

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Центральноукраїнський національний технічний університет**

**Кафедра кібербезпеки та програмного забезпечення**

На правах рукопису

Кульчицький Олександр Сергійович

**Програмне забезпечення системи NB-IoT**

Спеціальність: 123 «Комп'ютерна інженерія»

Освітній ступінь: бакалавр

Науковий керівник:

**Доренський Олександр Павлович**

\_\_\_\_\_

(підпис)

(дата)

кандидат технічних наук

**ДОПУЩЕНО ДО ЗАХИСТУ**

**Завідувач кафедри**

\_\_\_\_\_ О.А. Смірнов

(підпис)

ПБ

« \_\_\_\_\_ » \_\_\_\_\_ 2021 р.

Міністерство освіти і науки України  
Центральноукраїнський національний технічний університет  
Факультет Механіко-технологічний  
Кафедра Кібербезпеки та програмного забезпечення  
Освітній ступінь бакалавр  
Спеціальність 123 Комп'ютерна інженерія

**ЗАТВЕРДЖУЮ**  
Завідувач кафедри  
д.т.н., проф.  
О.А.Смірнов  
« 11 » січня 2021 року

**З А В Д А Н Н Я**  
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Кульчицькому Олександр Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Програмне забезпечення системи NB-IoT

керівник роботи Доренський Олександр Павлович, канд. техн. наук

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

затверджені наказом вищого навчального закладу № 204-02 від 28.12.2020 року

2. Строк подання студентом роботи до захисту 22.05.2021 р.

3. Мета та завдання кваліфікаційної бакалаврської роботи: Метою розробки є програмне забезпечення системи NB-IoT

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

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи в промислову експлуатацію.

6. Висновки

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

Структурна схема системи 1 аркуш

Функціональна схема системи 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

6. Дата видачі завдання « 11 » січня 2021 р.

### КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної бакалаврської роботи	Строк виконання етапів кваліфікаційної бакалаврської роботи	Примітка
1.	Аналіз існуючих систем	10.03.2021 р.	
2.	Постановка задачі, оформлення ТЗ	15.03.2021 р.	
3.	Розробка моделі компонента	20.03.2021 р.	
4.	Розробка структур даних	25.03.2021 р.	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2021 р.	
6.	Програмування алгоритмів	10.04.2021 р.	
7.	Оформлення ПЗ	17.04.2021 р.	
8.	Попередній захист роботи	14.05.2021 р.	

**Студент** \_\_\_\_\_

( підпис )

\_\_\_\_\_ (прізвище та ініціали)

**Керівник роботи** \_\_\_\_\_

( підпис )

\_\_\_\_\_ (прізвище та ініціали)

## АНОТАЦІЯ

**Кульчицький О.С. Програмне забезпечення системи NB-ІоТ. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2021.**

В даній кваліфікаційній бакалаврській розроблено програмне забезпечення, яке призначено для системи NB-ІоТ.

Метою розробки є програмне забезпечення системи NB-ІоТ.

Результат роботи – програмна реалізація системи NB-ІоТ.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ архітектури IBM PC з ОС Windows XP/Vista/7/8/10.

Програму розроблено в середовищі Builder C++.

**Ключові слова:** комп'ютерна інженерія, NB-ІоТ

## ABSTRACT

**Kulchytskyi O.S. NB-IoT system software. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2021**

In this bachelor's qualification the software which is intended for the NB-IoT system is developed.

The purpose of the development is the software of the NB-IoT system.

The result is a software implementation of the NB-IoT system.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

Developed user-friendly interface. Instructions for working with software are given.

The program can be used on an IBM PC with Windows XP / Vista / 7/8/10.

The program is developed in the Builder C ++ environment.

**Keywords:** computer engineering, NB-IoT

## ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ .....	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ.....	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ .....	8
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми кваліфікаційної бакалаврської роботи.....	8
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування.....	11
2.3 Розгорнута постановка завдання .....	13
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ .....	15
3.1 Опис функціонування системи.....	15
3.2 Розробка структурної схеми .....	37
3.3 Розробка функціональної схеми.....	44
3.4 Розробка діаграми процесів.....	52
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ ...	55
4.1 Розробка блок-схем та опис алгоритмів функціонування системи .....	55
4.2 Захист розробленого програмного забезпечення .....	69
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ.....	71
6 ОСНОВНІ ВИСНОВКИ.....	73
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....	75

**КБР-123.21.0034.00.00.ПЗ**

Вим.	Арк.	№ докум.	Підп.	Дата				
Розроб.		Кульчицький О.С.			Програмне забезпечення системи NB- IoT	Лім.	Аркуш	Аркушів
Перев.		Доренський О.П.				Б	1	83
Н.контр.		Гермак В.С.			ЦНТУ КІ-18-3СК			
Затв.		Смірнов О.А.						

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

- AS – Application Server – Сервер застосунків
- C-SGN – Cellular IoT Serving Gateway Node – умовне об'єднання в єдиний елемент механізмів оптимізації CP і UP для NB – IoT, які реалізуються на вузлах MME, SGW і PGW
- eNodeB – Evolved NodeB – Поліпшений вузол базових станцій у мережах LTE
- IoT – Інтернет речей
- NB-IoT – Інтернет речей який використовує потенціал сучасних стільникових мереж
- LTE – Стандарт стільникового зв'язку 4 покоління 4G
- MME – Mobility Management Entity – Державний оператор зв'язку
- PGW – Packet Data Network SAE Gateway або просто Packet Data Network Gateway – Шлюз, призначений для маршрутизації трафіка мережі LTE до інших (зовнішнім) мережам передачі даних
- SGW – Serving SAE Gateway або просто Serving Gateway – Обслуговуючий шлюз
- ПЗ – Програмне забезпечення

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		2

## ВСТУП

**Актуальність теми.** Інтернет речей (IoT) є важливою частиною цифрової трансформації світової економіки. Однак поширення IoT може сповільнитися у зв'язку з недостатньою пропускну здатністю мереж. Одним зі способів підвищення продуктивності IoT може бути протокол NB-IoT, який використовує потенціал сучасних стільникових мереж.

До 2022 р. глобальний обсяг даних, генеруємих IoT, може досягти 50 трлн гігабайт, а кількість підключених користувачів – 4 млрд. Це зажадає нових підходів до передачі даних і моніторингу продуктивності мережних систем. У той же час, у більшості випадків інтернет-речі передають невеликі порції даних з відомими інтервалами, наприклад інформацію про серцебиття пацієнта, тиску газу в трубі, вологості ґрунту і т.д. Для таких мережних пристроїв потрібні не канали зв'язку з високою пропускну здатністю, а повсюдно доступна бездротова мережа. Кращим кандидатом на цю роль є мережі мобільного зв'язку, але їх сучасні протоколи занадто громіздкі для простих пристроїв IoT.

В 2016 р. консорціум 3GPP представив першу специфікацію стандарту стільникового зв'язку для пристроїв з невеликими обсягами переданих даних. Стандарт одержав назву NB-IoT (Narrowband IoT). Він може використовуватися на устаткуванні LTE, а також окремо від існуючих мереж зв'язку.

NB-IoT спеціально створений для інтернету речей, тому враховує специфічні потреби, такі як поліпшена чутливість до модуляції сигналу для підключення сотень тисяч пристроїв. Також для роботи з NB-IoT не потрібна SIM-карта й досить невеликої потужності приймачепередатчика, тобто пристрою IoT можуть працювати багато років від однієї батарейки.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

**Мета й завдання дослідження.** Метою роботи є програмне забезпечення системи NB-IoT.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем NB-IoT.
- Дослідження системи NB-IoT.
- Програмна реалізація системи NB-IoT.

**Практична цінність отриманих результатів** полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі NB-IoT.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи NB-IoT, є актуальною задачею, яка потребує вирішення у даній кваліфікаційній бакалаврській роботі.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

# 1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

## 1.1 Призначення системи

Розгортання NB-ІоТ почате в ЄС. В Україні в найближчі два роки оператори мобільному зв'язку також запуснуть мережі NB-ІоТ.

Стандарт NB-ІоТ може розгортатися в трьох варіантах:

- автономний (standalone);
- на захисній смузі частот (guard-band);
- внутріполосний (in-band).

### Різні типи розгортання NB-ІоТ

Найпоширенішим є внутріполосний. Він широко використовується в Європі, де мережі з NB-ІоТ in-band розгорнуті телекомунікаційними компаніями Vodafone, Deutsche Telekom, Telecom Italia Mobile і іншими.

Внутріполосний спосіб розгортання дозволяє використовувати NB-ІоТ усередині існуючих мереж LTE, які мають велике покриття й забезпечують необхідна якість обслуговування інтернету речей. Це оптимальний шлях для підключення ІоТ, оскільки він дозволяє операторам зв'язку використовувати сучасне устаткування без істотних змін апаратного забезпечення. У такий спосіб in-band NB-ІоТ дає можливість задовольнити поточний попит на підключення розумних пристроїв.

Незважаючи на поширеність внутріполосного способу використання NB-ІоТ, у нього є недоліки. Так, узкополосний сигнал in-band NB-ІоТ займає частоту 180 кГц і в мережах LTE може створювати перешкоди для блоків фізичного ресурсу (PRB). У такому режимі NB-ІоТ віднімає функціональні ресурси стільникових мереж.

При внутріполосному використанні PRB стандарту NB-ІоТ відділяються від інших PRB за допомогою динамічних характеристик потужності. Зокрема,

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

звичайний PRB для LTE могутніше на 6 Дб, чому PRB для NB-IoT в in-band і guard-band. Також специфікації стандарту NB-IoT припускають інші відмінності в структурі сигналу, наприклад, підтримувані типи модуляції сигналу, частотна погрішність, амплітуда вектора помилок (EVM) і параметри синхронізації й керування каналами.

Показник EVM (Error Vector Magnitude) є важливим критерієм якості модуляції й продуктивності каналу приймання й передачі даних у складних бездротових мережах, включаючи LTE і NB-IoT. Фактично, EVM – це різниця між «еталонним» переданим сигналом і прийнятим (обмірюваним) сигналом. EVM – корисний індикатор якості переданого бездротового сигналу, який допомагає оцінити продуктивність NB-IoT.

При запуску нового сервісу на основі in-band NB-IoT перешкоди між PRB є основною проблемою. Тому перевірка взаємних перешкод PRB при вимірі EVM – найбільш точна й комерційно ефективна процедура тестування.

## 1.2 Область застосування

Для перевірки розгортання застосовуються сучасні аналізатори базових станцій, такі як, наприклад, VIAVI Celladvisor JD745B або JD785B. Це портативні прилади, які здатні виміряти параметри NB-IoT у відповідності зі специфікаціями від 3GPP.

### Аналізатор VIAVI Celladvisor JD785B

Аналізатори можуть виміряти наступні параметри сигналу NB-IoT:

- максимальна потужність PRB;
- динамічні характеристики сигналу NB-IoT;
- EVM для спадного каналу зв'язку NPDSCH і інших каналів керування й синхронізації;
- частотну погрішність.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

Дані показники необхідно перевіряти на етапах розгортання NB-ІоТ і проведення регулярних перевірок при техобслуговуванні. Тільки в такий спосіб оператори мобільного зв'язку можуть гарантувати надійну підтримку ІоТ, максимальні покриття й потужності, а також високу якість обслуговування.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи NB-ІоТ, є актуальною задачею, яка потребує вирішення у даній кваліфікаційній бакалаврській роботі.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

## 2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

### 2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми кваліфікаційної бакалаврської роботи

#### Azure IoT

Azure IoT надає самий широкий у галузі портфель служб і можливостей, який допоможе вам виконувати завдання на периферії й у хмарі з урахуванням ваших потреб і галузевих вимог.

Відкритий підхід Azure IoT спрощує розробку й інтеграцію. Підключайте, відслідковуйте мільярди пристроїв і управляйте ними на своїх умовах завдяки швидкій і простій розробці на повністю керованій платформі застосунків або створюйте гнучкі розв'язки за допомогою надійних служб платформи.

Створюйте й поставляйте розв'язку швидше завдяки розробці сучасних застосунків.

Azure IoT – це колекція керованих і платформних служб на периферії й у хмарі, які дозволяють підключати мільярди ресурсів Інтернету речей, відслідковувати їхній стан і управляти ними. Вона включає системи безпеки й операційні системи для пристроїв і устаткування, а також дані й засоби аналітики, які допомагають підприємствам створювати, розгортати застосунки Інтернету речей і управляти ними. Під час обговорення Azure IoT ми враховуємо, як ці служби взаємодіють у таких трьох аспектах:

Фізичні об'єкти ("речі"), такі як промислове устаткування, пристрої або датчики, які підключені до хмари (постійно або час від часу).

Що збираються пристроями відомості, які аналізуються й перетворюються фахівцями або ШІ в корисні знання.

Те, як люди реагують на такі корисні відомості й застосовують їх у своєму бізнесі, а також із системами й інструментами, які вони вже використовують.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

## **Звіт IoT Signals Edition 2**

Звіт IoT Signals покликано поліпшити роботу наших партнерів і клієнтів, а також спростити для бізнес-керівників розробку власних стратегій Інтернету речей. Із цього звіту, який вийшов в жовтні 2020 року, ви дізнаєтеся актуальні аналітичні відомості, отримані на основі відкликань більш 3000 керівників великих компаній по усьому світу, які зараз користуються розв'язками Інтернету речей.

### **Знайдіть оптимальний підхід до Інтернету речей для свого бізнесу**

Прискорте вихід на ринок завдяки оптимальному запуску свого проекту Інтернету речей. Виконуйте розробку, користуючись широким спектром засобів з урахуванням потреб, ресурсів і цілей своєї організації.

- Сервіси платформи.
- Керована платформа застосунків.
- Пошук партнера.

Центр Інтернету речей Azure і Azure Digital Twins надають компаніям базові блоки для створення спеціалізованих розв'язків для складних сценаріїв Інтернету речей. Цей розв'язок гарний пасує компаніям із хмарним розв'язком і досвідом роботи із пристроями, а також відповідає таким підходам:

- Керування. Мені потрібний повний контроль над базовими службами мого розв'язку, у тому числі можливість дістати пр ава володіння для керування й масштабування відповідно до моїх потреб, а також використовувати досвід фахівців моєї компанії або компанії-партнера для підключення пристроїв і служб.
- Контроль. Моєму бізнесу потрібні можливості повного налаштування й контролю архітектури розв'язків.
- Вартість. Я прагну адаптувати служби для керування всіма витратами.

### **Центр Інтернету речей Azure**

Забезпечте надійний обмін даними з високим рівнем безпеки між своїм додатком Інтернету речей і пристроями, якими воно управляє. Центр Інтернету

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

речей Azure дозволяє серверній частині розв'язку, розміщеного в хмарі, віртуально підключатися до будь-якого пристрою.

### **Azure Digital Twins**

Одержуйте аналітичні дані, які допоможуть вам підвищити якість продуктів, оптимізувати операції й витрати, а також створити нові можливості для клієнтів. Застосовуйте свій досвід роботи з доменом на основі Azure Digital Twins для створення підключених розв'язків.

### **Пройдіть сертифікацію Azure IoT**

Станьте сертифікованим розроблювачем Azure IoT і розкрийте весь потенціал продуктів Azure IoT за допомогою покрокових керівництв. Зануртеся в мир знань прямо сьогодні за допомогою наших схем і модулів навчання.

### **Центр Інтернету речей Azure**

Підключайте, адмініструйте й масштабуйте мільярди пристроїв Інтернету речей, переносячи їх із прикордонного середовища в хмару.

### **Azure IoT Central**

Прискорте створення розв'язків Інтернету речей і скоротите витрати часу й засобів на керування розв'язками Інтернетом речей, їхню експлуатацію й розробку.

### **Time Series Insights**

Одержуйте корисні практичні відомості для розвитку бізнесу завдяки аналізу, зберіганню й адмініструванню всіх даних, що збираються.

### **Azure Digital Twins**

Створюйте розв'язку нового покоління для просторової аналітики Інтернету речей, реплікуючи реальний фізичний простір і створюючи підключені середовища.

