидкість передачі	Час затримки «$t_{лп}$»
«1 Мбит/с»	«12,791 мс»
«800 кбит/с»	«15,988 мс»
«500 кбит/с»	«25,581 мс»
«250 кбит/с»	«51,162 мс»
«125 кбит/с»	«97,565 мс»
«50 кбит/с»	«255,811 мс»
«20 кбит/с»	«639,527 мс»
«10 кбит/с»	«1279,055 мс»

Можна помітити, що дана затримка пов’язана зі швидкістю передачі даних по лінії. Крім того, дана затримка є найсуттєвішою за часом, з усіх розглянутих до цього моменту.

Проведемо загальний розрахунок затримок. Розглянувши основні види обмежень, при використанні мережі «CANopen» можна вивести формулу затримки сигналу:

$$t_з = t_{лф} + t_{лп} + t_{mess} + t_{con} \tag{2.5}$$

де: $t_{лф}$ - час затримок в лінії на фізичному рівні;

$t_{лп}$ – час затримок в лінії на прикладному рівні;

t_{mess} – час затримки «PDO» при обробці повідомлення;

t_{con} – час затримок апаратних компонентів, «CAN»-контролер, CAN-трансівер.

Для отриманих рекомендованих значень складемо таблицю відповідності швидкості передачі даних, довжини лінії і часів затримок.

При цьому приймемо, що цикл контролера, який обробляє повідомлення:

$$t_{mess} = 50 \text{ мс} \tag{2.6}$$

А час затримок апаратних компонентів (див. таблицю 2.7):

$$t_{con} = 2 \text{ мс} \tag{2.7}$$

Таблиця 2.7 – Час затримок апаратних компонентів

Швидкість кбит/с	Довжина, м	$t_{лф}$, мс	$t_{лп}$, мс	$t_{з}$, мс
«1000»	«25»	«0,000125»	«12,791»	«64,791»
«800»	«50»	«0,00025»	«15,988»	«67,988»
«500»	«100»	«0,0005»	«25,581»	«77,582»
«250»	«250»	«0,00125»	«51,162»	«103,163»
«125»	«500»	«0,0025»	«97,565»	«149,568»
«50»	«1000»	«0,005»	«255,811»	«307,816»
«20»	«2500»	«0,0125»	«639,527»	«691,54»
«10»	«5000»	«0,025»	«1279,055»	«1331,08»

2.4 Висновок до другого розділу

В другому розділі дипломної роботи розкрито основні поняття «CANopen» для «IoT»-проектів «розумних міст». Описано мережеві сервіси «CANopen». Проведено дослідження процесів, що впливають на роботу «CANopen» в умовах «IoT»-пристроїв для «розумного міста».

3 МОДЕЛЮВАННЯ ПРОЦЕСІВ У МІСЬКИХ IOT-МЕРЕЖАХ НА БАЗІ «CANOPEN»

3.1 Побудова ідеальної моделі

Представивши обмеження інтерфейсу зв’язку «IoT»-пристрою інтегрованого в обчислювальне середовище «розумного міста» в чисельному вигляді можна провести моделювання для вироблення практичних вказівок. Для цього розглянемо найпростіший об’єкт управління першого порядку з ланкою чистого запізнювання.

$$W_{\text{оу}}(s) = \frac{K}{Ts+1} \cdot e^{-\tau} \tag{3.1}$$

Нехай, час запізнення «τ = 0.5с», постійна часу «Т = 1.45с», а коефіцієнт передачі «К = 1».

Включимо даний об'єкт управління в замкнутий контур з підрегулятором, попередньо налаштувавши його на деякий перехідний процес [44]. «Simulink»-модель такої моделі представлена на рисунку 3.1.

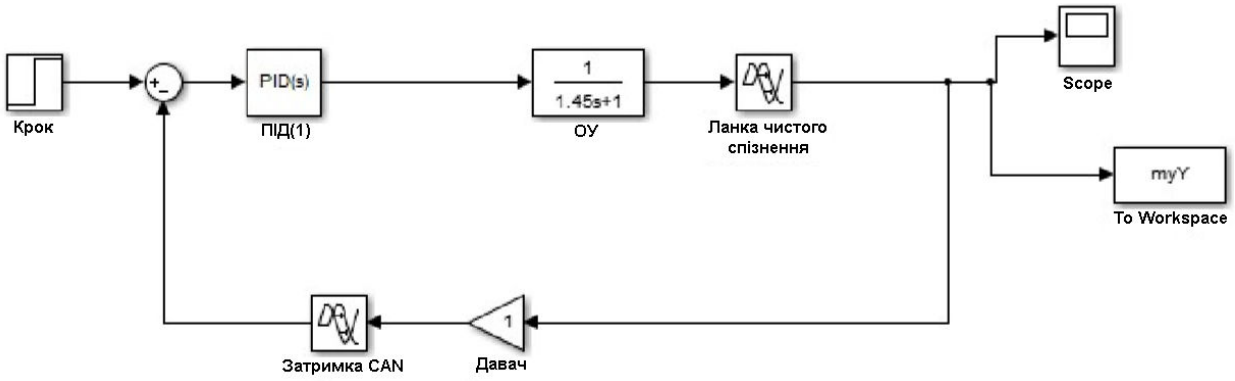


Рисунок 3.1 – «Simulink»-модель розглянутої початковій системи

Приймемо даний перехідний процес за еталонний.

Параметри ПІД-регулятора наступні:

– Пропорційна складова «kp = 3».

– Інтегральна складова «ki = 1.76».

– Диференціальна складова «kd = -0.45».

За допомогою бібліотеки «Linear Analisys Tool» були отримані параметри перехідного процесу від одиничного ступеневого сигналу:

– Час першого узгодження – 0.968 с.

– Перегулірованіе – 33,5%.

– Входження в трубку точності – 5.43 с.

Вивчення впливу затримок на перехідний процес. Після цього приймаємо, що в зворотного зв'язку передача інформації відбувається по інтерфейсу «CANopen», наприклад, це може бути «CANopen»-давач, заведений на контролер.

Будемо ставити затримку для різних швидкостей передачі даних і довжини лінії. Тим самим отримуємо ситуацію, коли аналіз зворотного зв’язку і обробка підрегулятора відбувається в контролері-майстра мережі, після чого сигнал посилає на «ОУ», а інформація з датчика відправляється назад по мережі «CANopen».

На рисунку 3.2 наведені результати моделювання відпрацювання ступеневої впливу в замкнутій системі при різних швидкостях передачі даних по інтерфейсу «CANopen». Можна помітити, що при появі затримок в зворотного зв'язку відбувається різке погіршення перехідного процесу. Так, навіть при найшвидшою швидкості передачі даних в «1 Мбіт/сек» регулювання збільшилася на «8%», з «1.078» до «1.159». Якщо ж продовжувати зменшувати швидкість передачі даних, то процес і зовсім може стати розходяться при швидкостях нижче «50 кбіт/с».

В результаті проведеного моделювання можна запропонувати використання швидкості в «500 кбіт/сек» в якості оптимальної з точки зору швидкодії і можливої довжини лінії в «100» метрів.

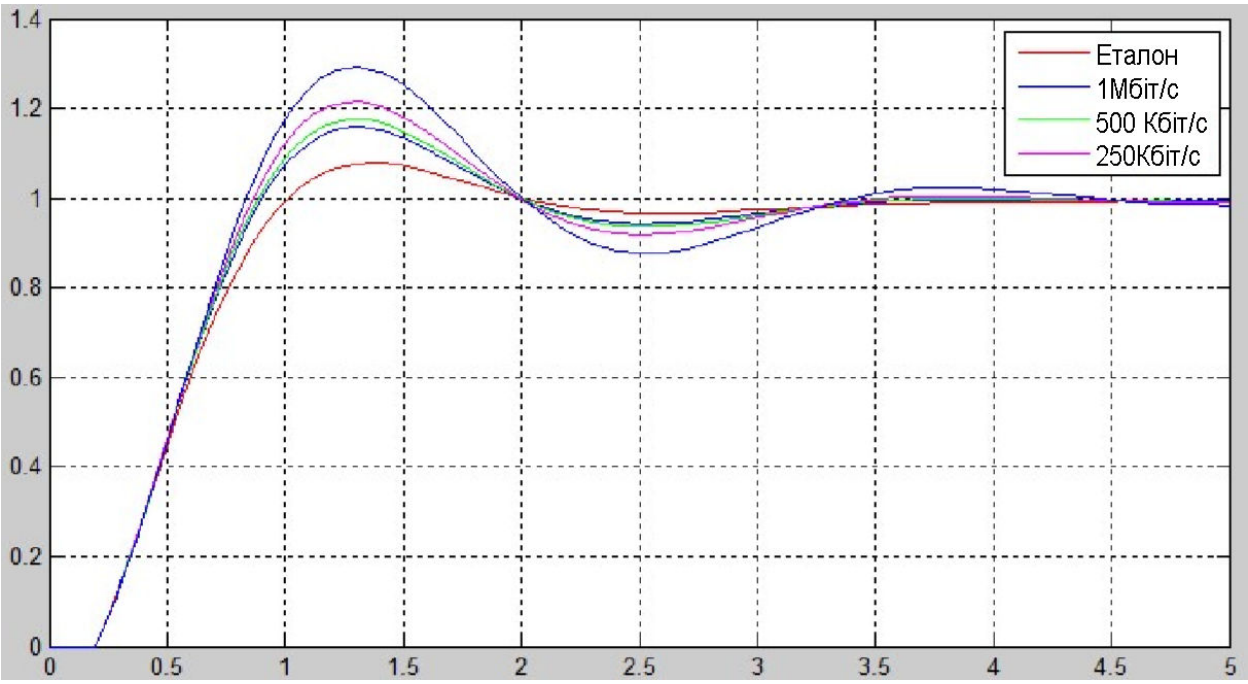


Рисунок 3.2 – Перехідний процес при зміні параметрів шини «CANopen»

Моделювання при додаткових обмеженнях.

Використання ідеального регулятора некоректно при описі в реальних системах, оскільки можуть бути встановлені обмеження параметрів на виході з нього. Це можуть бути як обмеження операційних підсилювачів, або, як у нашому випадку, обмеження вихідних модулів «ПЛК».

Основна проблема при обліку обмежень – інтегральне насичення регулятора. При вході сигналу на вході «ОУ» в зону насичення і ненулевом сигналі неузгодженості, інтегратор «ПІД»-регулятора продовжує інтегрувати, тим самим ще більше вганяючи сигнал в зону насичення. Система в такому випадку, фактично, стає розімкнутої і відбувається серйозне затягування перехідного процесу (див. рисунок 3.3).

Так, в порівнянні з ідеальною системою, для швидкості «500 кбіт/с» час першого узгодження збільшилася в 2 рази. В цілому, сталася велика втрата в швидкодії системи.

Для зменшення впливу ефекту інтегрального насичення регулятора існує множина методів.

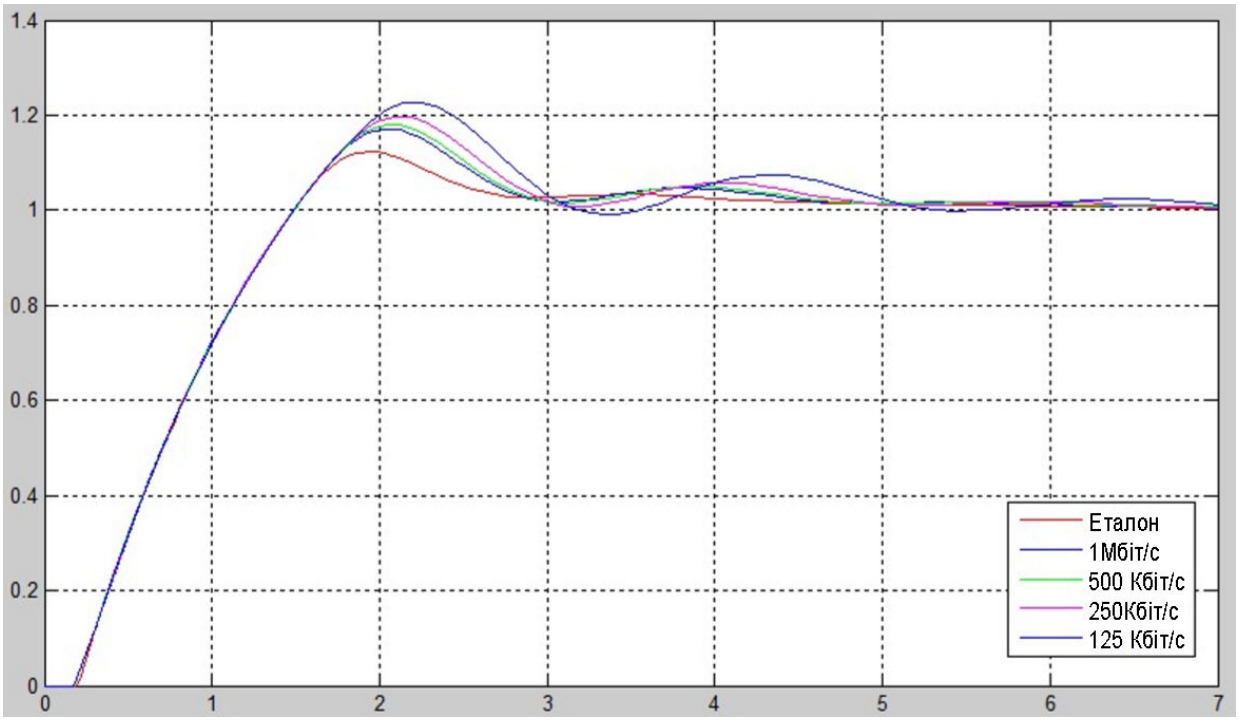


Рисунок 3.3 – Перехідний процес при насиченні з виходу регулятора

В даному випадку скористаємося методом алгоритмічного заборони на інтегрування (див. рисунок 3.4).

