МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ

ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему:

«УДОСКОНАЛЕННЯ АРХІТЕКТУРИ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ПІДВИЩЕННЯ ЇХ КОНФІДЕНЦІЙНОСТІ»

Виконав: здобувач групи ІТ-41
спеціальності 126 «Інформаційні системи та технології»

_____ Ониськів В.М.
(прізвище та ініціали)

Керівник: _____ Пташник В. В.
(прізвище та ініціали)

Рецензент: _____
(прізвище та ініціали)

ДУБЛЯНИ-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Перший (бакалаврський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____
(підпис)
д.т.н., професор, Тригуба А. М.
(вч. звання, прізвище, ініціали)
“____” _____202 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ониськів Віталій Михайлович
(прізвище, ім’я, по батькові)

1. Тема роботи *«Удосконалення архітектури мережі інтернету речей для підвищення їх конфіденційності»*
керівник роботи *к. т. н., доцент., Пташник В. В.*
(наук.ступінь, вч. звання, прізвище, ініціали)
затверджені наказом Львівського НУП *від 27.11.2023 року № 641/к-с*
2. Строк подання студентом роботи *10 червня 2024 року*
3. Вихідні дані до роботи: *характеристика сучасних рішень безпеки у галузі IoT; технічна документація щодо методів обміну даними та конфіденційності користувачів засобів Інтернету речей; науково-технічна і довідкова література.*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Аналіз проблем збереження даних в мережах інтернету речей
2. Методи вирішення проблем захисту та конфіденційності інформації
3. Реалізація та аналітична оцінка запропонованого методу
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки
Список використаних джерел
5. Перелік графічного матеріалу
Графічний матеріал подається у вигляді презентації

6. Консультанти розділів

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата		Відмітка про виконання
		завдання видав	завдання прийняв	
1, 2, 3	*Пташник В. В., к.т.н., доцент*			
4	*Городецький І. М., к.т.н., доцент*			

7. Дата видачі завдання *28 листопада 2023 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Відмітка про виконання
1	*Складання характеристики об'єкту проектування*	*28.11.2023 – 31.12.2023*	
2	*Аналіз методів вирішення проблем захисту та конфіденційності інформації*	*01.01.2024 – 28.02.2024*	
3	*Вибір концепції удосконалення архітектури мережі IoT*	*01.03.2024 – 31.03.2024*	
4	*Моделювання запропонованих рішень, аналітична оцінка отриманих результатів*	*01.04.2024 – 30.04.2024*	
5	*Розгляд питань з охорони праці та безпеки у надзвичайних ситуаціях*	*01.05.2024 – 14.05.2024*	
6	*Завершення оформлення розрахунково-пояснювальної записки та презентаційного матеріалу*	*15.05.2024 – 31.05.2024*	
7	*Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи*	*01.06.2024 – 10.06.2024*	

Здобувач _____ *Ониськів В. М.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Пташник В. В.*
(підпис) (прізвище та ініціали)

УДК 681.521 / 681.518

Удосконалення архітектури мережі інтернету речей для підвищення їх конфіденційності. Ониськів В. М. Кафедра інформаційних технологій – Дубляни, Львівський національний університет природокористування, 2024.
Кваліфікаційна робота: 48 сторінок текстової частини, 18 рисунків, 3 таблиці, 19 джерел літератури.

Мета кваліфікаційної роботи полягає у підвищенні ефективності управління конфіденційною інформацією користувачів IoT мереж та забезпечити збереження даних шляхом удосконалення архітектури мережі IoT.

Об'єктом дослідження є процес управління персональною інформацією та забезпечення збереження даних.

Предмет дослідження вивчає методи та засоби удосконалення архітектури мережі IoT для підвищення рівня конфіденційності даних.

В даний час розроблено метод надання безкоштовних послуг в обмін на дані користувачів. Технологія IoT приносить багато переваг користувачам, але вона також викликає проблеми з безпекою та конфіденційністю. Більшість пристроїв можуть передавати особисті дані третім особам. Таким чином, існує очевидна потреба в розробці хмарної інфраструктури IoT, щоб дозволити користувачам контролювати свої дані. У роботі запропоновано шляхи удосконалення методів управління персональними даними користувачів. Проведено моделювання та аналітичний аналіз отриманих даних. Окремо проведено аналіз умов праці травматичних ситуацій при виконанні різних робіт з комп'ютерною технікою, викладено питання охорони праці.

Ключові слова: інформаційна система, інтернет речей, мережа, інформаційна безпека, конфіденційні дані.

ЗМІСТ

ВСТУП

Актуальність даної роботи полягає в тому, що з кожним роком зростає кількість користувачів Інтернету, кількість вузлів обміну інформацією між машинами та обсяг переданих даних. Тому існує тенденція, коли користувачі оплачують інформаційні послуги за рахунок доступу до даних та відповідної статистичної обробки. Експоненційне зростання кількості користувачів Інтернету та обміну даними справді змінило спосіб доступу до інформації та її використання в повсякденному житті. Із зростанням використання онлайн-платформ для спілкування, досліджень, розваг і ділових операцій зріс попит на надійні та відповідні інформаційні послуги. Ця тенденція породила безліч онлайн-платформ і сервісів, які задовольняють зростаючу потребу в доступі та аналізі даних.

Ситуація ускладнюється появою Інтернету речей (IoT), який дозволяє пристроям збирати великі обсяги персональних даних і передавати їх на хмарні сервери. Тому існує очевидна потреба в розробці хмарної інфраструктури IoT, щоб дозволити користувачам контролювати свої дані.

Для досягнення мети дослідження були визначені та вирішені наступні основні завдання:

– провести аналіз збереження даних в мережах IoT;

– проаналізувати існуючі методи забезпечення конфіденційності інформації в мережах IoT;

– покращити архітектуру мережі IoT на основі концепцій баз даних;

– запропонувати метод управління інформацією для вдосконалення архітектури Інтернету речей;

– оцінити запропоновані рішення.

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ ЗБЕРЕЖЕННЯ ДАНИХ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Технології хмарних сервісів та Інтернету речей

Інтернет речей (IoT) відкриває нові можливості для розробки програм, які покращують життя людини. Ці програми охоплюють різні сфери, такі як розумні міста, промислове застосування, домашня автоматизація та медицина. Крім того, постійні інновації в апаратному забезпеченні, програмному забезпеченні та бездротових технологіях за останнє десятиліття зробили IoT інноваційною концепцією та призвели до розширення смарт-об’єктів та збільшення їх кількості.

Завдяки хмарному IoT великі обсяги даних, зібраних через бездротові сенсорні мережі, можна зберігати в хмарі та робити доступними для кількох користувачів. Використання цього підходу зменшує загальну вартість збору даних системи та користувачів. Оскільки різні бездротові сенсорні мережі мають різних власників, різні програми розміщуються в хмарних службах. Під час використання сервісів хмарних обчислень користувачі помічають, що затримка є критичною точкою для забезпечення потоку даних у реальному часі. Наприклад, датчики на транспортній інфраструктурі, повинні надавати дані про транспортні потоки в реальному часі, щоб водії в могли використовувати ці дані для вибору менш завантажених доріг. Ці дані необхідно зберігати та ефективно передавати.

Однією з проблем розподілених серверів є забезпечення високої доступності. Впровадження такої послуги є складним завданням, коли обсяг даних, що зберігаються в хмарі, швидко зростає. В основному проблеми з доступністю даних виникають через неефективність організації зберігання даних. Відсутність ефективної організації зберігання даних може в довгостроковій перспективі призвести до того, що деякі сервери будуть перевантажені з точки зору процесорів і пам'яті, а інші залишаться неактивними [2].

1.2 Класифікація моделей хмарної інфраструктури Інтернету речей

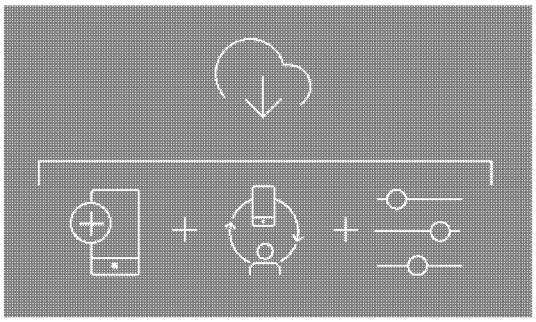
IoT отримує переваги від масштабованості, продуктивності та економічності інфраструктури хмарних обчислень. Оскільки програми IoT генерують великі обсяги даних і містять кілька обчислювальних компонентів, таких як обробка даних і аналітичні алгоритми, їх інтеграція в інфраструктуру хмарних обчислень може забезпечити економічно ефективне масштабування. Подібно до інфраструктури хмарних обчислень, хмарну інфраструктуру IoT і пов'язані з нею послуги можна розділити на такі моделі:

– Програмне забезпечення як послуга (SaaS) (рис. 1.1).

Рисунок 1.1 – Програмне забезпечення як сервіс

Програмне забезпечення як послуга, також відоме як служби хмарних додатків, є найпоширенішим вибором для підприємств на хмарному ринку. SaaS використовує мережу Інтернет, щоб надавати користувачам доступ до програм, якими керує сторонній постачальник. Більшість програм SaaS запускаються безпосередньо з веб-браузера, тобто для них не потрібно завантажувати чи інсталювати клієнт.

– Платформа як послуга (PaaS) (рис. 1.2).



PaaS

Прикладне програмне забезпечення

Підтримка циклу прийняття рішень

Веб-технології

Потокова передача даних

Рисунок 1.2 – Платформа як сервіс

Сервіси хмарної платформи надають хмарні компоненти для певного програмного забезпечення, яке переважно використовується в програмах. PaaS надає розробникам структуру для створення та використання спеціальних програм. Усіма серверами, сховищами та мережею може керувати підприємство або сторонні постачальники, тоді як розробники можуть підтримувати керування додатками.

Модель доставки PaaS схожа на SaaS, за винятком того, що замість доставки програмного забезпечення через Інтернет PaaS надає платформу для створення програмного забезпечення. Платформа надається через Інтернет, що дає розробникам свободу зосередитися на створенні програмного забезпечення, не турбуючись про операційні системи, оновлення програмного забезпечення, сховище чи інфраструктуру. PaaS дозволяє підприємствам використовувати спеціальні програмні компоненти для розробки та створення програм, вбудованих у PaaS.

– Інфраструктура як послуга (IaaS) (рис. 1.3).

