Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Розробка програмної реалізації системи управління політикою конфіденційності місцезнаходження

Виконав: студент IV курсу, групи СНс-41
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Яремчук Н.М.
(підпис) (прізвище та ініціали)

Керівник _____ Фриз М.Є.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Козак Р.О.
(підпис) (прізвище та ініціали)

Тернопіль
2026

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«_8_» _червня_ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп’ютерні науки
(шифр і назва спеціальності)

Студенту Яремчуку Назарію Мар‘яновичу
(прізвище, ім’я, по батькові)

1. Тема роботи Розробка програмної реалізації системи управління політикою конфіденційності місцезнаходження

Керівник роботи кандидат технічних наук, доцент кафедри КН Фриз Михайло Євгенович
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*14*» *травня* 2026 року № *4/9-237*

2. Термін подання студентом завершеної роботи 22 червня 2026 р.

3. Вихідні дані до роботи Дані користувачів, дані про місцезнаходження, системні журнали

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ.
1. Аналіз предметної області та постановка завдання.
2. Система управління політикою конфіденційності місцезнаходження
3. Дослідження продуктивності системи
4. Безпека життєдіяльності, основи охорони праці
Висновки. Перелік джерел

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	кандидат технічних наук, доцент кафедри МТ Гурик Олег Ярославович		

7. Дата видачі завдання 26 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	26.01.2026	
2.	Підбір та опрацювання літературних джерел по темі кваліфікаційної роботи	27.01.2026-16.02.2026	
3.	Виконання дослідження щодо перевірки цілісності	17.02.2026-10.05.2026	
	реплікованих даних у хмарі з використанням		
	гомоморфного шифрування		
4.	Оформлення розділу «Аналіз предметної	11.05.2026-17.05.2026	
	області та постановка завдання»		
5.	Оформлення розділу «Перевірка цілісності	18.05.2026-24.05.2026	
	реплікованих даних у хмарі»		
6.	Оформлення розділу «Ефективна перевірка цілісності	25.05.2026-31.05.2026	
	реплікованих даних у хмарі		
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	01.06.2026-08.06.2026	
8.	Виконання завдання до підрозділу «Основи охорони	01.06.2026-08.06.2026	
	праці»		
9.	Оформлення кваліфікаційної роботи	09.06.2026-11.06.2026	
10.	Нормоконтроль	12.06.2026-15.06.2026	
11.	Перевірка на плагіат	16.06.2026	
12.	Попередній захист кваліфікаційної роботи	18.06.2026	
13.	Захист кваліфікаційної роботи	27.06.2026	

Студент _____ Яремчук Н.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Фриз М.Є.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка програмної реалізації системи управління політикою конфіденційності місцезнаходження // Кваліфікаційна робота освітнього ступеня «Бакалавр» // Яремчук Назарій Мар‘янович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНс-41 // Тернопіль, 2026 // С. 72, рис. – 25, табл. – 0 кресл. – 12, додат. – 0, бібліогр. – 50.

Ключові слова: управління, конфіденційність, місцезнаходження, алгоритм, безпека.

Кваліфікаційна робота присвячена дослідженню систем забезпечення конфіденційності місцезнаходження в цілях безпеки В першому розділі кваліфікаційної роботи описано предметну область дослідження, зокрема щодо захисту геоданих користувачів. Проаналізовано загрози, які становить витік місцезнаходження для користувачів геосервісів. Висвітлено підхід до шифрування геоданих на основі політик безпеки.

В другому розділі кваліфікаційної роботи описано основну концепцію системи управління політиками конфіденційності місцезнаходження. Розглянуто склад таких політик, виявлення конфліктів, видано рекомендації щодо реалізації певних політик.

В третьому розділі кваліфікаційної роботи описано процес розробки інтерфейсу користувача для налаштування політик конфіденційності Проаналізовано ефективність розробленої системи.

Об’єкт дослідження: процес захисту геоданих політиками безпеки.

Предмет дослідження: система управління політиками конфіденційності

ANNOTATION

Development of a Software Implementation for a Location Privacy Policy Management System // Qualification work of the educational level «Bachelor» // Yaremchuk Nazarii// Ternopil Ivan Pulyu National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group SNs-41 // Ternopil, 2026 // P. 72, fig. – 25, tabl. – 0, chair. – 12, annexes. – 0, references – 50.

Keywords: management, privacy, location, algorithm, security.

The qualification work is devoted to the study of location privacy systems for security purposes. The first section of the qualification work describes the subject area of the study, in particular, regarding the protection of users' geodata. The threats posed by location leakage for users of geoservices are analyzed. The approach to encrypting geodata based on security policies is highlighted.

The second section of the qualification work describes the basic concept of the location privacy policy management system. The composition of such policies, conflict detection, and recommendations for the implementation of certain policies are considered.

The third section of the qualification work describes the process of developing a user interface for configuring privacy policies. The effectiveness of the developed system is analyzed.

Object of the study: the process of protecting geodata with security policies.

Subject of the study: privacy policy management system

ЗМІСТ

ВСТУП 7
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАННЯ. 9
1.1 Оцінка актуальності питання та постановка завдань роботи 9
1.2 Огляд літератури 14
1.3 Політико-орієнтований підхід 15
1.4 Підхід до анонімності 19
1.5 Підхід на основі заплутування 24
1.6 Підхід до шифрування на основі політик 27
1.7 Висновок до першого розділу 29
РОЗДІЛ 2. СИСТЕМА УПРАВЛІННЯ ПОЛІТИКОЮ КОНФІДЕНЦІЙНОСТІ МІСЦЕЗНАХОДЖЕННЯ 30
2.1 Визначення політики конфіденційності щодо місцезнаходження 30
2.2 Виявлення конфліктів політик 35
2.3 Склад політики 44
2.4 Система політичних рекомендацій 46
2.5 Висновок до другого розділу 49
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ СИСТЕМИ 50
3.1 Розробка інтерфейсу користувача для налаштування політик 51
3.2 Ефективність використання системи 57
3.3 Висновок до третього розділу 58
РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 59
4.1 Ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером 59
4.2 Організація безпечної роботи електроустаткування задіяного при роботі системи електронного навчання 62
4.3 Висновок до четвертого розділу 64