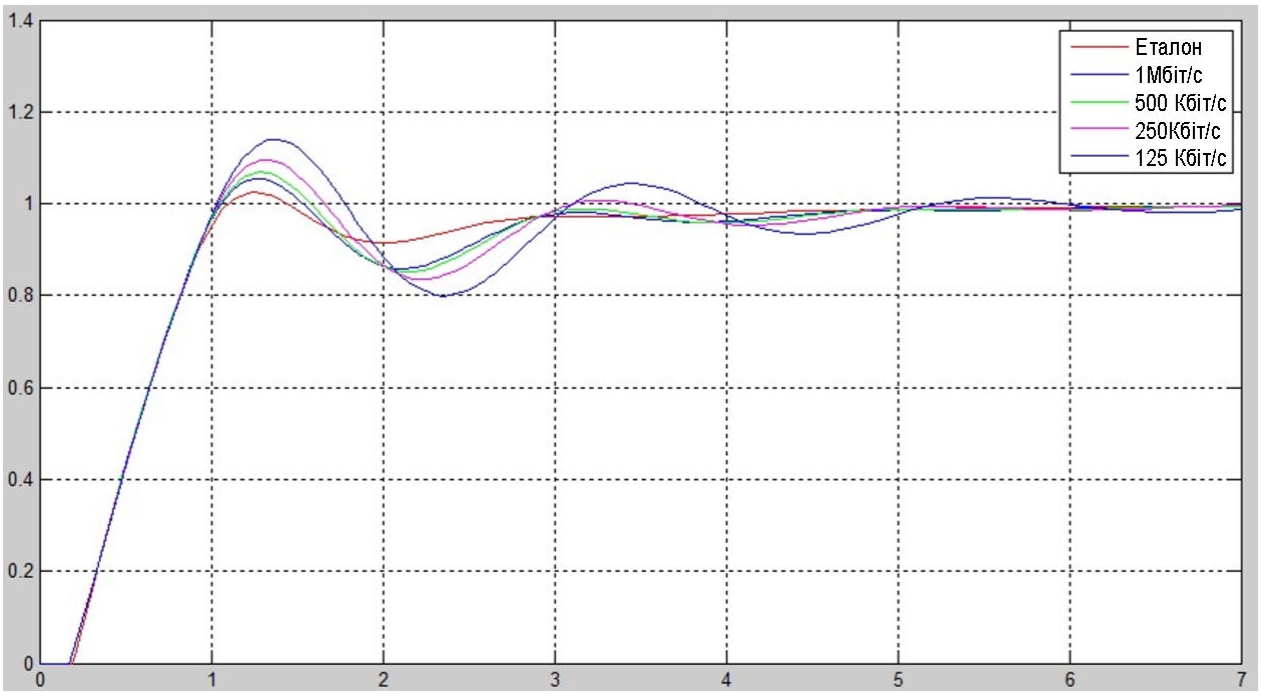


Рисунок 3.4 – Перехідний процес при використанні алгоритмічного заборони на інтегрування

Його суть полягає в тому, що контролер стежить за величиною керуючого впливу на «IoT»-об'єкт інтегрований у фізичне середовище «розумного міста», і при вході його в зону насичення, негайно вводиться програмний заборону інтегрування для інтегральною складовою регулятора.

Можна помітити, що сталося якісне поліпшення характеристик перехідного процесу. Значення перерегулювання в середньому зменшилася на «10%», як і час першого узгодження, яке тепер стало схожим на ідеальний випадок, «1 секунда», проти «1.5» в попередньому випадку. При цьому можна помітити, що в реальності поліпшень перехідного процесу також можна було досягти за допомогою зміни параметрів самого регулятора. Зазвичай регулятори реалізують на основі програмованих логічних контролерів у вигляді окремих програмних блоків з можливістю коригування їх параметрів. Більш того, гарним вибором буде вивід даних параметрів «IoT»-пристрою безпосередньо оператору/технологу «розумного міста» на верхній рівень з можливістю їх коригування.

Впровадження блоку відмов на лінії. Реагування вузлів на відмови лінії не регламентоване стандартами «CANopen», є тільки припис для «CAN», щоб уникнути поломки мережі через можливий брак контролера. Тому дуже важливо розуміти реакцію систему на можливі поломки мережі.

Для моделювання цих процесів був створений блок відмови, завдання якого полягає в моделюванні випадкових виникнень відмови на лінії. Вище було висловлено припущення, що з імовірністю «87%» відмови на лінії не відбувається зовсім. У решти «13%» буде наступний розподіл відмов:

– «50%», що станеться одиночний відмова.

– «30%», що подвійний відмову.

– «20%», що потрійний відмова.

В результаті даний блок був вбудований в спрощену модель системи без обмежень з наступним алгоритмом – при виникненні відмови на лінії ведучий пристрій відкидає отримані дані, а вузол намагається відправити

дані ще раз. Тим самим пропорційно збільшується затримка на лінії, з додаванням деякої постійної складової, що позначає час таймаута лінії між повторними посилками.

Були проведені кілька дослідів при різних значеннях випадкової помилки і відповідно, кількості відмов. На рисунку 3.5 подані результати моделювання при виникненні переважно одиничних відмов в момент перехідного процесу.

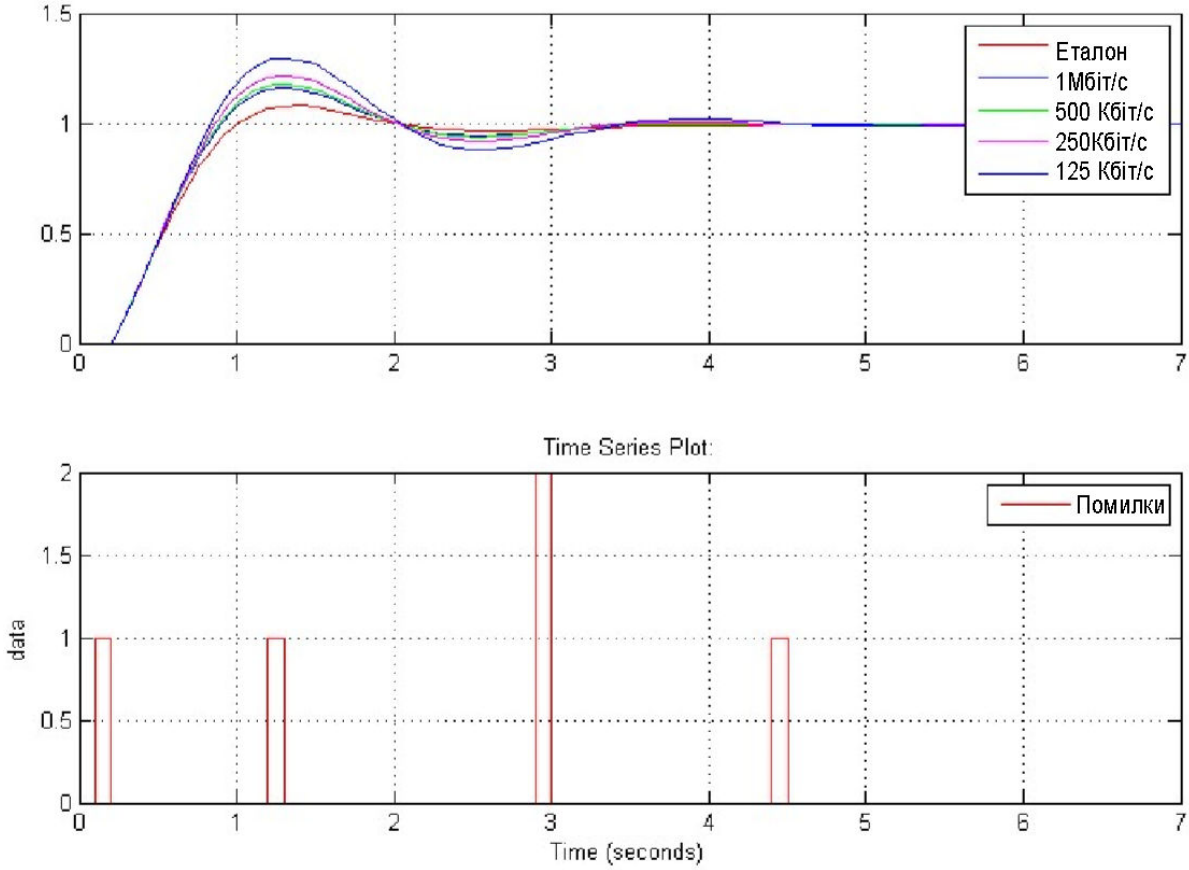


Рисунок 3.5 – Перехідний процес при одиночних відмовах

Можна помітити, що в цьому випадку відмова не вносить будь-яких серйозних змін в перехідний процес. Для розглянутої в якості кращою швидкості «500 кбіт/с» зміна часу першого узгодження і перерегулювання знаходяться в межах «2%». Подвійний відмову, який стався на «3 секунді» процесу також практично непомітний, оскільки перехідний процес до того моменту вже близький до сталого.

Розглянемо більш несприятливий випадок, коли відмови на лінії походять з ймовірністю «20%». Перехідний процес такої системи показаний на рисунку 3.6.

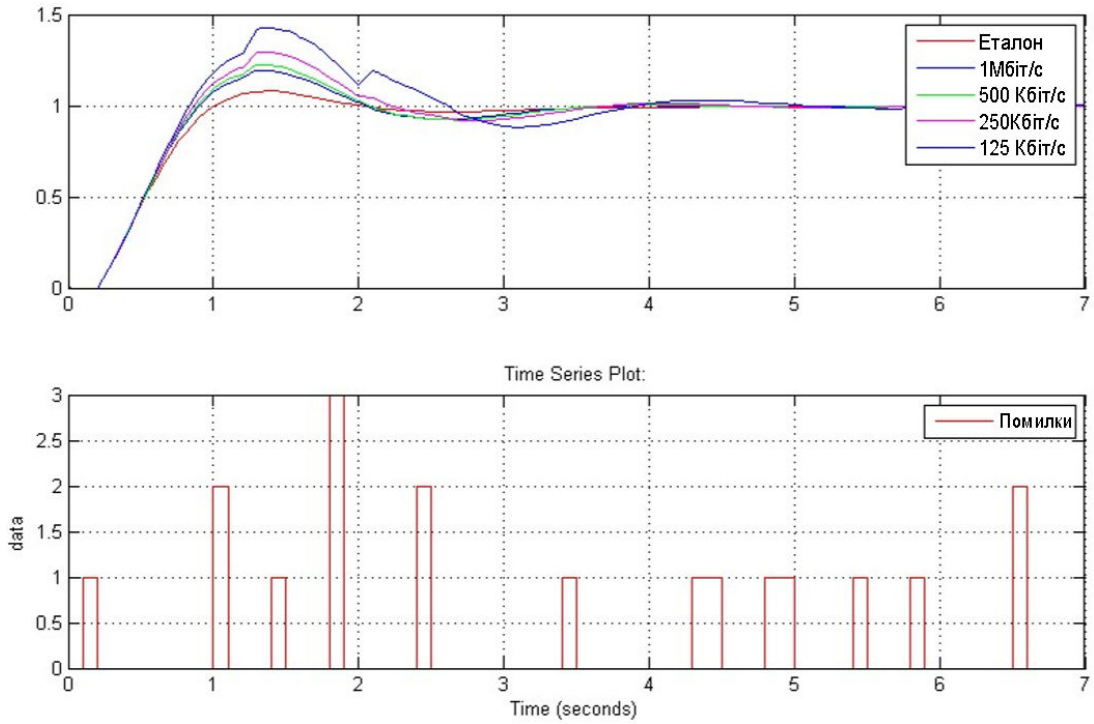


Рисунок 3.6 – Перехідний процес при множинних відмовах

В даному випадку видно значні спотворення вхідного значення при перехідному процесі, особливо на низьких швидкостях. Можна помітити, що вплив одиночних відмов на передачу даних при швидкостях «500 кбіт/с» менше, ніж на більш низьких. Однак, найчастіше ситуація відмов не є допустимою при роботі «IoT»-обладнання в критичних умовах «розумного» міського середовища.

3.2 Рекомендації щодо використання «CANopen» в «IoT»-проектах класу «розумне місто»

В результаті проведеного дослідження були детально досліджені і чисельно описані різні фактори, що впливають на появу затримок в

інтегрованій в міське середовище системі з передачею даних по інтерфейсу «CANopen». Було виявлено, що при використанні цифрового каналу зв'язку необхідно враховувати обмеження: як фізичні, так і програмні. Фізичні обмеження визначають рекомендовані співвідношення по довжині лінії зі швидкістю передачі даних. Це є найважливішим критерієм при проектуванні реальної системи управління, оскільки зазвичай управляє обладнання розташовується в єдиному центрі на видаленні від об'єктів управління. При отриманої рекомендованої швидкості в «500 Кбіт/с» довжина окремої лінії може досягати «100 метрів», що має бути досить для вирішення завдань в межах окремих міських локацій, або міських мануфактур та цехів. Програмні обмеження впливають на появу затримок на лінії через особливості роботи протоколів зв’язку. В рамках даної дипломної роботи розглянуто вплив тільки основного протоколу «PDO» на швидкодію обміну інформації між вузлами інтегрованими в міське середовище «IoT»-проектів класу «розумне місто». На практиці ці обмеження впливають на можливість розширення систем. Затримки, пов’язані з обміном даних по шині, будуть зростати, при додаванні на неї додаткових вузлів. Тому, при проектуванні, необхідно відразу розуміти про можливість розширення «IoT»-пристроїв та мереж інтегрованих в проекти «розумних міст» систем в майбутньому і закладати цю інформацію при виборі робочих швидкостей, що в свою чергу спричинить зміни можливостей вибору довжини ліній.

Було проведено моделювання найпростішої системи з об'єктом управління першого порядку і «CANopen»-давачем в колі зворотного зв'язку. В результаті була отримана залежність з якої видно, що можливості використання в даній ситуації інтерфейсу «CANopen» визначається обраною швидкістю передавання даних на лінії. При швидкостях менших «250 кбіт/с» якість перехідного процесу різко погіршується аж до розходиться процесу при швидкостях менших «50 кбіт/с». Тим самим було виявлено, що не всі описані стандартом швидкості передачі даних підходять для використання в

управлінні об’єктом зі зворотним зв'язком. Для вирішення таких завдань можна рекомендувати використання швидкостей в діапазоні «250 Кбіт/с» – «1 Мбіт/с». При цьому різниця характеристик якості перехідного процесу між швидкостями «1 Мбіт/с» і «500 Кбіт/с» мінімальна, а можлива довжина лінії різниться в «2 рази». Саме тому в якості основної рекомендованої швидкості для використання інтерфейсу «CANopen» в умовах міського середовища та замкнутій системі регулювання можна назвати швидкість «500 Кбіт/с».

3.2.1 Підвищення надійності та дублювання муніципальних мереж

Як було розглянуто раніше, несприятливі обставини, такі як множинні відмови на лінії, можуть привести до погіршення перехідного процесу в замкнутій системі регулювання, аж до його розбіжності. Незважаючи на те, що ймовірність таких множинних відмов мала, в деяких випадках в реальних міських умовах необхідна можливість поліпшення надійності системи. Як правило, ці питання постають при небезпечних виробництвах, коли поломка обладнання може призвести до людських жертв або значного збитку.

Основний критерій при використанні мережі в такому випадку – можливість виявлення втрати зв'язку з подальшим переходом в безпечний стан. «CANopen» відповідає цьому критерію, але при цьому необхідно усвідомлювати, що відповідальність за перехід обладнання в безпечний стан лежить на віддалених вузлах, а не на провідному пристрої.

Підвищення надійності муніципальних мереж побудованих з використанням протоколу «CANopen» можна виробляти з боку обладнання, за допомогою програмних засобів або їх комбінацій.

Дублювання має на увазі собою використання частин компонентів мережі в гарячому резерві з використання спеціальних програмних засобів для вибору поточного обладнання для роботи. Приклад найпростішого дублювання показаний на рисунку 3.7.