### **Підтримка прикордонних середовищ і пристроїв**

#### **Azure IoT Edge**

Розширення охопту засобів хмарної й традиційної аналітики за рахунок переносу робочих навантажень і бізнес-логіки із хмари на прикордонні пристрої.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

## Azure Sphere

Безпека підключення пристроїв з мікроконтролерами – від мікросхеми до хмари.

## Windows IoT

Довгострокова підтримка ОС і служби для керування пристроями.

## Azure RTOS

Простота підключення й розробки впроваджених розв'язків Інтернету речей.

## 2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Оскільки потрібно розробити просту та легку у користуванні програму, яка б виконувалась під операційною системою Windows, то для її реалізації я обрав Builder C++. Існує велике число бібліотек написаних під Builder C++ , тому це одна з важливих причин вибору мови програмування. Середовище Builder C++ досить просте в користуванні, його вихідний код значно менше по об'єму в порівнянні з Delphi чи деякими іншими програмами такого типу. Досить легко організувати взаємодію між модулями програм, об'єктно-орієнтований підхід дає можливість значно скоротити код програми, а отже і час його виконання.

На заміну старого розробленого набору елементів управління у Builder C++ інтегрована бібліотека візуальних компонентів VCL, представлених на палітрі компонентів. Після переносу на форму методом перетягування (drag-and-drop) компоненти відразу становляться діючими об'єктами вашої програми. Окрім типізованих інтерфейсних елементів Windows (кнопки, смуги прокручування, редагуємі текстові області, прості та комбіновані списки, та інше) у бібліотеку включені елементи підтримки діалогових вікон, обслуговування баз даних та багато іншого. Можливо не тільки модифікувати поведінку існуючих компонентів, але і будувати нові.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

Builder C++ підтримує останні розширення стандарту мови C++ та забезпечує швидку компіляцію та складання 32-розрядних програм для Windows. Результуючі програми оптимізовані з точки зору швидкості виконання програм та затрат пам'яті. Зручний відладгоджувальник (з асемблерним вікном, можливістю крокового виконання, завдання точок зупинки, трасування та інше) повністю інтегрований у систему проектування. Дизайнер форм, редактор коду, інспектор об'єктів та інші інструменти залишаються доступними під час виконання програми, саме через це вносити зміни до коду можна прямо у процесі відлагодження.

Дизайнер форм, Інспектор об'єктів і інші засоби залишаються доступними під час роботи програми, тому вносити зміни можна в процесі відлагодження.

Builder C++ поставляється в трьох варіантах: Standard (стандартний), Professional (для професіоналів розробників, орієнтованих на мережеву архітектуру) і Client/Server Suite (для розробки систем в архітектурі клієнт/сервер). Останні два варіанти доповнюють стандартний початковими текстами візуальних компонентів, різномасштабним словником даних, новими функціями мови запитів SQL для бази даних, пакетом підтримки систем Internet, службою моніторингу програм, а також рядом інших засобів.

Builder C++ підтримує зв'язок з різними базами даних 3-х видів: dBASE і Paradox; Sybase, Oracle, InterBase і Informix; Excel, Access, FoxPro і Btrieve. Механізм BDE (Borland Database Engine) додає обслуговуванню зв'язків з базами даних дивовижну простоту і прозорість. Провідник Database Explorer дозволяє зображати зв'язки і об'єкти баз даних графічно. Використовуючи компоненти баз даних, я побудував електронний записник згідно таблиці dBASE за півгодини роботи на комп'ютері. Спадкоємство готових форм і їх "підгонка" під специфічні вимоги помітно скорочують тимчасові витрати на вирішення подібних завдань.

Довідкова служба Builder C++ надавала мені допомогу в цій і багатьох інших подібних ситуаціях. Є повний опис кожного управляемого компонента, включаючи списки властивостей і методів, а також численні приклади. Виклад матеріалу в книзі був значно покращуваний і систематизований завдяки

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

відомостям, почерпнутим мною з довідкової служби.

Завдяки засобам управління проектами, двосторонній інтеграції застосунку і синхронізації між засобами візуального і текстового редагування, а також вбудованому відладнику (з асемблерним вікном прокрутки, покрокового виконання, точок останову, трасуванням і тому подібне) – Builder C++ корпорації Borland надає собою вражаюче середовище розробки, яка, мабуть, витримає конкурентну боротьбу з такими модними продуктами як Developer Studio фірми Microsoft.

### 2.3 Розгорнута постановка завдання

Згідно з технічним завданням на кваліфікаційну бакалаврську роботу, реалізації підлягає програмне забезпечення, яке призначено для системи NB-ІоТ.

В процесі розробки кваліфікаційної бакалаврської роботи необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформулювати висновки про виконаний обсяг робіт та одержані результати.

Кафедра КБПЗ – 2021 рік

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

## 3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

### 3.1 Опис функціонування системи

Інтернет речей (Internet of Things, IoT) – новітній етап тривалої революції, що й ще не закінчився, в області обчислювальних систем і засобів зв'язку. Його розмір, різноманіття й вплив на повсякденне життя, комерційну діяльність і державне керування затьмарюють попередню історію технічного прогресу. IoT – це термін, яким позначається всі комплекс, що розростається, підключених друг до друга інтелектуальних пристроїв, від побутової техніки до малюсінських датчиків. Домінантною темою є вбудовування мобільних приймачепередатчиків малого радіуса дії в різноманітні гаджети й предмети повсякденного побуту, що відкриває нові форми комунікації між людьми й речами, а також між різними речами. Сьогодні Інтернет забезпечує з'єднання між собою мільярдів промислових і побутових предметів, як правило, за допомогою хмарних систем. Такі предмети передають інформацію датчиків, діють у відповідності зі своїм оточенням, а іноді можуть самомодифікуватися, створюючи загальне середовище керування більшою системою, такий як завод або навіть місто [1].

«Речами» в інтернеті речей є, головним чином, глибоко вбудовані пристрої з такими відмінними рисами, як вузька смуга пропускання, збір даних з низькою повторюваністю й малий обсяг використовуваних даних. Ці пристрої обмінюються даними один з одним і надають дані через користувацькі інтерфейси. Деякі вбудовані пристрої IoT, такі як охоронні відеокамери високого дозволу, відеотелефони VoIP і деякі інші, вимагають для роботи ширококутового стримінгу. Але незліченне число інших продуктів вимагає передачі пакетів даних усього лише час від часу.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

У цьому розділі ми приведемо огляд IoT, а потім розглянемо мережну архітектуру й архітектуру безпеки IoT, які допоможуть у розробці, реалізації й розгортанні IoT.

Інтернет, що розвивається, охоплює мільярди об'єктів, що використовують стандартні архітектури комунікації для надання послуг кінцевим користувачам. Ця еволюція створює нові взаємодії між фізичним миром і миром обчислень, цифрового контенту, аналізу, застосунків і послуг. Виниклий у результаті інтернет речей (IoT) відкриває безпрецедентні можливості користувачам, виготовлювачам пристроїв і постачальникам послуг у самих різних секторах. У числі напрямків, яким підуть на користь можливості збору даних, автоматизації й аналізу, надавані IoT, – охорона здоров'я й фітнес-індустрія, моніторинг і автоматизація житлових будинків, енергозбереження й «інтелектуальна електромережа», сільське господарство, транспорт, екологічний моніторинг, інвентаризація й керування продукцією, безпека, відеоспостереження, утвір і багато інші.

Технологічний розвиток відбувається в багатьох областях. Не дивно, що дослідженні бездротових мереж й зараз, й вже досить тривалий час, щоправда, раніше вони називалися інакше: мобільні обчислення, що всепроникаючий комп'ютинг, бездротові сенсорні й кіберфізичні мережі.

Розроблено безліч пропозицій і продуктів в області енергоефективних протоколів, безпеки й конфіденційності, адресації, економічних радіо, енергозберігаючих схем для продовження терміну служби батарейок, надійності мереж, складених з ненадійних і безсистемно «, що засинають» вузлів. Подібний прогрес в області бездротових технологій життєво важливий для росту IoT. Крім того, мають місце такі напрямки розробки, як додання IoT-пристроям можливості взаємодії із соціальними мережами, використання міжмашиної взаємодії, зберігання й обробка більших обсягів інформації в реальному часі, програмування застосунків, що надають кінцевим користувачам інтелектуальні й корисні інтерфейси із цими пристроями й даними.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

Багато ділилися своїм баченням IoT. Stankovic [2] говорить про переваги для людей, таких як переклад повсякденної діяльності в цифрову сферу; використання фрагментів біоничної шкіри для комунікації з навколишніми інтелектуальними об'єктами для більшого комфорту, здоров'я й безпеки; інтелектуальний годинник і натільний пристрої, оптимізуючі доступ до міських послуг. Серед переваг для міста можна назвати відсутність затримок на транспорті за рахунок відмови від світлофорів і використання 3D-транспортних пристроїв. Інтелектуальні будинки можуть не тільки контролювати енергоспоживання й безпека, але й підтримувати діяльність для зміцнення здоров'я. Так само, як люди одержали нові способи доступу до навколишнього світу за допомогою смартфонів, IoT створить нову парадигму в тому плані, що надасть нам безперервний доступ до необхідної інформації й послугам.

По оцінках Cisco, за наступне десятиліття чистий прибуток економіки IoT складе \$14,4 трлн [3]. Згідно з дослідженнями компанії, у цьому відіграють роль п'ять основних рушійних сил:

- Використання активів (\$2,5 трлн): IoT скорочує витрати на продажі, загальні й адміністративні витрати й вартість проданих товарів, оптимізуючи виконання й ефективність бізнес-процесів.

- Продуктивність праці (\$2,5 трлн): IoT підвищує продуктивність праці за рахунок ефективного використання людино-годин.

- Ланцюжка поставок і логістика (\$2,7 трлн): IoT знижує кількість відходів і підвищує ефективність процесів.

- Задоволеність клієнтів (\$3,7 трлн): IoT підвищує цінність для замовника й збільшує частку ринку, додаючи нових клієнтів.

- Інновації, включаючи зниження часу виходу на ринок (\$3,0 трлн): IoT підвищує віддачу від вкладень у НДОКР, знижує час виходу на ринок і створює додаткові потоки доходів за рахунок нових бізнес-моделей і можливостей.

Аналогічно опублікований в 2015 році звіт Mckinsey Global Institute [4] констатує, що прогнозований загальний економічний ефект IoT зараз становить

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

\$3,9 трлн, а до 2025 року досягнеться 11,1 трлн. По самій верхній оцінці обсяг цього ефекту – включаючи додаткові доходи від споживачів – до 2025 року буде еквівалентний 11% світової економіки.

### Масштаб інтернету речей

Відділ стандартів зв'язки МСЕ (Міжнародний союз електрозв'язку, International Telecommunication Union) опублікував Рекомендацію Y.2060, озаглавлену «Огляд інтернету речей» (Overview of the Internet of Things) [5]. У цьому документі втримуються наступні визначення, що описують охопат IoT:

– Інтернет речей (IoT): Глобальна інфраструктура для інформаційного суспільства, яка забезпечує можливість надання більш складних послуг шляхом з'єднання один з одним (фізичних і віртуальних) речей на основі існуючих, що й розвиваються функціонально сумісних інформаційно-комунікаційних технологій.

– Річ: Стосовно до інтернету речей означає предмет фізичного миру (фізичні речі) або інформаційного миру (віртуальні речі), який може бути ідентифікований і інтегрований у мережі зв'язку.

– Пристрій: Стосовно до інтернету речей означає елемент устаткування, який має обов'язкові можливості зв'язку й додатковими можливостями виміру, спрацьовування, а також уведення, зберігання й обробки даних.

У більшості літератури IoT вважається пов'язаним з комунікацією між інтелектуальними предметами. Рекомендація Y.2060 поширює цю концепцію на віртуальні речі – нижче ми розглянемо це докладніше. Згідно з Рекомендацією Y.2060, IoT характеризується додаванням виміру “комунікація між будь-якими РЕЧАМИ” до технологій інформації й зв'язки, які вже забезпечують комунікацію “у будь-який ЧАС” і “у будь-якому МІСЦІ”.

У книзі Designing the Internet of Things [6] елементи IoT зведені в просту формулу:

Фізичні об'єкти + контролери, сенсори, виконавчі механізми + Інтернет = IoT

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

Ця формула чітко описує саму суть інтернету речей. Екземпляр IoT складається з набору фізичних об'єктів, кожний з яких:

- містить мікроконтролер, що забезпечує інтелектуальність;
- містить датчик, що вимірює який-небудь фізичний параметр, і/або виконавчий механізм, що спрацьовує від якого-небудь фізичного параметра;
- має можливість комунікації по Інтернеті або якій-небудь іншій мережі.

Елементом, що не входять у цю формулу й охопленим визначенням по У.2060, є спосіб ідентифікації окремої речі, звичайно називаний тегом.

Зверніть увагу, що хоча в літературі завжди використовується термін «інтернет речей», точніше було б назвати його мережею речей, оскільки мова йде не про «великий» Інтернет (тому «інтернет речей» і пишеться по-російському з маленької букви – переу.). Наприклад, інсталяція «розумного будинку» складається з набору речей у будинку, що обмінюються інформацією з Wi-Fi або Bluetooth із центральним контролером. На заводі або фермі інтернет речей може підтримувати корпоративні застосунки, які будуть взаємодіяти із середовищем і запускати застосунки, що використовують інтернет речей. У цих прикладах дистанційний доступ по Інтернеті звичайно є, але його може й не бути. Незалежно від того, чи є таке підключення до Інтернету чи ні, набір «розумних» об'єктів на майданчику, у комплекті з будь-якими іншими обчислювальними пристроями й пристроями зберігання, можна охарактеризувати як «мережа речей» або «інтернет речей» (з маленької букви).

### **Стандарти сумісності IoT**

Найближчим часом різнорідні «острівці» розв'язків, швидше за все, будуть обганяти у своєму розвитку розгортання IoT-розв'язків, заснованих на функціонально-сумісних стандартах. Так обстають справи з кожної новою технологією на етапі її зародження. Наприклад, Sutaria and Govindachari [8] відзначають, що дві характеристики мережних IoT-пристроїв найбільші проблеми, що викликає, – це наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу місяцями й роками без підзарядки) і частий обмін

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

даними по мережах із втратою пакетів. Нинішні стандартні протоколи Інтернету в цих умовах неоптимальні. У більш широкому змісті має місце дисбаланс між величезною кількістю пристроїв, що генерують дані зі скаженою швидкістю в різних місцях, і використанням мережних технологій і хмарних систем, які зберігають величезні обсяги даних у невеликій кількості локацій при відносно низькій швидкості відновлення даних. Інтеграція цих двох класів систем для задоволення потреб користувачів вимагає певних можливостей від мережних протоколів у всій архітектурі мережі й протоколів, від фізичного рівня до прикладного.

Над розв'язком цих питань працює кілька організацій і стандартизаційних форумів, прагнучи розширити або адаптувати протоколи Інтернету для пристроїв IoT. Для створення єдиної структури й класифікації необхідних функцій по їхнім місці в стеці протоколів ряд цих груп також займається питанням формальної архітектури для IoT. У той час як існуючі й стандарти й Інтернет зробили IoT можливим, у найближчому майбутньому чи навряд можлива поява стека нових стандартів, які доповнять або модифікують існуючі для сфери IoT. Як і багато інші досягнення, що стали можливими завдяки Інтернету, IoT буде якийсь час стихійний розбудовуватися й проходити через процеси природного добору, поки поступово не виявляться життєздатні технології й механізми протоколів. У даному розділі ми розглянемо два напрямки роботи зі створення загальних концепцій, які можуть виявитися корисними в процесі, що вже йде, стандартизації.

### **Еталонна модель IoT від МСЕ-Т**

З урахуванням складності IoT має сенс створення архітектури, яка б специфікувала основні компоненти і їх взаємозв'язок. Архітектура IoT може надати наступні переваги:

– дати адміністраторові мережі або It-Менеджерові корисний контрольний список для оцінки функціональності й повноти пропозицій від різних постачальників;

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

- служити орієнтиром для розроблювачів у плані того, які функції потрібні в IoT і як вони взаємодіють;
- бути основою для стандартизації, стимулюючи сумісність і скорочення витрат.