ВИСНОВКИ..... 65
ПЕРЕЛІК ДЖЕРЕЛ..... 66

ВСТУП

Актуальність теми. Розвиток систем бездротового зв'язку та позиціонування дозволив розробити велику різноманітність послуг на основі місцезнаходження, які, наприклад, можуть допомогти людям легко знаходити членів сім'ї або найближчу заправку чи ресторан. Зі зростанням популярності послуг на основі місцезнаходження зростає занепокоєння щодо неправомірного використання інформації про місцезнаходження зловмисниками. Для збереження конфіденційності місцезнаходження багато зусиль було спрямовано на запобігання визначенню постачальниками послуг точного місцезнаходження користувачів. Мало які роботи намагалися допомогти користувачам керувати своїми налаштуваннями конфіденційності; проте управління конфіденційністю є важливим питанням у реальних застосуваннях.

Складання політик дозволяє користувачам вставляти та видаляти політики. Виявлення конфліктів політик автоматично перевірятиме конфлікти між політиками щоразу, коли відбуваються будь-які зміни. Система рекомендацій політик генеруватиме рекомендовані політики на основі основних вимог користувачів, щоб зменшити навантаження на користувачів. Прототип системи був впроваджений та оцінений з точки зору ефективності та результативності..

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є розробити просту у використанні систему управління конфіденційністю місцезнаходження. Зокрема, вона має визначати лаконічні, але виразні конструкції політики конфіденційності місцезнаходження, які можуть бути легко зрозумілі звичайним користувачам. Система має надавати різні функції управління політиками, включаючи складання політик, виявлення конфліктів політик та рекомендації політик.

Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати стан досліджень в галузі перевірки цілісності даних;

– Розробити систему управління політикою конфіденційності;

– Дослідити продуктивність системи.

Практичне значення одержаних результатів.

Полегшення навантаження на кінцевих користувачів під час управління їхніми налаштуваннями конфіденційності, щоб вони могли повною мірою користуватися перевагами LBS.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАВДАННЯ.

1.1 Оцінка актуальності питання та постановка завдань роботи

Досягнення в системах бездротового зв'язку та позиціонування (наприклад, GPS) дозволили розробити велику різноманітність послуг на основі місцезнаходження (LBS). Такі служби можуть повідомляти користувачам час очікування столика в найближчому ресторані або повідомляти користувачеві, коли друзі знаходяться в межах пішої досяжності.

Оскільки сервіси на основі місцезнаходження стають дедалі популярнішими, зростає занепокоєння щодо зловмисного використання інформації про місцезнаходження зловмисниками. Оскільки постачальники послуг визначення місцезнаходження (LBS) тепер можуть безперервно відстежувати та передавати інформацію про місцезнаходження користувача, користувачі отримують LBS ціною втрати конфіденційності свого місцезнаходження. Пристрої визначення місцезнаходження становлять серйозну загрозу конфіденційності своїх користувачів, оскільки вони відстежують та передають приватну інформацію. Розголошення інформації про місцезнаходження може наразити користувачів на небезпеку злочинної поведінки. Викрадачі можуть скористатися LBS для отримання інформації про місцезнаходження цілі. Крім того, можливо, що ваш рухомий пристрій, такий як мобільний телефон, буде заблокований небажаними повідомленнями від рекламодавців, якщо існує зв'язок між номерами телефонів та службами визначення місцезнаходження. Деякі користувачі не бажають розкривати інформацію про місцезнаходження за певних обставин у певний час. Конфіденційність місцезнаходження є серйозною проблемою через її поширене використання в нашому повсякденному житті. Наприклад, користувач може хотіти знати час очікування столика в найближчому ресторані. Користувач також може хотіти отримувати сповіщення, коли друзі знаходяться в пішій

доступності. Усі ці програми вимагають широкого використання даних про місцезнаходження [1]. Багато урядів та організацій ініціювали дослідження конфіденційності місцезнаходження. Уряди певних країн ініціюють обговорення конфіденційності у зв'язку із Законом про захист конфіденційності місцезнаходження [2]. Робоча група Geoprive Робочої групи з питань інтернет-інженерії (IETF) [3] також вивчає вимоги до конфіденційності місцезнаходження. Підсумовуючи, конфіденційність місцезнаходження стосується права осіб вирішувати, як, коли та для яких цілей інформація про їхнє місцезнаходження може бути розкрита іншим сторонам. Відсутність захисту конфіденційності місцезнаходження може бути використана зловмисною стороною для здійснення атак без згоди користувача, що ставить під загрозу особисту конфіденційність та безпеку користувача. Серйозні проблеми конфіденційності необхідно вирішити, щоб задовольнити як занепокоєння громадськості, так і необхідність дотримання чинного законодавства.

Щоб зменшити зусилля щодо відстеження переміщень особи, було запропоновано багато методів захисту конфіденційності місцезнаходження. Проблеми конфіденційності інформації зросли в усьому світі [4, 5]. Проблеми варіюються від детальних, загальнодоступних супутникових знімків, збору в Інтернеті, до баз даних ДНК. Більшість існуючих зусиль зосереджені на запобіганні тому, щоб постачальники послуг знали точне місцезнаходження користувачів. Конфіденційність можна захистити в таких додатках, зробивши дані анонімними перед тим, як поділитися ними з постачальниками послуг додатків. Анонімний набір даних про місцезнаходження забезпечує надійний захист конфіденційності, дозволяючи одночасно обмінюватися даними з довільними споживачами, оскільки жодне прив'язування до мети не обмежує дані для певних цілей. Однак цей підхід вимагає методів, що виходять за рамки виключення очевидних ідентифікаторів, оскільки просторово-часові характеристики даних дозволяють відстежувати та повторно ідентифікувати анонімні транспортні засоби, коли щільність користувачів низька. Тому