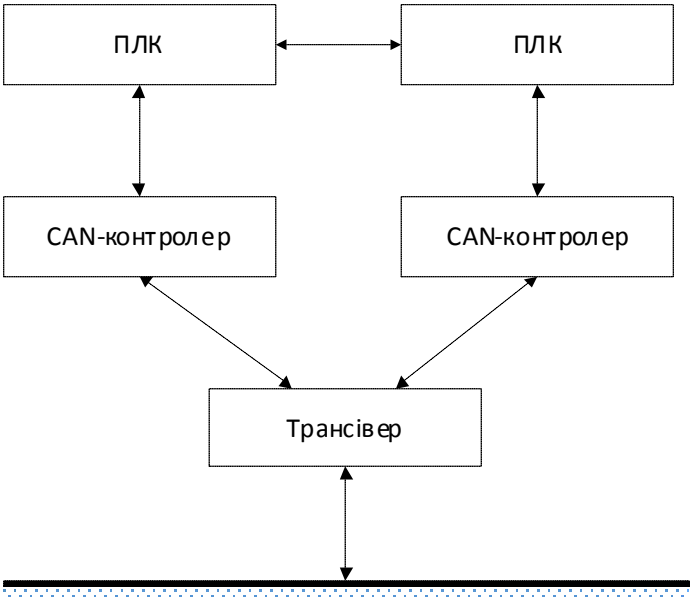


Рисунок 3.7 – Дублювання контролерів

В даному випадку в міському середовищі використовуються дубльовані контролери з «CAN»-контролерами, які підключені до однієї шині даних. Однак, в такому випадку «слабкою ланкою» виступає трансивер і сама фізичне середовище передачі даних на лінії розміщеній в міському середовищі. Тому рекомендується для забезпечення надійності за допомогою дублювання використовувати структуру, показану на рисунку 3.8.

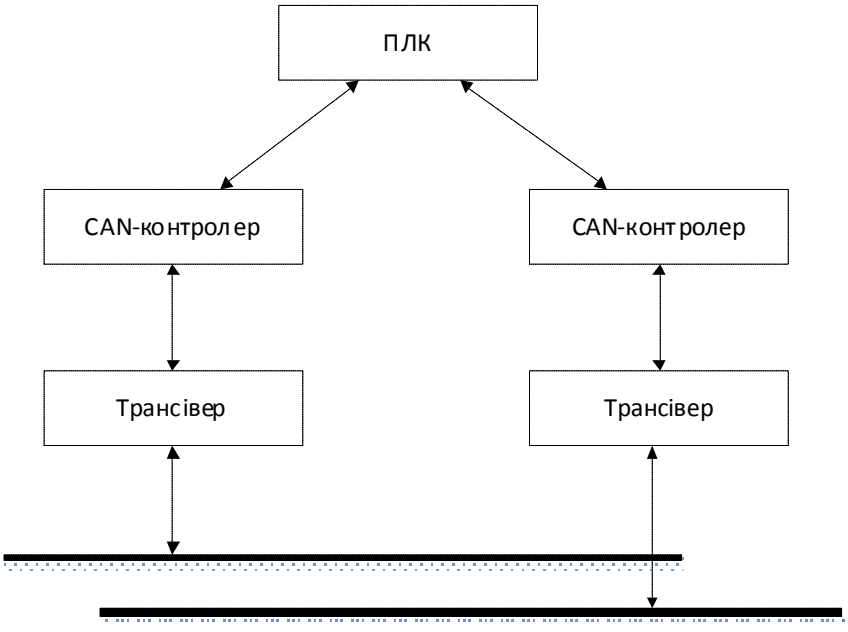


Рисунок 3.8 – Дублювання шин

У разі використання дублювання при реалізації муніципальних мережевих рішень необхідно передбачати додаткові програмні модулі для управління дублюванням. Так, при використанні структури, показаної на рисунку 3.7 один з контролерів призначається ведучим, а другий знаходиться в гарячому резерві. На кожному циклі відбувається розрахунок параметрів і їх порівняння між двома контролерами. При розбіжності параметрів ведений контролер запускає діагностику і бере керування на себе при виявленні помилок в першому контролері. При відновленні першого ПЛК він повертає собі права майстра.

«SRDO» – програмний засіб підвищення надійності. Основна ідея полягає в тому, що на лінію посилається відразу два повідомлення. Перше повідомлення – звичайне «PDO», а друге – копія першого з інвертованими бітами даних і мінімум двома інвертованими бітами ідентифікатора повідомлення. Визначення несправності при цьому відбувається за двома тимчасових інтервалах:

– SCT – основний період між двома основними повідомленнями.

– SRVT – максимальна затримка між приходом основного повідомлення і дублюючого – інвертованого (див. рисунок 3.9).

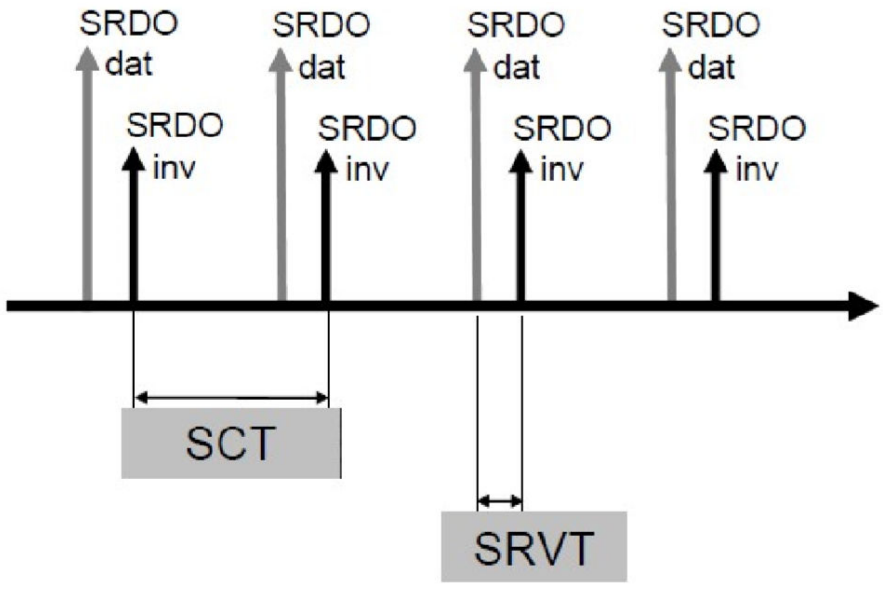
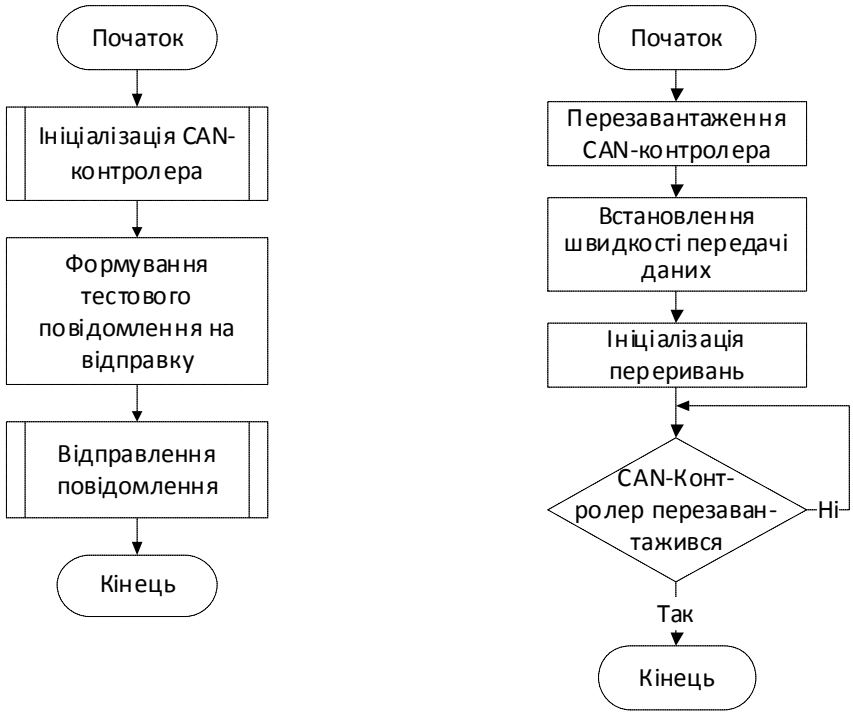


Рисунок 3.9 – Тимчасова діаграма посилки «SRDO»

У будь-яких випадках «IoT»-застосування в проектах класу «розумне місто» способів підвищення надійності, необхідно розуміти, що гарантувати стовідсоткову працездатність системи неможливо. Тому необхідно передбачати на кінцевому обладнанні безпечні стани, наприклад, входів-виходів, при будуть мінімальні збитки при будь-якому режимі роботи, в які воно (муніципальне обладнання) буде переводитися автоматично при критичних відмовах.

3.3 Розроблення програмної частини

Для передачі повідомлень по шині «CAN» необхідно реалізувати програмну обробку даного інтерфейсу засобами мікроконтролера. Для тестування пристрою написана програма (див. рисунок 3.10) по обробці отримання повідомлень і відправки цих повідомлень на лінію на основі бібліотеки «CAN» для мікроконтролера «MCP2515». [45]



а) Головної програми; б) Ініціалізації контролера

Рисунок 3.10 – Блок схеми

Вище було розглянуто програмний модуль для передачі повідомлень по шині «CAN». Однак, для використання «IoT»-пристрою в інтегрованій до проекту класу «розумне місто» мережі «CANopen» необхідно, щоб програмна обробка була реалізована на бібліотеці «CANopenNode». [46]

На Рисунку 3.11 показана загальна блок-схема алгоритму обробки кожного вузла за допомогою даної бібліотеки.

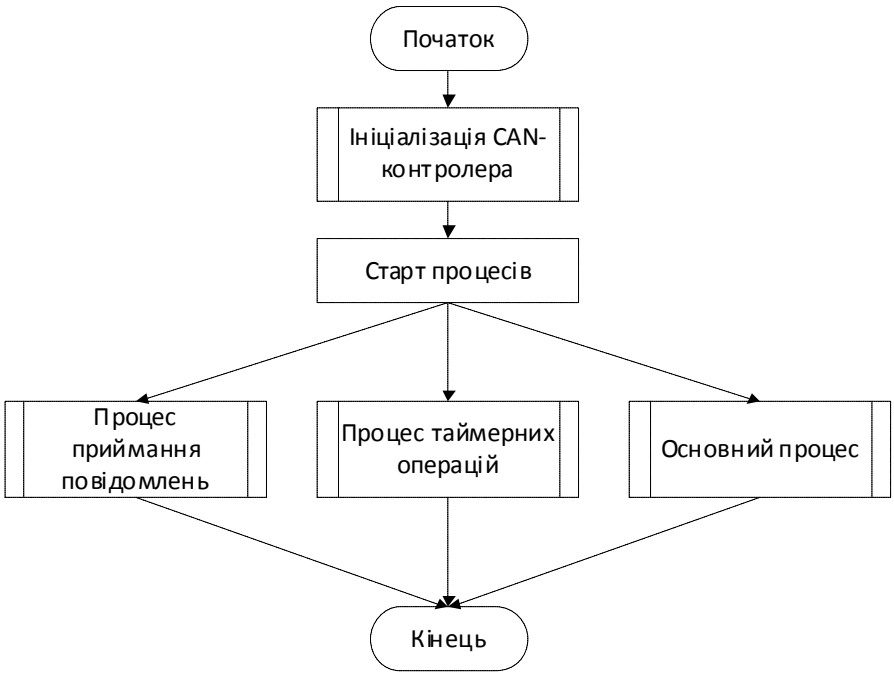


Рисунок 3.11 – Алгоритм опрацювання вузла «CANopen»

Етапи роботи алгоритму:

1. Процес прийому повідомлення. Даний процес призначений для швидкого відгуку на повідомлення, що приходять, вибірки ідентифікатора повідомлення, обробки повідомлення і копіювання його даних в об'єкти «CANopen» («PDO», «SDO» і т.д.). [47]

2. Процес таймерних операцій. Даний процес виконується за таймером з інтервалом «1 мс» і виробляє синхронізацію мережі за допомогою сигналу «SYNC», копіювання входів «RPDO» в словник об’єктів і навпаки копіювання значень словника об’єктів в «TPDO».

3. Основний процес. Основний процес відповідає за функціонування сервера «SDO» повідомлень, відправлення повідомлень помилок «EMCY», сервіс «NMT» і синхронізуюче повідомлення. [48]

Блок-схема алгоритму програми основного процесу подана на рисунку 3.12.

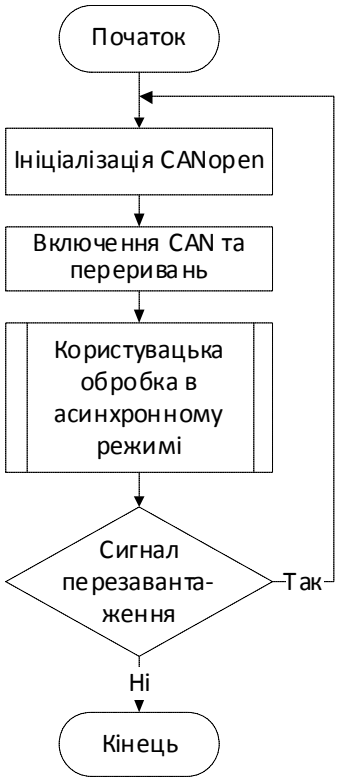


Рисунок 3.12 – Блок-схема алгоритму основного процесу

Також за допомогою зазначеної бібліотеки можна окремо налаштувати «SDO»-клієнт для ведучого пристрою мережі, за допомогою якого можна читати і записувати дані в словник об’єктів будь-якого вузла мережі. [49]

3.4 Висновок до третього розділу

В результаті виконання роботи було досліджено інтерфейс «CAN» і протокол «CANopen» в контексті їх використання для «IoT»-пристроїв в проектах класу «розумне місто», при використанні в рамках управління

замкнутою системою регулювання. Виявлені фактори, що впливають на швидкодію системи, і вироблені практичні рекомендації щодо застосування даного інтерфейсу в муніципальних мережах. Розглянуто питання застосування різних інтерфейсів і протоколів для «IoT»-пристроїв в сучасних «розумних містах», їх перспективи, а також проведено детальний розбір роботи «CANopen» на всіх рівнях.

Було проведено моделювання процесів, що відбуваються в системах управління з каналом зв'язку «CANopen» і виявлені закономірності, що відбуваються при різних параметрах даної мережі. Також були розглянуті випадки обмеження сигналу і виникнення обривів на лінії з пропозиціями щодо мінімізації даного впливу на роботу системи за рахунок збільшення надійності. Було спроектовано програмно-алгоритмічне рішення для можливого підключення до шини «CAN» і побудови експериментальної моделі для виконнаня програмного моделювання.

4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Проектування елементів пристрою для тестового підключення до шини «CAN»

Для вивчення процесів, що відбуваються в мережах «CAN» інтегрованих з «IoT»-пристроями в проектах класу «розумне місто», було прийнято рішення в необхідності створення власного пристрою, який би відповідав наступним вимогам:

– Можливість підключення до шини «CAN» для передачі і прийому інформації від інших пристроїв на даній шині.

– Легкість конфігурації пристрою і повідомлень для розгляду різних режимів роботи і їх аналізу.