Рисунок 1.3 - Інфраструктура як сервіс

Сервіси хмарної інфраструктури складаються з автоматизованих обчислювальних ресурсів, які високо масштабуються. IaaS — це повністю незалежна служба для доступу та моніторингу комп'ютерів, мереж, сховищ та інших служб. IaaS дозволяє компаніям купувати ресурси на вимогу, а не купувати обладнання відразу. IaaS використовує технологію віртуалізації для забезпечення інфраструктури хмарних обчислень, включаючи сервери, мережі, операційні системи та сховища.

Ці хмарні сервери зазвичай надаються організаціям через інформаційну панель або API, що дає клієнтам IaaS повний контроль над усією інфраструктурою. IaaS забезпечує ту саму технологію та функціональність, що й традиційний центр обробки даних, без необхідності фізичного обслуговування чи керування. Клієнти IaaS все ще мають прямий доступ до своїх серверів і сховищ даних, але все це маршрутизується через «віртуальні центри обробки даних» у хмарі [5].

Основна відмінність між цими архітектурами полягає в управлінні компонентами, включеними в їх область дії (рис. 1.4).

Рисунок 1.4 – Основні відмінності IaaS, PaaS та SaaS

1.3 Проблеми безпеки та конфіденційності в мережі IoT

В IoT кожен підключений пристрій може стати потенційним шлюзом до інфраструктури IoT або персональних даних. Питання безпеки та конфіденційності даних є важливими, але потенційні ризики, пов’язані з IoT, досягнуть нових рівнів, оскільки сумісність, гібридні програми та автономне прийняття рішень почнуть збільшувати складність системи, уразливості безпеки та потенційні вразливості. Інтернет речей створює ризики для конфіденційності, оскільки складні мережеві структури створюють більше вразливостей. В Інтернеті речей значна частина інформації пов’язана з особистими даними користувачів, такими як дата народження, місцезнаходження, особисті облікові записи тощо. Це один із аспектів

проблеми з великими даними, де спеціалісти з безпеки повинні переконатися, що всі потенційні ризики конфіденційності даних враховано.

Інтернет речей має бути впроваджений у законодавчо, етично, соціально та політично прийнятний спосіб, беручи до уваги правові питання, системні підходи, технічні проблеми та питання бізнесу [6]. Основні проблеми IoT продемонстровані на рисунку 1.5.

Рисунок 1.5 – Проблеми пов’язані з Інтернетом речей

Такі технології, як програмування пристроїв, шифрування пам’яті та списки контролю доступу (ACL), є досить повільними за своєю природою. Мало уваги приділено застосуванню ефективних заходів безпеки та конфіденційності для захисту даних і контролю доступу на основі динаміки ресурсів, середовищ, користувачів або програм. Крім того, ще однією проблемою є збільшення втручання користувачів у захист власних даних [7].

Таким чином, користувачам необхідно надати детальний контроль доступу та кілька параметрів конфіденційності. Питання безпеки необхідно вирішувати протягом життєвого циклу IoT, від початкового проектування до операційних служб. Тому важливо визнати, що методи безпеки та конфіденційності мають бути динамічнішими та надійнішиими, щоб відповідати зростаючим вимогам.

1.4 Ризики та випробування пов’язані з використанням пристроїв IoT

Сенсорні пристрої IoT, такі як фітнес-трекери, пристрої моніторингу здоров’я та NFC пристрої, обробляють дуже конфіденційні споживчі та фінансові дані. Стрімке зростання обсягів даних, кількості підключених пристроїв або складних систем, таких як інтелектуальні пристрої та транспортні засоби, монітори здоров’я та датчики, призвело до загострення проблеми обробки даних, передачі, безпеки та контролю доступу.

Мережі пристроїв записують, керують, зберігають і передають великі обсяги конфіденційних даних. Оскільки методи обробки та аналізу згенерованих даних продовжують розвиватися, проблеми конфіденційності та безпеки неминучі. Несанкціонований доступ і зловживання даними з таких датчиків, як глюкометри, ваги, монітори серцевого ритму та артеріального тиску не можуть призвести до серйозної небезпеки для здоров’я. А от доступ до мережевих пристроїв, таких як побутова техніка, дверні замки, камери спостереження, печі може наразити власника помешкання на значну небезпеку. Проблеми безпеки при використанні кредитних карток або керуванні транспортними засобами небезпечно як з фізичних, так і з фінансових причин.

Однак у розумних пристроях IoT операції на стороні сервера, такі як аналіз даних, обробка та вихід, більш роззосереджені. Дані, що передаються через канал зв'язку, варіюються від показань датчиків до аналітичної інформації. Це робить канали передачі даних більш вразливими для хакерів і зловмисників.

Порівняно з типовою клієнт-серверною або розподіленою вебінфраструктурою, архітектури IoT відрізняються обсягом і різноманітністю даних, можливостями підключення, керуванням контролем і розподілом обчислень між різними рівнями. Тому важливо розуміти проблеми безпеки, з якими стикаються мережі IoT з точки зору багаторівневої архітектури. На рис. 1.6 показана архітектура з чотирьох частин, яка підтримує багато сучасних систем IoT [10].

Рисунок 1.6 – Загальна архітектура мережі Інтернету речей

Датчики і виконавчий рівень

Особливістю датчиків є їх здатність перетворювати інформацію, отриману із зовнішнього світу, в дані для аналізу. Іншими словами, важливо почати з четвертого етапу включення датчиків у структуру архітектури IoT, щоб отримати інформацію, яку можна фактично обробити. Для актуаторів процес йде ще далі — пристрої, здатні втручатися у фізичну реальність.

Рівень збору даних

Хоча цей рівень архітектури IoT все ще передбачає тісну співпрацю з датчиками та виконавчими механізмами, існують також мережеві інтерфейси та системи збору даних (DAS). Система збору даних підключається до сенсорної мережі, а інтернет-шлюз працює через Wi-Fi, дротові локальні мережі та здійснює подальшу обробку. На цьому етапі вкрай важливо опрацювати значний обсяг

інформації, зібраної на попередньому етапі, і стиснути його до оптимального розміру для подальшого аналізу. Крім того, зі структурної точки зору є необхідні зміни.

Рівень системи обробки та обчислення

На цьому етапі архітектури IoT підготовлені дані передаються в мультисервісну систему для локального зберігання, обчислень або логічної обробки. Сучасні IT-системи виконують розширений аналіз і попередню обробку даних.

Рівень центру обробки даних

Основні процеси на завершальних етапах архітектури IoT відбуваються в центрі обробки даних або хмарі. Хмарні центри обробки даних містять програми, які надають послуги для керування архітектурою IoT. На цьому рівні ефективність служби безпеки є критично важливою, щоб запобігти протиправному проникненню зловмисників та використанню кінцевих точок.

РОЗДІЛ 2. МЕТОДИ ВИРІШЕННЯ ПРОБЛЕМ ЗАХИСТУ ТА КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

2.1 Концепція Data Box

Серед способів використання хмарних рішень IoT для вирішення питань безпеки та конфіденційності персональних даних користувачів виділяються три найпоширеніших підходи. Це концепції використання DataBox, персональної бази даних і загальної бази даних.

Розглянемо основні ідеї використання Databox. Характеристики цієї концепції можна умовно розділили на чотири частини: Databox має бути надійною платформою; надавати ефективні та зручні засоби для керування даними; надавати контрольований доступ іншим сторонам, які бажають використовувати її дані; підтримувати використання різноманітних методів стимулювання [11].

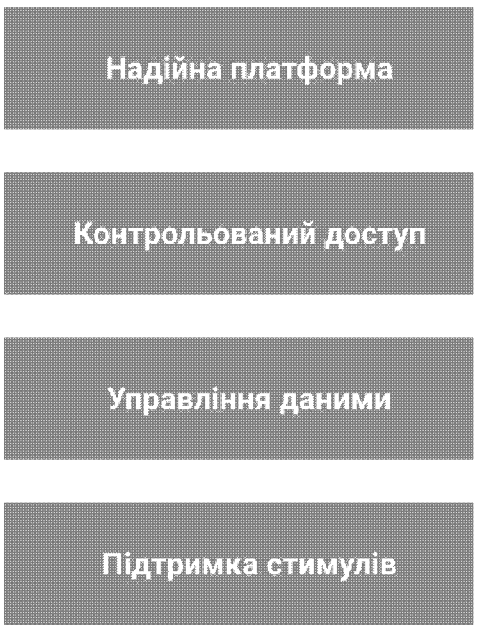


Рисунок 2.1 – Характеристика концепції Databox

Надійна платформа

Databox є основою присутності користувача в Інтернеті. Він фіксує, індексує, зберігає та керує даними про користувача, що вимагає значного рівня довіри до платформи. Databox отримує дані із різних джерел, таких як встановлені програми, параметри перегляду та вебповедінка. Це може зробити таку систему більш когнітивною та нав'язливою, хоча й більш корисною.

Довіра до платформи також вимагає її надійної поведінки як частини інфраструктури. Тобто Databox повинен мати права доступу, щоб ефективно допомагати користувачам керувати їх онлайн-взаємодіями. У той же час він повинен надати користувачам простий спосіб контролювати та втручатися в операції збору та обміну даними, які виконуються. Це дозволить запобігти порушенням у випадку, якщо автоматичні дії, що випливають із конфігурації та політики, матимуть непередбачувані наслідки. Нарешті, усі ці дії повинні супроводжуватись всеохоплюючим журналюванням і відповідними інструментами, щоб користувачі та (потенційні) сторонні аудитори могли створити впевненість у тому, що система працює, як очікувалося, і що, якщо станеться щось несподіване, результат системи може відслідковувати помилки.

Контрольований доступ

Метою Databox є не лише збір усіх особистих даних в одному місці, а й забезпечення контролю доступу до них. Користувачі повинні контролювати, які дані передаються третім особам. Складніші функції включають підтримку методів інтелектуального аналізу даних, що зберігають конфіденційність, наприклад диференціальну конфіденційність і гомоморфне шифрування.

Важливим фактором, який часто не враховують є необхідність контролювати періоди доступу в кожному окремому випадку. У певних ситуаціях потрібно скасовувати надані раніше права доступу. У системі, яка надає доступ до локальної обробки даних, це відносно просто реалізувати; а у системі, яка за замовчуванням копіює дані для спільної роботи, це досить складне завдання. Завдання полягає в тому, щоб зберегти або отримати інформацію про поточний і майбутній статус усіх потенційних третіх сторін, які можуть мати доступ до останніх даних.