поширеною стратегією є використання агента анонімізації [6, 7, 8] для спотворення даних користувачів, реальні місця розташування та надсилати спотворені місця розташування постачальнику послуг. Постачальник послуг безпосередньо оброблятиме спотворені дані для відповіді на запити на основі місцезнаходження. Агент анонімізації відповідає за перетворення результатів запиту назад у форму, зрозумілу кінцевим користувачам. Наприклад, у [9, 10] агент анонімізації «маскує» місцезнаходження користувачів перед надсиланням їх до LBS, надаючи їхнє місцезнаходження з нижчою роздільною здатністю в часі та просторі. Іншими словами, замість того, щоб надавати точне місцезнаходження та момент часу, агент повідомлятиме про більший регіон, охоплений часовими рамками. K-анонімність також часто використовується для вимірювання загальної конфіденційності [11, 12-22]. Вона вимагає, щоб кожен користувач міг повідомляти своє місцезнаходження лише тоді, коли в тому ж регіоні є більше k-1 інших користувачів. Ці підходи допомагають покращити конфіденційність місцезнаходження кінцевих користувачів.

Незважаючи на масштабні роботи щодо захисту конфіденційності користувачів від постачальників послуг, було проведено мало робіт, щоб допомогти користувачам керувати своїми налаштуваннями конфіденційності; проте управління конфіденційністю є важливим питанням, яке потребує вирішення в реальних застосуваннях. У [23, 24-29] було запропоновано кілька простих політик конфіденційності місцезнаходження, які регулюють, хто може використовувати дані про місцезнаходження особи за яких умов. Однак, наскільки нам відомо, не існує комплексної системи управління політикою конфіденційності місцезнаходження. У роботі розроблено просту у використанні систему управління конфіденційністю місцезнаходження. Зокрема, вона визначає лаконічні, але виразні конструкції політики конфіденційності місцезнаходження, які можуть бути легко зрозумілі звичайним користувачам. Система надає різні функції управління політиками, включаючи складання політик, виявлення конфліктів політик та рекомендації політик. Складання політик дозволяє користувачам вставляти та видаляти

політики. Виявлення конфліктів політик автоматично перевірятиме конфлікти між політиками щоразу, коли відбуваються будь-які зміни. Система рекомендацій політик генеруватиме рекомендовані політики на основі основних потреб користувачів з метою зменшення навантаження на користувачів. Було впроваджено та оцінено прототип системи з точки зору як ефективності, так і результативності.

Рис. 1.1. ілюструє огляд запропонованої системи управління політикою конфіденційності місцезнаходження (LPPM). Система є системою конфіденційності місцезнаходження на основі політик. Усі аспекти системи складаються з невеликих пакетів правил, які називаються політиками. Її основне завдання полягає у відображенні місцезнаходження користувачів один одному. Система складається з політик, причому кожен тип політики створює власну інформацію, та способів обміну цією інформацією. Головне завдання системи полягає у врахуванні політик та використанні інформації, яку надають різні типи політик, для створення звіту, який розрізняє, яку інформацію може бачити кожен член системи, що має відношення до неї. Політики налаштовані таким чином, щоб їхня інформація повідомлялася у певний час доби та у певні дні. Політики в системі можна додавати, змінювати та видаляти в будь-який час, що надає користувачам широкий спектр можливостей налаштування. Коли політики вводяться в систему, вони порівнюються з встановленими політиками, щоб переконатися, що вони не конфліктують. Політики також порівнюються з встановленими політиками, щоб визначити, чи можна їх об'єднати. Інтерфейс користувача налаштовано таким чином, щоб бути зручним та зрозумілим для користувача. Оцінюючи прототип системи, можна встановити базовий рівень продуктивності для повнофункціональної системи. Іншими словами, вартість прототипів можна використовувати для оцінки вартості працюючої системи. Оцінка прототипу системи конфіденційності місцезнаходження покаже можливості системи, а отже, і корисність цієї системи.