– Можливість зчитування даних і контролю роботи пристрою за допомогою комп'ютера.

– Низика вартість кінцевого пристрою і як результат, відмова від готових схемних рішень.

Створюваний пристрій повинен складатися з трьох основних компонентів:

– Мікроконтролер для управління прийомом і передачі повідомлень, зберігання інформації і т.д.

– «CAN»-контролер для формування посилок і їх прийому, арбітражу на шині при взаємодії з іншими пристроями і інших комунікаційних функцій.

– «CAN»-трансивер для безпосереднього підключення пристрою до шини.

Перейдемо до вибору приладів і обладнання. Відповідно поставленому до поставленого завдання були вибрано наступне обладнання:

– Мікроконтролер – «Arduino UNO». [50]

– «CAN»-контролер – «Microchip MCP2515». [51]

– «CAN»-трансивер – «Microchip MCP2551». [52]

Мікроконтролер «Arduino UNO» обраний за рахунок своєї простоти програмування через «USB»-порт, наявності готового ПО і можливості аналізу роботи системи за допомогою комп'ютера.

«CAN»-контролер «MCP2515» є готовим програмно-апаратним продуктом, який не потребує окремого програмування і, відповідно, програматора, зв’язок з яким здійснюється за рахунок інтерфейсу «SPI». [53]

Проведемо проектування апаратної частини. Плата «Arduino UNO» є основним керуючим контролером пристрою, що передає за допомогою інтерфейсу «SPI» команди на CAN-контролер. На рисунку 4.1 показаний зовнішній вигляд входів і виходів з плати.

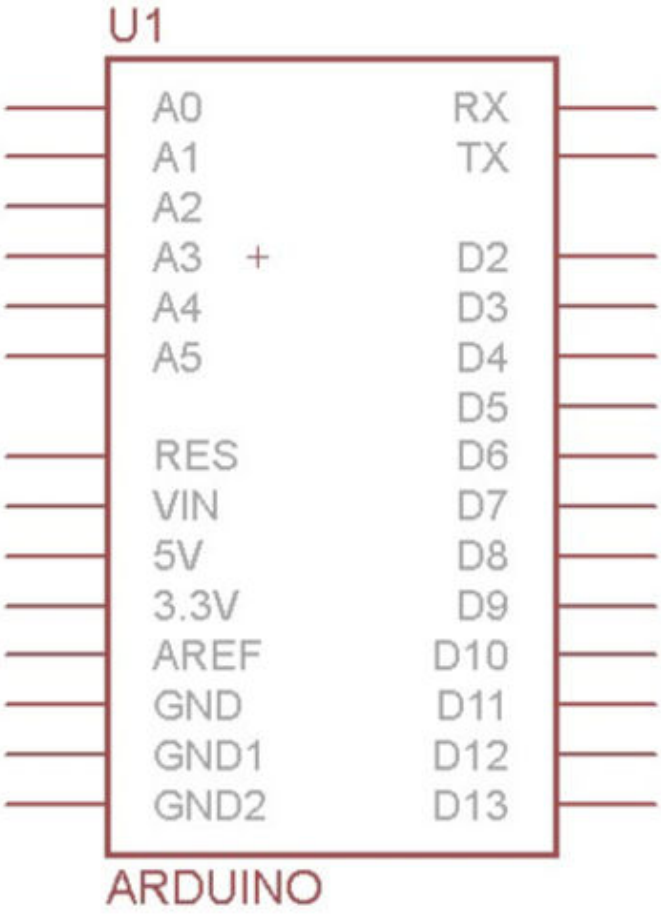


Рисунок 4.1 – Розпіновка плати «UNO»

Опис призначення контактів (пінів) плати «UNO» подано в таблиці 4.1.

Таблиця 4.1 – Розпіновка плати «UNO»

№	Назва	Опис
«1..6»	«A0..A5»	Аналогові входи.
«7»	«RES»	Апаратне скидання.
«8»	«V_{IN}»	Вхідне живлення від зовнішнього джерела.
«9»	«5V»	Вихід живлення на «+5 В».
«10»	«3.3V»	Вихід живлення на «+3.3 В».
«11»	«AREF»	Вхід апаратної налаштування аналогових входів «A0..A5».
«12..14»	«GND»	Земля.
«15»	«RX»	Канал прийому протоколу «UART».
«16»	«TX»	Канал відправки протоколу «UART».
«17»	«D2»	В даному проекті: сигнал переривання з «CAN»-контролера.
«18..24»	«D3..D9»	Дискретні входи.
«25»	«D10 (CS)»	Сигнал вибору (CS) CAN-контролера по інтерфейсу SPI
«26»	«D11»(«MOSI»)	Канал відправки даних від майстра по інтерфейсу SPI
«27»	«D12»(«MISO»)	Канал відправки даних від майстра по інтерфейсу SPI
«28»	«D13»(«SCK»)	Тактова частота інтерфейсу SPI

«CAN»-контролер «MCP2515» – це готове програмно-апаратне рішення, призначене для передачі і прийому інформації за допомогою інтерфейсу «CAN». При цьому даний контролер підтримує обидва стандарти інтерфейсу і може приймати короткі або довгі повідомлення «CAN 2.0A» або «CAN 2.0B» відповідно. Зв’язок «CAN»-контролера з керуючим контролером здійснюється за рахунок інтерфейсу «SPI». Зовнішній вигляд мікросхеми із зазначенням ніжок показаний на рисунку 4.2. [54]

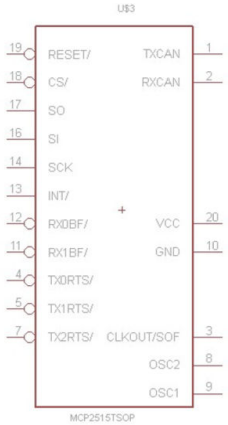


Рисунок 4.2 – Розпіновка «MCP2515»

Призначеня ніжок мікросхеми «MCP2515» подано в таблиці 4.2.

Таблиця 4.2 – Розпіновка «MCP2515»

№	Ім’я	«I/O/P»	Опис
1	«TXCAN»	«O»	Передавальний вихід на шину «CAN».
2	«RXCAN»	«I»	Приймаючий вхід з шини «CAN».
3	«CLKOUT»	«O»	Вихід годин або сигнал початку посилки.
4	«TX0RTS»	«I»	Сигнал передачі з буфера «TXB0».
5	«TX1RTS»	«I»	Сигнал передачі з буфера «TXB1».
6	–		
7	«TX2RTS»	«I»	Сигнал передачі з буфера «TXB2».
8	«OSC2»	«O»	Вихід осцилятора.
9	«OSC1»	«I»	Вхід осцилятора.
10	«V_{SS}»	«P»	Земля.
11	«RX1BF»	«O»	Сигнал про переривання від приймаючої буфера «RXB1».
12	«RX0BF»	«O»	Сигнал о прерывании от принимающего буфера RXB0.
13	«INT»	«O»	Сигнал переривання.
14	«SCK»	«I»	Вхід тактової частоти для інтерфейсу «SPI».
15	–		
16	«SI»	«I»	Вхід даних для інтерфейсу «SPI».
17	«SO»	«O»	Вихід даних для інтерфейсу «SPI».
18	«CS»	«I»	Сигнал вибору веденого для інтерфейсу «SPI».
19	«RESET»	«I»	Апаратний скидання пристрою.
20	«V_{DD}»	«P»	Харчування («+5В»).

«CAN»-трансивер «MCP2551» призначений для фізичного зв’язування виходів «CAN»-контролера з «CAN»-шиною. За допомогою даної мікросхеми відбувається перетворення цифрових сигналів «TXCAN» і «RXCAN» в диференційний сигнал для фізичної шини. Також «CAN»-трансивер служить захистом для «CAN»-контролера від можливих перенапруг і наведень на лінії. Зовнішній вигляд мікросхеми із зазначенням ніжок показаний на рисунку 4.3. Призначеня ніжок мікросхеми «MCP2551» подано в таблиці 4.3. [55]

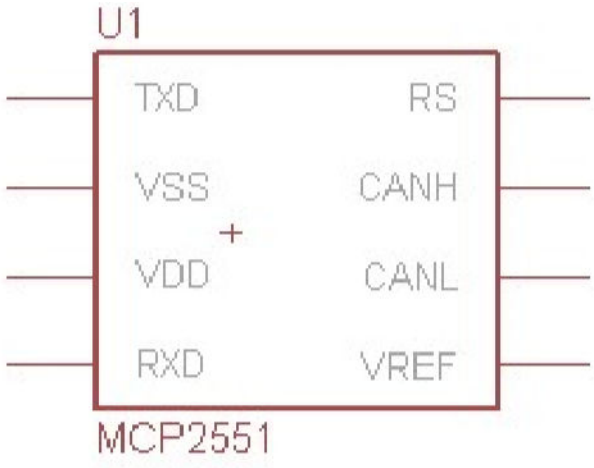


Рисунок 4.3 – Розпіновка «MCP2551»

Таблиця 4.3 – Розпіновка «MCP2551»

№	Ім'я	«I/O/P»	Опис
1	«TXD»	«I»	Вхід з контролера для передавального сигналу на шину.
2	«V_{SS}»	«P»	Земля.
3	«V_{DD}»	«P»	Живлення («+5В»).
4	«RXD»	«I»	Вхід з контролера для приймаючого сигналу з шини.
5	«V_{REF}»	«P»	Живлення вихід («V_{DD}/2»).
6	«CANL»	«I/O»	Лінія низької напруги шини «CAN».
7	«CANH»	«I/O»	Лінія високої напруги шини «CAN».
8	«R_S»	«I»	Вхід для апаратного вибору режиму.

Для живлення плати «UNO» використовується «USB»-порт. При цьому може спостерігатися не повні «+5 В» на виході з плати для живлення «CAN»-контроллера і трансивера. Тоді необхідно завести окреме джерело живлення «+12В» на вхід плати «VIN».

4.2 Висновок

В даному розділі дипломної роботи освітнього рівня «магістр» виконано проектування елементів фізичного пристрою для тестового підключення до шини «CAN».

5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою дипломної роботи освітнього рівня «Магістр» є дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст». Головною метою розділу є встановлення економічної доцільності проведення даної розробки.

Щоб виконати оцінку економічної ефективності необхідно розрахувати трудомісткість дослідження, витрати на оплату праці найманим працівникам, витрати апаратного і програмного забезпечення, амортизаційні відрахування, витрати енергоресурсів та інші витрати які є основними пунктами виконання обчислень, а також показники економічної ефективності дослідження.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» складається з низки послідовних та взаємопов’язаних етапів.

Кожен із етапів дослідження характеризується метою та змістом, оцінкою часу виконання, кількістю та спеціалізацією виконавців, а також приблизною оцінкою вартості.

Дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» складається із підготовчого етапу, етапу технічної пропозиції, створення технічного завдання, проектування системи, практичної реалізації, тестування, верифікації та заключного етапу.

Норми часу на виконання науково-дослідницької роботи розраховуватимуться на основі середнього часу виконання стадії в годинах, що наведені в таблиці 5.1 разом із інформацією про виконавців і сумарною кількості затраченого часу.

Таблиця 5.1 – Операції науково-дослідного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Підготовча стадія	Проектний менеджер	4
		Інженер-програміст	
2.	Технічна пропозиція	Проектний менеджер	72
		Інженер-програміст	
3.	Створення технічного завдання	Проектний менеджер	78
		Інженер-програміст	
4.	Проектування системи	Проектний менеджер	73
5.	Практична реалізація	Інженер-програміст	48
6.	Тестування системи	Тестувальник	43
7.	Верифікація системи	Проектний менеджер	27
		Інженер-програміст	
		Тестувальник	
8.	Створення документації	Інженер-програміст	25
9.	Заключна стадія	Проектний менеджер	18
Разом			388

В підсумку на дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» необхідно 388 людино-годин, залучення трьох спеціалістів та виконання дев’яти різноманітних стадій реалізації проекту.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Визначення витрат на оплату праці та відрахувань на соціальні заходи прямо залежить від кількості витраченого працівниками часу на роботу,

ставки в годину чи місяць, кількість відрахувань на соціальні заходи встановлених в законному порядку на час розрахунку.

В результаті розрахунку потрібно визначити основну та додаткову заробітну плату, витрати на соціальні заходи та на основі цих даних визначити сумарні витрати на оплату праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Наймані працівники для розробки інформаційної системи управління доступом з використанням інформаційних технологій розпізнавання образів працюють згідно контракту, який в якому вказано їхню погодинну ставку. Тобто розрахунок заробітної плати працівників відбуватиметься на базі тарифної ставки та кількості відпрацьованих годин.

У штаті найманих працівників для розробки інформаційної системи залучено проектного менеджера, інженера-програміста і тестувальника.

Тарифні ставки учасників процесу розробки інформаційної системи управління доступом з використанням інформаційних технологій розпізнавання образів:

– Проектний менеджер – 150 грн./год.

– Інженер-програміст – 130 грн./год.

– Тестувальник – 100 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г, \qquad (5.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує три спеціалісти, то основна заробітна плата буде розраховуватись за даною формулою 5.1.

$$З_{осн.} = 150 \cdot 177 + 130 \cdot 159 + 100 \cdot 52 = 52420{,}00 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати й визначається за формулою 5.2. Коефіцієнт додаткових виплат працівникам становить 0,1 .

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам.

$$З_{дод.} = 52420{,}00 \cdot 0{,}1 = 5242{,}00 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$ – фонд заробітної плати) визначаються за формулою 5.3:

$$В_{о.п.} = З_{осн.} + З_{дод.}. \quad (5.3)$$

$$В_{о.п.} = 52420{,}00 + 5242{,}00 = 57662{,}00 \text{ грн.}$$

З цієї суми утримуються обов’язкові відрахування на заробітну плату:

– Єдиний соціальний внесок (ЄСВ), що становить – 22%.

– Військовий збір (ВЗ), що становить – 1,5%.

Сума відрахувань становить 23,5 % від фонду оплати праці та визначається за формулою 5.4:

$$B_{с.з.}=Ф_{ОП}\ 0{,}235, \qquad (5.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$B_{с.з.} = 57662{,}00 \cdot 0{,}235 = 13550{,}57 \text{ грн.}$$

Усі витрати обчислюються детально наведені в таблиці 5.2 та обчислюються за формулою 5.5.

$$B_{З.П.}= Ф_{ЗП}+Ф_{ОП}, \qquad (5.5)$$

$$B_{З.П.} = 52420{,}00 + 5242{,}00 + 13550{,}57 = 71212{,}57 \text{ грн.}$$

Таблиця 5.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн. *6=3+4+5*
		Тарифна ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	Проектний менеджер	150	177	26550,00	2655,00		
2	Інженер-програміст	130	159	20670,00	2067,00		
3	Тестувальник	100	52	5200,00	520,00		
Разом		380	388	52420,00	5242,00	13550,57	71212,57

Опираючись на розрахунки витрат на оплату та зведену таблицю результатів 5.2 видно, що всього витрати на плату праці становлять 71212,57 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати є невід'ємною частиною дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» та визначаються як добуток кількості витрачених матеріалів та їх ціни за формулою 5.6:

$$M_{Bi} = q_i \cdot p_i, \tag{5.6}$$

де: q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 5.7:

$$З_{мв.} = \sum M_{Bi}. \tag{5.7}$$

Результати проведених розрахунків наведено у таблиці 5.3.