У справжньому розділі ми приведемо огляд архітектури IoT, розроблювальної сектором стандартизації Міжнародного союзу електрозв'язку (МСЕ-Т або ІТУ-Т). У наступному розділі ми обговоримо архітектуру, розроблювальну Всесвітнім форумом IoT (IoT World Forum). Остання, створювана індустріальною групою, використовує корисний альтернативний підхід для розуміння масштабу й функціональності IoT.

Еталонна модель IoT від МСЕ-Т описана в Рекомендації Y.2060 [5]. На відміну від більшості інших еталонних моделей і архітектурних моделей, описаних у літературі, модель МСЕ-Т деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що висвічує елементи екосистеми IoT, які повинні бути з'єднані, інтегровані, керовані й надані застосункам. Детальна специфікація екосистеми описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, – той факт, що IoT на ділі не є мережею фізичних речей. Це скоріше мережа пристроїв, взаємодіючих з фізичними речами, разом із прикладними платформами – такими як комп'ютери, планшети й смартфони, – які взаємодіють із цими пристроями. Тому огляд моделі МСЕ-Т ми почнемо з обговорення пристроїв.

Нижче наведений список визначень ключових термінів з Рекомендації Y.2060.

**Мережа зв'язку (Communication Network):** інфраструктурна мережа, що з'єднує пристрої й застосунку, така як мережа на основі стека протоколів IP або Інтернет.

**Річ (Thing):** предмет фізичного миру (фізичні речі) або інформаційного миру (віртуальні речі), який може бути ідентифікований і інтегрований у мережі зв'язку.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

Пристрій (Device): елемент устаткування, який має обов'язкові можливості зв'язку й додатковими можливостями виміру, спрацьовування, а також уведення, зберігання й обробки даних.

Пристрій перенесення даних (Data-carrying Device): пристрій перенесення даних підключається до фізичної речі й непрямим образом з'єднує цю фізичну річ із мережами зв'язку. Прикладами можуть служити активні бирки RFID.

Пристрій збору даних (Data-capturing Device): під пристроєм збору даних розуміється зчитувальне/записуючий пристрій, що має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися непрямим образом за допомогою пристроїв перенесення даних або прямо за допомогою носіїв даних, підключених до фізичних речей.

Носій даних (Data Carrier): безбатарейний об'єкт перенесення даних, підключений до фізичної речі, що й має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає штрих-коди й QR-коди, наклеєні на фізичні речі.

Сенсорний пристрій (Sensing Device): пристрій, який може виявляти або вимірювати інформацію, що ставиться до навколишнього середовища, і перетворювати її в цифрові електричні сигнали.

Виконавчий пристрій (Actuating Device): пристрій, який може перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, у дії.

Пристрій загального призначення (General Device): пристрій загального призначення має вбудовані можливості обробки й зв'язку й може обмінюватися даними з мережами зв'язку з використанням провідних або бездротових технологій. Пристрою загального призначення включають устаткування й прилади, що ставляться до різних областей застосування IoT, наприклад, верстати, побутові електроприлади й смартфони.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

Шлюз (Gateway): елемент IoT, що з'єднує пристрої з мережами зв'язку. Він виконує необхідну трансляцію між протоколами, використовуваними в мережах зв'язку й у пристроях.

Унікальним аспектом IoT, у порівнянні з іншими мережними системами, очевидно є наявність безлічі фізичних речей і пристроїв, відмінних від обчислювальних пристроїв і пристроїв обробки даних. Модель розглядає IoT як мережу пристроїв, тісно пов'язаних з речами. Сенсорні й виконавчі пристрої взаємодіють із фізичними речами в навколишньому середовищі. Пристрої збору даних зчитують дані з фізичних речей або записують дані на фізичні речі шляхом взаємодії із пристроями перенесення даних або носіями даних, підключеними або пов'язаними з фізичним об'єктом тем або іншим способом.

Ця модель проводить відмінність між пристроями перенесення даних і носіями даних. Пристрій перенесення даних є пристроєм у змісті Рекомендації Y.2060. Як мінімум, пристрій завжди має можливість зв'язку й може мати інші електронні можливості. Прикладом пристрою перенесення даних є Rfid-Бирка. У той же час носій даних – це елемент, приєднаний до фізичної речі з метою ідентифікації або інформування.

У Рекомендації Y.2060 відзначається, що технології, використовувані для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне й гальванічне порушення. Приклади кожної з них:

– Радіочастотні: радіочастотні ідентифікаційні (RFID)-бирки, або радіомітки.

– Інфрачервоні: інфрачервоні мітки, використовувані в Збройних Силах, лікарнях і інших середовищах, де потрібно відслідковувати розташування й переміщення персоналу. інфрачервоні нашивки, Що це й відбивають, на військовій формі, що й працюють від батарейок бейджи, що випромінюють ідентифікаційну інформацію. Останні можуть містити кнопку, при натисканні якої бейдж може використовуватися для проходу через портал, і бейджи, що

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

автоматично повторюють сигнал для контролю над переміщеннями персоналу. Пульти дистанційного керування, використовувані в побуті або в інших середовищах для керування електронними пристроями, теж можна легко інтегрувати в IoT.

– Оптичні: штрих-коди й QR-коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.

– Гальванічне порушення: прикладом можуть служити медичні імпланти, що використовують електропровідні властивості людського тіла [9]. У ході комунікації між імплантом і поверхнею гальванічна пара передає сигнали з імпланта на електроди, виведені на шкіру. Ця схема використовує дуже мало енергії, що дозволяє знизити розмір і складність імплантованого пристрою.

Останнім типом пристроїв є пристрої загального призначення. Вони мають можливості обробки даних і зв'язку, які можуть бути інтегровані в IoT. Гарним прикладом є технологія «розумного будинку», яка може інтегрувати практично будь-який пристрій у будинку в мережу для централізованого або дистанційного керування.

Є ще один пристрій, пов'язане з IoT: шлюз. Як мінімум шлюз працює транслятором між протоколами. Шлюзи вирішують одну з головних проблем при проектуванні IoT, а саме проблему сумісності, як між різними пристроями, так і між пристроями й Інтернетом або корпоративною мережею. «Розумні» пристрої підтримують широкий спектр бездротових і провідних технологій передачі даних і мережних протоколів. Крім того, можливості обробки даних у таких пристроїв, як правило, обмежені.

Рекомендація Y.2067 [10] закріплює вимоги до шлюзів IoT, які звичайно розпадаються на три категорії:

– Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроям обмінюватися даними один з одним і з мережею – Інтернетом або корпоративною мережею, що містить застосунок IoT. Такі схеми доступу можуть, наприклад, включати Zigbee, Bluetooth і Wi-Fi.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

– Шлюз підтримує необхідні мережні технології як для локальних, так і для глобальних мереж. Ці технології можуть містити в собі Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, DSL і кабельний доступ до Інтернету й глобальним корпоративним мережам.

– Шлюз підтримує взаємодія з застосунками, керування мережею й функції безпеки.

Дві перші вимоги містять у собі трансляцію протоколів між різними мережними технологіями й стеками протоколів. Третя вимога звичайна називається функцією IoT-агента. По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних з декількох пристроїв для передачі в IoT-застосунки, забезпечення протоколів і функцій безпеки й взаємодія із системами керування мережею.

Тут слід зазначити, що термін «мережа зв'язки» прямо не визначається в серії IoT-стандартів Y.206x. Мережа (або мережі) зв'язку підтримує зв'язок між пристроями й може безпосередньо підтримувати прикладні платформи. Вона може мати розміри невеликого IoT, такого як домашня мережа «розумних» пристроїв. У більш загальному змісті мережа (або мережі) пристроїв з'єднується з корпоративними мережами або Інтернетом для зв'язку із системами застосунків і серверами, на яких розташовані бази даних, пов'язані з IoT.

Перша можливість – зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу сенсорне або виконавчий пристрій з підтримкою Bluetooth може здійснювати зв'язок із пристроєм збору даних або пристроєм загального призначення, що використовують Wi-Fi. Друга можливість – зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої в мережі «розумного будинку» підтримують Bluetooth, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою Bluetooth. Третя можливість – прямий зв'язок пристроїв між собою по окремій локальній мережі, у той час як зв'язок із зовнішньою мережею (на рисунку не показана) здійснюється через шлюз LAN. Приведемо приклад такої можливості. Уявіть собі, що на великій території, наприклад, на

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

фермі або заводі, перебуває велика кількість датчиків з низьким енергоспоживанням. Ці пристрої взаємодіють між собою для послідовної передачі даних на пристрій, підключене до шлюзу в мережу зв'язку.

Кожна фізична річ в інтернеті речей може бути представлено в інформаційному світі однієї або декількома віртуальними речами, але при цьому віртуальна річ може існувати без відповідної фізичної речі. Фізичні речі зіставлені віртуальним речам, що зберігаються в БД і інших структурах даних. Застосунки обробляють віртуальні речі й працюють із ними.

Еталонна модель IoT від МСЕ-Т, що полягає із чотирьох рівнів плюс можливості керування й безпеки, що діють між рівнями. Дотепер ми говорили про рівень пристрою. У термінах функціональності зв'язки рівень пристрою містить у собі, грубо говорячи, фізичний і канальний рівні OSI. Тепер перейдемо до інших рівнів.

Рівень мережі виконує дві базові функції. Можливості мережі ставляться до взаємодії пристроїв і шлюзів. Транспортні можливості ставляться до транспорту інформації служб і застосунків IoT, а також інформації керування й контролю IoT. Грубо говорячи, ці можливості відповідають мережному й транспортному рівням OSI.

Рівень підтримки послуг і підтримки застосунків надає можливості, які використовуються застосунками. Багато різноманітних застосунків можуть використовувати загальні можливості підтримки. До прикладів ставляться загальна обробка даних і керування БД. Спеціалізовані можливості підтримки – це конкретні можливості, які призначені для задоволення потреб конкретної підмножини застосунків IoT.

Рівень застосунку складається із усіх застосунків, взаємодіючих з IoT-пристроями.

Рівень можливостей керування охоплює традиційні функції керування мережею, тобто керування несправностями, керування конфігурацією, керування обліком, керування показниками роботи й керування безпекою.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

У Рекомендації Y.2060 у якості прикладів загальних можливостей керування перераховані:

– керування пристроями: приклади включають виявлення пристроїв, автентифікацію, дистанційну активацію й деактивацію пристроїв, конфігурацію, діагностику, відновлення прошивання й/або ПЗ, керування робочим статусом пристрою;

– керування топологією локальної мережі: прикладом є керування конфігурацією мережі;

– керування трафіком і перевантаженнями: наприклад, виявлення умов перевантаженості мережі й реалізація резервування ресурсів для термінових і/або життєво важливих потоків трафіка.

Спеціалізовані можливості керування тісно пов'язані з вимогами застосунків, наприклад, вимогами по контролю лінії передачі електроенергії в «розумній» електромережі.

Рівень можливостей забезпечення безпеки включає загальні можливості забезпечення безпеки, які не залежать від застосунків. У Рекомендації Y.2060 приклади загальних можливостей забезпечення безпеки включають:

– на рівні застосунку: авторизацію, автентифікацію, захист конфіденційності й цілісності даних застосунки, захист недоторканності приватного життя, аудит безпеки й антивірусний захист;

– на рівні мережі: авторизацію, автентифікацію, конфіденційність даних про використання й даних сигналізації, а також захист цілісності даних сигналізації;

– на рівні пристрою: автентифікацію, авторизацію, перевірку цілісності пристрою, керування доступом, захист конфіденційності й цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами застосунків, наприклад, вимогами безпеки мобільних платежів.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

## Еталонна модель Всесвітнього форуму IoT

Всесвітній форум IoT (IoT World Forum, IWF) – спонсуєма галуззю щорічна подія, що поєднує представників бізнесу, держструктур і вузівської науки з метою просування IoT на ринок. Комітет з архітектури Всесвітнього форуму IoT, складений з лідерів індустрії, включаючи IBM, Intel і Cisco, у жовтні 2014 року опублікував еталонну модель IoT. Ця модель служить загальною структурою, покликаною допомогти галузі прискорити розгортання IoT. Модель призначена для того, щоб стимулювати співробітництво й сприяти створенню повторюваних моделей впровадження.

Ця еталонна модель є корисним доповненням до моделі MCE-T. Документи MCE-T наголошують на рівнях пристрою й шлюзу, описуючи верхні рівні лише загальною. І дійсно, у Рекомендації Y.2060 увесь опис рівня застосунку вмістився в одну фразу. Найбільша увага рекомендації серії Y.206x приділяють визначенню концепції для підтримки розробки стандартів взаємодії із пристроями IoT.

IWF стурбований більш масштабним питанням розробки застосунків, проміжного ПЗ й функцій підтримки для корпоративного інтернету речей.

Документальний опис моделі IWF, опубліковане Cisco [11], указує, що розроблена модель відрізняється наступними характеристиками:

- спрощує: допомагає розбити складні системи на частині так, щоб кожна із цих частин стала зрозуміліше;
- проясняє: надає додаткові відомості для точної ідентифікації рівнів IoT і виробітку загальної термінології;
- ідентифікує: ідентифікує аспекти, у яких ті або інші типи обробки оптимізовані в різних частинах системи;
- стандартизує: являє собою перший крок до того, щоб постачальники могли створювати продукти IoT, здатні взаємодіяти один з одним;
- організує: робить IoT реальним і доступним, а не просто абстрактною концепцією.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

Рівень 1 утворюють фізичні пристрої й контролери, які можуть управляти декількома пристроями. Рівень 1 моделі IWF приблизно відповідає рівню пристрою в моделі MCE-T. Як і в моделі MCE -T, елементи на цьому рівні – не фізичні речі як такі, а пристрою, взаємодіючі з фізичними речами, такі як сенсорні й виконавчі пристрої. Серед інших можливостей ці пристрої можуть уміти здійснювати аналого-цифрове й цифро-аналогове перетворення, генерацію даних, а також підтримувати дистанційне опитування й/або дистанційне керування.

З логічної точки зору цей рівень реалізує зв'язок пристроїв між собою й між пристроями й низькорівневою обробкою на рівні 3. З фізичної точки зору цей рівень складається з мережних пристроїв, таких як маршрутизатори, комутатори, шлюзи й брандмауери, використовуваних для створення локальних і глобальних мереж і підключення до Інтернету. Цей рівень дозволяє пристроям здійснювати зв'язок один з одним і за допомогою більш високих логічних рівнів обмінюватися даними із прикладними платформами, такими як комп'ютери, пристрої дистанційного керування й смартфони.

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі MCE-T. Основна відмінність у тому, що модель IWF відносить шлюзи до рівня 2, у той час як у моделі MCE-T вони ставляться до рівня 1. Оскільки шлюз є мережним пристроєм і пристроєм зв'язки, віднесення його до рівня 2 має більше змісту.

У багатьох впроваджуваних системах IoT розподілена мережа датчиків може генерувати більші обсяги даних. Наприклад, офшорні нафтові родовища й нафтопереробні заводи можуть генерувати до терабайта даних щодня. Літак може генерувати трохи терабайт даних у годину. Замість того, щоб зберігати всі ці дані постійно (або хоча б довгий час) у централізованому сховищі, доступному для застосунків IoT, часто більш доцільно виконувати як можна більшу частину обробки даних якнайближче до датчиків. Тому завданням рівня периферійних обчислень (edge computing level) є перетворення мережних потоків даних в інформацію, придатну для зберігання й більш високорівневої обробки. Елементи

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

обробки на цьому рівні можуть мати справу з великими обсягами даних і виконувати операції перетворення даних, у результаті яких зберігати доводиться вже набагато менший обсяг. Опублікований Cisco документ по моделі IWF [11] містить наступні приклади операцій на рівні периферійних обчислень:

- аналіз: аналіз даних за критеріями того, чи підлягають вони обробці на більш високому рівні;
- форматування: переформатування даних для однакової високорівневої обробки;
- розархівування/декодування: обробка криптографічних даних з додатковим контекстом (таким як походження);
- дистилляція/скорочення: скорочення й/або резюмування даних для того, щоб мінімізувати ефект на обсяг даних і трафік у мережі й у високорівневих системах обробки;
- оцінка: визначення того, чи представляють дані граничне значення або аварійний сигнал; цей процес повинен включати перенапрямок даних додатковим одержувачам.