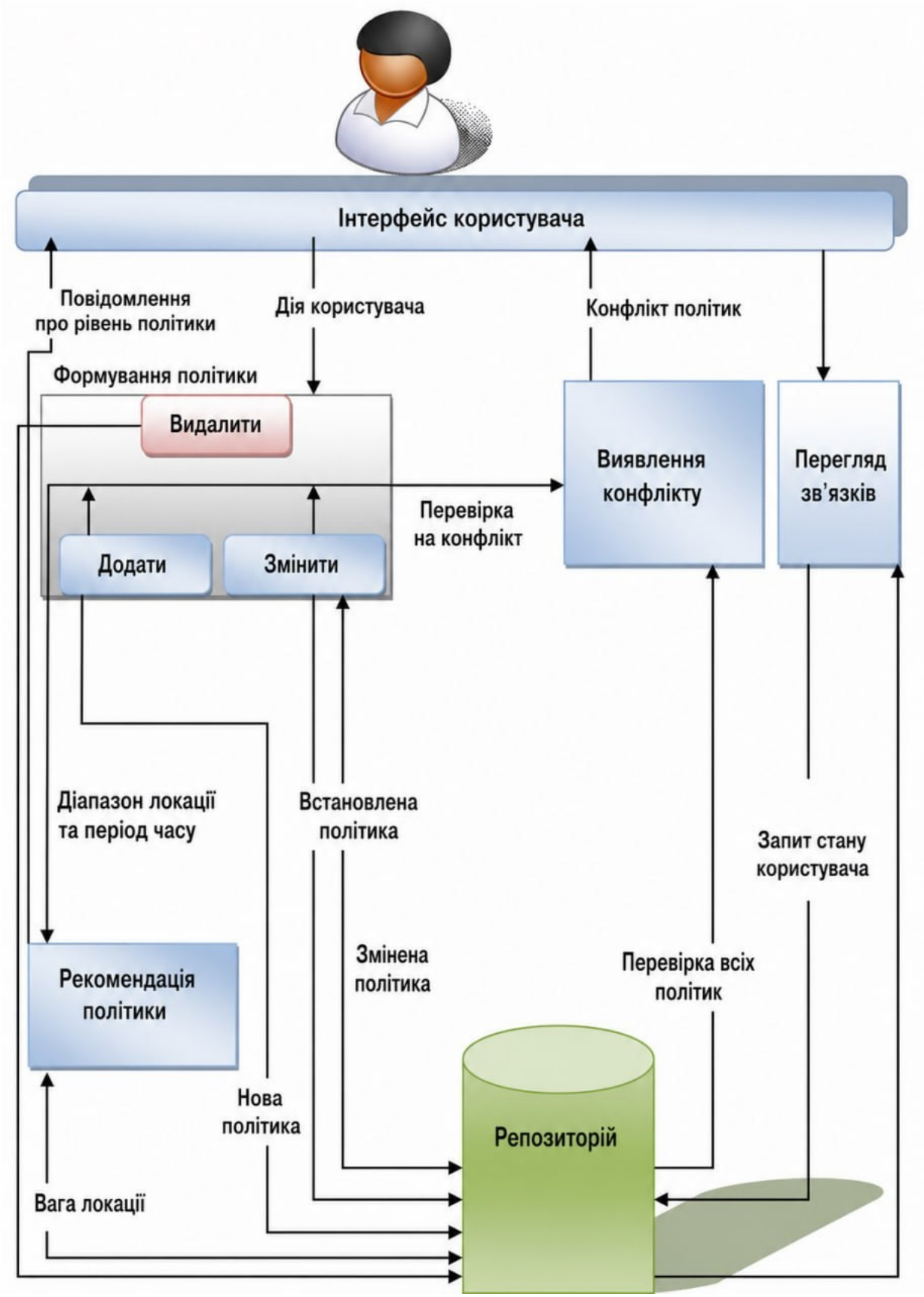

Рисунок 1.1 – Потік даних для системи.

1.2 Огляд літератури

Інформація про місцезнаходження була визначена як набір даних, пов'язаних з особою, які описують її місцезнаходження протягом певного періоду часу. Часова роздільна здатність та роздільна здатність місцезнаходження залежать від технології, яка використовується для їх збору. Існує кілька методів, які використовувалися для визначення місцезнаходження користувача. Однією з найдавніших систем, розроблених для відстеження місцезнаходження, є Глобальна система позиціонування (GPS) та WLAN (бездротова локальна мережа).

Здебільшого люди не стурбовані конфіденційністю свого місцезнаходження. Однак вони чутливі до того, як можуть бути використані дані про їхнє місцезнаходження, і ця чутливість може бути підвищена завдяки їхній обізнаності про витоки конфіденційності. Каасінен провів інтерв'ю з 55 людьми, розділеними на 13 груп з різних куточків світу та різним походженням. Результатом цієї оцінки є те, що користувачі довіряють чинним постачальникам послуг та політикам у питаннях, пов'язаних із захистом конфіденційності.

Дж. Крумм у своєму проєкті переконав понад 250 людей зі свого закладу надати їм два тижні даних GPS, записаних у їхньому автомобілі. Він запитав 97 із них, чи можна поділитися даними про їхнє місцезнаходження за межами їхнього закладу, і в результаті лише 20% з них відповіли «ні».

Данезіс та ін. запитали 74 студентів, скільки їм доведеться заплатити за обмін даними про їхнє місцезнаходження за місяць. Середня ціна становила 10 або 20 фунтів стерлінгів. Основна проблема з конфіденційністю місцезнаходження може виникнути під час спілкування між користувачем та постачальником послуг; коли користувач надає інформацію SB, зловмисник може скористатися цією інформацією про місцезнаходження. Андреас та ін. класифікували атаку на два типи: спілкування з перших рук, коли зловмисник отримує конфіденційну інформацію через комунікацію з перших рук, коли

особа мимоволі надає її безпосередньо зловмиснику. Комунікація з других рук: зловмисники передають інформацію від однієї сторони іншій неавторизованій стороні; у цьому випадку особа більше не контролює інформацію.

Було докладено багато зусиль для забезпечення конфіденційності місцезнаходження користувачів під час користування LBS. Підходи, запропоновані дослідниками, можна розділити на такі категорії: підходи, що базуються на політиках, шифруванні, обфускації та анонімності.

1.3 Політико-орієнтований підхід

Політика конфіденційності – це юридичні повідомлення, що містять твердження, що визначають, що постачальники послуг можуть робити з персональними даними користувача. Політика конфіденційності публікується постачальниками послуг, і користувачі вирішують, чи є така політика прийнятною для них. Ці політики охоплюють багато концепцій, і для їх визначення використовується специфічна мова [23, 30]. Користувачі досягають угоди з постачальниками щодо того, які дані збираються, для чого ці дані використовуються та як вони можуть бути поширені третім сторонам. У цій методиці конфіденційність розуміється як здатність осіб вирішувати, коли, яка і як інформація про них розкривається іншим. В ідеалі користувачі можуть вибирати серед різних політик. Тому, залежно від обраної політики, користувачі можуть заощадити певні гроші, але, з іншого боку, постачальники можуть поширювати/продавати деякі зі своїх даних.

Цей підхід простий у використанні, оскільки він не лише задовольняє персоналізовані вимоги користувача щодо конфіденційності, але й звільняє користувача від постійного втручання системи, якого інакше було б потрібно для вирішення конкретних випадків.