Управління даними

Окрім збору даних і забезпечення контрольованого доступу до них, Databox також повинен надавати можливість користувачам взаємодіяти з ним і відображати дані, які він містить. Це дозволить користувачам приймати більш обґрунтовані рішення щодо дій, які вони виконують, безпосередньо або опосередковано, делегуючи контроль іншим. У рамках цієї взаємодії та для підтримки довіри платформи повинні дозволяти користувачам редагувати та видаляти дані в Databox, щоб враховувати неминучі інциденти.

Databox може автоматично забувати дані, які більше не актуальні або стали неправильними. Навіть якщо дані використовувалися раніше, користувачам, які захочуть їх редагувати в майбутньому, все одно потрібно «вилучити їх з використання».

Підтримка стимулів

Наслідком описаного вище контрольованого доступу є те, що користувачі можуть заборонити доступ до своїх даних стороннім службам, таким як рекламодавці або постачальники хмарних послуг. У деяких випадках це може призвести до того, що користувачі взагалі більше не зможуть користуватися віддаленими послугами. Однак було б корисніше надати цим послугам інший спосіб стягувати з користувачів оплату: ті, хто хоче платити комфортно може це зробити онлайн, ідентифікувавши себе, а той, хто не хоче розкривати особисту інформацію, може платити традиційними методами.

Тим не менш, Databox повинен мати можливість дозволити користувачам відстежувати потік платежів та інших сторонніх послуг, які пропонуються через певні додатки. Databox також може служити механізмом пом’якшення ризику для комерційних організацій, які не зацікавлені безпосередньо зберігати та контролювати низку приватних даних, таких як медичні записи. Комерційні організації все ще можуть отримувати доступ і запитувати дані, однак делегують повноваження з їх збереження. Це особливо вірно для міжнародних організацій, яким в іншому випадку потрібно розуміти численні правові тонкощі.

2.2 Концепція Personal Data Vaults

Сховище PDV — це сховище персональних даних, яке підтримує механізми володіння персональними даними, вибірковий обмін і аудит, що забезпечує видимість спільного використання даних. Ця система базується на двох принципах [12].

- кожен власник даних має персональний PDV;

- коли власник ділиться даними з іншою комерційною організацією, існує неявна або явна юридична угода щодо того, як ця комерційна організація використовуватиме отримані дані.

Такі принципи проектування вимагають, щоб окремі рішення щодо спільного використання керованих даних не були надто складними та трудомісткими, оскільки це призведе до того, що система стане непридатною до використання. Для реалізації цих принципів PDV розміщується між користувачами та постачальниками контент-послуг, як показано на рисунку 2.2.

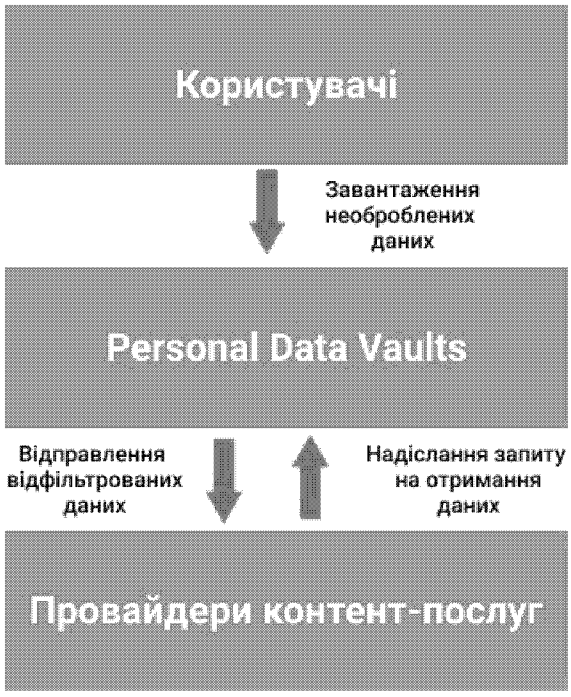


Рисунок 2.2 – Принципи взаємодії PDV

PDV містить три механізми керування політикою даних: списки контролю доступу (ACL), trace-аудит (аудит відстеження) та систему рекомендацій правил. Непрямий обмін даними через PDV має багато переваг перед використанням централізованого стороннього сховища даних.

Серед переваг можна виділити:

– право користувачів володіти персональними даними;

– право постачальників контент-послуг отримувати доступ до даних із дозволом користувача;

– зменшення ймовірності надмірності даних;

– зменшення випадків втрати даних і проблем з обмеженням ресурсів.

Стандартні *списки контролю доступу* (ACL) вказують, яким користувачам або системним процесам дозволено доступ до даних і які операції дозволено виконувати з даними. Списки доступу до соціальних мереж зосереджені на управлінні групами, тобто на тому, хто до яких даних може отримати, а не на контролі обміну даними.

Навпаки, розробники PDV намагаються підкреслити важливість детального контролю даних, що знаходяться у спільному використанні. Прототип PDV наразі підтримує такі три обмеження: поточні значення (bounds); їх точність (precision), та частота згадування (frequency), детально описані у табл. 2.1.

Trace-аудит

Прототип системи PDV передбачає два типи механізмів аудиту трасування: локальний аудит трасування для операцій реєстрації, що виконуються всередині PDV, і аудит трасування для сторонніх додатків для моніторингу операцій, що відбуваються за межами PDV (тобто на третій стороні). Локальний контрольний журнал веде доступ щодо зчитування даних користувача, які зберігаються в сховищі даних. Кожен запис журналу представлено у вигляді такого кортежу: <#timestamp, appId, #onType, dataTable, *dataField1, *dataField2, ..., $startRow, $endRow>. Отримана інформація запису даних потім візуалізується та надається власнику PDV, щоб пояснити, обмін якими даними відбувався.

Таблиця 2.1 – Типи обмежень, що підтримуються в PDV.

Обмеження	Тип	Атрибути
Ступінь точності	час місце число	value (private, hour, minute, second) timeframe (minute, week, hour, day, month) value (private, zipcode, exact, street, region, country) value (private, average),
Значення	час місце число текст	starttime, endtime format (out-circle, in-circle), radius (in km), center (GPS coordinates) upper, uppersymbol (=, >, >=), lower, lowersymbol (=, <, <=) symbol(=, !=), attrname, text
Частота повторення	час	unit(minute, second), value

Модуль аудиту сторонніх програм дозволяє зрозуміти, що відбувається з даними користувача, отриманими від PDV у програмі. Як і для локального аудиту, у програмі реалізований модуль Traceaudit для реєстрації даних, до яких здійснюється доступ, який виконується разом з організацією, представленою даними, до яких здійснюється доступ.

Система рекомендацій правил забезпечує високорівневий інтерфейс для встановлення політик обміну. Зокрема, він попередньо обчислює набір загальних ACL високого рівня отриманих на основі історичних даних, і система рекомендацій робить обчислені значення доступними для користувача (або довіреної особи від імені користувача), таким чином реалізується полегшення реконфігурації ACL.

Використовуючи систему рекомендацій політики, користувачі можуть більш активно брати участь у контрольованому обміні даними, а безперервний досвід роботи з системою дозволить користувачам повніше зрозуміти значення політики конфіденційності. Простого використання системи рекомендацій недостатньо, оскільки з часом запропоновані стратегії можуть не відповідати намірам користувача. Користувачам потрібно самостійно періодично перераховувати встановлені обмеження.

2.3 Концепція Data Bank

Data Bank — це платформа для керування даними з пристроїв IoT, які передаються до хмарних служб, як показано на рис. 2.3. Така платформа надає користувачам механізм для визначення політики збору даних на рівні пристрою та політики обміну даними на рівні хмари. Архітектура цієї концепції складається з чотирьох рівнів: прикладний рівень, хмарний рівень, локальне сховище та сенсорний рівень [13].

Прикладний рівень є верхнім рівнем мережі, що складається з інтерфейсу користувача, який визначає, як користувачі взаємодіють із Data Bank (його можна розгорнути на підключеному до Інтернету пристрої, через вебсайт або мобільну програму) та інтерфейсу обміну даними, який розглядається як прикладний інтерфейс програм (API) і керує потоками даних для служб та серверів.

Програмний інтерфейс діє як месенджер, приймаючи запити сервісів, передаючи їх модулю контролю доступу та повертає результат. Користувачі є власниками даних у такій системі, а служби виконують роль зовнішніх користувачів (третьої особи), які намагаються отримати доступ до даних або програм, встановлених у Data Bank.

Хмарний рівень складається з п’яти основних компонентів:

- у модуль контролю доступу надходять запити від служб, він перевіряє чи має служба доступ до запитаних даних на основі політики конфіденційності та готує дані у відповідь на запити;

- модуль аудиту формує журнал усіх транзакцій даних, які проходять у Data Bank, наприклад, наданий доступ до даних, відхилений доступ, транзакції даних тощо;

- сховище знаходиться в хмарі і зберігає всі дані користувача. У формі, визначеній політикою збору даних (так дані можна відфільтрувати та обробити перед збереженням у хмарному сховищі). Крім того, Data Bank може містити посилання на зовнішні сховища (наприклад, стороннє хмарне сховище), підключені до бази даних;

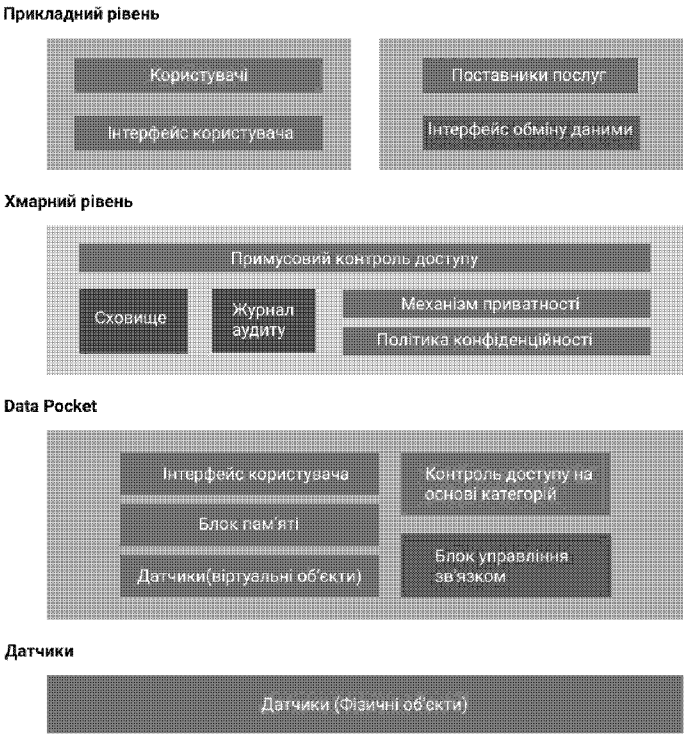


Рисунок 2.3 – Архітектура концепції Data Bank

- механізм конфіденційності співпрацює з користувачем на основі заданих налаштувань конфіденційності. Він генерує токени доступу до пов'язаних служб. Механізм також виконує аналіз даних, наприклад ідентифікує регулярні запити;

- політика конфіденційності – це довідкові рішення, запропоновані практичними механізмами конфіденційності та налаштовані користувачами. Ця політика застосовується до модуля контролю доступу, який перевіряє, чи має служба дозвіл на доступ до запитаних даних, і до механізму утиліти конфіденційності, який використовується для розподілу маркерів між службами.