Елементи обробки на цьому рівні відповідають пристроям загального призначення в моделі МСЕ-Т. Як правило, вони розгортаються фізично на краю мережі IoT, тобто поруч із сенсорами й іншими пристроями генерації даних. Таким чином, частина базової обробки більших обсягів генеруємих даних знімається із прикладних програм IoT, розташованих центрально.

Обробка на рівні периферійних обчислень іноді називається мрячними обчисленнями (Fog Computing). Мрячні обчислення й мрячні служби, як очікується, стануть відмітною характеристикою IoT. Цей принцип проілюстрований на мал. 6. Мрячні обчислення представляють у сучасних мережних технологіях тренд, протилежний хмарним обчисленням. У хмарних обчисленнях великий обсяг централізованих ресурсів зберігання й обробки даних доступний розподіленим споживачам за допомогою хмарних мережних структур для відносно невеликого числа користувачів. У мрячних обчисленнях велике

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

число окремих інтелектуальних об'єктів здійснюють зв'язок із мрячними мережними структурами, які здійснюють обчислення й зберігають ресурси поруч із периферійними пристроями в IoT. Мрячні обчислення вирішують проблеми, що виникли внаслідок діяльності тисяч або мільйонів «розумних» пристроїв, включаючи проблеми безпеки, конфіденційності, обмежених можливостей мережі й затримки. Термін «мрячні обчислення» обраний тому, що туман стелиться по землі, у той час як хмари перебувають високо в небі.

На рівні 4, рівні нагромадження даних, дані, що зробили з різних пристроїв, профільтровані й оброблені рівнем периферійних обчислень, містяться в сховище, де будуть доступні для більш високих рівнів. Цей рівень різуче відрізняється й від низькорівневих (мрячних), і від високорівневих (хмарних) обчислень по особливостях конструкції, вимогам і методам обробки.

Дані, що проходять крізь мережу, називаються «даними в русі». Швидкість і організація даних у русі визначається пристроями, що генерують дані. Генерація даних відбувається по подіях, або періодично, або по виникненню якої-небудь події в середовищі. Для збору даних і їх обробки необхідно реагувати на їхню появу в реальному часі. Напроти, багатьом застосункам не потрібно обробляти дані зі швидкістю мережної передачі. На практиці ні хмарна мережа, ні прикладні платформи не змогли б устигати за обсягами даних, генеруємих гігантською кількістю IoT-пристроїв. Замість цього застосунку мають справа з «даними в спокої», тобто даними в тому або іншому легкодоступному сховищі. Застосунки можуть звертатися до даних у міру необхідності або поза режимом реального часу. Таким чином, високі рівні функціонують за принципом транзакцій, у той час як три нижні рівні працюють по подіях.

Нижче перераховані названі в [13] операції, виконувані на рівні нагромадження даних:

- перетворення «даних у русі» в «дані в спокої»;
- перетворення формату з мережних пакетів у реляційні таблиці БД;

- перехід від обчислень по подіях до обчислень по запиту;
- значне зниження обсягу даних за рахунок фільтрації й вибіркового зберігання.

Ще один погляд на рівень нагромадження даних полягає в тому, що він являє собою границю між інформаційними технологіями (ІТ), під якими розуміється цілий спектр технологій обробки інформації, включаючи ПЗ, устаткування, технології зв'язку й супутні служби, і операційними технологіями (Operational Technology, ОТ), що представляють собою устаткування й ПЗ, що виявляють або зухвалі зміни шляхом прямого моніторингу й/або контролю фізичних пристроїв, процесів і подій на підприємстві.

Рівень нагромадження даних усмоктує велика кількість даних і поміщає їх у сховище, практично не пристосовуючи до потреб конкретних застосунків або груп застосунків. З рівня периферійних обчислень у сховище може надходити безліч різних видів даних у різних форматах і від різнорідних оброблювачів. Рівень абстракції даних може агрегувати і форматовувати такі дані способами, які роблять доступ застосунків більш керованим і ефективним. У числі зв'язаних завдань можуть бути наступні:

- Комбінування даних з різних джерел, включаючи вивірку декількох форматів даних.
- Виконання необхідних перетворень для забезпечення однакової семантики даних з різних джерел.
- Приміщення відформатованих даних у відповідну базу даних, наприклад, більші обсяги повторюваних даних містяться в систему більших даних, таку як Hadoop. Дані подій направляються в реляційну СУБД, що відрізняється більш швидким часом реакції й адекватним інтерфейсом для таких типів даних.
- Оповіщення застосунків більш високого рівня про те, що дані заповнені або досягнуть певний рівень даних.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

– Консолідація даних в одному місці ( за допомогою ETL (extract, transform, load), ELT (extract, load, transform) або реплікації даних) або надання доступу до декільком джерелам даних шляхом віртуалізації даних.

– Захист даних шляхом відповідної автентифікації й авторизації.

– Нормалізація/денормалізація й індексація даних для швидкого доступу застосунків.

Рівень застосунку містить застосунки будь-якого типу, що використовують дані IoT на вході або керуючі IoT-пристроями. Як правило, застосунки взаємодіють із рівнем 5 і з даними в спокої, тому їм необов'язково функціонувати на швидкостях мережі. Слід передбачити спрощений режим роботи, який дозволить застосункам минути проміжні рівні й прямо взаємодіяти з рівнем 3 або навіть рівнем 2. Модель IWF не визначає застосунку по всій строгості, вважаючи цей аспект вихідним за рамки дискусії про модель IWT.

Рівень взаємодії й процесу з'явився в результаті визнання того, що IoT буде корисний лише тоді, коли з ним зможуть взаємодіяти люди. Цей рівень може включати кілька застосунків і обмін даними й/або керуючою інформацією з Інтернету або корпоративної мережі.

IWF вважає еталонну модель IoT прийнятої в галузі базовою структурою, спрямованої на стандартизацію концепцій і термінології, пов'язаних з IoT. Що ще більш важливо, модель IWF визначає необхідний функціонал і проблеми, які потрібно розв'язати до того, як галузь зможе реалізувати цінність IoT. Ця модель корисна як для постачальників, що розробляють функціональні елементи усередині моделі, так і для замовників, допомагаючи їм виробити свої вимоги й оцінювати пропозиції постачальників.

### **Фреймворк безпеки IoT**

Компанія Cisco Systems, що зіграла провідну роль у розробці моделі Всесвітнього форуму IoT, розробила фреймворк безпеки IoT [13], що став корисним доповненням до еталонної моделі Всесвітнього форуму IoT.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

Модель Cisco IoT являє собою спрощену версію моделі Всесвітнього форуму IoT. Вона складається з наступних рівнів:

– «Розумні» об'єкти/вбудовані системи: цей рівень містить у собі сенсорні/виконавчі пристрої й інші вбудовані системи на границі мережі. Ця частина IoT найбільш уразлива. Пристрої можуть перебувати в середовищі, не захищеної фізично, і від них може вимагатися функціонування протягом декількох років. Доступність теж є важливою проблемою. Крім того, менеджерам мережі необхідно опікуватися про автентичність і цілісності даних, генеруємих сенсорами, і про захист виконавчих пристроїв і інших «розумних» пристроїв від несанкціонованого використання. Також можуть бути присутнім такі вимоги, як конфіденційність і захист від підслуховування.

– Мрячна/периферійна мережа: цей рівень представляє провідні й бездротові з'єднання пристроїв IoT. Крім того, на цьому рівні може здійснюватися певний обсяг обробки й консолідації даних. Ключовою проблемою є більша варіативність мережних технологій і протоколів, використовуваних різними пристроями IoT, і необхідність виробітку й втілення єдиної політики безпеки.

– Ядро мережі: рівень ядра мережі надає шляху для передачі даних між платформами в центрі мережі й пристроями IoT. Тут проблеми безпеки ті ж, що в традиційних мережах. Однак величезна кількість прикінцевих вузлів, з якими треба взаємодіяти й управляти ними, створює значну проблему для безпеки.

– Центр даних/хмара: цей рівень містить платформи для застосунків, зберігання даних і керування мережею. IoT не привносить на цей рівень ніяких нових проблем безпеки, крім необхідності мати справу з гігантською кількістю окремих прикінцевих вузлів.

За допомогою цієї чотирьохрівневої архітектури модель Cisco визначає чотири загальні можливості безпеки, що охоплюють кілька рівнів:

– Безпека на основі ролей: системи керування доступом на основі ролей (Role-Based Access Control, RBAC) призначають права доступу ролям, а не

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

окремим користувачам. Користувачам, у свою чергу, зіставляються різні ролі, або статично, або динамічно, відповідно обов'язкам. RBAC широко використовується в комерційних хмарних і корпоративних системах. Цей інструмент, зрозумілий адміністраторам, може використовуватися для керування доступом до IoT-пристроїв і генеруємим ними даним.

– Захист від втручання й виявлення втручань: ця функція особливо важлива на рівні пристроїв і мрячної мережі, але поширюється також і на рівень ядра мережі. Усі ці рівні можуть використовувати компоненти, що фізично перебувають поза фізично охоронюваною територією підприємства.

– Захист даних і конфіденційність: ці функції охоплюють усі рівні архітектури.

– Захист протоколів Інтернету: захист «даних у русі» від підслуховування й перехоплення важлива для всіх рівнів.

У документі Cisco [13] також пропонується концепція безпеки IoT, що визначає компоненти функції безпеки для IoT, що охоплює всі рівні, як показано на мал. 8. Перелічимо чотири компоненти:

– Автентифікація: цей компонент охоплює елементи, що ініціюють доступ, і першою справою ідентифікує пристрою IoT. На відміну від типових корпоративних мережних пристроїв, для яких ідентифікація може здійснюватися по ідентифікаційних ознаках людини (таким як ім'я/пароль або бейдж), прикінцеві пристрою IoT повинні оснащуватися такими методами автентифікації, які не вимагають втручання людини. До таких методів ставляться радіочастотні мітки, сертифікати x.509 або Mac-адреси прикінцевих пристроїв.

– Авторизація: авторизація управляє доступом до пристрою через структуру мережі. Цей елемент містить у собі контроль доступу. Разом з рівнем автентифікації він виробляє необхідні параметри для того, щоб дозволити обмін інформацією між пристроями й між пристроями й прикладними платформами, тим самим забезпечуючи роботу IoT-служб.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

– Мережна політика: цей компонент охоплює всі елементи, що здійснюють маршрутизацію й транспортування трафіка з прикінцевих пристроїв по інфраструктурі, будь те контроль, керування або властиво трафік даних.

– Аналітика безпеки, включаючи видимість і контроль: цей компонент включає всі функції, необхідні для централізованого керування пристроями IoT. У першу чергу він охоплює видимість IoT пристроїв, що означає попросту те, що центральні функції керування безпечно сповіщені про парк розподілених пристроїв IoT, включаючи ідентичність і атрибути кожного пристрою. На основі такої видимості виникає здатність здійснювати контроль, включаючи конфігурацію, патчи й відновлення, а також контрзаходу для припинення погроз.

Важливим елементом цієї концепції є довірчі відносини. У цьому контексті довірчі відносини означають здатність двох партнерів по обміну бути впевненими в ідентичності й правах доступу один одного. Автентифікаційний компонент концепції довіри реалізує базовий рівень довіри, що доповнюється авторизаційним компонентом.

У документі Cisco [13] наведений приклад того, що автомобіль може встановити довірчий стосунки з іншою машиною того ж виготовлювача. Такі довірчі відносини, однак, можуть дозволити машинам обмінюватися тільки відомостями про безпеку. При встановленні довірчих відносин між тією ж самою машиною й дилерською мережею машина може передавати й одержувати додаткову інформацію, таку як показання одометра й результати останнього техобслуговування.

Відповідно процитованому вище звіту Mckinsey [4], приблизно 40% загальної економічної цінності IoT припадає на здатність усіх фізичних пристроїв «розмовляти» один з одним за допомогою комп'ютерів, тобто на сумісність. Якщо сумісність обмежена, то цінність IoT може скласти всього \$7 трлн, у той час як розвинений сумісність здатна довести цінність IoT для глобальної економіки до \$11 трлн до 2025 року. Приблизно 40% усієї можливої цінності залежить від здатності різних систем IoT взаємодіяти один з одним.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

Щоб добитися такого типу сумісності, який необхідний для розкриття цих переваг, необхідно виробити стандарти для всіх рівнів функціонала IoT, від рівня пристрою до рівня застосунку. Хоча ці стандарти поки ще перебувають у зародковому стані, описані в даному розділі архітектурні моделі є корисним базисом для майбутніх зусиль.

### 3.2 Розробка структурної схеми

Технологія NB-IoT багато чого успадкувала від LTE – починаючи з фізичної структури радіосигналу й закінчуючи архітектурою. Усі неможливо перелічити, тому спробуємо сфокусуватися на основних особливостях, заради яких і створювалася ця технологія.

#### Особливості радіосигналу NB-IoT:

Найважливіше в NB-IoT – можливість роботи при більш низьких рівнях сигналу й при високому рівні шумів, а також економія батареї. Також NB-IoT призначений для передачі коротких повідомлень, і від нього не потрібна передача аудіо-відео контенту, більших файлів і іншого.

Виходячи із цього, на фізичному рівні є певні особливості, які допомагають забезпечити необхідних характеристик:

- загальна смуга для NB-IoT обмежена в один RB шириною в 180кГц;
- радіотракт користувацького пристрою має всього одну антену, приймач і передавач;
- передача й приймання рознесене за часом, тобто це по суті напівдуплексний режим;
- можливість передавати в напрямку UL на одній, що піднесе;
- використовувані типи модуляції обмежені BPSK і QPSK;
- переповтори переданого сигналу (coverage enhancement).

Нижче ми зупинимося на деяких з них докладніше.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

Використання вузької смуги частот в один RB, однієї антени й напівдуплексного режиму передачі дозволяє спростити пристрій і досягти:

- зниження вимоги до процесорної потужності;
- зниження енергоспоживання;
- зменшення габаритів;
- здешевлення пристрою.

Для NB-IoT можуть використовуватися практично всі ті ж діапазони частот, що й для 2G/3G/4G в «низьких» band. Це B20 (800 МГц), B8(900 МГц), B3(1800 МГц). Більш «високі» частоти змісту використовувати немає через більше загасання сигналу.

У ядрі мережі відбулися значні зміни. Почнемо з того, що з'явився новий елемент, а також ряд механізмів, які визначені стандартом як “CIoT EPS Optimization” або оптимізації опорної мережі для стільникового інтернету речей.

Як відомо, у мобільних мережах існує два основні канали комунікацій, які називаються Control Plane (CP) і User Plane (UP). Control Plane призначений для обміну службовими повідомленнями між різними елементами мережі й служить для забезпечення мобільності (Mobility management) пристроїв (UE) і встановлення/підтримки сесії передачі даних (Session Management). User Plane – це, властиво, канал передачі користувацького трафіка.

Механізми оптимізації CP і UP для NB-IoT реалізуються на вузлах MME, SGW і PGW, які умовно поєднуються в єдиний елемент за назвою C-SGN (Cellular IoT Serving Gateway Node). Також стандарт припускає поява нового елемента мережі – SCEF (Service Capability Exposure Function). Інтерфейс між MME і SCEF називається T6a і реалізований на базі протоколу DIAMETER. Незважаючи на те, що DIAMETER це сигнальний протокол, в NB-IoT він адаптований для передачі малих обсягів non-IP даних.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38



пристроїв (UE), надаючи можливість серверам застосунків (Application Server, далі AS) одержувати дані й управляти пристроями через єдиний API інтерфейс.