Смайлагіч та ін. [31] запропонували модель та методологію конфіденційності, засновані на контекстно-залежній системі Portable Help Desk. Конфіденційність інформації про місцезнаходження описується теорією

множин та правилами. Кожне правило встановлює список користувачів, яким дозволено або заборонено знати місцезнаходження користувача протягом заданого періоду часу. Правило встановлює один часовий проміжок та можливе повторення події. Правило встановлює авторизацію на основі однієї з чотирьох видимостей: «Видима для всіх», «Невидима для деяких», «Видима для деяких» та «Невидима для всіх». Ці видимості розташовані за зростаючою обмеженістю набору. «Видима для всіх» дозволяє будь-кому знати місцезнаходження клієнта-користувача, «Невидима для деяких» обмежує лише скінченний список користувачів, «Видима для деяких» обмежує всіх користувачів, крім скінченної кількості користувачів, а «Невидима для всіх» обмежує всіх. Висновок показує розподіл, де вдвічі більше людей готові автоматично передавати свою особисту інформацію будь-якому користувачеві, а друга група обирає більшу конфіденційність шляхом суворого налаштування того, хто може запитувати їхню особисту інформацію. Мало хто з користувачів вирішує надавати або забороняти доступ до інформації окремо для кожного запиту. Щоб вирішити конфлікти між кількома правилами конфіденційності; якщо одне правило стверджує, що користувач А має право бачити місцезнаходження клієнта в певний час, а інше правило стверджує протилежне, яке правило матиме пріоритет. Дослідники описали користувачам таку ситуацію; вони могли відповісти, включивши «Не бачу», що означає, що клієнт не бажає, щоб його інформацію надавали, якщо існує конфлікт, та «Можу бачити», що означає, що клієнт бажає, щоб його інформацію надавали, якщо такий конфлікт існує.

Майлз та ін. [32] створили об'єднуючу службу визначення місцезнаходження під назвою Loc-Serv, службу проміжного програмного забезпечення, яка знаходиться між програмами на основі місцезнаходження та технологіями відстеження місцезнаходження. Основною метою LocServ є об'єднання технологій відстеження місцезнаходження, щоб програма на основі місцезнаходження могла використовувати кілька систем позиціонування.

По суті, користувачі LocServ можуть вказати запит на місцезнаходження, використовуючи будь-яку із символічних або геометричних моделей

місцезнаходження, які розуміє Loc-Serv. Система потребує механізму для контролю доступу до інформації про місцезнаходження користувачів без необхідності повторного втручання користувача. Вона використовує ті ж основні концепції, що й у P3P та pawS, використовуючи машинозчитувані політики конфіденційності та налаштування користувача для автоматизації процесу вирішення питання про те, чи можна певну частину інформації про місцезнаходження розголошувати третій стороні. Їхній підхід може зменшити навантаження на користувача, пов'язане з обробкою запитів на інформацію про їхнє місцезнаходження. Користувачі можуть користуватися послугами визначення місцезнаходження без постійних перебоїв з боку системи, яка запитує дозвіл на розкриття поточної інформації про місцезнаходження. Крім того, автори запропонували визначити приватні політики для повсюдних сценаріїв, а не просто встановлювати прості моделі конфіденційності для певних сфер, таких як бізнес чи трафік, як пропонували попередні дослідники. Однак вони не вважають, що збір рішень користувача для різних сценаріїв сам по собі є важким навантаженням для користувача, особливо за деяких обставин, коли конфіденційність місцезнаходження може не бути великою проблемою для користувача.

Снеккенесс [23] запропонував, щоб люди були оснащені інструментами, які дозволяли б їм формулювати власну політику конфіденційності щодо місця розташування, відповідно до чинних правил і норм. Автор визначає концепції, які можуть бути корисними під час формулювання такої політики. Ключова концепція пов'язана зі спостереженням за знайденим об'єктом. Спостереження зазвичай включає місцезнаходження, ідентичність об'єкта, час спостереження та швидкість об'єкта. Ідея полягає в тому, що людина повинна мати можливість регулювати точність, з якою ці спостереження публікуються, залежно від таких параметрів, як цільове використання інформації та особа одержувача. Цей підхід надає фрагменти мови для формулювання політик конфіденційності персонального місцезнаходження. Основна ідея полягає в тому, що має бути створений певний реєстр за відомою адресою, який для кожного знайденого

об'єкта містить вказівник на місцезнаходження, де зберігається політика конфіденційності персонального місцезнаходження для цього знайденого об'єкта. Постачальник даних про місцезнаходження тоді буде зобов'язаний отримати «схвалення на випуск» від зберігача політики, перш ніж будь-які дані про місцезнаходження можуть бути оприлюднені. Оскільки конфіденційність місцезнаходження базується на певній відомому адресі, конфіденційність місцезнаходження користувача може бути не захищена, коли користувач знаходиться в приватному місці, такому як місце проживання. Недоліком цього підходу є те, що він не забезпечує користувачам повного захисту, незважаючи на різниця в місцезнаходженні.

Пов'язані дослідження в галузі керування доступом на основі ролей (RBAC) нещодавно отримали значну увагу, і їх також можна використовувати для підтримки конфіденційності місцезнаходження. У RBAC дозволи пов'язані з ролями; користувачам призначаються відповідні ролі, і вони отримують надані цим ролям дозволи. Такий підхід значно спрощує управління дозволами. Ролі можна створювати для різних функцій організації, а потім користувачам можна призначати ролі на основі їхніх обов'язків та кваліфікації. Користувачів можна легко перепризначати з однієї ролі на іншу. Ролям можна надавати нові дозволи в міру інтеграції нових програм та систем, а дозволи для певних ролей можна скасовувати за потреби. У конфіденційності місцезнаходження ми можемо визначити такі ролі, як керівник, родина, друзі та незнайомці. Кожній ролі призначається різний дозвіл на інформацію про місцезнаходження користувача залежно від часу запиту та місцезнаходження. Таким чином, можна забезпечити конфіденційність особистого місцезнаходження користувача, а також не турбуватися про велику кількість різних політик. Однак, оскільки це керування доступом на основі ролей, обмежена кількість та значення ролей можуть не задовольняти різні потреби користувачів у різних ситуаціях повсякденного життя.

Мета цього підходу – задовольнити потреби користувача щодо особистої конфіденційності. Для досягнення цієї мети необхідна велика кількість політик.