Таблиця 5.3 – Результати розрахунків матеріальних витрат

1	Найменування матеріальних ресурсів	Одиниця виміру	Фактично витрачено матеріалів	Ціна за одиницю, грн	Загальна сума витрат, грн
1	2	3	4	5	6
1. Основні матеріали					
1.1	Використання мережі Інтернет, місячна абонплата	міс		150	300,00
2. Допоміжні витрати					
2.1	Папір	уп.	0,2	85,00	17,00
2.2	Тонер	уп.	1	50,00	50,00
2.3	CD диск	шт.	2	10	20,00
Разом:					387,00

Загальні матеріальні витрати на Інтернет, папір формату А4, тонер та CD-диски становлять 387,00 грн.

5.4 Розрахунок витрат на електроенергію

Однією із статей витрат є витрати на електроенергію під час проходження усіх етапів реалізації кінцевого продукту. Затрати на електроенергію одиниці обладнання визначаються за формулою 5.8:

$$З_е = W \cdot T \cdot S \ , \qquad (5.8)$$

де W – необхідна потужність, кВт; T – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютерів для реалізації кінцевого продукту – 400 Вт, кількість годин роботи обладнання згідно таблиці 5.1 – 388 годин.

Визначимо витрати на електроенергію згідно формули 5.8

$$З_е = 0{,}4 \cdot 388 \cdot 2{,}42 = 375{,}58 \text{ грн.}$$

Отже, затратами на електроенергію для дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» буде 375,58 грн.

5.5 Розрахунок суми амортизаційних відрахувань

Для будь якої діяльності характерною є властивість зношування на зниження якості властивостей інструментарію та фондів за допомогою яких ведеться діяльність. Для вирішення проблеми із відновленням даних фондів

використовується амортизація, що являє собою процес трансформації вартості основних фондів на вартість продукції, яка щойно була створена, задля повного відновлення основних фондів. Для визначення амортизаційних відрахувань використовується формула 5.9:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \quad (5.9)$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %). Річний робочий фонд становитиме 2352 годин, так як робочий день становить 8 годин, а кількість робочих днів в місяці становить 24,5 годин.

Для даної розробки засобом розробки є комп'ютер. Його сума становить 18580 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 18580 \cdot 5 \% / 100 \% = 929{,}00 \text{ грн.}$$

Згідно проведених обчислень амортизаційні відрахування становлять 929,00 грн.

5.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці. В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20-60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6, \quad (5.10)$$

де $H_В$ – накладні витрати.

Отже, накладні витрати становлять згідно формули 5.10:

$$H_в = \ 57662{,}00 \ \cdot \ 0{,}2 \ = \ 11532{,}40 \text{ грн.}$$

Отже, накладні витрати для науково-дослідних робіт промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» будуть становити 11532,40 грн.

5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	57662,00	68,3
Відрахування на соціальні заходи	13550,57	16
Матеріальні витрати	387	0,46
Витрати на електроенергію	375,584	0,44
Амортизаційні відрахування	929,00	1,1
Накладні витрати	11532,40	13,7
Собівартість	84436,55	100

Собівартість ($C_в$) дослідження розрахуємо за формулою:

$$C_В = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_е + A + H_в. \quad (5.11)$$

Отже, собівартість дослідження дорівнює:

$$C_В = 57662{,}00 + 13550{,}57 + 387 + 375{,}584 + 929{,}00 + 11532{,}40 =$$

$$= 84436{,}55 \text{ грн.}$$

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 84436,55 грн.

5.8 Розрахунок ціни проведених науково-дослідних робіт

Ціну науково-дослідної роботи можна визначити можна визначити за формулою:

$$Ц = \frac{C_В \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ), \quad (5.12)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

K – кількість замовлень, од.;

$B_{н.і.}$ – вартість носія інформації, грн.;

$ПДВ$ – ставка податку на додану вартість, (20 %).

Оскільки розробка є науково-дослідною, і використовуватиметься тільки один раз, то для розрахунку ціни не потрібно вказувати коефіцієнти К та $B_{н.і}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.13)$$

Звідси ціна проведення науково-дослідних робіт складе:

$$Ц = 84436{,}55\ (1 + 0{,}3\ ) \cdot (1 + 0{,}2\ ) = 131721{,}02 \text{ грн.}$$

Отже, для дослідження промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» необхідно 131721,02 грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = \frac{П}{C_B}, \quad (5.14)$$

де $П$ – прибуток;

C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_B. \quad (5.15)$$

Розраховуємо плановий прибуток:

$$П_{пл} = 131721{,}02 - 84436{,}55 = 47284{,}47 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_p = \frac{П_{пл}}{Св}. \quad (5.16)$$

Тоді,

$$E_p = 47284,47 \ / \ 84436,55 = 0,56 \ .$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = \frac{1}{E_p}, \quad (5.17)$$

Термін окупності дорівнює:

$$T_p = 1 / \ 0,56 = 1,8 \ \text{р.}$$

Згідно формул плановий прибуток від проведених науково-дослідних робіт становить 47284,47 грн., економічна ефективність дорівнює 0,56 , а термін окупності становить 1,8 роки що вважається доцільним та економічно вигідним.

5.10 Висновок

В розділі «Обґрунтування економічної ефективності» дипломної роботи освітнього рівня «магістр» розраховано основні техніко-економічні показники проведених досліджень промислових інтерфейсів CANopen для інтернету-речей в проектах «розумних міст» (див. таблицю 5.5).

Розраховане значення економічної ефективності становить 0,56 , що є високим значенням.

Так само нормальним є термін окупності, який повинен коливатися від 1 до 3 років. Для проведених в дипломній роботі досліджень він становить 1,8 років.

Таблиця 5.5 – Техніко-економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	84436,55
2.	Плановий прибуток, грн.	47284,47
3.	Ціна, грн.	131721,02
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Отже, отримані в рамках дипломного проектування результати науково-дослідних робіт можуть бути впроваджені та мати подальший розвиток, оскільки вони є економічно вигідним за всіма основними техніко-економічними показниками.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Організаційно-технічні засоби та санітарно-гігієнічні заходи щодо збереження працездатності працівників, які працюють в галузі ІТ

Для збереження працездатності працівників в галузі ІТ передбачаються організаційні та технічні заходи захисту.

Технічні заходи – технічні засоби, що забезпечують безпечні і нешкідливі умови праці, та пов'язані з впровадженням нового обладнання, пристроїв і приладів безпеки і безпечною експлуатацією засобів виробництва. [56]

Нормативно-методичні заходи:

– розробка посібників і рекомендацій;

– розробка нормативно-правової бази з охорони праці на підприємстві;

– забезпечення необхідною нормативно-правовою документацією функціональних служб, окремих структурних підрозділів та робочих місць;

– забезпечення програм і розробка методик навчання з питань охорони праці;

– розробка розділів охорони праці в посадових інструкціях, інструкціях за професіями;

– перегляд НПАОП підприємства.

Організаційні заходи [57]:

– контроль за технічним станом обладнання, інструментів, будівель і споруд;

– контроль за дотриманням вимог нормативних документів з охорони праці;

– нагляд за обладнанням підвищеної небезпеки;

– організація навчання, перевірка знань з питань охорони праці і інструктажів робітників підприємства;

– контроль за виконанням технологічного процесу відповідно до вимог охорони праці;

– організація належних умов до проїздів і проходів відповідно до вимог охорони праці;

– забезпечення працівників засобами індивідуального та колективного захисту;

– забезпечення відповідними знаками безпеки, плакатами.

Санітарно-гігієнічні заходи [58]:

– контроль за впливом виробничих факторів на здоров'я працівників;

– забезпечення санітарно-побутових умов згідно з діючими нормами;

– атестація робочих місць відповідно до їх нормативним актам з охорони праці;

– планування заходів щодо поліпшення санітарно-гігієнічних умов праці;

– паспортизація санітарно-технічного стану умов праці.

6.2 Основні завдання та функції системи управління охороною праці на підприємстві (СУОП)

Основні завдання управління охороною праці – це [59]:

– відпрацювання заходів, що стосуються державної політики з охорони праці на регіональному і галузевому рівнях;

– підготовка, прийняття і реалізація заходів із забезпечення безпечних умов праці, утримання у належному стані обладнання, споруд, інженерних мереж;

– організація і проведення навчання працівників охороні праці та проведення професійного відбору; облік, аналіз і оцінка стану умов безпеки праці;

– забезпечення страхування працівників від нещасних випадків на виробництві та від профзахворювань (див. таблицю 6.1);

Таблиця 6.1 – Розподіл функцій з реалізації завдань СУОПП між структурними підрозділами і службами підприємств

Завдання СУОПП	Структурні підрозділи	
	Керівні	Виконавчі
Забезпечення безпеки: виробничих процесів	ВГТ	КП, ПК, СПЛ, ВГМетр, ВОП, ВГМ, ВГЕ
устаткування	ВГМ	ВОП, ВТК, ПК, КП, ВГК, СПЛ
будинків, споруд	ВКБ	КП, ВОП, ВМТП, ПК
Нормалізація гігієнічних умов	КП	ВОП, ПК, СПЛ, КП, ВОП, ПК
Забезпечення ЗІЗ і т.п.	ВМТЗ	

Примітка: ВГТ – відділ головного технолога; ВГМ – відділ головного механіка; ВКБ – відділ капітального будівництва; КП – керівник підрозділу; ВМТЗ – відділ матеріально-технічного забезпечення; ВМТП – відділ матеріально-технічного постачання; ПК – профспілковий комітет; СПЛ – санітарно-промислова лабораторія; ВГМетр – відділ головного метролога; ВОП – відділ охорони праці; ВГЕ – відділ головного енергетика; ВТК – відділ технічного контролю; ВГК – відділ головного конструктора.

– організаційно-методичне керівництво на регіональному і галузевому рівнях;

– стимулювання інтеграції управління охороною праці в єдину систему загального управління організацією виробництва;

– широке впровадження позитивного досвіду у галузь охорони праці.

Основні функції СУОП, пов'язані з її функціонуванням, передбачають:

– планування робіт; розробку, прийняття і скасування нормативних актів; професійний відбір;

– навчання з питань охорони праці; регламентацію процесу праці; атестацію робочих місць щодо умов праці;

– паспортизацію об'єктів; реєстрацію та облік; експертизу;

– ліцензування і сертифікацію; забезпечення безпеки устаткування, процесів, будинків, споруд і територій; забезпечення санітарно-гігієнічних умов праці, санітарно-побутового, лікувально-профілактичного і медичного обслуговування;

– узгодження і видача дозволів; попередження про виникнення небезпечних ситуацій;

– розслідування та облік нещасних випадків; розслідування та облік хронічних професійних захворювань; розслідування та облік аварій;

– фінансування робіт з охорони праці; стимулювання охорони праці;

– пропаганда і виховання безпечної поведінки;

– контроль та інспектування; наукове забезпечення; міжнародне співробітництво.

6.3 Забезпечення безпеки життєдіяльності при роботі з ПК

При виконанні робіт на комп’ютерах необхідно дотримуватись вимог загальної та даної інструкції з охорони праці.

До самостійної роботи на комп’ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочому місці один раз на півріччя, періодичні медичні огляди один раз на два роки.

Під час роботи на комп'ютерах можуть діяти такі небезпечні та шкідливі фактори, як:

– фізичні;

– психофізіологічні.

Основним обладнанням робочого місця користувача комп'ютера є монітор, системний блок та клавіатура.

Робочі місця мають бути розташовані на відстані не менше 1,5 м від стіни з вікнами, від інших стін на відстані 1м, між собою на відстані не менше 1,5 м. Відносно вікон робоче місце доцільно розташовувати таким чином, щоб природне світло падало на нього збоку, переважно зліва.

Робочі місця слід рошташовувати так, щоб уникнути попадання в очі прямого світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Для уникнення світлових відблисків екрану, клавіатури в напрямку очей користувача, від світильників загального освітлення або сонячних променів, необхідно використовувати антиполискові сітки, спеціальні фільтри для екранів, захисні козирки, на вікнах – жалюзі. [60]

Фільтри з металевої або нейлонової сітки використовувати не рекомендується, тому що сітка спотворює зображення через інтерференцію світла

Найкращу якість зображення забезпечують скляні поляризаційні фільтри. Вони усувають практично всі відблиски, роблять зображення чітким і контрастним.

При роботі з текстовою інформацією (в режимі введення даних та редагування тексту, читання з екрану) найбільш фізіологічним правильним є зображення чорних знаків на світлому (чорному) фоні.

Монітор повинен бути розташований на робочому місці так, щоб поверхня екрана знаходилася в центрі поля зору на відстані 400-700 мм від

очей користувача. Рекомендується розміщувати елементи робочого місця так, щоб витримувалася однакова відстань очей від екрана, клавіатури, тексту.

Зручна робоча поза при роботі з комп'ютером забезпечується регулюванням висоти робочого столу, крісла та підставки для ніг. Раціональною робочою позою може вважатися таке положення, при якому ступні працівника розташовані горизонтально на підлозі або підставці для ніг, стегна зорієнтовані у горизонтальній площині, верхні частини рук – вертикальні. Кут ліктєвого суглоба коливається в межах 70-90°, зап'ястя зігнуті під кутом не більше ніж 20°, нахил голови 15-20°.

Для нейтралізації зарядів статичної електрики в приміщенні, де виконується робота на комп'ютерах, в тому числі на лазерних та світлодіодних принтерах, рекомендується збільшувати вологість повітря за допомогою кімнатних зволожувачів. Не рекомендується носити одяг з синтетичних матеріалів.

Згідно статті 18 Закону України "Про охорону праці" працівник зобов'язаний:

а) знати і виконувати вимоги нормативних актів про охорону праці, правила поводження з устаткуванням та іншими засобами виробництва, користуватися засобами колективного та індивідуального захисту;

б) дотримуватись зобов'язань щодо охорони праці, передбачених колективним договором та правилами внутрішнього трудового розпорядку підприємства;

в) співробітничати з власником у справі організації безпечних і нешкідливих умов праці, особисто вживати посильних заходів щодо усунення будь-якої виробничої ситуації, яка створює загрозу його життю чи здоров'ю, або людей, які його оточують, повідомляти про небезпеку свого безпосереднього керівника або іншу посадову особу.

Вимоги безпеки перед початком роботи:

– увімкнути систему кондиціювання в приміщенні;

– перевірити надійність встановлення апаратури на робочому столі. Повернути монітор так, щоб було зручно дивитися на екран – під прямим кутом (а не збоку) і трохи зверху вниз, при цьому екран має бути трохи нахиленим, нижній його край ближче до оператора;

– перевірити загальний стан апаратури, перевірити справність електропроводки, з'єднувальних шнурів, штепсельних вилок, розеток, заземлення захисного екрана;

– відрегулювати освітленість робочого місця;

– відрегулювати та зафіксувати висоту крісла, зручний для користувача нахил його спинки;

– приєднати до системного блоку необхідну апаратуру. Усі кабелі, що з'єднують системний блок з іншими пристроями, слід вставляти та виймати при вимкненому комп'ютері;

– ввімкнути апаратуру комп'ютера вимикачами на корпусах в послідовності: монітор, системний блок, принтер (якщо передбачається друкування);

– відрегулювати яскравість свічення монітора, мінімальний розмір світної точки, фокусування, контрастність. Не слід робити зображення надто яскравим, щоб не втомлювати очей.