Ідентифікатором UE стає не телефонний номер (MSISDN) або IP адреса, як це було в класичній мережі 2G/3G/LTE, а так званий «external ID», який визначений стандартом у звичному для розроблювачів застосунків форматі «<Local Identifier>@<Domain Identifier>». Це окрема більша тема, що заслуговує окремого матеріалу, тому докладно про це зараз говорити не будемо.

Тепер розберемося с найбільш значимими нововведеннями. «CIoT EPS Optimization» – це оптимізація механізмів передачі трафіка й керування абонентськими сесіями. От основні з них:

- Donas.
- NIDD.
- Механізми енергозбереження PSM і eDRX.
- HLCOM.

#### **Donas (Data over NAS):**

Це механізм, розроблений для оптимізації передачі малих обсягів даних.

У класичному LTE абонентський пристрій при реєстрації в мережі встановлює PDN connection (далі PDN) через eNodeB до MME-SGW-PGW. З'єднання Ue-eNodeB-Mme – це так званий “Signaling Radio Bearer” (SRB). При необхідності передати/одержати дані UE встановлює ще одне з'єднання з eNodeB – “Data Radio Bearer” (DRB), для передачі користувацького трафіка до SGW і далі на PGW (інтерфейси S1-U і S5 відповідно). По закінченню обміну й при відсутності трафіка протягом деякого часу (звичайно 5-20 секунд) ці з'єднання розриваються й пристрій переходить у режим очікування або “Idle Mode”. При необхідності обміну новою порцією даних SRB і DRB переустановлюються.

В NB-IoT передача користувацького трафіка може здійснюватися через сигнальний канал (SRB), у повідомленнях протоколу NAS (<http://www.3gpp.org/more/96-nas>). Установлення DRB більше не потрібно. Це

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

значно знижує сигнальне навантаження, заощаджує радіоресурси мережі й, найважливіше – продовжує строк життя батареї пристрою.

На ділянці eNodeB – MME користувацькі дані починають передаватися по інтерфейсу S1-MME, чого не було в класичній технології LTE, і використовується для цього протокол NAS, у якому з'являється “User data container”.

Для здійснення передачі “User Plane“ від MME до SGW з'являється новий інтерфейс S11-U, який призначений для передачі малих обсягів користувацьких даних. В основі протоколу S11-у лежить GTP-U v1, який використовується для передачі User Plane і на інших інтерфейсах мережі 3 Gpp-архітектури.

#### **NIDD (non-IP data delivery):**

У рамках подальшої оптимізації механізмів передачі малих обсягів даних, на додаток до вже існуючих типів PDN, таким як Ipv4, Ipv6 і Ipv4v6, з'явився ще один тип – non-IP. У цьому випадку UE не привласнюється IP адреса, і дані передаються без використання протоколу IP. На тобто кілька причин:

– IoT пристрою, такі як датчики, можуть передавати дуже малі обсяги даних, 20 байт і навіть менше. Враховуючи, що мінімальний розмір IP заголовка – 20 байт, інкапсуляція в IP іноді може бути досить дорогим задоволенням;

– Немає необхідності реалізації в чипі Ip-стека, що веде до їхнього здешевлення (питання до обговорення в коментарях).

По великому рахунку, IP адреса необхідна IoT пристроям, щоб передавати дані через інтернет. У концепції NB-IoT SCEF виступає в ролі єдиної точки підключення AS, і обмін даними між пристроями й серверами застосунків відбувається за допомогою API. При відсутності SCEF non-IP дані до AS можуть передаватися через Point-to-Point (PtP) тунель від PGW і інкапсуляція в IP буде проводитися вже на ньому.

Усе це вписується в парадигму NB-IoT – максимальне спрощення й здешевлення пристроїв.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

## Механізми енергозбереження PSM і eDRX:

Одним із ключових переваг LPWAN мереж є енергоефективність. Заявляється строк до 10 років автономної роботи пристрою на одній батареї. Розберемося, яким образом досягаються такі значення.

Коли пристрій споживає найменше енергії? Правильно, коли воно виключене. І якщо повністю знеструмити девайс не можна, давайте знеструмимо радіо модуль, на той час, поки в ньому немає необхідності. Тільки попередньо треба погодити це з мережею.

### PSM (Power saving mode):

Режим енергозбереження PSM дозволяє пристрою надовго виключати радіо модуль, залишаючись при цьому зареєстрованим у мережі, і не переустановлювати PDN щораз при необхідності передати дані.

Щоб мережа знала, що пристрій як і раніше доступне, воно періодично ініціює процедуру актуалізації – Tracking Area Update (TAU). Частота цієї процедури задається мережею за допомогою таймера T3412, значення якого передається пристрою під час процедури Attach або чергового TAU. У класичному LTE дефолтне значення цього таймера 54 хвилини, а максимальне – 186 хвилин. Однак, для забезпечення високої енергоефективності, необхідність виходу в радіоефір кожні 186 хвилин – це занадто дороге задоволення. Для розв'язку цієї проблеми й був розроблений механізм PSM.

Пристрій активує режим PSM передаючи в повідомленнях «Attach Request» або «Tracking Area Request» значення двох таймерів T3324 і T3412-extended. Перший визначає час, який пристрій буде доступно після переходу в «Idle Mode». Другий – це час, через який повинен бути зроблений TAU, тільки тепер його значення може досягати 35712000 секунд або 413 днів. Залежно від налаштувань, MME може прийняти значення таймерів, отримані від пристрою, або змінити їх, передавши нові значення в повідомленнях «Attach Accept» або «Tracking Area Update Accept». Тепер пристрій може не включати радіо модуль 413 днів і залишатися при цьому зареєстрованим у мережі. У результаті

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

одержуємо колосальну економію ресурсів мережі й енергоефективність пристроїв!

Однак у цьому режимі пристрій недоступний тільки для вхідних комунікацій. При необхідності передати що-небудь у бік сервера застосунків пристрій може в будь-який момент вийти з PSM і відправити дані, залишившись після цього активним протягом таймера T3324 для приймання інформаційних повідомлень від AS (якщо такі будуть).

#### **eDRX (extended discontinuous reception):**

eDRX, розширений режим переривчастого приймання. Щоб передати дані на пристрій, який перебуває в «Idle mode», мережа виконує процедуру оповіщення – «Paging». При одержанні пейджинга пристрій ініціює встановлення SRB для подальшої комунікації з мережею. Але щоб не пропустити адресоване йому повідомлення Paging, пристрій повинний постійно моніторити радіоефір, що також досить енергозатратно.

eDRX – це режим, при якому пристрій ухвалює повідомлення від мережі не постійно, а періодично. Під час процедур Attach або TAU пристрій погоджує з мережею тимчасові проміжки, у які воно буде «слухати» ефір. Відповідно, у ці ж проміжки буде проводитися процедура Paging. У режимі eDRX робота пристрою розбивається на цикли (eDRX cycle). На початку кожного циклу йде так зване «вікно пейджинга» (Paging Time Window, далі PTW) – це час, який пристрій слухати радіоканал. По закінченню PTW пристрій відключає радіо модуль до кінця циклу.

#### **HLCOM (high latency communication):**

При необхідності передати дані в Uplink пристрій може вийти з кожного із цих двох режимів енергозбереження, не чекаючи закінчення PSM або eDRX циклу. Але от передати дані на пристрій можливо, тільки коли воно активно.

Функціонал HLCOM або комунікація з високими затримками – це буферизація Downlink пакетів на SGW на час, поки пристрій перебуває в режимі енергозбереження й недоступно для комунікації. Буферизовані пакети будуть

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

доставлені, як тільки пристрій вийде з PSM, зробивши TAU або передавши Uplink трафік, або, коли настане PTW.

Це, безумовно, вимагає усвідомлення з боку розроблювачів IoT-продуктів, оскільки спілкування із пристроєм виходить не в реальному часі й вимагає певного підходу до конструювання бізнес логіки роботи застосунків.

### 3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Нижче розглянемо її більш докладно. Модульна інтегрована NB-IoT дозволяє вибрати ті компоненти, які необхідні користувачеві.

#### Компоненти нижнього рівня

##### 1. Система Реального Часу Контролерів (СРЧК).

До складу базової версії середовища виконання контролерів входять:

- Модулі зв'язку зі станцією оператора.
- Модуль зв'язку зі станцією інжинірингу.
- Драйвери плат введення/виводу.
- Модуль сервера бази даних реального часу.
- Служба автовідновлення програм.
- Модуль візуалізації.
- Передача керування резервному процесорному модулю у випадку виходу з ладу основного процесорного модуля.
- Дзеркалізація даних з основного процесорного модуля контролера на резервний і забезпечення автоматичного відновлення інформації про зміни конфігурації на резервному процесорному модулі.
- Забезпечення ненаголошеного переходу регуляторів при переході з основного на резервний процесорний модуль.
- Передача керування резервному контролеру у випадку виходу з ладу процесорного модуля або модулів введення/виводу основного контролера.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

- Дзеркалізація даних з основного контролера на резервний, діагностика каналів передачі даних .
- Забезпечення ненаголошеного переходу регуляторів при переході з основного на резервний контролер або процесорний модуль.
- Синхронізація контролерів при старті (або команді оператора) шляхом повної дзеркалізації даних СРЧК по дубльованим мережам Ethernet.
- Збереження безперервності інформаційного обміну при відмові одного із процесорних модулів або каналів введення/виводу.
- Забезпечення ненаголошеного переходу регуляторів при відмові одного з контролерів кластера.

2. Модуль міжконтролерного обміну. Модуль міжконтролерного обміну призначений для створення розподілених систем з використанням обміну даними між декількома контролерами. Модуль виконує наступні функції:

- обмін оперативними й розрахунковими значеннями бази даних;
- обмін значеннями атрибутів змінні бази даних;
- підтримка резервування мережі Ethernet для міжконтролерного обміну;
- діагностика каналів зв'язку міжконтролерного обміну.

3. Модуль резервування мережі. Модуль робить діагностику мережі Ethernet для зв'язку із сервером БД/АБД, реєстрацію несправностей мережі й забезпечує можливість автоматичного переходу на резервну мережу у випадку відмови одного з каналів зв'язку.

4. Модуль реєстрації аварійних ситуацій (РАС). Модуль РАС використовується для реєстрації аварійних ситуацій у контролері, тобто для збереження заздалегідь заданих параметрів у певному інтервалі часу при виникненні аварійної ситуації. Модуль забезпечує період реєстрації від 50 мс.

Модуль виконує наступні функції:

- Підтримка двох режимів реєстрації РАС:
  - а) режим реєстрації значень параметрів із заданою періодичністю;
  - б) режим реєстрації значень параметрів по зміні.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

– Формування перед- і післяаварійних протоколів на енергонезалежному накопичувачі в контролері. Для перегляду протоколів РАС використовується спеціалізована програма верхнього рівня.

При цьому модуль має можливості:

- контролювати кілька РАС;
- задавати кілька умов формування РАС;
- налаштовувати період і глибину реєстрації.

5. Модуль функції регулювання. Модуль забезпечує підтримку регуляторів. Дозволяє створювати контури ПІД-регулювання (у тому числі каскадного й багатозв'язного). Користувальницькі алгоритми, розгалужена система сигналізацій, функції динамічних і статичних балансувань, компенсації люфтів, а також безліч інших додаткових налаштувань дозволяють реалізувати найрізноманітніші системи регулювання.

6. Зберігання архіву на контролері. Дозволяє формувати й зберігати архіви в пам'яті контролера. Архіви можуть зберігатися як в оперативній, так і в енергонезалежній пам'яті контролера залежно від розв'язуваного завдання.

7. Модуль ТМ-канал. ТМ-канал дозволяє організувати інформаційний обмін по повільних і нестійких каналах зв'язку. Ідеально підходить для зв'язку із пристроями по радіоканалі або GSM/ GPRS-каналу низької якості й т.п.

8. Бібліотека драйверів нижнього рівня. Дозволяє організувати інформаційний обмін між контролером під керуванням СРЧК і різноманітними приладами, модулями введення/виводу, панелями операторів, а також контролерами під керуванням власних ОС, таких як Omron, CIU 850 серії й т.д. Багато хто із драйверів мають додаткового функціонала, наприклад, дозволяють використовувати резервуємі канали зв'язку, зчитувати архіви приладів і т.д.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

9. OPC-сервер СРЧК (підтримка специфікації DA+HDA). Призначений для передачі оперативних і архівних даних відповідно до стандарту OPC з контролера під керуванням СРЧК у будь-які SCADA/HMI-системи сторонніх виробників (NB-ІоТ підтримує прямий інформаційний обмін з контролером), може бути використаний для одночасної передачі даних у кілька інформаційних систем верхнього рівня. Додаткове програмне забезпечення.

1. WEB-контроль для NB-ІоТ. Забезпечує перегляд поточної інформації у вигляді мнемосхем, друкованих документів, трендів, протоколу подій на будь-якому персональному комп'ютері за допомогою MS Internet Explorer. Взаємодіє із серверами БД і АБД. Підтримка списку улюблених кадрів. Захист від несанкціонованого доступу. Можлива робота як у режимі без функцій керування, так і з функціями керування.

2. Універсальний конвертер даних. Конвертує дані (у т.ч. друковані документи, тренди, протоколи повідомлень) у формат MS Excel і XML. Дозволяє робити вибірку по параметрах і за часом.

3. Архівний центр. Призначений для збору архівних і інших даних від різних АСУ ТП, побудованих на базі пакета NB -ІоТ для Windows, з подальшою можливістю їхнього перегляду. Має власний протокол подій, колірну й звукову сигналізацію, має можливість дубльованого копіювання даних. Для перегляду архівів на комп'ютері Архівного центра необхідно мати або Середовище Розробки (поставляється безкоштовно), або Універсальний конвертер даних.

4. Модуль модемних каналів зв'язку. Дозволяє будь-яким драйверам NB-ІоТ і OPC-серверам, використовувати GSM- і GPRS-канали стільникових мереж, лінії телефонної мережі, що комутирується, загального користування й інші модемні канали зв'язку.

5. Станція інжинірингу. Конфігурування й налаштування контролерів; діагностика роботи контролерів у режимі реального часу. Віддалене програмування контролерів під керуванням СРЧК. Крім того, станція

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

інжинірингу дозволяє робити діагностику каналів зв'язку, а також виконувати ряд додаткових сервісних функцій.

### Компоненти верхнього рівня

1. Середовище розробки. Головними функціями Середовища розробки є:

- Конфігурування системи контролю й керування.
- Створення й верифікація Бази Даних реального часу.
- Розробка графічного інтерфейсу користувача (відеокадрів бази даних).
- Вибір і налаштування алгоритмів керування.
- Імітація роботи системи контролю й керування.
- Створення ієрархічної (об'єктної) структури змінних БД.
- Створення й редагування користувальницьких скриптів.
- Надання програмного інтерфейсу (API) для створення прикладних програм користувача.

2. Сервер БД. Забезпечує виконання функцій обробки змінних БД, ведення оперативних трендів, програмного перезапуску, обробки подій, статистики, OPC-сервера, драйвера ODBC. OPC (OLE for Process Control) – набір повсюдно прийнятих специфікацій, що надають універсальний механізм обміну даними в системах контролю й керування. OPC технологія забезпечує незалежність споживачів від наявності або відсутності драйверів або протоколів, що дозволяє вибирати встаткування й програмне забезпечення, що найбільше повно відповідає реальним потребам бізнесу.

3. Сервер АБД. Забезпечує виконання всіх функцій Сервера БД (див. Сервер БД), а також функцій обробки й зберігання архівів трендів, протоколу подій, друкованих документів від року й більше.

4. Сервер вводу-виводу. Забезпечує організацію зв'язку різних УСО з NB-ІоТ через драйвери верхнього рівня, що підключаються, (не СРВ РС -сумісних контролерів), а також виконання стандартних обробок.

5. Графічний інтерфейс (з керуванням). Під керуванням розуміється можливість оператора за допомогою динамічних елементів (кнопка, поле

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		48

введення й т.п.) внесення змін у роботу АСУ ТП (наприклад, зміна завдання або коефіцієнтів налаштування регуляторів, включення/вимикання виконавчих механізмів, зміна границь сигналізації, керування каналами зв'язку й резервуванням і т.д.)