Зі збільшенням кількості користувачів кількість політик також може зростати в геометричній прогресії. Це робить підхід на основі політик не таким масштабованим, як підходи на основі шифрування.

Накладні витрати такого підходу пов'язані з підтримкою цих політик. Для зберігання політики конфіденційності кожного користувача потрібен великий простір для зберігання даних, і щоразу, коли користувач підтверджує запит, сервер має перевірити політику, а потім може бути вжито дія відповідно до політики користувача. Ця вимога створює величезні накладні витрати, особливо коли користувачі мають детальні та складні політики.

1.4 Підхід до анонімності

Підходи, засновані на анонімності, є найдосконалішим варіантом конфіденційності місцезнаходження на основі довірених третіх сторін. Замість того, щоб піклуватися про політики чи ідентифікатори користувачів, ці підходи припускають, що спілкування є анонімним. Вони спрямовані на приховування справжньої особи користувачів щодо наданої інформації про місцезнаходження.

Поширеним способом приховування реального місцезнаходження користувачів від постачальника LBS є використання властивості K-анонімності. Ця властивість вирішує конфлікт між втратою інформації та ризиком розкриття [13].

K-анонімність та маскування.

Підходи мають деякі обмеження. По-перше, за своєю сутністю маскування спирається на довірену сутність, щоб зробити місцезнаходження користувачів анонімними. Таким чином, усі запити повинні довіряти цій сутності під час нормального режиму роботи системи. Ця сутність також може стати єдиною точкою відмови; потенційно створюючи вузьке місце масштабованості, оскільки між користувачем та сутністю має відбутися кілька рукостискань, щоб дозволити обмін профілями користувачів та заходами

анонімності. Ще одним обмеженням методів маскування є те, що якість обслуговування або загальна продуктивність системи значно знижуються, оскільки користувачі обирають більш суворі налаштування конфіденційності. Наприклад, якщо користувачеві потрібна краща K-анонімність, системі потрібно збільшити K для цього користувача, що призведе до великої області маскування та, отже, менш точних відповідей на запити. Або ж, якщо потрібно підтримувати якість обслуговування, сервер визначення місцезнаходження повинен вирішувати просторовий запит для кожної точки в області маскування та надсилати весь об'ємний результат сутності для фільтрації. Цей процес явно впливає на загальну продуктивність системи, пропускну здатність зв'язку та пропускну здатність сервера, а також призводить до більш складної обробки запитів. Нарешті, концепція K-анонімності працює не у всіх сценаріях. Наприклад, у менш населеному районі розмір розширеної зони може бути надмірно великим, щоб включити інших користувачів K-1.

Багато робіт, заснованих на маскуванні, можна знайти в літературі [11, 33, 34]. Одне з найновіших досягнень у підходах, заснованих на анонімності, було запропоновано в [35], яке розширює ранню версію підходу, заснованого на анонімності [33]. Це розширення дозволяє користувачам визначати свої особисті вимоги до конфіденційності (тобто кількість K користувачів, серед яких вони бажають залишатися анонімними) та максимальну затримку та збурення місцезнаходження, які вони готові прийняти.

Ще один подібний метод під назвою PrivacyGrid описано в [36]. Хоча сторонній об'єкт, описаний у [35], та підхід PrivacyGrid дуже схожі, останній здається ефективнішим завдяки методам маскування, заснованим на сітках.

Мохамед та ін. [37] вирішують проблему конфіденційності таким чином, щоб захистити конфіденційність користувачів, зберігаючи при цьому функціональність LBS. Основна ідея полягає у використанні третьої довіреної сторони, яка називається анонімайзером місцезнаходження, який:

- отримує точне місцезнаходження точки від мобільного користувача,

- розмиває точку місцезнаходження в замасковану просторову область відповідно до певних обмежень, наданих користувачем,

- надсилає замасковану просторову область на сервер бази даних на основі місцезнаходження.

Потім сервер бази даних на основі місцезнаходження оснащений спеціальними модулями, які змінюють його функціональність для роботи з замаскованою просторовою областю, а не з точним місцезнаходженням точки. Недоліком розмитої інформації про місцезнаходження є те, що сервер бази даних на основі місцезнаходження може не мати можливості надавати високоякісні послуги своїм користувачам. Користувачі матимуть можливість встановити набір параметрів, щоб збалансувати обсяг інформації, яку вони хочуть розкрити про своє місцезнаходження, та якість обслуговування, яку вони отримують від сервера бази даних на основі місцезнаходження. Ці параметри включають:

1) рівень анонімності (k), який користувачі повинні вказати для себе, вводячи параметр анонімності k,

2) мінімальну площу, яка представляє мінімальну вимогу до площі маскованої просторової області,

3) максимальну площу, яка представляє максимальну вимогу до площі маскованої просторової області,

4) часові обмеження, що встановлюють час, протягом якого застосовуються ці параметри.

Недоліком цього підходу є наявність компромісу між анонімністю та точністю обслуговування. Щоб налаштувати точність, користувач повинен знати різні параметри. Це фактично створює незручності у використанні сервісу на основі місцезнаходження, якщо користувач хоче знайти найкращий баланс між конфіденційністю та точністю для окремої особи.

Грутезер та Грюнвальд. Представлена архітектура проміжного програмного забезпечення та алгоритми, які можуть використовуватися централізованою службою брокера місцезнаходження. Адаптивні алгоритми

коригують роздільну здатність інформації про місцезнаходження вздовж просторових або часових вимірів, щоб відповідати заданим обмеженням анонімності на основі об'єктів, які можуть використовувати служби місцезнаходження в заданій області. У їхній моделі мобільні вузли зв'язуються із зовнішніми службами через центральний сервер анонімності, який є частиною довіреної обчислювальної бази. На етапі ініціалізації вузли встановлюють автентифіковане та зашифроване з'єднання із сервером анонімності.