Кишеньковий рівень даних Pocket Data призначений для інтерфейсів користувача, працює на локальних комп'ютерних пристроях (таких як центри Інтернету речей) і опрацьовує політики збору даних. Метою цього інтерфейсу є фіксація налаштувань конфіденційності користувача.

Сенсорний рівень (фізичні об'єкти) включає пристрої IoT, об'єднані через Інтернет або локальну мережу. Фізичні пристрої підключаються до бази даних через вбудовані драйвери. У цьому шарі об'єктам заборонено спілкуватися між собою. Зв'язок між пристроями здійснюється за допомогою віртуальних об'єктів.

Порівняльний опис рішень щодо захисту персональних даних користувача, управління та конфіденційності наведено в таблиці 2.2.

Таблиця 2.2 – Порівняння характеристик технологій захисту персональних даних

	DataBox	PDV	Data Bank
Модель збору даних	—	+	+
Політики обміну даними	+	+	+
Контроль збору даних на рівні пристроїв	+	—	+
Можливість анонімізації даних	+	—	+
Підтримка оновлень політик	+	+	+
Специфікація політик	—	+	+

Як видно з таблиці, Data Bank забезпечує користувачам детальний контроль над даними та дозволяє користувачам ділитися даними зі службами відповідно до визначених користувачем політик, тим самим максимізуючи переваги для користувачів.

Щоб вирішити проблеми з конфіденційністю, засоби контролю даних застосовуються до збору та обміну даними: вони включають механізми для визначення політики збору даних на рівні пристрою, механізми для фільтрації та обробки даних перед надсиланням їх у хмарне сховище (замість того, щоб скидати всі необроблені дані до хмари), а також включає засоби контролю доступу, щоб гарантувати, що зовнішні служби не можуть отримати прямий доступ до збережених даних. Користувачі можуть керувати політиками збору та обміну даними, застосованими в базі даних, і оновлювати політики в будь-який час.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА АНАЛІТИЧНА ОЦІНКА ЗАПРОПОНОВАНОГО МЕТОДУ

3.1 Опис методу узгодження конфіденційності

На основі проведеного аналізу сформовано загальну схему досліджуваного методу узгодження конфіденційності наведену на рис. 3.1. Запропонований метод узгодження конфіденційності дозволяє досягнути відкритості в середовищі IoT. Мережі IoT діятимуть як інфраструктурний об'єкт, подібно до електромережі. Мережа доступна для користувачів IoT у будь-який час і в будь-якому місці [15].

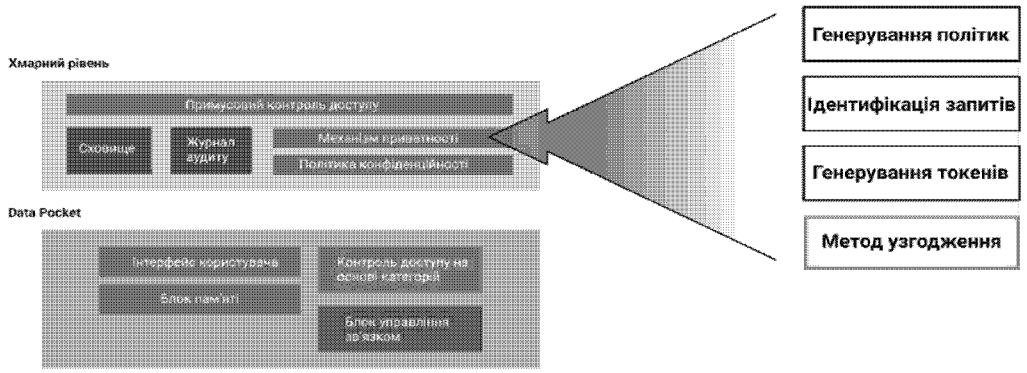


Рисунок 3.1 – Досліджуваний механізм приватності у мережі IoT

Відкрите середовище вимагає від сторін, які беруть участь в обміні інформацією, чіткого висвітлення своїх вимоги щодо конфіденційності. Це схоже на протокол P3P [16], де браузер узгоджує від імені користувача запити конфіденційності, зроблені користувачем із відвіданого веб-сайту, щоб контролювати особисту інформацію, яку веб-сайт може збирати про користувача.

У такому підході користувачі та власники Інтернету речей зберігають свої вимоги до конфіденційності у файлах політики, які зберігаються локально та використовують мову розмітки XML. На рис. 3.2 та рис. 3.3 показано приклади сценаріїв політики конфіденційності для користувачів і власників IoT відповідно.

```
<!-- Початок декларації політики конфіденційності -->
<privacy-policy>

  <!-- Початок секції введення даних -->
  <data-in type="image" priority="1"> <!-- Дані типу "зображення" з високим пріоритетом (1) -->
    <retention>3-month</retention> <!-- Дані зберігаються протягом 3 місяців -->
    <shared>no</shared> <!-- Дані не будуть передаватися іншим сторонам -->
    <inferred>yes</inferred> <!-- Дані будуть використані для висновків або аналітики -->
  </data-in>
  <!-- Кінець секції введення даних -->

  <!-- Початок секції виведення даних -->
  <data-out>
    <!-- Дані типу "відео" з високим пріоритетом (1) -->
    <data-out type="video" priority="1">
      <retention>1-year</retention> <!-- Дані зберігаються протягом 1 року -->
      <shared>no</shared> <!-- Дані не будуть передаватися іншим сторонам -->
      <inferred>no</inferred> <!-- Дані не будуть використані для висновків або аналітики -->
    </data-out>
  </data-out>
  <!-- Кінець секції виведення даних -->

</privacy-policy>
<!-- Кінець декларації політики конфіденційності -->
```

Рисунок 3.2 – Лістинг політики конфіденційності користувача.

```
<!-- Початок декларації політики конфіденційності -->
<privacy-policy>

  <!-- Початок секції введення даних -->
  <data-in type="video" priority="1"> <!-- Дані типу "відео" з високим пріоритетом (1) -->
    <retention>1-year</retention> <!-- Дані зберігаються протягом 1 року -->
    <shared>no</shared> <!-- Дані не будуть передаватися іншим сторонам -->
    <inferred>yes</inferred> <!-- Дані будуть використані для висновків або аналітики -->
  </data-in>
  <!-- Кінець секції введення даних -->

  <!-- Початок секції виведення даних -->
  <data-out>
    <!-- Дані типу "виявлення облич" з високим пріоритетом (1) -->
    <data-out type="face-detection" priority="1">
      <retention>1-year</retention> <!-- Дані зберігаються протягом 1 року -->
      <shared>no</shared> <!-- Дані не будуть передаватися іншим сторонам -->
      <inferred>no</inferred> <!-- Дані не будуть використані для висновків або аналітики -->
    </data-out>

    <!-- Дані типу "зображення" з високим пріоритетом (1) -->
    <data-out type="image" priority="1">
      <retention>1-year</retention> <!-- Дані зберігаються протягом 1 року -->
      <shared>no</shared> <!-- Дані не будуть передаватися іншим сторонам -->
      <inferred>yes</inferred> <!-- Дані будуть використані для висновків або аналітики -->
    </data-out>
  </data-out>
  <!-- Кінець секції виведення даних -->

</privacy-policy>
<!-- Кінець декларації політики конфіденційності -->
```

Рисунок 3.3 – Лістинг політики конфіденційності власника

Як видно з рис. 3.2, політику конфіденційності користувача IoT визначає тег <data-in>, який визначає тип даних, які користувач бажає отримати від власника IoT, і піделементи, які визначають сценарії використання цих даних. Теги <data-in> політики конфіденційності користувача IoT порівнюватимуться з тегами <data-out> політики власника IoT, оскільки остання визначає метод збору даних, прийнятий власником IoT. Натомість тег <data-in>, указаний у політиці власника IoT на рис. 3.3, буде зіставлено з тегом <data-out> у політиці конфіденційності користувача IoT, щоб гарантувати, що рівень збору даних, який виконує власник IoT, є прийнятним для користувача Інтернет речей.

Стратегії прогнозування для кожного користувача можна передбачити шляхом аналізу кількох сценаріїв збору даних. Використання передбачень може допомогти уникнути виснажливих і схильних до помилок екранів налаштувань конфіденційності. Це досягається завдяки дозволу на багаторівневе узгодження послуг із різноманітними сценаріями збору даних.

Підхід до узгодження моделює взаємозв'язок між збором даних і послугами Інтернету речей як компроміс між конфіденційністю та корисністю, як показано в рівнянні 1. Це дозволяє власникам IoT пропонувати кілька варіантів конфіденційності на основі рівня обслуговування визначеного користувачем.

У формулі прогнозування переваг використовуються чотири форм-фактори, які впливають на налаштування конфіденційності в середовищах IoT. Ці чотири фактори зберігаються в XML-представленні політики конфіденційності як піделементи кожного тегу <data-in> і <data-out>.

Кожен із цих чотирьох елементів описується наступним чином:

1. Тип даних (t). Тип датчика, до якого здійснюється доступ, може мати різний ступінь конфіденційності для власника цього датчика. Такі датчики, як камери чи мікрофони, чутливі за своєю природою. Тому доступ до цих датчиків слід дозволяти з обережністю. Відомі методи, які можуть мінімізувати ступінь порушення конфіденційності під час доступу до цих датчиків, такі як розмиття обличчя [17] або ретельний вибір аудіофункцій, щоб уникнути побудови мови із

захопленого аудіо [18]. Такі методи потрібно додати до XML-файлу як частину процесу узгодження.

2. Утримання. (r) Політика зберігання визначає, як довго зберігаються журнали даних обміну. У програмах реального часу, які не потребують зберігання даних, власники або користувачі Інтернету речей можуть використовувати цей фактор для примусового очищення своїх даних, залишивши цей елемент порожнім.