6. Графічний інтерфейс (без керування). Користувач не може вносити які-небудь зміни в хід технологічного процесу, крім квітування світлової й звукової сигналізації.

7. Перегляд архівів. Обов'язковий модуль для комплексів, що працюють із архівними даними. Забезпечує доступ до архівів трендів і до архівів протоколів подій.

8. Дзеркалізація 2-х серверів БД. Дзеркалізація (періодичне резервне копіювання в режимі on-line) даних з основного в резервний сервер. Мережа, по якій здійснюється дзеркалізація, призначається Користувачем на етапі генерації. Основний і резервний сервери БД встановлюються на двох різних АРМ. Дзеркалізуєма інформація: оперативна БД, тренди, друковані документи, протокол подій.

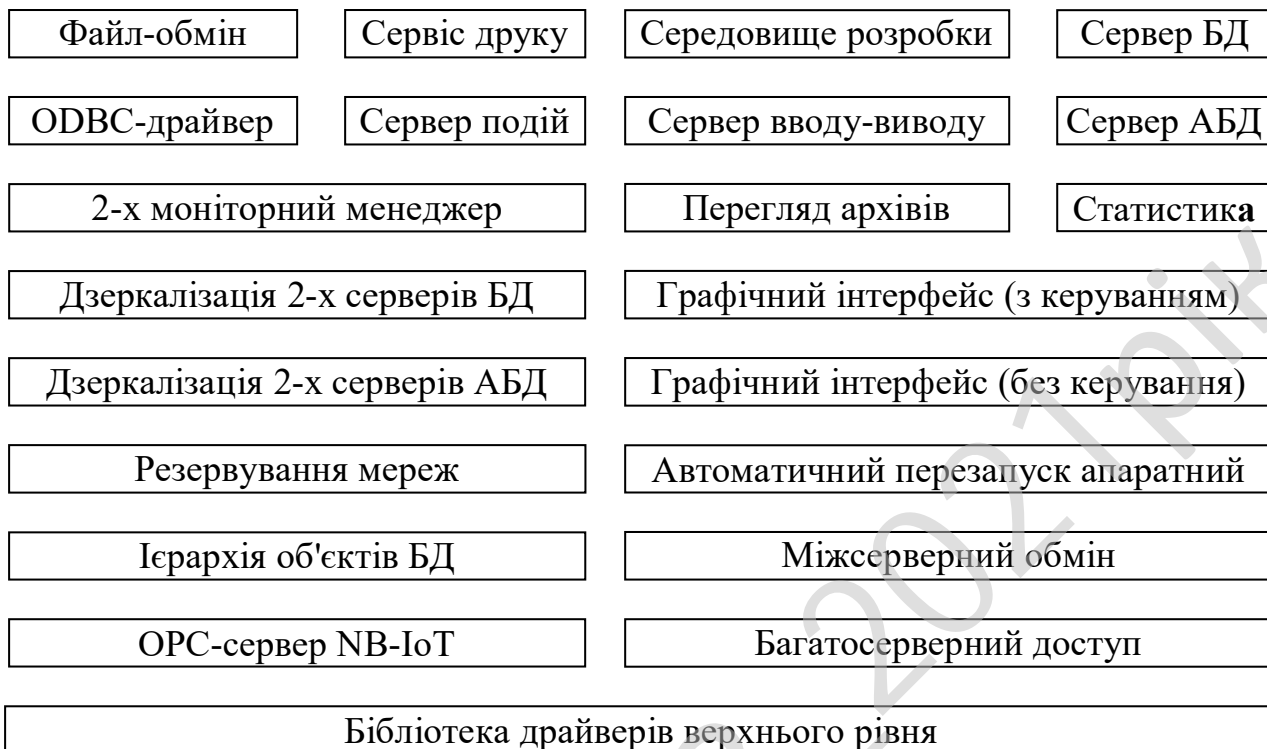
9. Дзеркалізація 2-х серверів АБД. Аналогічно дзеркалізації 2-х серверів БД. Крім того, дзеркалізуються архіви історичних трендів, архіви друкованих документів і архіви протоколів подій.

10. Автоматичний перезапуск апаратний. Використовується при установці в комп'ютер (АРМ) спеціальної плати автоматичного перезапуску. Разом із платою забезпечується автоматичний перезапуск операційної системи у випадках зависання й зациклення.

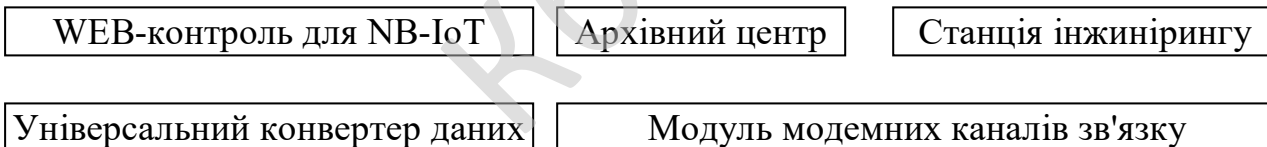
11. Сервіс друку. Забезпечує функції автоматичної видачі звітних документів і протоколу подій на пристрої друку.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		49

### Компоненти верхнього рівня системи NB-ІоТ



### Додаткове програмне забезпечення системи NB-ІоТ



### Компоненти нижнього рівня системи NB-ІоТ



Рисунок 3.2 – Функціональна схема системи

Вим.	Арк.	№ докум.	Підпис	Дата

КБР-123.21.0034.00.00.ПЗ

Арк.

50

12. Файл-обмін. Забезпечує прийом/передачу файлів даних з/у систему NB-ІоТ. Даними для прийому/передачі можуть бути наступні: поточні значення змінних, атрибути змінних (параметри налаштування). Обмін файлами даних здійснюється як з ініціативи зовнішньої системи, так і з ініціативи системи NB-ІоТ. Дані передаються у двійковому форматі.

13. Резервування мереж. Забезпечує виконання наступних функцій резервування: мережа контролера – сервер БД/АБД; мережа сервер БД/АБД – клієнти сервера БД/АБД (у тому числі при резервуванні серверів і клієнтів).

14. 2-х моніторний менеджер. Забезпечує функціонування АРМ із двома моніторами. Потрібна установка в системний блок комп'ютера графічного адаптера, що підтримує двомоніторний режим роботи. Реалізує функції менеджера вікон, що забезпечує просте й зручне автоматичне керування вікнами на двох моніторах.

15. Ієрархія об'єктів БД. Створення ієрархічної структури даних РВ відповідно до конструкторського, технологічного або іншого угруповання параметрів. Формування узагальнених ознак сигналізації й вибірок. Підтримує існуючі системи кодувань і дозволяє створювати власні.

16. Статистика. Дозволяє провести вибірку змінних для будь-якого часового інтервалу, за який є тренди, і застосувати бібліотечні функції статистичної обробки. Можливість роботи з архівними даними. Отриманий результат може бути використаний у графічному інтерфейсі й при формуванні звітних документів

17. Сервер подій. Нова система подій створена для організації більш гнучкого й ефективного відстеження реакцій системи на виникаючі події в контрольованому об'єкті. Система подій надає Користувачеві величезні можливості по вибірках (фільтрам) найрізноманітніших видів і категорій подій, починаючи від комбінацій символів у позиції змінної (підтримка систем класифікації типу АКС, ККС і будь-яких інших), вибіркою подій по одному агрегату або пристрою й закінчуючи всіма подіями для однієї змінної. Для

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		51

обробки, формування й візуалізації подій розроблені й істотно модифіковані багато компонентів як середовища розробки, так і середовища виконання NB-ІоТ.

18. Міжсерверний обмін. Міжсерверний обмін призначений для прямого обміну інформацією між серверами різних АСУ ТП на базі NB-ІоТ. Обмін виробляється паспортами обраних змінних і пов'язаними з ними подіями. Дозволяє будувати системи контролю й керування зі складними багатопаровими архітектурами й функціоналом.

19. Багатосерверний доступ. Багатосерверний доступ – це можливість легкого перемикання доступу клієнтських станцій до декількох Серверів бази даних через інтерфейс Користувача. Клієнтські додатки одержують можливості по керуванню й діагностиці декількох Серверів бази даних: відображення узагальненої звукової сигналізації із заданих Серверів БД; зміна графічного проекту й підключення клієнта до іншого Сервера БД по команді із графічного інтерфейсу.

20. OPC-сервер NB-ІоТ (специфікація DA+HDA). Модуль призначений для передачі оперативних і архівних даних з NB-ІоТ у системи сторонніх виробників відповідно до стандартів OPC DA і OPC HDA.

21. Бібліотека драйверів верхнього рівня. Безкоштовна бібліотека драйверів для різних контролерів, модулів введення/виводу й інших цифрових приладів.

22. ODBC-драйвер. Відкритий інтерфейс доступу до БД NB-ІоТ являє собою бібліотеку функцій, що дозволяє прикладній програмі звертатися до бази даних NB-ІоТ, використовуючи структуровану мову запитів SQL.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		52

### 3.4 Розробка діаграми процесів

Відповідно до методичних рекомендацій розроблення графічної частини кваліфікаційної бакалаврської роботи розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3.

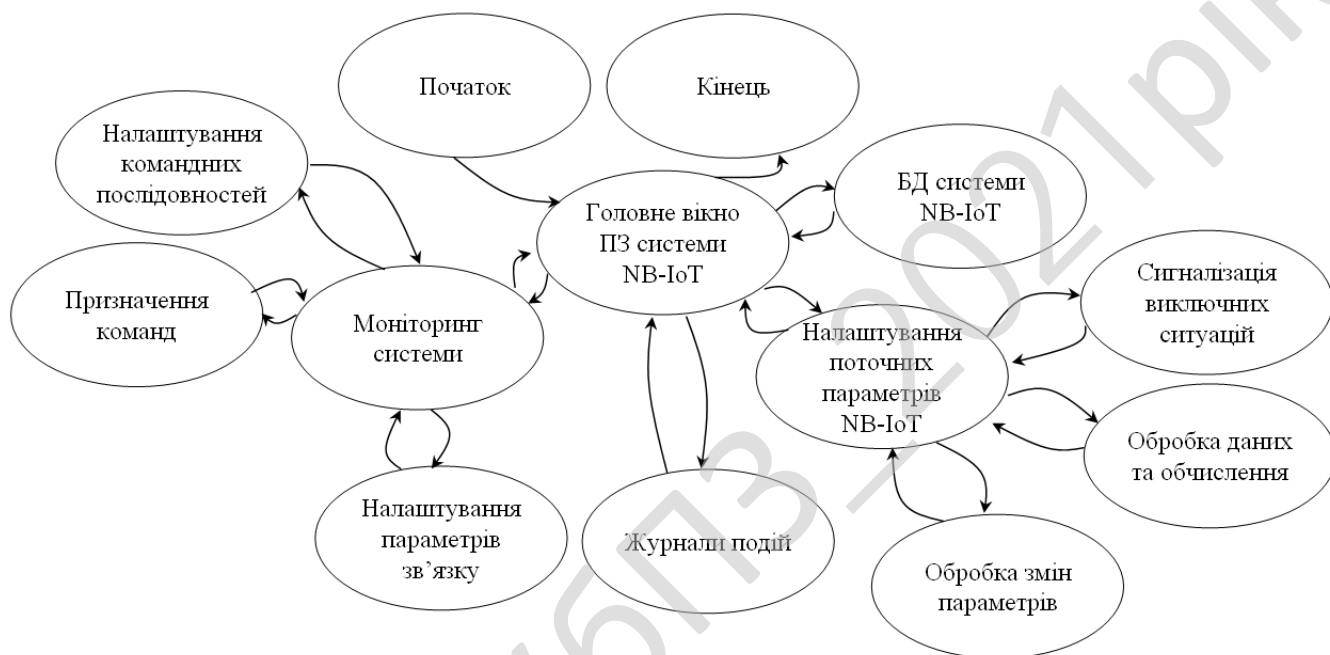


Рисунок 3.3 – Діаграма взаємодії процесів

Розроблена діаграма взаємодії процесів використовується для представлення та візуалізації процесів обробки даних тобто структурного проектування бакалаврської роботи.

Основні складові елементи діаграми взаємодії процесів це потоки даних:

- Репозиторії, потік сховища даних.
- Потоки зовнішні по відношенню до системи сутності.
- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Потоки даних гібридні між елементами трьох попередніх типів.

Відповідно до документації основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей. Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

Для схематичного представлення системи що розробляється необхідно спочатку представити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи в цілому у подальшому. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі. Розроблена діаграма взаємодії процесів системи в подальшому уточнюється шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

Таким чином у результаті після розгляду, вищеописаної системи, схеми структурної, функціональної, діаграми взаємодії процесів перейдемо до опису та розгляду блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.



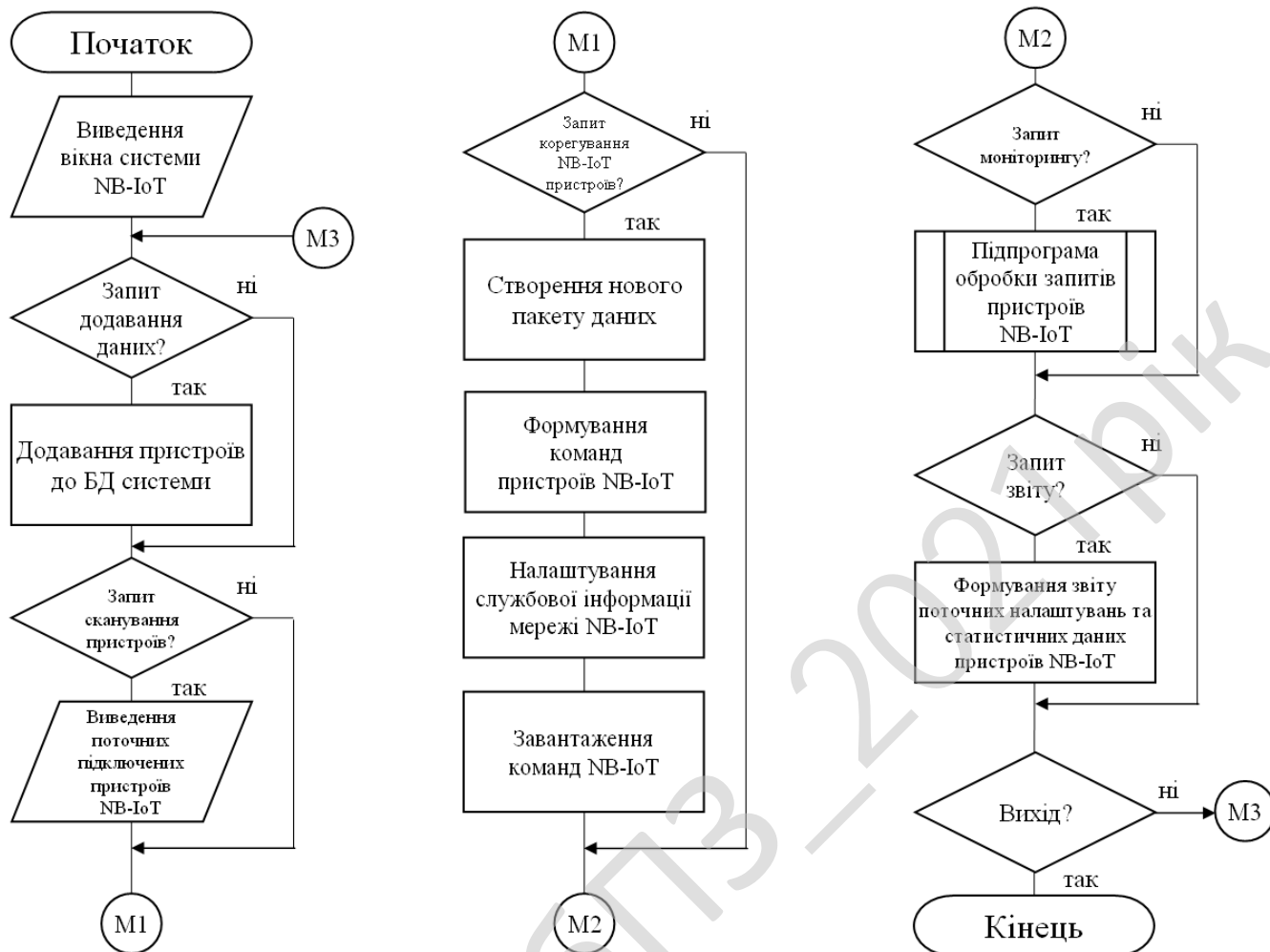


Рисунок 4.1 – Блок-схема основної програми

```

unsigned int index;
int i;
next_code=256;
/* Next_code – следующий доступный код строки */
for (i=0;i<TABLE_SIZE;i++)
/* Очистка таблице строку перед стартом */
code_value[i]=-1;
i=0;
string_code=getc(input); /* Get the first code*/
/* Основной цикл. Він виконується до тих пір, поки
можливо читання вхідного потоку. Відзначимо, що
він припиняє заповнення таблиці рядків після того,
як всі можливі коди були використані.
*/
while ((character=getc(input)) != (unsigned)EOF)