Коли мобільний вузол надсилає інформацію про місцезнаходження та час до зовнішньої служби, сервер анонімності змінює дані про місцезнаходження відповідно до алгоритму маскування, щоб зменшити ризик повторної ідентифікації. Крім того, сервер анонімності діє як мікс-маршрутизатор, який випадковим чином перевпорядковує повідомлення від кількох мобільних вузлів, щоб запобігти зв'язуванню вхідних та вихідних повідомлень зловмисником на сервері анонімності. Нарешті, сервер анонімності пересилає повідомлення до зовнішньої служби. Вони вважають суб'єкта k-анонімним щодо інформації про місцезнаходження тоді і тільки тоді, коли представлена інформація про місцезнаходження не відрізняється від інформації про місцезнаходження принаймні k-1 інших суб'єктів. Ключова ідея, що лежить в основі алгоритму маскування, полягає в тому, що певний ступінь анонімності може бути підтриманий шляхом зниження точності розкритих просторових даних.

Для цього алгоритм вибирає достатньо велику область, щоб достатня кількість інших суб'єктів населяла цю область для задоволення обмеження анонімності. Однак, зі збільшенням розміру області для задоволення k-анонімності, точність швидко знижується. Крім того, оскільки між сервером анонімності та вузлами користувача існує зашифроване з'єднання, цей підхід також може мати недоліки підходів на основі шифрування.

Бересфорд і Стаяно прагнуть зробити інформацію про місцезнаходження анонімною. Їхній підхід вимагає, щоб користувачі могли неодноразово

змінювати псевдоніми, навіть під час відстеження. Користувачі можуть використовувати нові програми, з якими вони взаємодіють, але якщо просторова та часова роздільна здатність системи достатньо висока, програми можуть без труднощів пов'язувати старі та нові псевдоніми. Автори прагнули вирішити цю проблему, ввівши зону змішання.

Програма не отримує жодної інформації про місцезнаходження, коли користувачі перебувають у зоні змішання, де ідентичності «змішані». Якщо припустити, що користувачі змінюють свій псевдонім на новий невикористаний щоразу, коли вони входять у зону змішання, програми, які бачать користувача, що виходить із зони змішання, не можуть відрізнити цього користувача від будь-якого іншого, хто перебував у зоні змішання одночасно, і не можуть пов'язати людей, які входять у зону змішання, з тими, хто її залишає. Інфраструктура затримує та перевпорядковує повідомлення від абонентів у зоні змішання, щоб заплутати спостерігачів. Проблема цієї системи полягає в тому, що в зоні змішання має бути достатня кількість абонентів, щоб забезпечити належний рівень анонімності. Крім того, якщо діаметр зони змішання значно перевищує відстань, яку користувач може подолати протягом одного періоду оновлення місцезнаходження, система може неадекватно змішувати користувачів.

Лін та ін. [38] зазначили, що постачальники послуг можуть надавати користувачам необхідну інформацію, але вони повинні відстежувати переміщення та місцезнаходження користувачів. У цій статті вони розглядають таку проблему, створюючи систему захисту конфіденційності місцезнаходження. Основна ідея їхньої системи полягає в пересиланні перетворених даних про місцезнаходження користувача постачальнику послуг. Вони припускають низку різних типів перетворень, таких як масштабування, перетворення або обертання, щоб приховати інформацію про користувача. Вони використовують m агентів, розміщених між користувачами та постачальниками послуг, для реалізації цих перетворень, таким чином уникаючи негативних наслідків дії одного агента. Наприклад, якщо ворог

зламає одного агента, він все одно не зможе відстежувати користувача. Якщо деякі агенти незаконно зберігають дані про споживачів, вони не зможуть виявити інформацію про користувачів без змови з іншими об'єктами. Однак проблема цього підходу може полягати в тому, що накладні витрати на перетворення даних зростатимуть зі збільшенням кількості функцій перетворення. Також цей підхід ускладнює запити, ніж будь-коли, оскільки запити необхідно перетворювати, щоб отримати правильну відповідь.

Підходи на основі довіреного агента та анонімності не масштабуються зі збільшенням кількості користувачів у системі так само, як підходи на основі шифрування. Ця слабкість пов'язана з проміжним рівнем, відомим як довірений агент, який існує між користувачем та постачальником послуг. Обчислювальні можливості цього агента обмежені; тому зі збільшенням кількості користувачів у системі продуктивність знижується через вузьке місце на стороні довіреного агента.

Оскільки щоразу, коли користувач надсилає запит, довірений агент повинен задовольняти умову k-анонімності, це пов'язано з накладними витратами на обробку для виконання цієї умови. Більш важливо, щоразу, коли користувачі надсилають інформацію агенту, агент повинен використовувати певну функцію маскування, щоб приховати саме цю інформацію. Це неминуче збільшить обчислювальне навантаження та знизить продуктивність.

1.5 Підхід на основі заплутування

Методи на основі обфускації спрямовані на захист конфіденційності місцезнаходження шляхом зниження точності інформації про місцезнаходження, зберігаючи при цьому явний зв'язок зі справжньою особою користувача.

Було запропоновано кілька методів, заснованих на обфускації, для збереження конфіденційності користувачів контекстно-залежних сервісів. Припустимо, що користувач не повністю довіряє сервісу; отже, оскільки він

вважає свою поточну діяльність (наприклад, зустріч з клієнтами) конфіденційною інформацією, дозвіл чи заборона доступу до його точної поточної діяльності може бути незадовільним. Фактично, відмова в доступі до цих даних визначатиме неможливість скористатися цим сервісом, тоді як дозвіл доступу може призвести до порушення конфіденційності. У цьому випадку єдиним гнучким рішенням є обфускація конфіденційних даних перед їх передачею постачальнику послуг. Методи обфускації застосовувалися в минулому для захисту мікроданих, що видаються з баз даних.