3. Загальний доступ (s). Якщо власник або користувач Інтернету речей ділиться даними, зібраними для завдання Інтернету речей, потрібно вказати будь-яких сторонніх одержувачів.

4. Прогнозований результат (i). Одержувач даних повинен вказати, чи будуть використані методи виведення для отримання додаткової інформації з даних. Наприклад, дані акселерометра можна використовувати для моніторингу вправ користувача в медичних програмах, але також можна використовувати для визначення місцезнаходження користувача в приміщенні.

Інші формальні фактори, які також можуть бути розглянуті, включають причину запиту даних, місце, мету та переваги збору даних. Після вивчення згаданих вище факторів, що впливають на конфіденційність, їх буде включено до розрахунку корисності конфіденційності. Наступна функція використовуються для оцінки корисності конфіденційності:

$$U = -\gamma \cdot Pe(t,r,s,i) + B(t,r,s,i), \quad (1)$$

де, U – позначає загальну корисність, яка буде досягнута при здійсненні обміну інформацією при запуску програми IoT,

Pe –це ступінь конфіденційності для обраної політики конфіденційності,

B – це перевага від обміну даними з точки зору власника конфіденційних даних

γ – є загальним фактором сприйняття чутливості конфіденційності.

Перевага B для власника IoT може бути грошовим стимулом або соціальною вигодою від надання можливості запуску додатків IoT до своїх даних. Щодо користувача IoT, то перевагою буде послуга, що надається додатком IoT.

Різні політики призведуть до різних рівнів впливу на конфіденційність залежно від форм-факторів впливу, вибраних у політиці. Наприклад, для

високочутливих даних, описаних у *t*, довший період зберігання, представлений через *r*, призведе до вищого значення *Pe*.

Фактор γ може варіюватися в залежності від місця розташування або контексту користувача. Значення γ множиться на *Pe* для збільшення або зменшення загального витоку конфіденційності для конкретних даних. Знак мінус у правій частині рівняння забезпечує відповідність умові переваг *B*.

3.2 Процес узгодження політик конфіденційності

Координація політики відбувається у двох контекстах (рис. 3.4).

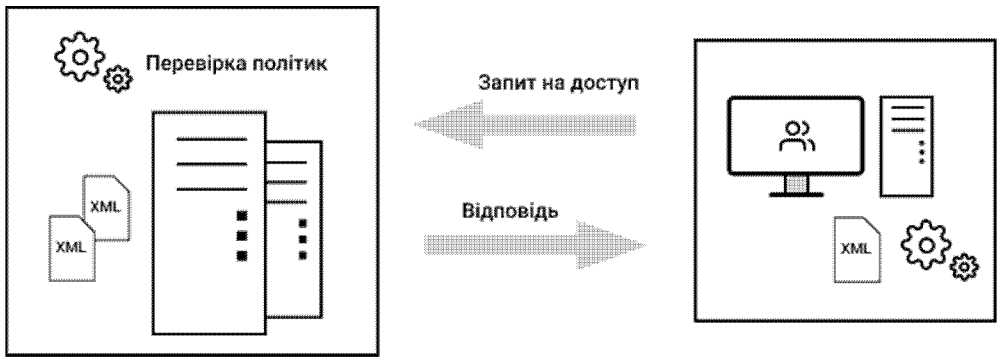


Рисунок 3.4 – Процес роботи методу узгодження

Сценарій починається з того, що користувач IoT надсилає власнику IoT запит на доступ до певного типу даних (датчика). Дані беруться з елемента <data-in> таких даних у політиці користувача. Після отримання запиту на доступ власник IoT перевіряє корисність запиту, замінюючи його функцією. Якщо припустити, що корисність запиту дорівнює або перевищує корисність елемента <data-out> для тих самих даних у політиці конфіденційності власника IoT, запит приймається. Потім власник IoT підключається до користувача IoT і починає діяти як ретранслятор, передаючи інформацію датчиків, отриману від інфраструктури IoT.

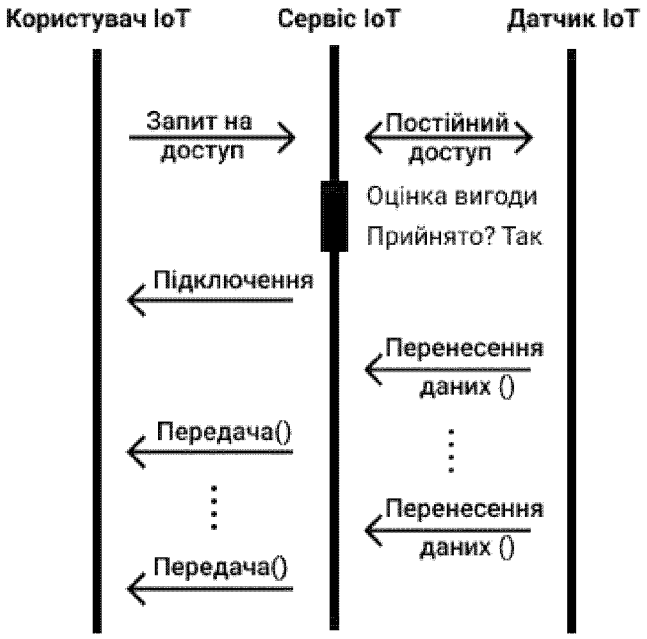


Рисунок 3.5 – Процес однофазного узгодження

Процес двофазного узгодження показаний на рисунку 3.6. Цей сценарій починається аналогічно, коли користувач IoT надсилає запит на доступ до даних власнику IoT. Однак корисність запиту була визнана утилітою неприйнятною для власника IoT.

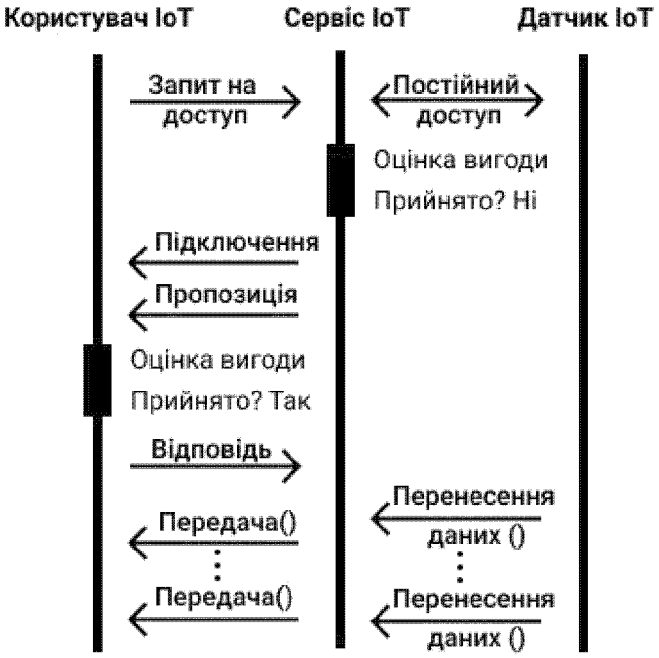


Рисунок 3.6 – Процес двофазного узгодження

Тоді, власник IoT надішле користувачу елемент <data-out> запитаного елемента даних із власної політики конфіденційності. Це відбувається лише під час підключення до користувача IoT.

Потім пристрій IoT користувача перевіряє корисність цієї пропозиції на відповідність політиці другого пріоритету (якщо ця політика визначена у файлі політики конфіденційності). Кожен тег <data-in> і <data-out> у політиці конфіденційності містить атрибут пріоритету, який дозволяє користувачам і власникам Інтернету речей вказувати альтернативну політику для використання під час узгодження.

Зазначення лише одного правила політики пріоритету для елемента даних означає, що політика елемента даних не підлягає обговоренню. Якщо припустити, що користувач IoT прийняв альтернативу, власник IoT почне передачу даних, як тільки він їх отримає безпосередньо від джерела даних.

3.3 Загальна структура використання Data Bank

Розглянемо діаграми класів, що показують загальні зв'язки між компонентами всередині кожного шару та між окремими шарами і пропонують шляхи реалізації компонентів.

Прикладний рівень містить чотири основні класи. UserInterface та DataSharingInterface відповідають за автентифікацію, представлення інформації та перевірку даних. Вони містять функції перегляду та контролери для оперування даними про користувачів і служби.

Представлення складається з усіх методів, які безпосередньо взаємодіють з користувачами та службами. Наприклад, клас UserInterface має метод для створення графічного інтерфейсу користувача (GUI), який дозволяє користувачам взаємодіяти з базою даних для створення інтерфейсу прикладного програмування (API).

Крім того, функція перегляду має методи для представлення інформації користувачам і службам у певних форматах (фігури, зображення, діаграми, текстові файли тощо). Частина контролера є посередником, який спілкується з функціями перегляду та моделлю даних; він має метод для перевірки даних у представленні та метод для передачі цих даних у модель даних.

Клас User зберігає та керує даними про користувачів, а клас Service зберігає та керує даними про служби. Прикладами даних користувача та служби є ім'я, ідентифікатор тощо. Класи User і Service також містять методи та конструктори, які підтримують інкапсуляцію, наприклад методи get і set для маніпулювання даними в класі. Усі класи цього рівня працюють на веб-сервері.

Хмарний рівень містить класи, які в основному використовуються для маніпулювання даними. Repository має методи для створення схем баз даних (сховища, наданого Data Bank), створення підключення до бази даних, виконання команд SQL і створення API для взаємодії з зовнішнім сховищем даних.

Через обмежену локальну пам'ять пристроїв IoT клас DataRetentionPolicy керує часовими обмеженнями. Він визначає тривалість збереження елементів даних в локальній пам'яті пристрою та у сховищі. Цей клас має метод очищення сховища.

У класі PrivacyPolicy розміщено деталі політики конфіденційності, там є методи для оновлення політики та сповіщення користувачів про зміни політик.

Клас PrivacyUtilityMechanism містить методи для оптимізації конфіденційності, генерації політик за замовчуванням і генерації маркерів служби.

Клас EnforcementAccessControl має методи для оцінки авторизації служби, методи для оцінки запитів і методи для створення даних, які використовуються у відповідь на запити до служби.

Клас AuditingLog містить метод генерації журналу, метод очищення журналу та метод, який повертає файл журналу, який зберігає історію транзакцій.