```

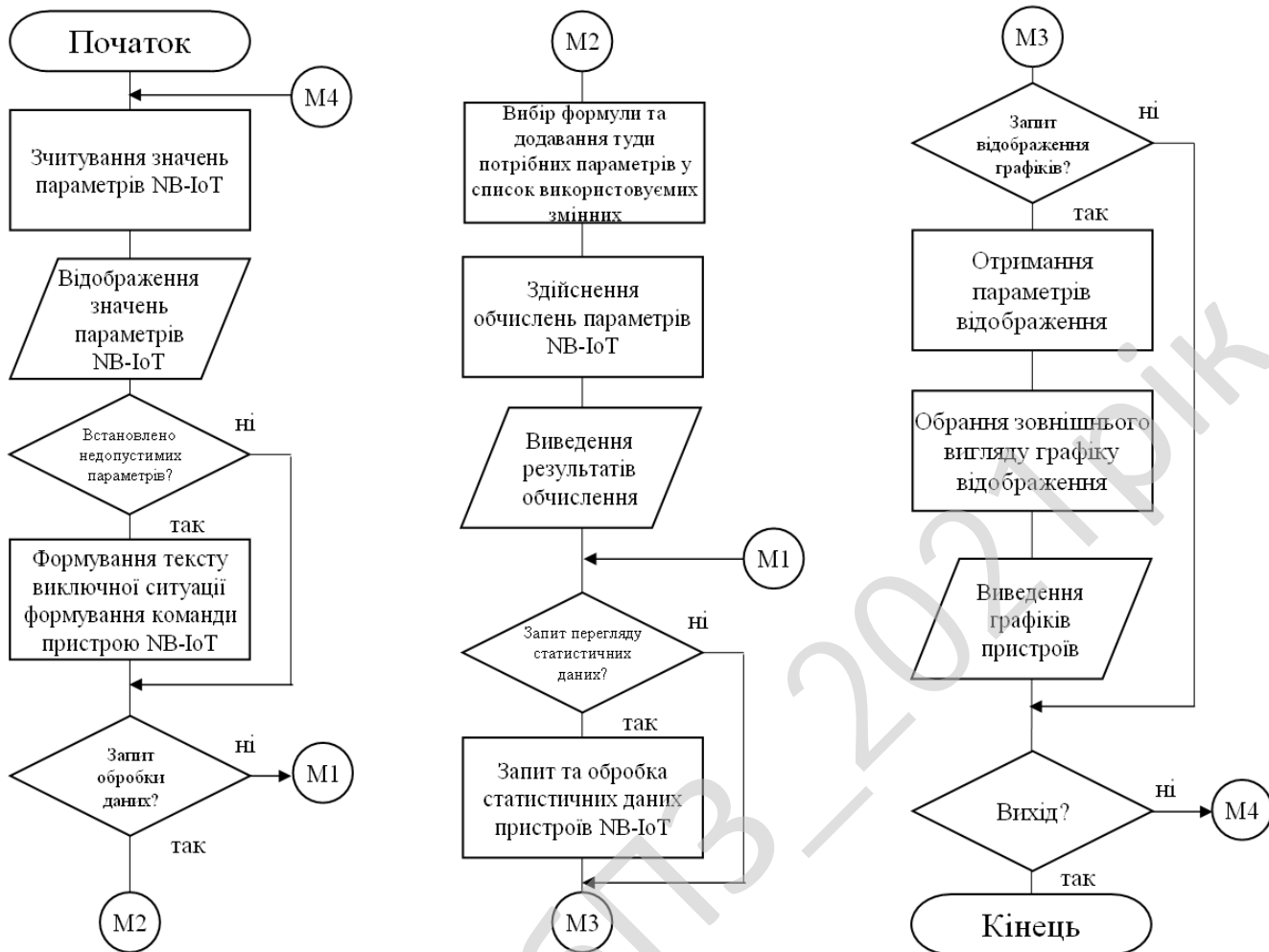


Рисунок 4.2 – Блок-схема роботи підпрограми

```

{
/* Дивиться, чи є рядок */
index=find_match(string_code,character);
if (code_value[index] != -1)
    string_code=code_value[index];
else
{
    if (next_code <= MAX_CODE)
    {
        code_value[index]=next_code++;
        prefix_code[index]=string_code;
        append_character[index]=character;
    }
    output_code(output,string_code);
    string_code=character;
}
}

```

```

    }
}
output_code(output,string_code); /* Виведення останнього коду */
output_code(output,MAX_VALUE); /* Виведення ознаки кінця потоку */
output_code(output,0); /* Очищення буфера виводу */
}
/*
** Процедура розпакування. Вона читає файл LZW-формату і розпаковує
** його у вихідний файл.
*/
expand(FILE *input,FILE *output)
{
unsigned int next_code;
unsigned int new_code;
unsigned int old_code;
int character;
unsigned char *string;
char *decode_string(unsigned char *buffer,unsigned int code);
next_code=256; /* Наступний доступний код. */

old_code=input_code(input);/* Читается перший код, инициализируется */
character=old_code; /* змінна character і надсилається перший */
putc(old_code,output); /* код в вихідний файл. */
/*
** Основний цикл розпакування. Читаються коди з LZW-файлу до тих пір,
** поки не зустрінеться спеціальний код, який вказує на кінець даних.
*/
while ((new_code=input_code(input)) != (MAX_VALUE))
{
/*
** Перевірка коду для спеціального випадку
** STRING + CHARACTER + STRING + CHARACTER +
** STRING, коли генерується невизначений код.
** Це змушує його декодувати останній код,
** додавши CHARACTER в кінець ДЕКОДАХ. рядки.
*/
if (new_code>=next_code)
{
*decode_stack=character;
string=decode_string(decode_stack+1,old_code);
}
}
}
/*

```

Вим.	Арк.	№ докум.	Підпис	Дата

КБР-123.21.0034.00.00.ПЗ

Арк.

58

```

** Інакше декодується новий код.
*/
    else
        string=decode_string(decode_stack,new_code);
/*
** Виводиться декодуємою рядок у зворотному порядку.
*/
    character=*string;
    while (string >= decode_stack)
        putc(*string--,output);
/*
** Нарешті, якщо можливо, додається новий код в таблицю рядків.
*/
    if (next_code <= MAX_CODE)
    {
        prefix_code[next_code]=old_code;
        append_character[next_code]=character;
        next_code++;
    }
    old_code=new_code;
}
}
/*
** Процедура хешування. Вона намагається знайти зіставлення для рядка
** префікс + символ в таблиці рядків. Якщо знайдено, повертається індекс.
** Якщо немає, то повертається перший доступний індекс.
*/
find_match(int hash_prefix,unsigned int hash_character)
{
    int index;
    int offset;

    index = (hash_character << HASHING_SHIFT) ^ hash_prefix;
    if (index == 0)
        offset = 1;
    else
        offset = TABLE_SIZE - index;
    while (1)
    {
        if (code_value[index] == -1)
            return(index);
        if (prefix_code[index]==hash_prefix

```

Вим.	Арк.	№ докум.	Підпис	Дата

КБР-123.21.0034.00.00.ПЗ

Арк.

59





Але вже до кінця 1980-х років існуюча тоді реляційна модель перестала задовольняти розробників в силу низки обмежень. Відповіддю на зростаючу складність програм баз даних стали два нових напрямки розвитку СКБД: об'єктно-орієнтовані СКБД і об'єктно-реляційні СКБД.

У 1991 був утворений консорціум ODMG, основною метою якого стало вироблення промислового стандарту об'єктно-орієнтованих баз даних. Між 1993 та 2001 роками ODMG опублікувала п'ять ревізій своїх специфікацій. Остання версія стандарту має індекс 3.0, після чого група розпустилася. До кінця 1990-х існувало близько десяти компаній, що виробляли комерційні продукти, що позиціонуються на ринку як СКБД. Найбільш відомими системами даного класу стали Objectivity, Versant виробництва однойменних компаній, а також СКБД Jasmine, випущена компанією CA. Незважаючи на переваги, що дозволяють ефективніше вирішувати певний ряд завдань, об'єктно-орієнтовані системи так і не змогли завоювати значущу частку ринку СКБД, залишившись «нішевим» продуктом.

Постачальниками традиційних реляційних СКБД також була проведена значна робота з об'єднання об'єктно-орієнтованих і реляційних систем. Розробники постаралися розширити мову SQL, щоб включити в неї концепції об'єктно-орієнтованого підходу, зберігаючи переваги реляційної моделі (об'єктні розширення мови SQL були зафіксовані в стандарті SQL:1999).

Основний принцип – це еволюційний розвиток можливостей СКБД без поломки попередніх підходів та зі збереженням наступності з системами попереднього покоління.

Поняття СКБД третього покоління, якими, власне кажучи, і є об'єктно-реляційні СКБД, з'явилося після опублікування групою відомих фахівців в області баз даних «Маніфесту систем баз даних третього покоління». Основні принципи СКБД третього покоління, позначені в маніфесті:

Крім традиційних послуг з управління даними, СКБД третього покоління повинні забезпечити підтримку розвиненіших структур об'єктів і правил.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

Розвинутіша структура об'єктів характеризує засоби, необхідні для зберігання і маніпулювання нетрадиційними елементами даних (тексти, просторові дані, мультимедіа).

СКБД третього покоління повинні включити в себе СКБД другого покоління. Системи другого покоління внесли вирішальний вклад у двох областях – непроедурний доступ за допомогою мови запитів SQL і незалежність даних. Ці досягнення обов'язково повинні враховуватися в системах третього покоління.

СКБД третього покоління повинні бути відкриті для інших підсистем. Це включає оснащення різноманітними інструментами підтримки прийняття рішень, доступом з багатьох мов програмування, інтерфейсами до існуючих популярних систем і бізнес-застосунків, можливістю запуску програм з бази даних на іншій машині і розподілені СКБД. Весь набір інструментів і СКБД має ефективно функціонувати на різноманітних апаратних платформах з різними операційними системами.

Крім того, СКБД, що розраховує на широку сферу застосування, повинна бути оснащена мовою четвертого покоління (4GL).

У середині 1990 років було лише кілька дослідних прототипів СКБД, які поєднали найкращі риси реляційних і об'єктно-орієнтованих СКБД. Першим комерційним продуктом, якому були властиві об'єктно-реляційні риси, став Universal Server компанії Informix (згодом була поглинена IBM). В даний час більшість цих ідей вже втілено в реальних комерційних рішеннях, в тому числі і в продуктах основних постачальників СКБД (Oracle Database і IBM DB2).

Розвиток індустрії систем керування базами даних базується на значних фундаментальних наукових дослідженнях. Найчастіше, між самими дослідженнями та їхньою конкретною реалізацією в прикладних рішеннях минають роки, а іноді й десятиліття. Роботу в області управління даними проводять як університетські дослідницькі групи (MIT, Berkeley), так і центри розробок основних постачальників СКБД (Oracle, IBM, Microsoft). Інвестування в

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

управління даними – це довгострокове, і разом з тим, вигідне вкладення коштів. В даний час дослідники мають у своєму розпорядженні засоби, що дозволяють ефективно реалізувати найскладніші запити, що маніпулюють терабайтами й петабайтами різних даних.

Основними тенденціями, які дали привід для проведення різних масштабних досліджень в області баз даних стали:

Експонентний ріст даних. Обсяг даних, у тому числі синтетичних, що генеруються автоматизованими системами, значно зріс. Збільшилося і число прикладних областей, в яких вимагається обробка великих обсягів даних. До таких областей тепер відносяться не тільки традиційні корпоративні програми, пошук у веб, але також і наукові дослідження, обробка природних мов, аналіз соціальних мереж тощо.

Значне ускладнення структур використовуваних даних. Прості види даних у вигляді чисел і символічних рядків стали доповнятися численною мультимедійною інформацією, просторовими, процедурними даними та великою кількістю інших складних форматів.

Широке поширення дешевих високопродуктивних апаратних засобів. Щорічно ми спостерігаємо зростання обчислювальних можливостей мікропроцесорів, збільшення ємності і зниження вартості доступних і зручних в експлуатації пристроїв дискової оперативної пам'яті.

Активний розвиток засобів комунікації та «всесвітньої павутини» World Wide Web. WWW стає єдиним інформаційним середовищем, що пронизує весь світ і об'єднує величезне число користувачів та електронних пристроїв.

Поява нових важливих областей застосування СКБД. У першу чергу, це пов'язано з інтелектуальним аналізом даних, сховищами даних, а останнім часом – з паралельними обчисленнями і хмарними технологіями.

### **Основні характеристики СКБД**

1. Контроль за надлишковістю даних.
2. Несуперечливість даних.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		64

3. Підтримка цілісності бази даних (коректність та несуперечливість).
4. Цілісність описується за допомогою обмежень.
5. Незалежність прикладних програм від даних.
6. Спільне використання даних.
7. Підвищений рівень безпеки.

### **Можливості СКБД**

1. Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (Data Definition Language)).

2. Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів)

3. Можна надавати контрольований доступ до БД за допомогою: Системи забезпечення захисту, яка запобігає несанкціонованому доступу до БД; Системи керування паралельною роботою прикладних програм, яка контролює процеси спільного доступу до БД; Система відновлення – дозволяє відновлювати БД до попереднього несуперечливого стану, що був порушений в результаті збою апаратного або програмного забезпечення.

### **Основні компоненти середовища СКБД**

1. Апаратне забезпечення.
2. Програмне забезпечення.
3. Дані.
4. Процедури – інструкції та правила, які повинні враховуватись при проектуванні та використанні БД.
5. Користувачі: адміністратори даних (керування даними, проектування БД, розробка алгоритмів, процедур) та БД (фізичне проектування, відповідальність за безпеку та цілісність даних); розробники БД; прикладні програмісти; кінцеві користувачі.



підтримують повнотекстовий пошук, так і таблиці InnoDB, що підтримують транзакції на рівні окремих записів. Більш того, СКБД MySQL поставляється із спеціальним типом таблиць EXAMPLE, що демонструє принципи створення нових типів таблиць. Завдяки відкритій архітектурі і GPL-ліцензуванню, в СКБД MySQL постійно з'являються нові типи таблиць.

26 лютого 2008 року Sun Microsystems придбала MySQL AB за 1 млрд доларів, 27 січня 2010 року Oracle придбала Sun Microsystems за 7,4 млрд доларів і включила MySQL в свою лінійку СКБД.

Спільнотою розробників MySQL створені різні відгалуження коду, такі як Drizzle (англ.), OurDelta, Percona Server і MariaDB. Всі ці відгалуження вже існували на момент поглинання компанії Sun корпорацією Oracle.

MySQL має подвійне ліцензування. MySQL може розповсюджуватися відповідно до умов ліцензії GPL. Але за умовами GPL, якщо якась програма використовує бібліотеки MySQL, то вона теж повинна розповсюджуватися за ліцензією GPL. Проте це може розходитися з планами розробників, які не бажають відкривати сирцеві тексти своїх програм. Для таких випадків передбачена комерційна ліцензія компанії Oracle, яка також забезпечує якісну сервісну підтримку.