Рекомендується:

– яскравість свічення екрана – не менше 100Kg/M2;

– відношення яскравості монітора до яскравості оточуючих його поверхонь в робочій зоні – не більше 3:1;

– мінімальний розмір точки свічення не більше 0,4 мм для монохромного монітора і не менше 0,6 мм для кольорового, контрастність зображення знаку – не менше 0,8.

При вивленні будь-яких несправностей роботу не розпочинати, повідомити про це керівника.

Вимоги безпеки під час виконання роботи:

– необхідно стійко розташовувати клавіатуру на робочому столі, не опускати її хитання. Під час роботи на клавіатурі сидіти прямо, не напружуватися;

– для забезпечення несприятливого впливу на користувача пристроїв типу ”миша” належить забезпечувати вільну велику поверхню столу для переміщення ”миші” і зручного упору ліктьового суглоба;

– не дозволяються сторонні розмови, подразнюючі шуми;

– періодично при вимкненому комп’ютері прибирати ледь змоченою мильним розчином бавовняною ганчіркою порох з поверхонь апаратури

Екран ВДТ та захисний екран протирають ганчіркою, змоченою у спирті. Не дозволяється використовувати рідинні або аерозольні засоби чищення поверхонь комп’ютера.

Забороняється:

– самостійно ремонтувати апаратуру. Ремонт апаратури здійснюється спеціалістами з технічного обслуговування комп’ютера, 1 раз на півроку повинні відкривати процесор і вилучати пилососом пил і бруд, що накопичилися;

– класти будь-яку предмети на апаратуру комп'ютера;

– закривати будь-чим вентиляційні отвори апаратури, що може призвести до її перегрівання і виходу з ладу.

Для зняття статичної електики рекомендується час від часу доторкатися до металевих поверхонь.

Розташувати принтер необхідно поруч з системним блоком таким чином, щоб з'єднювальний шнур не був натягнутий. Забороняється ставити принтери на системний блок.

Для досягнення найбільш чистих, з високою розподільністю зображень і щоб не зіпсувати апарат, має використовуватися папір, вказаний в інструкції до принтера. При заминанні паперу потрібно відкрити кришку і обережно витягнути лоток з папером.

Згідно з інструкцією фірми-виробника потрібно дотримуватися правил зберігання картриджа.

Забороняється:

– зберігати картриджі без упаковки;

– ставити картриджі вертикально;

– перевертати картридж етикеткою донизу;

– відкривати кришку валика і доторкатися до нього;

– самому заповнювати використаний картридж.

Вимоги безпеки після закінчення роботи:

– закінчити та записати у пам'ять комп'ютера файл, що знаходиться в роботі;

– вимкнути принтер та інші периферійні пристрої. Штепсельні вилки витягнути з розеток. Накрити клавіатуру кришкою запобігання попаданню в неї пилу;

– прибрати робоче місце;

– ретельно вимити руки теплою водою з милом;

– вимкнути кондиціонер, освітлення і загальне електроживлення;

– пройти в спеціально обладнаному приміщенні сеанс психофізіологічного розвантаження і зняття втоми з виконанням спеціальних вправ аутогенного тренування.

6.4 Джерела, зони дії та рівні забруднення навколишнього середовища у разі аварій на хімічно і радіаційно небезпечних об’єктах

На підприємствах хімічної, нафтопереробної, харчової промисловості можливе виникнення аварійних ситуацій з викидом СДОР, Причинами таких ситуацій може бути порушення правил експлуатації, вимог правил безпеки. В Україні є 877 хімічно небезпечних об'єктів, них 39 розташовані на території Львівської області. Нарощення хімічного виробництва призвело до зростання

кількості промислових відходів, які становлять небезпеку для оточуючого середовища і людей. Тільки токсичних відходів в Україні накопичено більше 4 млрд. т, при середньорічному утворенні 103 млн. т. Проблема безпеки населення в зонах можливого хімічного зараження займає важливе місце в переліку завдань щодо захисту людей у надзвичайних ситуаціях"?

Аварії на хімічно небезпечних об'єктах мають свої особливості до яких, зокрема, відносяться:

1. Неможливість прогнозування аварії у часі.

2. Велика ймовірність важких наслідків для життя і здоров'я людини.

3. Складнощі завчасного вжиття ефективних захисних заходів. Непередбачуваність економічних і екологічних наслідків тощо. У надзвичайних ситуаціях з потенційно небезпечними хімічними речовинами важливе значення має розуміння властивостей СДОР. Найрозповсюдженішими і небезпечними речовинами, що використовуються у промисловості і побуті, є аміак і хлор.

Аміак – за звичайних умов – це газ, легший за повітря, який легко зріджується під тиском, а при випаровуванні поглинає тепло – сильно охолоджується. Ця властивість використовується у промислових та побутових холодильниках на м'ясокомбінатах, молокозаводах, овочевих базах, тобто там, де є необхідність в охолодженій продукції. Крім того, він є сировиною багатьох хімічних виробництв. Аміак зберігається і транспортується у зрідженому стані. Як рідина, він легший за воду, має меншу густину і при виході на повітря утворює слабкий дим. Вогненебезпечний, створює вибухові суміші з повітрям, отруйний. Особливо небезпечний для очей. При малих концентраціях діє збуджуючи, при великих – людина непритомніє. Крім того, він викликає задуху, сильний кашель. Найкращі методи захисту – ізолюючий протигаз, респіратор РПГ-67КД, захисний костюм типуЛ-1, гумові чоботи, рукавички. Оскільки аміак легший

за повітря, то він буде здійматися вгору, тому безпечніше від аміачної хмари ховатися у низинах, підвалах, тунелях.

Хлор – отруйний, негорючий жовто-зелений газ, зі специфічним запахом хлорки, отруйніший за аміак у 20 разів. Хлор – газоподібний, він трохи важчий за повітря, легко зріджується під тиском. Тому зберігають його і транспортують у сталевих балонах або цистернах. У рідкому стані він важчий за воду. При випаровуванні утворює білий туман. Розчинний у воді, але гірше за аміак.

Хлор широкорозповсюджений промисловий продукт, використовується для знезараження питної води, відбілювання тканин, як сировина ця багатьох хімічних підприємствах. У зв'язку з таким способом його використання трапляється чимало випадків отруєння. Так, наприклад, у Брукліні (район Нью-Йорка), коли хлор з віддаленого магнієвого заводу накопичувався у станцію підземки, від нього постраждало понад тисячі чоловік. Це приклад того, що хлор може пересуватися низинами на значні відстані. При концентрації хлору у повітрі понад 0,2 мг/л може статися миттєва смерть. При потраплянні його на шкіру виникають опіки. Як запобігти ураженню хлором? Найкраще використовувати ізолюючий протигаз, кисневий ізолюючий прилад, спеціальний захисний костюм, умові чоботи, рукавиці. За відсутності індивідуальних засобів у нагоді може стати одяг з цупкої тканини, протигаз з активованим вугіллям. А якщо і цього немає, то слід вдихати повітря через хустинку, змочену розчином соди чи антихлору (розчин фітофіксину з содою). Можна також вмочити тканину сечею, яка частково знешкоджує хлор, або простою ізодою. Слід пам'ятати, що хлор накопичується у низинах, тому треба підніматися догори. На жаль, як показала практика, солдати під час хлорної газової атаки у першу світову війну ховалися, навпаки, у підвалах, землянках та окопах, що значно збільшило кількість жертв та ефективність хімічної зброї.

При отруєнні хлором рекомендується вдихати пари спирту та ефіру, але перед цим постраждалим необхідно забезпечити свіже повітря. При відсутності дихання слід зробити штучне дихання.

Ступінь хімічної небезпеки населення при аваріях з виходом (СДОР) залежить від масштабу аварії, властивостей СДОР, стану атмосфери, рельєфу місцевості тощо. У системі цивільної оборони розроблена «Методика прогнозування масштабів зараження СДОР при аваріях». Вона дозволяє розраховувати можливі площі хімічного зараження та визначати втрати людей. Унаслідок аварій на об'єктах, які виробляють СДОР, обслуговуючий персонал і населення, яке мешкає поблизу об'єкта, можуть отримати тяжкі ураження. [61]

Велике значення має своєчасне та якісне проведення розвідки осередка ураження. Цю роботу ведуть підрозділи хімічної розвідки Збройних сил, ЦО та інші. Вони визначають місце аварії та вид СДОР, ступінь зараження місцевості, шляхи безпечного виходу з неї, беруть проби ґрунту, води тощо і відправляють їх у лабораторію. На початку виникнення і проникнення СДОР в атмосферу або на місцевості негайно оповіщають робітників і службовців об'єктів і населення, яке мешкає поблизу зони, про небезпеку. Люди, які є в будинках, зачиняють вікна, проводять повну герметизацію житла, вимикають нагрівальні прилади, газ. Евакуація населення з районів можливого зараження СДОР проводиться до підходу зараженої хмари. На об'єкті, де була аварія, в першу чергу здійснюється робота з припинення викиду СДОР. Ураженим надається медична допомога. Краплини СДОР на одязі знешкоджують за допомогою індивідуального протихімічного пакета ІПП-8. При роботах в осередках ураження СДОР треба дотримуватись правил безпеки. Всі люди повинні мати протигази, індивідуальні засоби захисту шкіри, вміти користуватись індивідуальними протихімічними пакетами ІПП-8, а також індивідуальними аптечками АІ-2, вміти надавати першу медичну допомогу.

Особливе місце у забрудненні оточуючого середовища займає радіоактивне забруднення. Чорнобильська катастрофа стала наслідком радіоактивного забруднення території України, Білорусі та Росії. Загальна площа радіоактивного забруднення становить понад 30 тис. кв. км. Випадання радіоактивних речовин простежувалося і у державах Західної Європи, підвищився радіоактивний фон у Скандинавії, Японії та США. Через 15 місяців після катастрофи в Чорнобилі у Великій Британії, яка, здавалось би, далеко розташована від України, було виявлене надзвичайно велике забруднення рослинності радіоактивними опадами, а також великий вміст цезію у м'ясі овець.

Аварії на АЕС мають значні відмінності від ядерних вибухів. Вони відрізняються від ядерних вибухів більшою тривалістю викидів, що змінює напрямок потоків повітряних мас. Тому практично не має можливості прогнозувати розміри зон ураженості.

Радіоактивне забруднення оточуючого середовища діє на людину шляхом зовнішнього та внутрішнього опромінення.

Зовнішнє опромінення – це опромінення за рахунок радіоактивного забруднення місцевості. Воно підлягає контролю і залежить від рівня радіації на місцевості. Внаслідок чорнобильської катастрофи на території України радіацією забруднені місцевості 12 областей, 86 адміністративних районів, 2311 населених пунктів, де загалом мешкає близько 2 млн. 600 тис. жителів, у тому числі – 600 тис. дітей. Забруднено радіонуклідами понад 7 млн. гектарів землі, серед яких 3 млн. га сільськогосподарських угідь та 2 млн. лісових масивів. Викид радіонуклідів унаслідок вибуху реактора негативно вплинув на здоров'я населення України. В результаті потрапляння радіоактивних речовин в організм у багатьох людей булауражена щитовидна залоза, виникла променева хвороба. Нині спостерігається тенденція до збільшення онкологічних захворювань, захворювань ендокринної системи, систем кровообігу, травлення, а також захворювань, пов'язаних з імунною

системою. В зв'язку з тим, що в продуктах викиду перевагу мають довгоживучі радіонукліди – цезій-137 (30 років), стронцій-90 (28 років), плутоній-239 (20000 років), зараження буде тривалим. Верховна Рада України ухвалила Закон, який визначає чотири зони радіоактивного забруднення.

1. Зона періодичного радіоактивного контролю (низьке забруднення, 0,5-1 Кі/км^2). Дозволено збирання грибів, ягід, лікарських рослин, а також заготівлю деревини без обмежень. Полювання, рибальство у природних водоймах і річках дозволяється відповідно до правил, що діють на території України, з обов'язковою перевіркою м'яса і риби на вміст у них радіоактивних речовин. У підсобних господарствах ніяких обмежень щодо годівлі та утримання сільськогосподарських тварин і птиці не запроваджується.

2. Зона посиленого радіоактивного контролю (середнє забруднення, 1-5 Кі/км^2). Дозволено збирання, заготівлю грибів, ягід, лікарських рослин і сіна з обов'язковим попереднім дозиметричним контролем. Заготівля деревини і використання продуктів її переробки проводиться без обмежень. У підсобних господарствах рекомендується періодичний вибірковий контроль м'ясних і молочних продуктів, кормів.

3. Зона гарантованого добровільного відселення (високе забруднення, 5–15 Кі/км^2). У цій зоні заготівлю грибів, ягід, хвойної лапини і виробництво хвойно-вітамінного борошна заборонено. Необхідний особливий режим сільського господарства: обмежене землекористування (скорочення рільництва, зменшення обробітку земель), переспеціалізація товарного сільського господарства та насінництва, вирощування технічних культур (льон і інше), розвиток тваринництва, інтенсивне конярство тощо. Випас худоби на лісових пасовищах цієї зони здійснюється при досягненні вмсоти травостою не менше 10 см. При щільності забруднення понад 15 Кі/км^2 заготівля деревини допускається тільки у зимовий час і при наявності

снігового покриву. Використання деревини як палива, заготівля пнєвого смолу і дьогтю заборонені. Заборонено випасати молочну, м'ясну худобу, а заготовляти сіно дозволяється тільки як корм Для робочих коней. Використання гною як добрива заборонено.

4. Зона відчуження (надзвичайно високе забруднення). Це дослідницький полігон для боротьби із наслідками ядерних катастроф.

Серед виловленої в річках «зони жорсткого контролю» і у верхів'ях Київського водосховища риби – до 15–20 відсотків не відповідає вимогам. Уся риба, виловлена у цих водоймах, підлягає обов'язковому Радіометричному контролю. Промисловий відлов риби у верхів'ях Київського водосховища заборонений. Тимчасово допустимий рівень вмісту радіоактивних речовин у рибі становить 5 Х 103 Кі/кг.

Нині радіоактивний стан об'єкта ЧАЕС потужністю дози опромінення 15-300 мР/год., а на окремих ділянках 1–5 Р/год. Проектний термін служби саркофага, який захищає четвертий реактор, – 30 років. Зараз завершується будівництво «Саркофага-2», який вміщає «Саркофаг-1» і зробить його безпечним.