На рівні Data Pocket основним класом є PolicyInterface, який містить методи для створення графічного інтерфейсу користувача для запису налаштувань користувача та оновлення політик, а також методи перевірки інтерфейсу для

представлення політик у різних форматах (наприклад, текст, графіка тощо) та дані користувача та передати їх у клас EnformentDataCollection, також клас EnformentDataCollection, має методи для забезпечення виконання політик збору даних, методи для фільтрації даних перед їх надсиланням у хмару (як визначено політикою збору даних), а також методи для обробки даних.

Клас CommunicationControlUnit містить методи для керування зв'язком між віртуальними об'єктами на основі протоколів. У класі Sensor розміщено інформацію щодо датчиків. Він використовує методи для створення та знищення віртуальних об'єктів.

У класі Category розміщено інформацію про категорію, і аналогічно клас Action описує різноманітні операції з даними: шифрування, дешифрування тощо.

У класі DataItem розміщено інформацію про елементи даних. Action, Category та DataItem містять відповідні конструктори та службові методи отримання та підлаштування. Усі класи на цьому рівні працюють локально.

На сенсорному рівні фізичні об'єкти взаємодіють з віртуальними об'єктами (класами датчиків) через драйвери (пристрої IoT можуть обмінюватись даними за допомогою кількох стандартних протоколів, таких як Wi-Fi, Bluetooth, Z-wave, ZigBee).

3.4 Моделювання методу Data Bank узгодження конфіденційності

Для реалізації запропонованого підходу до управління інформацією та підвищення рівня конфіденційності використовується хмарний сервіс Amazon.

AWS є найпоширенішою у світі комерційною платформою хмарних обчислень, яку підтримує та розробляє Amazon. Надає понад 175 повнофункціональних послуг для центрів обробки даних по всьому світу. Технологія AWS базується на кластерах серверів (фермах), розташованих по всьому світу. Мільйони клієнтів, включаючи стартапи, що швидко розвиваються,

найбільші корпорації та провідні державні установи, використовують AWS для зниження витрат, підвищення гнучкості і прискорення інноваційного процесу [20].

Для серверної частини було вибрано EC2Instance від AWS. На ньому розгорнуті сервери для прийому запитів і їх обробки. Програмування виконано на Python – інтерпретованій об’єктно-орієнтованій мові програмування високого рівня зі строгою динамічною типізацією.

Програма клієнт (інтерфейс постачальника послуг) використовується для надсилання та отримання запитів на доступ до даних. Програма розташована на персональному комп'ютері і також реалізована мовою Python.

Щоб оцінити ефективність запропонованого підходу, необхідно визначити, що таке ефективність у даному контексті.

Оскільки запропонований метод порівнює політики користувачів, що відповідають їх уподобанням щодо конфіденційності під час обміну даними з постачальниками послуг, важливо, щоб час, витрачений на обробку цих запитів, не перевищував оптимального значення. Тобто під ефективністю вважатиметься час, витрачений на узгодження політики конфіденційності обох сторін. Блок-схема реалізації алгоритму узгодження представлена на рис. 3.7.

Однофазне узгодження. Постачальник послуг запитує доступ до даних, які він хоче отримати. Запит надсилається на хмарний сервер, де зберігається політика конфіденційності. На основі необхідних даних відбувається вибір політики, розробленої власником даних, і виконується її аналіз на відповідність. Якщо обидві сторони задоволені політикою то встановлюється з’єднання і розпочинається передача даних.

Двофазне узгодження подібне до фази перевірки політики при однофазному узгодженні. Якщо політику відхилено, встановлюється з’єднання з користувачем і надсилається політика конфіденційності, визначена постачальником послуг. Якщо політика постачальника відповідає умовам конфіденційності, визначеним користувачем, генерується позитивна відповідь і починається передача даних, інакше виконуються дії щодо повторного узгодження політик.

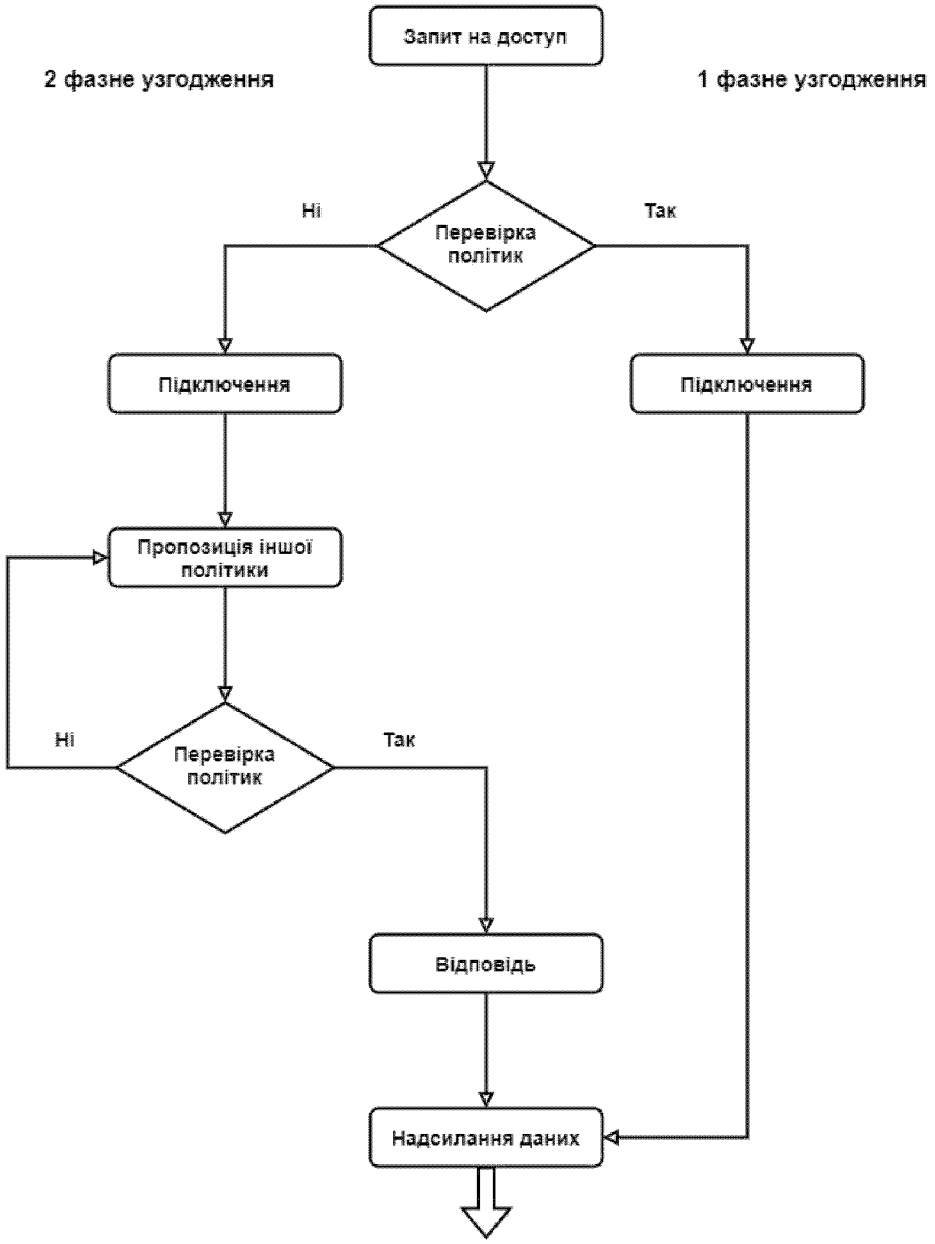


Рисунок 3.7 – Блок-схема алгоритму узгодження

Можливості використання запропонованого методу узгодження конфіденційності перевірялись на трьох варіантах загальноприйнятих сценаріїв: пряма передача, однофазне узгодження, двофазне узгодження. Згідно з результатами симуляції, одноетапний метод узгодження політики працює на кілька мікросекунд повільніше, ніж за умови отримання даних від датчиків без вимог конфіденційності через порівняння політик. Через необхідність повторної передачі різних політик для виконання процесу визначення переваг, двофазове узгодження відбувається в середньому на 30 мікросекунд повільніше. Результати моделювання

подано на рис. 3.8. Для більш простого розуміння результатів була проведена апроксимація методом найменших квадратів (рис. 3.9).