В разі використання та розповсюдження програмного забезпечення з іншими вільними ліцензіями, такими як BSD, Apache, MIT та інші, MySQL дозволяє використання бібліотек MySQL за ліцензією GPL.

MySQL виникла як спроба застосувати mSQL до власних розробок компанії: таблиць, для яких використовувалися ISAM – підпрограми низького рівня для індексного доступу до даних. У результаті був вироблений новий SQL-інтерфейс, але API-інтерфейс залишився в спадок від mSQL. Звідки походить назва «MySQL» – достеменно не відомо. Розробники дають два варіанти: або тому, що практично всі напрацювання компанії починалися з префікса My, або на честь дівчинки на ім'я My, дочки Майкла Монті Віденіуса, одного з розробників системи.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

Логотип MySQL у вигляді дельфіна носить ім'я «Sakila». Він був обраний з великого списку запропонованих користувачами «імен дельфіна». Ім'я «Sakila» було відправлено Open Source-розробником Ambrose Twebaze.

В січні-лютому 2008 Sun Microsystems придбала розробника системи керування базами даних MySQL за \$1 млрд. Після поглинання у 2009 році Sun Microsystems компанією Oracle Corporation MySQL стала власністю Oracle.

За час розвитку під орудою Oracle дедалі більше відокремлює MySQL від спільноти і робить процес розробки все менш прозорим. Наприклад, повернута практика поставки власницьких розширених функцій в Enterprise-версії MySQL, спостерігається приховування інформації про вразливості, зі складу виключений тестовий набір, закритий доступ до більшої частини системи відстеження помилок та припинено публікація згрупованого логу змін, що дозволяє судити про прив'язку патчів до конкретних змін.

### **Можливості**

MySQL – компактний багатопотоковий сервер баз даних. Характеризується високою швидкістю, стійкістю і простотою використання.

MySQL вважається гарним рішенням для малих і середніх застосувань. Сирцеві коди сервера компілюються на багатьох платформах. Найповніше можливості сервера виявляються в UNIX-системах, де є підтримка багатопоточності, що підвищує продуктивність системи в цілому.

### **Можливості сервера MySQL:**

1. Простота у встановленні та використанні.
2. Підтримується необмежена кількість користувачів, що одночасно працюють із БД.
3. Кількість рядків у таблицях може досягати 50 млн.
4. Висока швидкість виконання команд.
5. Наявність простої і ефективної системи безпеки.



модуль  $N$  на множники. Крім того, можна строго математично довести, що результат перевірки цифрового підпису  $S$  буде позитивним тільки в тому випадку, якщо при обчисленні  $S$  був використаний секретний ключ  $D$ , що відповідає відкритому ключу  $E$ . Тому відкритий ключ  $E$  іноді називають "ідентифікатором" того, хто підписав.

Кафедра КБПЗ – 2021 рік

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		70



На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення. Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий. Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

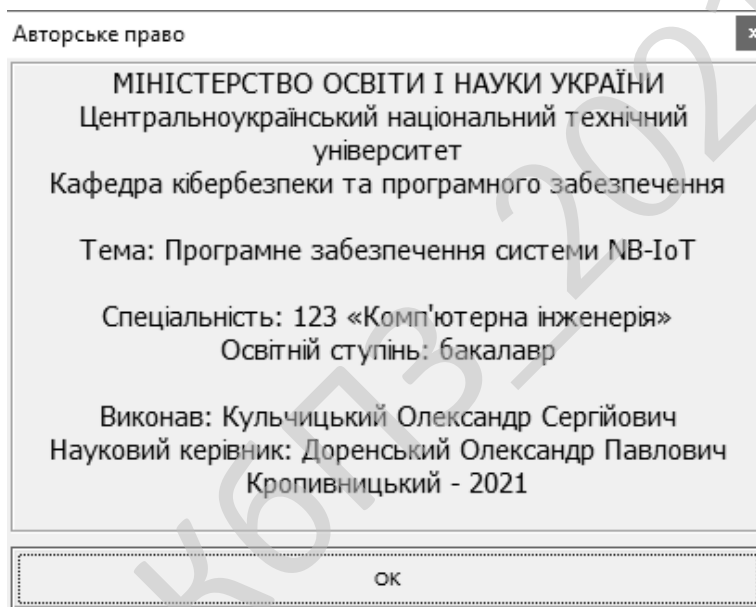


Рисунок 5.2 – Авторське право

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

## 6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання кваліфікаційної бакалаврської роботи, призначено для системи NB-ІоТ.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем NB-ІоТ.
- Досліджена система NB-ІоТ.
- На основі отриманих результатів досліджень створена програмна реалізація системи NB-ІоТ.

Розроблені під час виконання кваліфікаційної бакалаврської роботи алгоритми дозволяють успішно вирішувати завдання NB-ІоТ.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створенні програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Builder C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані призначені для системи NB-ІоТ. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм RSA.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Steve Crocker, “Host Software,” RFC 1, April 1969.
2. Nevil Brownlee and Heather Flanagan, “RFC Series Format Requirements and Future Development,” RFC 6949, May 2013.
3. Message to RFC-Interest mailing List, “Subject: Direction of the RFC Format Development effort,” <http://www.rfc-editor.org/pipermail/rfcinterest/2013-May/005584.html>
4. RFC Format Change FAQ: <http://www.rfc-editor.org/rse/format-faq/>
5. Heather Flanagan, “Digital Preservation Considerations for the RFC Series,” January 2015, Internet Draft, work in progress, draft-flanagan-rfc-preservation-03.
6. Jon Postel, “Transmission Control Protocol,” RFC 793, September 1981.
7. Beecham Research. “M2M Sector Map,” September 2011. <http://www.beechamresearch.com/downloads.aspx?page=2>
8. Sutaria, R., and Raghunath, G., “Making sense of interoperability: Protocols and Standardization initiatives in IoT,” International Conference on Recent Trends in Communication and Computer Networks – ComNet 2013, 2013.
9. Ferguson, J., and Redish, A., “Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body,” Expert Review of Medical Devices, Volume 6, No. 4, 2011, <http://www.expert-reviews.com>.
10. ITU-T, “Common Requirements and Capabilities of a Gateway for Internet of Things Applications,” Recommendation Y.2067, June 2014.
11. Cisco Systems, “The Internet of Things Reference Model,” White Paper, 2014. <http://www.iotwf.com/>
12. Vaquero, L., and Rodero-Merino, L., “Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing,” ACM SIGCOMM Computer Communication Review, October 2014.

					КБР-123.21.0034.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75



20. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2014. – № 4(17). – С. 90-95.

21. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.

22. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

23. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.

24. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. – № 3(20). – С. 134-141.

25. Смирнов С. А. Комплекс GERT-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. – практик. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

26. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, А. К. Дидык, С. А. Смирнов //

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2016. – № 2 (46). – С. 146-149.

27. Смирнов С. А. Модели системы нейросетевых экспертов безопасной маршрутизации в облачных антивирусных системах / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2016. – Вип. 3 (140). – С. 36-39.

28. Смирнов С. А. Метод безопасной маршрутизации на базовом множестве путей передачи метаданных в облачные антивирусные системы / В. Л. Бурячок, С. А. Смирнов // Системи управління, навігації та зв'язку. – Полтава, 2016. – Вип. 4(40). – С. 57-62.

29. Смирнов С. А. Способ контроля линий связи телекоммуникационной системы облачного антивируса / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2016. – № 2 (47). – С. 148-152.

30. Смирнов С. А. Дослідження та реалізація GERT-моделі технології розповсюдження комп'ютерних вірусів для захисту телекомунікаційних систем / В. Л. Бурячок, Мохамад Абу Таам Гани, С. А. Смирнов // Інформаційні технології та комп'ютерна інженерія: зб. тез доп. наук.-практ. конф., м. Кіровоград, 4 грудня 2014 р. – Кіровоград: КНТУ, 2014. – С. 168.

31. Смирнов С. А. Исследование математических моделей технологии распространения компьютерных вирусов / А. А. Смирнов, Мохамад Абу Таам Гани, С. А. Смирнов // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: зб. наук. праць міжнар. наук.-практ. конф., м. Київ, 25-28 лютого 2015 р. – К.: Європейський університет, 2015. – С. 90-91.

32. Смирнов С. А. Метод управления доступом к «облачным» ресурсам для защиты телекоммуникационных систем / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Всеукраїнська науково-практична конференція «Інформаційна безпека держави, суспільства та особистості», м. Кіровоград, 16 квітня 2015 р.: зб. тез доп. – Кіровоград: КНТУ, 2015. – С. 50-52.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78

33. Смирнов С. А. Разработка метода управления доступом в интеллектуальных узлах коммутации / А. А. Смирнов, Мохамад Абу Таам Гани, С. А. Смирнов // Проблемы і перспективи розвитку ІТ-індустрії: зб. тез VII міжнар. наук.-практ. конф., м. Харків, 17-18 квітня 2015 р. – Х.: ХНЕУ, 2015. – С. 14.

34. Смирнов С.А. Реализация метода управления доступом в интеллектуальных узлах коммутации / А.А. Смирнов, Мохамад Абу Таам Гани, С.А. Смирнов // Збірник тез XVII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 17-18 квітня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 91-92.

35. Смирнов С. А. Технология передачи сигнатур в облачные антивирусные системы для обеспечения защищенности телекоммуникационных сетей / А. А. Смирнов, С. А. Смирнов // Збірник тез V міжнародної науково-технічної конференції «ITSEC», Київ, 19-22 травня 2015 р. – К.: НАУ 2015. – С. 12-13.

36. Смирнов С. А. Реализация математической модели интеллектуального узла коммутации для обеспечения защищенности телекоммуникационной сети / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Інформаційна та економічна безпека (INFECO-2015): зб. тез II Міжнар. наук.-практ. Інтернет-конф., м. Харків, 21-22 травня 2015 р. – Х.: ХІБС УБС НБУ, 2015. – С. 20-24.

37. Смирнов С. А. Разработка математической модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Сборник тезисов XI международной конференции «Стратегия качества в промышленности и образовании», г. Варна, Болгария, 01-06 июня 2015 г. – Варна: ТУВ, 2015. – С. 488-491.

38. Смирнов С. А. Метод управления доступом к облачным телекоммуни-кационным ресурсам для обеспечения защиты данных / Мохамад

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Комп'ютерні технології та інформаційна безпека: зб. тез доп. міжнар. наук.-практ. конф., м. Кіровоград, 2-3 липня 2015 р. – Кіровоград: КНТУ, 2015. – С. 4-5.

39. Смирнов С. А. Имитационная модель системы управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Збірник тез першої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації» (м. Затока, 7-9 вересня 2015 р.). – Одеса: ОНАЗ, 2015. – С. 90-94.

40. Смирнов С. А. Разработка комплекса GERT-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформаційні технології та взаємодії» (IT & I): зб. тез II міжнар. наук. -практ. конф., м. Київ, 3-5 листопада 2015 р. – К.: КНУ ім. Тараса Шевченка, 2015. – С. 65-67.

41. Смирнов С. А. Разработка моделей телекоммуникационной системы формирования и обработки метаданных в облачных антивирусных системах / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Информационные и телекоммуникационные технологии: образование, наука, практика: сб. тезисов II междунар. научно-практ. конф., г. Алматы, Казахстан, 3-4 декабря 2015 г. – Алматы: КазНИТУ им. К.И. Сатпаева, 2015. – С. 309-313.

42. Смирнов С. А. GERT-модели технологии облачной антивирусной защиты / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Безпека українського суспільства в концепції вступу в постіндустріальне суспільство ЄС: зб. тез Круглого столу, м. Київ, 16 грудня 2015 р. – К.: Європейський університет, 2015. – С.41-43.

43. Смирнов С. А. Алгоритмы формирования множества маршрутов передачи метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: зб. наук. праць II Міжнар. наук.-

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		80

практ. конф., м. Київ, 24-27 лютого 2016 р. – К.: Європейський університет, 2016. – С. 140-142.

44. Смирнов С. А. Разработка и реализация метода безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Securitea informationala 2015-2016: Conferenta internationala (editia a XII-a), Chisinau, Moldova, 3 martie 2016. – Chisinau: ADSEM, 2016. – С. 90-96.

45. Смирнов С. А. Алгоритм формирования базового множества маршрутов передачи метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформатика та системні науки (ІСН-2016): зб. тез VII всеукр. наук.-практ. конф., м. Полтава, 10-12 березня 2016 р. – Полтава: ПУЕТ, 2016. – С. 261-263.

46. Смирнов С. А. Система обработки и формирования начального состояния маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: зб. тез наук. -практ. конф., м. Київ, 10-11 березня 2016 р. – К.: КНУ ім. Тараса Шевченка, 2016. – С. 81-82.

47. Смирнов С. А. Алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер облачной антивирусной системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформаційна безпека та комп'ютерні технології (IS&CT): зб. тез міжнар. наук. -практ. конф., м. Кіровоград, 24-25 березня 2016 р. – Кіровоград: КНТУ, 2016. – С. 73.

48. Смирнов С. А. Исследование способа контроля линий связи телекоммуникационной системы для облачных антивирусов / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Збірник тез першої міжнародної науково-практичної конференції «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі» (ПНПЗК-2016), м. Харків, 30 березня – 1 квітня 2016 р. – Х.: НТУ «ХПІ», 2016. – С. 14.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		81

49. Смирнов С. А. Разработка способа контроля линий связи телекоммуникационной системы для облачных антивирусов / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Матеріали XVIII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування» (м. Кіровоград, 15-16 квітня 2016 р.). –Кіровоград: КНТУ, 2016. – С. 182-186.

50. Смирнов С. А. Разработка и исследование способа контроля линий связи телекоммуникационных сетей для облачных антивирусных систем / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Проблеми і перспективи розвитку ІТ-індустрії: VIII міжнар. наук.-практ. конф., м. Харків, 28-29 квітня 2016 р.: зб. тез. – Х.: ХНЕУ, 2016. – С. 48.

51. Смирнов С. А. Модель системы нейросетевых экспертов безопасной маршрутизации для облачных антивирусных систем / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Інформаційна та економічна безпека (INFECO-2016): зб. тез III міжнар. наук.-практ. конф., м. Харків, 28-30 кві. 2016 р. – Х.: ХННІ ДВНЗ «УБС», 2016. – С. 178-182.

52. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. К. Дидык // Сборник тезисов XII международной конференции «Стратегия качества в промышленности и образовании» (г. Варна, Болгария, 30 мая – 02 июня 2016 г.). – Варна: ТУВ, 2016. – С. 581-585.

53. Смирнов С. А. Оценка эффективности метода безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, С. А. Смирнов, А. С. Коваленко // РадіоЕлектроніка та ІнфоКомунікації: зб. тез першої наук. – техн. конф., м. Київ, 11-16 вересня 2016 р. – К.: НТУУ «КПІ», 2016. – С. 17.

54. Современные телекоммуникации. Технологии и экономика / [В.Л. Банкет, О.В. Бондаренко, П.П. Воробьенко и др.]; под ред. С.А. Довгого. – М.: Эко-Трендз, 2003. – 320 с.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		82

55. Столлингс В. Современные компьютерные сети / Вильям Столлингс. – СПб.: Питер, 2003. – 778 с.

56. Таненбаум Э. Компьютерные сети / Эндрю Таненбаум; пер. с англ. А. Леонтьев. – СПб.: Питер, 2002. – 848 с.

57. Телекоммуникационные системы и сети: учебное пособие. В 3 томах / [В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев]; под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005, т. 3 – 592 с.

58. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1103 с.

59. Шелухин О.И. Фрактальные процессы в телекоммуникациях: моногр. / О.И. Шелухин, А.М. Тенякшев, А.В. Осин – М.: Радиотехника, 2003. – 480 с.

60. Elwalid, D. Mitra, I. Sanjee, and I. Widjaja. Routing and Protection in GMPLS Networks: From Shortest Paths to Optimized Designs // Journal of lightwave technology. – 2003. – №21(11), P. 2828-28-38.

					<b>КБР-123.21.0034.00.00.ПЗ</b>	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		83