На сьогодні практично ніхто не застрахований від впливу наслідків аварії чи будь-якої іншої аварії на об'єктах атомної промисловості. Навіть сотні і тисячі кілометрів від АЕС не можуть бути гарантією безпеки. Аварія на ЧАЕС стала прикладом того, що будь-які аварії на атомних станціях не можуть бути локальними. Наслідки аварії на ЧАЕС вийшли за межі однієї держави і наочно продемонстрували необхідність міжнародного співробітництва в ядерній енергетиці.

Основні джерела радіоактивного випромінювання:

– заводи з переробки та збагачення уранових руд;
– заводи з виробництва ядерного палива;
– АЕС, судові та ракетні ядерні установки;
– науково-дослідницькі заклади відповідного профілю.

За оцінками вчених, радіоактивне забруднення через кілька десятиріч збільшиться у сотні разів. Внутрішнє опромінення проходить в основному при вживанні продуктів харчування та води, які забруднені радіонуклідами. З рибою та іншими морськими продуктами в організм потрапляють радіонукліди: свинець-210 та полонІй-210. Полоній-210 потрапляє також з м'ясом, чаєм, рослинною їжею. Найбільшу радіоактивність серед рослинних продуктів мають горох, жито, пшениця, картопля, огірки. Яловичина майже в 3 рази радіоактивніша, ніж свинина. У зв 'язку з відсутністю належного контролю за якістю продуктів харчування та води це опромінення практично не підлягає контролю. Сьогодні в Україні є райони, де вміст цезію-137 у продуктах виробництва в 10–100 разів перевищує середній рівень його у межах більшої частини держави. Систематичне споживання продуктів харчування та води, що забруднені радіоактивними речовинами, призводить до накопичення радіонуклідів в організмі людини (йоду – в щитовидній залозі, стронцію – в кістках, цезію – в м'яких тканинах).

При опроміненні внаслідок потрапляння речовин на відкриті ділянки шкіри можуть утворюватись променеві дерматити та опіки. Ураження мають кілька стадій: рання реакція, інкубаційний період, період гострого запалення і період одужання. Рання реакція настає за кілька годин після дії радіоактивних речовин, виникає почервоніння шкіри, яке згодом зникає, настає інкубаційний період, ніяких зовнішніх ознак не виникає.

Період гострого запалення теж починається з почервоніння шкіри. Потім виникають пухирі, наповнені прозорою рідиною, які самі тріскають. При дуже великих дозах опромінення на їх місці виникають виразки, які погано заживають. Медичну допомогу при променевих ураженнях необхідно надавати в якомога стислі терміни.

Для цього дуже важливо своєчасно виявити уражених, яке проводиться дозиметричними приладами або розрахунками за відомими рівнями радіації і часу перебування на зараженій місевості. Потерпілих необхідно

винести (вивезти) з осередку ураження на місцевість, де нема радіаційного випромінювання. Людей, які отримали високі дози радіації, негайно доставити в лікувальні заклади транспортом. Лікування променевої хвороби – найскладніше питання сучасної медицини. До невідкладних лікувальних заходів відносяться:

– механічне усунення радіоактивних речовин з організму людини. Це проводиться шляхом промивання шлунка теплою водою, вживання проносних і сечогінних засобів, промивання рота й очей (якщо є можливість, промивання очей проводити розчином натрію гідрокарбонату);

– застосування відхаркувальних препаратів (іпекакуан, термопсис, сенега) при попаданні радіоактивних речовин у шляхи дихання. Через кілька днів, коли радіоактивні речовини, які залишилися в організмі, відкладуються в органах і тканинах, використовують засіб введення в організм комплексоутворюючих речовин. За їх допомогою радіоактивні речовини можна перевести у розчин, що полегшить виведення їх з організму. Як комплексоутворювачі використовують солі органічних кислот (лимонної, оцтової, молочної), а також вітамін Вг Лікування радіаційних опіків шкіри проводиться в процесі опіку. Воно спрямоване на зменшення запальних процесів і на відновлення ураженої тканини. У початковий період необхідно зробити протиінфекційні присипки (крохмаль, тальк, окис цинку). При важкій ранній реакції шкіри (почервоніння з крововиливом) для зменшення болю пропонуються охолоджуючі примочки (свинцева вода, риванол та ін). Важливо забезпечити ураженій ділянці спокій: уникати тертя з одягом, миття з милом, усунути дію ультрафіолетового опромінювання і подразнюючої терапії. Пропонується проведення новокаїнової блокади (введення вище місця ураження 0,25 – 0,5-процентного розчину новокаїну з інтервалом у 3-4 дні).

6.5 Висновок

В даному розділі описано організаційно-технічні засоби та санітарно-гігієнічні заходи щодо збереження працездатності працівників, які працюють в галузі ІТ. Окремо розглянуто технічні та нормативно-методичні засоби. Досліджено основні завдання та функції системи управління охороною праці на підприємстві (СУОП).

Висвітлено забезпечення безпеки життєдіяльності при роботі з ПК. Розглянуто джерела, зони дії та рівні забруднення навколишнього середовища у разі аварій на хімічно і радіаційно небезпечних об’єктах.

7 ЕКОЛОГІЯ

7.1 Стратегія і тактика збереження й розвитку життя на землі

Складність сучасного моменту в тому, що вперше за довгу історію розвитку планети стихійне управління системою, що самоорганізується, – біосферою повинно змінитися науковим, свідомим втручанням людей в цей процес на підставі законів природи. На це вказував на початку XX ст. В. І. Вернадський, маючи на увазі, що людство стало головною геологоутворюючою силою на планеті і рано чи пізно воно візьме на себе відповідальність за своє існування на ній. [62]

Саме він і створив остаточне вчення про ноосферу. В.І. Вернадський писав, що «...історики, взагалі вчені гуманітарних наук, а в певній мірі і біологи, свідомо не рахуються з законами біосфери – тієї її земної оболонки, де тільки може існувати життя. Стихійно людина від неї не може бути відокремлена. І ця нероздільність тільки тепер починає перед нами точно виявлятися».

Тепер людство за допомогою розуму, котрим його наділила природа, створило антропосферу, в якій воно діє за власними законами, які часто протирічать законам біосфери. Людство стало чинником, порівнянним із силами загальнопланетарного, космічного масштабів. На початку третього тисячоріччя ознаки ноосферних відношень поступово стають реальністю.

Вже тепер майже зникли расові забобони, руйнуються казкові, релігійні уявлення про сутність світу, природи. Народжується нова етика і мораль, економіка на основі екологічного світосприйняття. Якщо ноосферні принципи не будуть втілені в життя, цивілізація буде приречена на деградацію, самознищення. [63]

Порівняно недавно аморальними стали утиск, расові забобони, експлуатація у суспільстві, але не у відношеннях між людиною, суспільством

та природою. Тут існує проблема співвідношення свободи дій людини та принципу необхідності, достатності. Тільки доцільність може розв'язати ці протиріччя. Вона виявляється в ідеї Ле Руа, Тейяр-де-Шардена та В.І. Вернадського про ноосферу, про раціональну взаємодію суспільства з природою на науковій основі.

Сталий розвиток суспільства – результат нового екологічного мислення. Важливими ознаками стійкого гармонійного розвитку суспільства є поняття людського розвитку, яке було визначено Організацією Об'єднаних націй. Це характеристики стану ринку праці, матеріального добробуту, екологічних умов життя населення, стан охорони здоров'я та соціального середовища, рівня освіти. Людський розвиток характеризують індекси, які можуть змінюватися від нуля до одиниці.

У третій чверті XX ст. виникла концепція сталого розвитку як результат безупинного інтенсивно-екстенсивного розвитку промислової цивілізації за рахунок ресурсів природи. Тепер, на новому етапі розвитку, необхідно ноосферно, на принципах розумності і самодостатності оцінити можливості людини, суспільства при взаємодії з природою. Концепція розвитку, орієнтована на конкретну людину, а не на абстрактне суспільство, ставить головним завданням сприяти переходу до нової, ноосферної цивілізації. Її основу складають принципи: прогрес і безупинний розвиток не повинні бути результатом терациду, а людина – не хазяїн і не пан Землі, природи, але тільки її елемент. Природу не можна і не треба підкоряти, необхідно її розуміти і розумно користуватися тим, що вона може дати згідно з її можливостями, які ґрунтуються на її законах. Економічна діяльність людини не повинна формувати безлику систему накопичення, не керовану об'єктивними законами природи, а тільки її поточними потребами та бажаннями. Економіка повинна враховувати особові, етичні, духовні цінності і вартість повинні мати не тільки об'єкти, що можна порахувати, оцінити в грошовому еквіваленті. Гроші, речовинні предмети – не єдиний критерій

цінності, багатство не повинно бути основою влади, навіть законної, над людиною, суспільством, а світова економіка не повинна бути системою конкуруючих національних економік; ноосферна економіка – результат екологічної усталеності. [64]

Останнім часом ведеться багато розмов про торгівлю квотами на шкідливі промислові викиди, видаючи це за благо для економіки конкретного об'єкта – окремого промислового, галузі, держави. Проте це ілюзія – загальна маса забруднень, що надходять у природне середовище, не зміниться, але економічний стан «продавця» різко погіршиться, хоча б через неможливість запровадження нових промислових потужностей на своїх підприємствах. Створення екологічно стійкої економіки – найгостріша необхідність, що потребує зокрема впровадження заборони, або щонайменше обмежень, на споживання окремих видів природних ресурсів. Але це може призвести до руйнації усієї світової економіки. Порочність теперішньої економічної системи – в руйнації екологічних основ існування будь-якого живого об'єкта, виду, і в тому числі людини. Щоб уникнути руйнації природних екосистем, необхідно вирішити ряд найбільш пріоритетних завдань: уповільнити темпи росту народонаселення на планеті (при існуючих виробничих технологіях Земля вже перенаселена); запровадити використання альтернативних джерел енергії; обмежити зростання індивідуального матеріального споживання. Не можна створити екологічно стійку глобальну або регіональну економіку без розумного (ноосферного) обмеження рівня споживання природних багатств багатими людьми, країнами. Стала економіка тепер – стійкість екосистем та сталість економічного розвитку в майбутньому.

Серед значних прошарків населення існує поширена думка про практичну невичерпність природних ресурсів. Багато хто вважає, що економічне процвітання пов'язане тільки з безупинним ростом видобутку корисних копалин. Це теж проблема, що потребує вирішення в соціально-

педагогічному плані. Адже більшість населення вважає, що головне в житті – збагачення, накопичення капіталу в будь-якій формі – грошовій, речовій. Неможливо відновити природні ресурси, зокрема ті, що складають основу рекреації – території відпочинку, туризму, лікування.

Необхідно пам'ятати про певний самодостатній рівень накопичення, перевищення якого – загроза всьому живому і насамперед людині. Від того, чи зуміємо ми зупинитися в цьому порочному колі перетворень живого в неживе – залежить майбутнє цивілізації.

Розширення сфери впровадження в різноманітні галузі виробництва альтернативних джерел енергії дасть можливість, завдяки глобальним зусиллям позбутися парникового ефекту, руйнації озонового шару, замінити вуглеводневе паливо водневим, отриманим електролізом води за допомогою електроенергії. Під егідою ООН та її органів фінансуються інвестиційні програми збереження або відновлення інфраструктури біосфери – озонового шару, подолання результатів парникового ефекту, запобігання забрудненню атмосфери, захист і відновлення біорізноманіття.

Таким чином, найважливішою умовою сталого гармонійного розвитку є таке економічне співіснування з природою, в якому пріоритетом є екологічні принципи, які припускають стійке невиснажливе використання природних ресурсів, що не ставить під загрозу існування майбутніх поколінь. Економіка сталого – гармонійного розвитку не повинна сприяти виснаженню відновлюваних ресурсів, не повинна погіршувати природні умови комфортності життя. Сталий розвиток – це передусім екологічно освічене суспільство і як результат – екологічно безпечні виробничі технології, результат яких – мінімальні забруднення атмосферного повітря, вод, ґрунтів, які б не перевищули фонових, тобто природних, концентрацій речовин, факторів, небезпечних для життя взагалі і людини зокрема.

7.2 Вимоги до моніторів (ВДТ) і ПЕОМ

Чіткість зображення моніторів, в першу чергу залежать від роздільної здатності монітора, яка визначається числом дискретних елементів зображення, відтворених монітором по горизонталі і вертикалі. Чим вище роздільна здатність, тим точніше і чіткіше зображення на екрані, тим легше воно для сприйняття, тим менше стомлює зорову систему. При низькому розрізненні можливі помилки при прочитуванні символів (два різні символи при малий кількості складових можуть сприйматися як однакові). Існують стандартні значення роздільної здатності (у дужках наведена назва стандарту для ПК): 640x480 (VGA); 800x600 (SVGA); 1024x768 (XGA); 1280x1024 (EVGA); 1600x1200 або більше.

Чіткість зображення залежить, крім того, від кроку люмінофора (dot pitch) – відстані між дискретними точками люмінофора одного кольору на внутрішній поверхні екрана. Для апертурної гратки – це відстань між смугами одного кольору, для тіньової маски лінія мінімальної відстані між точками одного кольору становить з горизонталлю кут 30º. У різних моделей моніторів крок люмінофора лежить в діапазоні від 0,25 до 0,41 мм. Для інтенсивних робіт з графікою при розрізненні вище 1024x768 переважно крок 0,25 або 0,26 мм. Для ділового і домашнього застосування в більшості додатків, що використовують режим розрізнення 1024x768 або нижче, достатній крок 0,27 або 0,28 мм. В нормах встановлені такі вимоги до ВДТ (див. таблицю 7.1).

Таблиця 7.1 – Вимоги до відеотерміналів

Найменування параметра	Значення параметра
1	2
Яскравість знака (яскравість фону), кд/кв.м	від 35 до 120
Зовнішня освітленість екрана, лк	від 100 до 250

Продовження таблиці 7.1

1	2
Контраст (для монохромних зображень)	від 3 : 1 до 1,5 : 1
Нерівномірність яскравості в робочій зоні екрана	не більше 1,7 : 1
Відхилення форми робочої зони екрана від прямокутності:	
по горизонталі і вертикалі	не більше 2%
по діагоналі	не більше 4% відношення суми коротких сторін до суми довгих
Різниця довжин рядків або стовпчиків	не більше 2% середнього значення
Розмір мінімального елементу зображення (пікселя) для монохромних зображень, мм	0,3
Допустима тимчасова нестабільність зображення (мерехтіння)	не повинна бути зафіксована у 90 відсотків спостерігачів
Відбивна властивість, дзеркальне і змішане віддзеркалення (відблиск) %, (допускається виконання вимог при застосуванні приекранного фільтра)	не більше 1
Відношення ширини знака до його висоти для великих літер	від 0,7 до 0,9
Мінливість розміру знака	не більше 5% висоти
Ширина лінії контура знака	0, 15...0,1 висоти знака
Модуляція щодо яскравості растру:	
для монохромних зображень	не більше 0,4
для багатоколірних зображень	не більше 0,7
Відстань між рядками	не менше ширина контура знака або одного елемента зображення

Велике значення для чіткості зображення має якість фокусування електронних променів.

7.3 Висновок до розділу

В даному розділі магістерської роботи описана стратегія і тактика збереження й розвитку життя на землі. Зокрема підкреслено що сталий розвиток суспільства – результат нового екологічного мислення важливість впровадження в різноманітні галузі виробництва альтернативних джерел енергії.