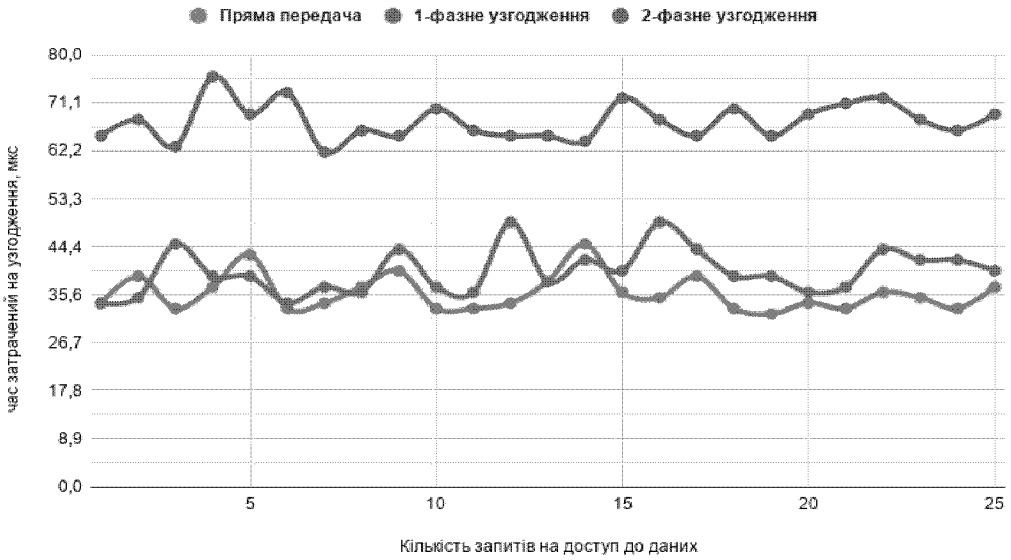


Рисунок 3.8 – Час необхідний для узгодження політик

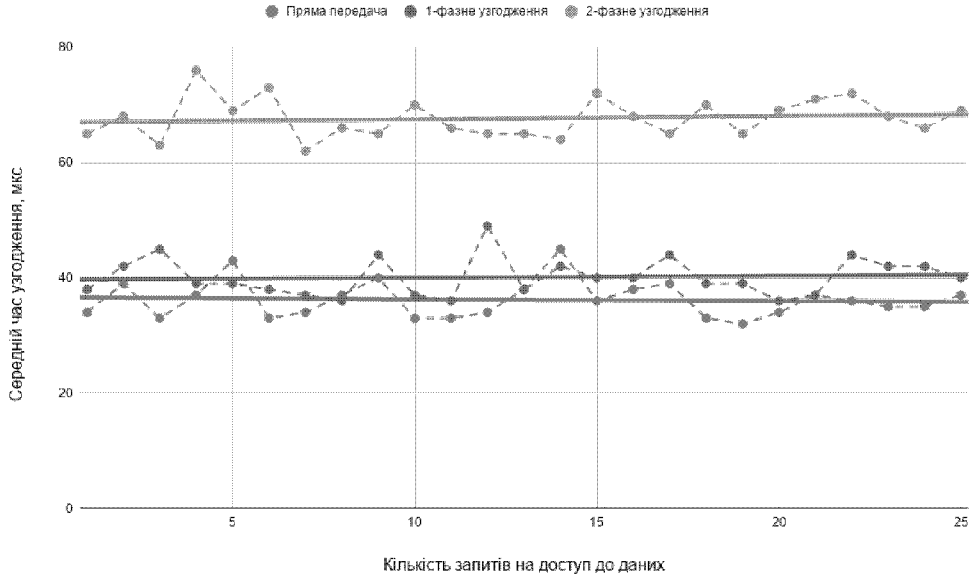


Рисунок 3.9 – Апроксимація часу затраченого на узгодження політик

Обидва розглянуті способи узгодження політик конфіденційності надають користувачам додаткові переваги у вигляді налаштувань правил конфіденційності та не обмежують інші зручності використання послуг. Запропонований у роботі підхід є практичним, адже він дозволяє узгодити політику конфіденційності

користувача з власником системи IoT уникаючи безпосереднього втручання користувача та підтримує вибір із різноманітних попередньо налаштованих політик конфіденційності.

У таблиці 3.1 показано порівняння інструментів, наданих у загальній архітектурі Data Bank і модифікованій архітектурі Data Bank, враховуючи характеристики, які впливають на прийняття рішень користувачем [11].

Таблиця 3.1 – Характеристики, що впливають на процес прийняття рішень користувачів.

	Базова архітектура IoT	Архітектура IoT з концепцією Data Bank
Користувач може контролювати дані, що буде накопичувати компанія	—	+
Користувач може відстежувати, які компанії збирають особисті дані	+	+
Користувач може узгоджувати запитувані дані	—	+
Користувач знає причину запиту даних	+	+
Користувач може переглядати оприлюднені дані	+	+
Користувач може зробити оприлюднену інформацію анонімною	—	+

З результатів моделювання та даних у таблиці 3.1 видно, що метод прямої передачі даних є швидшим, але він може задовольнити лише 50 % ситуацій, які впливають на прийняття рішень користувачем. Таким чином, запропонований підхід є кращим рішенням для збереження конфіденційності спільних даних завдяки запропонованому протокольному підходу, контролю над політикою збору та обміну даними, що застосовується в Data Bank, і можливості змінювати політику конфіденційності в будь-який час [12].

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

З розвитком науково-технічного прогресу важливу роль грає можливість безпечного виконання людьми своїх трудових обов'язків. У зв'язку з цим була створена і розвивається наука про охорону праці і життєдіяльності людини.

Безпека життєдіяльності (БЖД) - це комплекс заходів, спрямованих на забезпечення безпеки людини в середовищі проживання, збереження йог здоров'я, розробку методів і засобів захисту шляхом зниження впливу шкідливих і небезпечних факторів до допустимих значень, вироблення заходів по обмеженню збитку в ліквідації наслідків надзвичайних ситуацій мирного і воєнного часу.

Охорона здоров'я трудящих, забезпечення безпеки умов праці, ліквідація професійних захворювань і виробничого травматизму складає одну з головних турбот людського суспільства. Звертається увага на необхідність широкого застосування прогресивних форм наукової організації праці, зведення до мінімуму ручної, малокваліфікованої праці, створення обстановки, що виключає професійні захворювання і виробничий травматизм.

4.1 Характеристика умов праці програміста

Науково-технічний прогрес вніс серйозні зміни в умови виробничої діяльності робітників розумової праці. Їх праця стала більш інтенсивним, напруженим, які вимагають значних витрат розумової, емоційної і фізичної енергії. Це зажадало комплексного рішення проблем ергономіки, гігієни і організації праці, регламентації режимів праці та відпочинку.

В даний час комп'ютерна техніка широко застосовується у всіх областях діяльності людини. При роботі з комп'ютером людина піддається дії ряду

небезпечних і шкідливих виробничих факторів: електромагнітних полів (діапазон радіочастот: ВЧ, УВЧ і СВЧ), інфрачервоного і іонізуючого випромінювань, шуму і вібрації, статичної електрики і ін.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ЕОМ. Велике значення має раціональна конструкція і розташування елементів робочого місця, що важливо для підтримки оптимальної робочої пози людини-оператора.

У процесі роботи з комп'ютером необхідно дотримувати правильний режим праці та відпочинку. В іншому випадку у персоналу наголошуються значна напруга зорового апарату з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, в поясниці, в області шиї і руках.

4.2 Вимоги до виробничих приміщень

Забарвлення приміщень і меблів повинні сприяти створенню сприятливих умов для зорового сприйняття, гарного настрою.

Джерела світла, такі як світильники і вікна, які дають віддзеркалення від поверхні екрану, значно погіршують точність знаків і тягнуть за собою перешкоди фізіологічного характеру, які можуть виразитися в значній напрузі, особливо при тривалій роботі. Віддзеркалення, включаючи віддзеркалення від вторинних джерел світла, повинне бути зведено до мінімуму. Для захисту від надмірної яскравості вікон можуть бути застосовані штори і екрани.

Освітлення. Правильно спроектоване і виконане виробниче освітлення покращує умови зорової роботи, знижує стомлюваність, сприяє підвищенню продуктивності праці, благотворно впливає на виробниче середовище, надаючи

позитивну психологічну дію на працюючого, підвищує безпеку праці і знижує травматизм.

Недостатність освітлення приводить до напруги зору, ослабляє увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає засліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань, тому такий важливий правильний розрахунок освітленості.

Існує три види освітлення - природне, штучне і поєднане (природне і штучне разом).

Природне освітлення - освітлення приміщень денним світлом, що потрапляє через світлові прорізи в зовнішніх огороджуючих конструкціях приміщення. Природне освітлення характеризується тим, що змінюється в широких межах залежно від часу дня, пори року, характеру області і ряду інших чинників.

Штучне освітлення застосовується при роботі в темний час доби і вдень, коли не вдається забезпечити нормовані значення коефіцієнта природного освітлення (похмура погода, короткий світловий день).

Освітлення, при якому недостатнє за нормами природне освітлення доповнюється штучним, називається змішаним освітленням.

Згідно СНіП II-4-79 в приміщень обчислювальних центрів необхідно застосувати систему комбінованого освітлення.

При виконанні робіт категорії високої зорової точності (найменший розмір об'єкту розрізнення 0,3 ... 0,5 мм) величина коефіцієнта природного освітлення (КЕО) повинна бути не нижче 1,5%, а при зоровій роботі середньої точності (найменший розмір об'єкту розрізнення 0,5 ... 1,0 мм) КЕО повинен бути не нижче 1,0%. В якості джерел штучного освітлення звичайно використовуються люмінесцентні лампи типа ЛБ, або ДРЛ, які попарно об'єднуються в світильники, які повинні розташовуватися рівномірно над робочими поверхнями.

Вимоги до освітленості в приміщеннях, де встановлені комп'ютери, наступні: при виконанні зорових робіт високої точності загальна освітленістьповинна

складати 300лк, а комбінована - 750лк; аналогічні вимоги при виконанні робіт середньої точності - 200 і 300лк відповідно.

Параметри мікроклімату. Параметри мікроклімату можуть мінятися в широких межах, у той час як необхідною умовою життєдіяльності людини є підтримка постійності температури тіла завдяки терморегуляції, тобто здатності організму регулювати віддачу тепла в навколишнє середовище.

Принцип нормування мікроклімату - створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Обчислювальна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вологості в приміщенні. У приміщеннях, де встановлені комп'ютери, повинні дотримуватися певні параметри мікроклімату. У санітарних нормах СН-245-71 встановлені величини параметрів мікроклімату, що створюють комфортні умови. Ці норми встановлюються в залежності від пори року, характеру трудового процесу і характеру виробничого приміщення (табл. 3.1).

Об'єм приміщень, в яких розміщені працівники обчислювальних центрів, не повинен бути меншим 19,5 м 3/ людини з урахуванням максимального числа одночасно працюючих в зміну.

Для забезпечення комфортних умов використовуються як організаційніметоди (раціональна організація проведення робіт залежно від пори року і доби, чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціювання повітря, опалювальна система).

Шум і вібрація. Шум погіршує умови праці надаючи шкідливу дію на організм людини. Працюючі в умовах тривалої шумової дії випробовують дратівливість, головні болі, запаморочення, зниження пам'яті, підвищену стомлюваність, зниження апетиту, біль у вухах і т.д. Такі порушення в роботі ряду органів і систем організму людини можуть викликати негативні зміни в емоційному стані людини аж до стресових. Тривала дія інтенсивного шуму [вище 80 дБ (А)] на слух людини приводить до його часткової або повної втрати.

Ергономічні вимоги до робочого місця. Проектування робочих місць, забезпечених відеотерміналами, відноситься до числа важливих проблем ергономічного проектування в області обчислювальної техніки.

Робоче місце і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи.

Ергономічними аспектами проектування відеотермінальних робочих місць, зокрема, є: висота робочої поверхні, розміри простору для ніг, вимоги до розташування документів на робочому місці (наявність і розміри підставки для документів, можливість різного розміщення документів, відстань від очей користувача до екрану, документа, клавіатури і т.д.), характеристики робочого крісла, вимоги до поверхні робочого столу, регульованість елементів робочого місця.

Головними елементами робочого місця програміста є стіл і крісло. Основним робочим положенням є положення сидячи.

Оптимальне розміщення предметів праці і документації в зонах досяжності:

1) дисплей розміщається в зоні а (у центрі);

2) системний блок розміщається в передбаченій ніші столу;

3) клавіатура у зоні г/д;

4) «миша» в зоні в справа;

5) сканер в зоні а/б (зліва);

6) принтер знаходиться в зоні а (праворуч);

7) документація: необхідна при роботі в зоні легкої досяжності долоні в, а у висувних ящиках столу література, невикористовувана постійно.