В окремому параграфі розглянуті вимоги до моніторів (ВДТ) і ПЕОМ.

ВИСНОВКИ

В процесі виконання дипломної роботи освітнього рівня «магістр» було досліджено промислові інтерфейси CANopen для інтернету-речей в проектах «розумних міст». Зокрема, в першому розділі:

– описано програмно-алгоритмічні комплекси в сучасних інформаційно-технологічних проектах «розумних міст»;

– проаналізовано промислові інтерфейси для «IoT»-пристроїв у проектах класу «розумне місто»;

– досліджено протокол «CANopen».

В другому розділі дипломної роботи:

– подано основні поняття «CANopen» для «IoT»-проектів «розумних міст»;

– описано мережеві сервіси «CANopen»;

– досліджено процеси, що впливають на роботу CANopen в умовах «розумного міста».

В третьому розділі виконано моделювання процесів у міських Iot-мережах на базі «CANopen»:

– виконана побудова ідеальної моделі «CANopen» в «IoT»-пристроях;

– подано рекомендації щодо використання «CANopen» в «IoT»-проектах класу «розумне місто»;

– описано розроблення програмної частини.

В розділі «Спеціальна частина» описано проектування елементів пристрою для тестового підключення до шини «CAN».

В розділі «Обґрунтування економічної ефективності» розраховано основні техніко-економічні показники проведених досліджень.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» описано організаційно-технічні засоби та санітарно-гігієнічні заходи щодо збереження працездатності працівників, які працюють в галузі ІТ. Подано

основні завдання та функції системи управління охороною праці на підприємстві (СУОП). Описано забезпечення безпеки життєдіяльності при роботі з ПК. Розглянуто джерела, зони дії та рівні забруднення навколишнього середовища у разі аварій на хімічно і радіаційно небезпечних об’єктах.

В розділі «Екологія» описано стратегію і тактика збереження й розвитку життя на землі та вимоги до моніторів (ВДТ) і ПЕОМ.

ПЕРЕЛІК ДЖЕРЕЛ

1 VITAL – The future of Smart Cities [Електронний ресурс] – Режим доступу: URL: http://vital-iot.eu – Дата доступу: 17.11.2018.

2 Xively Developers [Електронний ресурс] – Режим доступу: URL: https://xively.com/platform/ – Дата доступу: 17.11.2018.

3 PLATFORM HI REPLY [Електронний ресурс] – Режим доступу: URL: http://www.reply.eu/en/content/hi-reply – Дата доступу: 17.11.2018.

4 J.-P. Calbimonte, S. Sarni, J. Eberle, and K. Aberer, ‘‘XGSN: An opensource semantic sensing middleware for the Web of things,’’ in Proc. 7th Int. Conf. Semantic Sensor Netw., Riva Del Garda, Italy, 2014, pp. 1–6.

5 O. Fambon, É. Fleury, G. Harter, R. Pissard-Gibollet, and F. Saint-Marcel, ‘‘FIT IoT-LAB tutorial: Hands-on practice with a very large scale testbed tool for the Internet of Things,’’ in Proc. UbiMob, 2014, pp. 1–5.

6 О. М. Дуда та ін., "Актори та діаграми прецедентів системи консолідації соціокомунікаційних інформаційних ресурсів «розумних міст»", *Науковий вісник НЛТУ України*, вип. 27(10), с. 129-136, 2017. ISSN 2519-2477.

7 O. Duda, N. Kunanets, O. Matsiuk, and V. Pasichnyk, "Information-Communication Technologies of IoT in the "Smart Cities" Projects", *CEUR Workshop Proceedings*, vol. 2105, pp. 317-330, 2018. ISSN 1613-0073.

8 O. Duda, O. Matsiuk, M. Karpinski, N. Veretennikova, N. Kunanets, and V. Pasichnyk, "Information Technologies of Internet Devices and BigData in the “Smart Cities” Projects", in Proc. *13 Intern Scientific and Techn. Conf. on Computer Science and Information Technologies (CSIT)*, vol. 2, Lviv, 2018, pp. 72-75. ISBN: 978-1-5386-6465-0.

9 O. Duda, S. Martsenko, O. Matsiuk, N. Kunanets, and V. Pasichnyk, "Software modelling complex of network operating parameters with variable input

data", in *Proc. 14th Intern. Conference on Computer sciences and Information technologies" (CSIT 2019), Lviv, 2019, pp.* 165-168. ISBN 978-1-5386-6463-6.

10 O. Duda, S. Martsenko, O. Matsiuk, N. Kunanets, and V. Pasichnyk, "The information system for planning the parameters of telecommunication operator networks", in *Proc. 14th Intern. Conference on Computer sciences and Information technologies" (CSIT 2019), Lviv, 2019, pp.* 177-182. ISBN 978-1-5386-6463-6.

11 O. Duda, V. Kochan, N. Kunanets, O. Matsiuk, V. Pasichnyk, and A. Sachenko, "Data Processing in IoT for Smart City Systems", in *Proc. 10th IEEE Intern. Conf. on. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2019)*, Metz, 2019. pp. 96-99.

12 V. Kochan et al, N. Kunanets, V. Pasichnyk, O. Roshchupkin, Anatoliy Sachenko, Iryna Turchenko, Oleksij Duda, Vita Semaniuk, Svitlana Romaniv, Oleksandr Matsiuk Sensing in IoT for Smart City Systems in *Proc. 10th IEEE Intern. Conf. on. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2019)*, Metz, 2019 pp. 579-586.

13 О. М. Дуда, Г. І. Липак, та Н. Е. Кунанець, "Соціокомунікаційний проект зі створення консолідованого інформаційного ресурсу невеликого за масштабами міста", *Science and Education a New Dimension. Humanities and Social Sciences,* vol (19), issue 119, pp. 51-55, 2017. ISSN 2308-1996.

14 NYC BigApps [Електронний ресурс] – Режим доступу: URL: http://bigapps.nyc/ – Дата доступу: 17.11.2018.

15 Khan, A. Anjum, K. Soomro, and M. A. Tahir, ‘‘Towards cloud based big data analytics for smart future cities,’’ J. Cloud Comput., vol. 4, p. 2, Dec. 2015.

16 D. Tabachyshyn, N. Kunanets, M. Karpinski, O. Duda, and O. Matsiuk, "Information Systems for Processes Maintenance in Socio-communication and Resource Networks of the Smart Cities", in *Advances in Intelligent Systems and Computing III*, vol. 871, pp 192-205, 2019. ISSN 2194-5365.

17 Amsterdam Smart City [Електронний ресурс] – Режим доступу: URL: http://amsterdamsmartcity.com/#/nl/home – Дата доступу: 17.11.2018.

18 V. Pasichnyk et al., "Telecommunication Infrastructures for Telemedicine in Smart Cities", *IDDM 2018 Informatics & Data-Driven Medicine*, vol. 2255, pp. 256-266, 2018. ISSN 1613-0073.

19 N. Shakhovska, O. Duda, O. Matsiuk, Y. Bolyubash, and R. Vovnyanka "Analysis of the Activity of Territorial Communities Using Information Technology of Big Data Based on the Entity-Characteristic Mode", in *Advances in Intelligent Systems and Computing III*, vol 871, pp. 155-170, 2019. ISSN 2194-5365.

20 Kumbhar, Minakshi S., and Pratibha S. Yalagi. "Survey on technology tools for water and garbage management for smart city planning." *International Journal of Computer Applications* 975: 8887.

21 Chen, Yiheng, and Dawei Han. "Water quality monitoring in smart city: A pilot project." *Automation in Construction* 89 (2018): 307-316.

22 Chai, Xudong, et al. "INDICS: An Industrial Internet Platform." *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2018.

23 Pires, Felipe Marques, Lorena León Quiñonez, and Leonardo de Souza Mendes. "A Cloud-Based System Architecture for Advanced Metering in Smart Cities." *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2019.

24 Reilly, Elizabeth, et al. "A Smart City IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client." *Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco*. 2019.

25 Wu, Yung Chang, Yenchun Jim Wu, and Shiann Ming Wu. "An outlook of a future smart city in Taiwan from posteInternet of things to." *Smart Cities: Issues and Challenges: Mapping Political, Social and Economic Risks and Threats* (2019): 263.

26 Anthopoulos, Leonidas, Marijn Janssen, and Vishanth Weerakkody. "A Unified Smart City Model (USCM) for smart city conceptualization and benchmarking." *Smart Cities and Smart Spaces: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2019. 247-264.

27 Wu, Yung Chang, Yenchun Jim Wu, and Shiann Ming Wu. "An outlook of a future smart city in Taiwan from posteInternet of things to." *Smart Cities: Issues and Challenges: Mapping Political, Social and Economic Risks and Threats* (2019): 263.

28 Wheeler, David McMakin, et al. "Smart city commodity exchange with smart contracts." U.S. Patent Application No. 15/720,305.

29 Pires, Felipe Marques, Lorena León Quiñonez, and Leonardo de Souza Mendes. "A Cloud-Based System Architecture for Advanced Metering in Smart Cities." *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2019.

30 Zhu, Xuebiao, et al. "Adaptive PID controller for cloud smart city system stability control based on chaotic neural network." *Cluster Computing* 22.6 (2019): 13067-13075.

31 Pires, Felipe Marques, Lorena León Quiñonez, and Leonardo de Souza Mendes. "A Cloud-Based System Architecture for Advanced Metering in Smart Cities." *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2019.

32 Mora, Luca, Mark Deakin, and Alasdair Reid. "Strategic principles for smart city development: A multiple case study analysis of European best practices." *Technological Forecasting and Social Change* 142 (2019): 70-97.

33 Bull, Richard, et al. "Sufficiently engaged? How smart metering systems help local authorities become smart cities." eceee, 2019.

34 Cagáňová, Dagmar, et al., eds. *Smart Technology Trends in Industrial and Business Management*. Springer International Publishing, 2019.

35 Chen, Wen, et al. "A DDoS attacks traceback scheme for SDN-based smart city." *Computers & Electrical Engineering* 81 (2020): 106503.

36 Pires, Felipe Marques, Lorena León Quiñonez, and Leonardo de Souza Mendes. "A Cloud-Based System Architecture for Advanced Metering in Smart Cities." *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, 2019.

37 Andrejevic, Mark. "Automating Surveillance." *Surveillance & Society* 17.1/2 (2019): 7-13.

38 Wheeler, David McMakin, et al. "Smart city commodity exchange with smart contracts." U.S. Patent Application No. 15/720,305.

39 Usman, Aminu Bello, Jairo A. Gutierrez, and Abdullahi Baffa Bichi. "Secure Routing Protocols Using Trust-Based Mechanisms in the Internet of Things for Smart City Environment Challenges and Future Trends." *Secure Cyber-Physical Systems for Smart Cities*. IGI Global, 2019. 103-129.

40 Montori, Federico, et al. "CrowdSenSim 2.0: a Stateful Simulation Platform for Mobile Crowdsensing in Smart Cities." *Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. ACM, 2019.

41 Ray, Korok, and Brent Skorup. "Smart Cities, Dumb Infrastructure: Policy-Induced Competition in Vehicle-to-Infrastructure Systems." *Mercatus Research Paper* (2019).

42 Nolte, Thomas, Hans Hansson and Christer Norstrom. “Probabilistic WorstCase Response-Time Analysis for the Controller Area Network”

43 CiA 308. CANopen Technical Report. Performance measurement basics. Ver. 1.0.1. 2006.

44 Денисенко В. ПИД – регуляторы: принципы построения и модификации. Ч. 1.//Современные технологии автоматизации. –2006. No4. –с. 66-74.

45 Din, M. A. C., et al. "Development of CAN Bus Converter for On Board Diagnostic (OBD-II) System." *IOP Conference Series: Materials Science and Engineering*. Vol. 705. No. 1. IOP Publishing, 2019.

46 Li, Hui, and Junli Ren. "Research on the Test of Fuel Cell Electric Rail Based on CANopen." *Chemical Engineering Transactions* 59 (2017): 259-264.

47 Deng, Dexiang, Yue Zhao, and Xi Zhou. "Smart city planning under the climate change condition." *IOP Conference Series: Earth and Environmental Science*. Vol. 81. No. 1. IOP Publishing, 2017.

48 Chintagunta, Lavanya, Priyanshu Raj, and Sundaravalli Narayanaswami. "Conceptualization to amendment: Kakinada as a smart city." *Journal of Public Affairs* 19.1 (2019): e1879.

49 Brown, Michael. "Smart Transport." *Smart Cities in Application*. Springer, Cham, 2020. 69-83.

50 Kamal, Miraal, et al. "IoT Based Smart City Bus Stops." *Future Internet* 11.11 (2019): 227.

51 Din, M. A. C., et al. "Development of CAN Bus Converter for On Board Diagnostic (OBD-II) System." *IOP Conference Series: Materials Science and Engineering*. Vol. 705. No. 1. IOP Publishing, 2019.

52 Arapantonis, Elpidoforos. "Data tampering in Vehicle CAN Bus networks." (2019).

53 Toma, Cristian, et al. "IoT solution for smart cities' pollution monitoring and the security challenges." *Sensors* 19.15 (2019): 3401.

54 Montori, Federico, et al. "CrowdSenSim 2.0: a Stateful Simulation Platform for Mobile Crowdsensing in Smart Cities." *Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. ACM, 2019.

55 Din, M. A. C., et al. "Development of CAN Bus Converter for On Board Diagnostic (OBD-II) System." *IOP Conference Series: Materials Science and Engineering*. Vol. 705. No. 1. IOP Publishing, 2019.

56 Зеркалов, Д. В. "Охорона праці в галузі (загальні вимоги)." (2011).

57 Жидецький, В. Ц., В. С. Джигирей, and О. В. Мельников. "Основи охорони праці." *Львів: Афіша* 350 (2000): 132-136.

58 Основні технічні та організаційні заходи щодо профілактики виробничого травматизму та професійної захворюваності [Електронний ресурс] Режим доступу: URL: https://pidruchniki.com/12281128/bzhd/osnovni_tehnichni_organizatsiyni_zahodi_schodo_profilaktiki_virobnichogo_travmatizmu_profesiynoyi_zahvoryuv – Заголовок з екрану.

59 Основні завдання і функції системи управління охороною праці [Електронний ресурс] Режим доступу: URL: https://pidruchniki.com/18060203/bzhd/osnovni_zavdannya_funktsiyi_sistemi_upravlinnya_ohoronoyu_pratsi – Заголовок з екрану.

60 Желібо, Євген Петрович, and І. С. Сагайдак. "Безпека життєдіяльності." (2011).

61 Депутат, О. П., І. В. Коваленко, and І. С. Мужик. "Цивільна оборона. Підручник/За ред. Полковника ВС Франчука.–2-ге вид., доп." *Львів, Афіша* (2001).

62 Бобильов, Ю. П., et al. "Екологія: базовий підручник для студентів вищих навчальних закладів." (2014).

63 Юрченко, Любов Іванівна. "Екологія." (2009).

64 Малимон, С. С. Основи екології: Підручник.–Вінниця. Нова Книга, 2009.