Для комфортної роботи стіл повинен задовольняти наступним умовам:

1) висота столу повинна бути вибрана з урахуванням можливості сидіти вільно, в зручній позі, при необхідності спираючись на підлокітники;

2) нижня частина столу повинна бути сконструйована так, щоб програміст міг зручно сидіти, не був змушений підбирати ноги;

3) поверхня столу повинна мати властивості, що виключають появу відблисків у поле зору програміста;

4) конструкція столу повинна передбачати наявність висувних ящиків (не менше 3 для зберігання документації, лістингів, канцелярських приналежностей);

5) висота робочої поверхні рекомендується в межах 680-760мм.

Висота поверхні, на яку встановлюється клавіатура, повинна бути близько 650мм.

Велике значення надається характеристикам робочого крісла. Так, рекомендована висота сидіння над рівнем підлоги перебуває в межах 420-550мм. Поверхня сидіння м'яка, передній край закруглений, а кут нахилу спинки - регульований.

4.3 Заходи та засоби протипожежного захисту

Під пожежною безпекою розуміють такий стан промислового або цивільного об’єкта, за якого з регламентованою ймовірністю виключається можливість виникнення і розвитку пожеж та впливу на людей небезпечних чинників пожежі, а також забезпечується захист матеріальних цінностей та довкілля.

Пожежна безпека об’єкта – доволі складне і багатоаспектне завдання, тому для його вирішення потрібно підходити комплексно. Комплекс заходів та засобів щодо пожежної безпеки складається із відповідних систем, зокрема:

1) системи запобігання пожеж, що містить підсистеми запобігання утворенню горючого середовища та виникненню в горючому середовищі джерела запалювання;

2) системи протипожежного захисту, що, своєю чергою, містить такі підсистеми: підсистема обмеження розвитку пожежі; підсистема забезпечення безпечної евакуації людей та майна; підсистема створення умов для успішного гасіння пожежі;

3) системи організаційно-технічних заходів, що передбачає організаційні, технічні, режимні та експлуатаційні заходи.

Організаційні заходи пожежної безпеки передбачають організацію пожежної охорони на об’єкті, проведення навчань з питань пожежної безпеки (інструктажі та пожежно-технічні мінімуми), застосування наочних засобів протипожежної пропаганди та агітації, організацію ДПД та ПТК, проведення перевірок, оглядів стану пожежної безпеки приміщень, будівель, об’єкта загалом та ін.

До первинних засобів пожежогасіння належать:

1) вогнегасники;

2) пожежні крани-комплекти, ручні насоси

3) лопати, ломи, сокири, гаки, пили, багри;

4) ящики з піском, бочки з водою;

5) азбестові полотнища, повстяні мати та ін.

Первинні засоби пожежогасіння розміщують на пожежних щитах, які встановлюють на території об'єкта з розрахунку один щит на 5000 м2. Вони мають бути пофарбовані у червоний колір, а пожежний інструмент у чорний.

Серед первинних засобів пожежогасіння найважливішу роль відіграють вогнегасники різних типів: водяні, водо-пінні, порошкові, вуглекислотні, газові.

Залежно від способу транспортування вони бувають: переносні (до 20 кг) та пересувні (до 450 кг).Залежно від об'єму вогнегасники бувають малолітражні (до 5л), ручні (до 10 л), пересувні (понад 10л).Вогнегасники маркують буквами, що означає їх вид та цифрами, що визначають їх об'єм.

Найбільш перспективними є порошкові вогнегасники, які застосовують для гасіння лужних металів, ЛЗР і ТР, електрообладнання, що горить під напругою до 1000В, твердих та газоподібних речовин.

Найбільш розповсюдженими є:

1) ОП-1, ОП-2, ОП-9, ОП-10 — переносні;

2) ОПА-50, ОПА-100 — пересувні.

Вони відрізняються між собою лише складом порошку та пристроєм для його подачі.

Вуглекислотні вогнегасники застосовуються для гасіння загорянь на машинах, автомобілях і для невеликих об'ємів нафтопродуктів, а також електроустановок під напругою до 1000В.

У корпусі вогнегасника міститься вуглекислий газ у рідкому стані під високим тиском 6мПа (ручні) і 15 мПА (переносні). У горловині балону змонтований спеціальний пусковий пристрій із сифонною трубкою, який приводиться у дію за допомогою вентильного або пістолетного пристрою.

Виникненню в горючому середовищі джерела запалювання запобігають використанням устаткування та пристроїв, при роботі яких не виникає джерел запалювання, використанням електроустаткування, що відповідає за досягнення класу пожежо- та вибухонебезпеки приміщеннями та зонами груп і категорій вибухонебезпечної суміші, виконанням вимог щодо сумісного зберігання речовин та матеріалів, використанням устаткування, що задовольняє вимоги електростатичної іскробезпеки, улаштуванням блискавкозахисту, організацією автоматичного контролю параметрів, що визначають джерела запалювання, використанням швидкодіючих засобів захисного вимкнення, заземленням устаткування, видовжених металоконструкцій, використанням при роботі з ЛЗР інструментів, що не допускають іскроутворення, ліквідацією умов для самоспалахування речовин і матеріалів, усуненням контакту з повітрям пірофорних речовин, підтриманням температури нагрівання поверхні устаткування, пристроїв, речовин та матеріалів, які можуть контактувати з горючим середовищем нижче гранично допустимої (80 %) температури займання.

ВИСНОВКИ

Проаналізовано існуючі моделі хмарної інфраструктури надання послуг IoT та збереження мережевих даних, на основі чого виявлено їх основні проблеми та недоліки, зокрема особливості збереження та передачі персональних та конфіденційних даних, зокрема у процесі ідентифікації та оплати наданих послуг.

Проаналізовано сучасні методи збереження конфіденційної інформації та управління даними в мережах Інтернету речей, що дозволяє обґрунтувати вибір прототипу. Проведено модифікацію діючої архітектури Інтернету речей у процесі обміну даними, шляхом впровадження концепції Data Bank. Показано зв'язки основних мережевих компонентів та специфікацію їх використання.

Розроблено новий спосіб обміну інформацією у IoT за рахунок використання узгодження політик конфіденційності, що надає користувачам детальний контроль над їх даними. Розглянуто сценарії використання і головні характеристики методу. Розглянуто загальну схему взаємодії компонентів на кожному рівні та зв'язок компонентів між окремими рівнями мережі, а також шляхи практичної реалізації компонентів.

Архітектура мереж IoT вдосконалена завдяки використанню концепції DataBank, що дозволяє узгодити вимоги щодо політики конфіденційності користувачів під час обміну даними.

Проведено моделювання запропонованого рішення, підтверджено його реалізованість, а аналітична оцінка модифікованої архітектури показала значне підвищення ефективності управління персональною інформацією та збереження даних.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Гогіташвілі Г.Г., Лапін В.М. Основи охорони праці: навч. посіб. Київ: Знання, 2008. 302с.

2. Безпека праці: ергономічні та естетичні основи: навч. посіб. Київ: Знання, 2006. 215 с.

3. Управління проектами : навч. посіб. Харків: ХНАУ ім. В. В. Докучаєва, 2010. 522 с.

4. Титоренко Г. А. / Інформаційні технології управління: навч. посіб. Миколаїв: Просвіта, 2007. 186 с.

5. Прокоп І.Г., Швайко Л.М., Буката Ю. В. С++. Основи програмування. Теорія та практика: підручник. Одеса: Фенікс, 2010. 544 с.

6. Інтегроване середовище розробки Visual Studio. URL: https://msdn.microsoft.com/ruru/library/dn762121.aspx

7. Мова програмування C# Огляд мови C#: URL: https://ci-sharp.ru/ukr/Teaching/mova-programmirovaniya-s-obzor-yazikas.html

8. Нові можливості .NET Framework. URL: https://msdn.microsoft.com/ruru/library/ms171868%28v=vs.110%29.aspx

9. Узагальнення досвіду використання АРМ. URL: http://biogr.znate.ru/docs/index-1467.html

10. WPF – Windows Presentation Foundation. URL: http://professorweb.ru/my/WPF/base_WPF/level1/info_WPF.ph

11. Басюк Т. М. Ранжування веб-сайтів в мережі інтернет. URL: http://science.lp.edu.ua/sites/default/files/Papers/3_2_0.pdf. (дата звернення: 15.05.2024).

12. Терещенко В. В. Аналіз сучасних методик пошукової оптимізації (SEO). URL: http://www.kdu.edu.ua/PUBL/statti/2015_6_48_6_2015.pdf. (дата звернення: 15.05.2024).

13. Brin S., Page L. The anatomy of a large-scale hypertextual Web search engine. Computer Networks and ISDN Systems. Stanford, 2004. P. 107–117.

14. Ganz A., Sieh L. Behavioral factors and SEO. Proceedings of 24th International Conference on Computer Communications and Networks. Las Vegas, 2015. P. 218–223.

15. Kostenko P. P., Levchenko I. V. Webservice for clarification relevant web-documents of search results of Google based on user behavior. Inzhenerni ta osvitni tehnologii. 2014. No 4 (8). P. 49–62.

16. Антонюк В. П., Плохіх, В. В. Безпека та конфіденційність в Інтернеті речей: теорія та практика. Київ: Наукова думка, 2020. 325 с.

17. Іванов І. Г. Основи захисту інформації в комп'ютерних системах: навч. посіб. Львів: Львівська політехніка, 2019. 252 с.

18. Коваленко А. С. Інформаційна безпека та криптографічні методи захисту даних. Київ: Політехніка, 2021. 185 с.

19. Мартинюк В. О. Інформаційна безпека та захист даних в Інтернеті речей. Харків: НТУ ХПІ, 2018. 162 с.

20. Петренко О. В. Захист персональних даних у системах Інтернету речей. Одеса: ОНПУ, 2019. 223 с.

21. Сидоренко А. М. Кібербезпека в Інтернеті речей: сучасні виклики та рішення. Київ: КНУ ім. Тараса Шевченка, 2020. 156 с.

22. Федоренко О. В. Конфіденційність і безпека в бездротових мережах: монографія. Суми: СумДУ, 2021. 235 с.

23. Чорний В. П. Методи та засоби захисту інформації в системах IoT. Львів: Львівської політехніки, 2019. 184 с.

24. Шевченко М. В. Безпека та приватність у розподілених системах: основи та сучасні підходи. Харків: Ранок, 2020. 231 с.

25. Яценко О. І. Приватність і конфіденційність в Інтернеті речей: правові та технічні аспекти. Київ: Юридична думка, 2018. 205 с.