Нещодавно було запропоновано різні методи на основі обфускації для контролю розголошення інформації про місцезнаходження, що базуються на узагальненні або збуренні положення користувача. Семантичний електронний гаманець є однією з перших спроб підтримки конфіденційності в загальних контекстно-залежних системах за допомогою механізмів обфускації. Користувачі семантичного електронного гаманця можуть висловлювати свої вподобання щодо точності контекстних даних на основі особи запитувача та контексту запиту. Шляхом абстракції користувач може узагальнити надані дані або пропустити деякі деталі про них.

Інші нещодавно запропоновані методи обфускації, де пропонується замінити реальне місцезнаходження користувачів LBS круговими областями зі змінним центром та радіусом. Однією з найновіших пропозицій щодо конфіденційності місцезнаходження без співпраці з довіреною третьою стороною є Space Twist. Цей підхід визначає точки інтересу, найближчі до реального місця розташування, але постачальник LBS не може визначити реальне місцезнаходження користувача. Основними перевагами цього підходу є те, що він не вимагає довіреної третьої сторони чи співпраці, і він приховує місцезнаходження користувача в контрольованій зоні. Однак цей метод не здатний досягти властивостей K-анонімності через відсутність співпраці.

Методи обфускації, спрямовані на захист конфіденційності місцезнаходження. Обфускація місцезнаходження доповнює анонімність. Зокрема, замість того, щоб робити користувачів анонімними, рішення на основі

обфускації припускають ідентифікацію користувачів та вносять збурення в зібрані дані про місцезнаходження, щоб знизити їхню точність.

Обфускація має кілька важливих переваг, що доповнюють інші стратегії захисту конфіденційності. Обфускація та анонімність схожі тим, що обидві стратегії намагаються приховати дані для захисту конфіденційності. Ключова відмінність між ними полягає в тому, що тоді як анонімність спрямована на приховування особистості людини, обфускація – це явно просторовий підхід до конфіденційності місцезнаходження, який має на меті дозволити розкриття особистості людини. Потенційно це бореться з одним із ключових обмежень підходів до анонімності: необхідністю автентифікації користувачів. Водночас, погіршення якості інформації про місцезнаходження ускладнює визначення особистості на основі місцезнаходження. Якщо обфускація достатньо гнучка, щоб її можна було адаптувати до конкретних вимог та контекстів користувача, вона (на відміну від регуляторних стратегій) не вимагає високого рівня складної інфраструктури та (на відміну від політик конфіденційності) менш вразлива до ненавмисного розкриття особистої інформації. На відміну від багатьох підходів до анонімності, вона достатньо легка, щоб використовувати її без необхідності залучати довірених брокерів конфіденційності.

Заплутування прагне балансу між рівнем конфіденційності персональної інформації та якістю LBS (системи позиціонування на основі даних про місцезнаходження). Недавні дослідження показали, що існує багато ситуацій, у яких можна очікувати високоякісних LBS на основі якісної інформації про місцезнаходження. Отже, у ситуації, коли користувачеві потрібна вища якість обслуговування, ніж може бути досягнута на мінімально прийнятному рівні конфіденційності користувача, тоді необхідно покладатися на інші стратегії захисту конфіденційності. Більше того, заплутування передбачає, що особа може вибирати, яку інформацію про своє місцезнаходження розкривати постачальнику послуг. Хоча це припущення може бути реалістичним при використанні систем позиціонування на основі клієнта або мережі, а також при обміні інформацією про місцезнаходження з третьою стороною, постачальник

послуг на основі місцезнаходження, який співпрацює з організаціями, що адмініструють мережу-Системи позиціонування на основі даних все ще вимагають захисту конфіденційності відповідно до нормативних актів.

1.6 Підхід до шифрування на основі політик

Традиційне шифрування з відкритим ключем є грубозернистим: відправник шифрує повідомлення M відносно відкритого ключа, і лише власник (унікального) секретного ключа, пов'язаного з відкритим ключем, може розшифрувати отриманий зашифрований текст і відновити повідомлення. Цієї прямої семантики достатньо для зв'язку "точка-точка", в якому зашифровані дані призначені для одного конкретного одержувача, який заздалегідь відомий відправнику. Однак в інших випадках відправник може натомість визначити політику, яка визначає, кому дозволено відновлювати зашифровані дані. Наприклад, секретні дані можуть бути пов'язані з певними ключовими словами, до яких мають доступ лише певні користувачі.

Одне з перших це рішень форма обробки зашифрованих запитів, що поєднує використання структури даних, придатної для керування просторовою інформацією, з криптографічною схемою для обміну секретом. На стороні сервера дані про місцезнаходження обробляються через орієнтований ациклічний граф (DAG), вузли якого відповідають областям Вороного, отриманим шляхом теселяції простору.

Нещодавно в було запропоновано криптографічний підхід, натхненний галуззю пошуку приватної інформації (PIR). Постачальник послуг будує теселяцію Вороного відповідно до збереженої точки poi та накладає на неї регулярну сітку довільної гранулярності. Деякі з переваг цього підходу полягають у тому, що дані про місцезнаходження ніколи не розкриваються; особа користувача прихована серед ідентифікаційних даних усіх користувачів. Однак, оскільки мобільні пристрої часто характеризуються обмеженими обчислювальними можливостями, запит шифрування та обробка відповідей, що

виконуються на стороні клієнта, мають сильний вплив на час відгуку служби та споживання енергії.

Криптографічна система з одним секретним або спільним ключем вимагає від користувачів безпечного поширення ключа, перш ніж вони зможуть спілкуватися конфіденційно. Такий розподіл може бути складним, особливо якщо кількість користувачів дуже велика.

Є також нові протоколи для реалізації послуг на основі місцезнаходження для користувачів мобільного бездротового зв'язку без використання довіреної третьої сторони. Один з них дозволяє користувачам контролювати, які суб'єкти можуть мати доступ до інформації про їхнє місцезнаходження. Вони виділяють два основні типи LBS: перший тип послуг безпосередньо передає інформацію про місцезнаходження користувачів уповноваженим суб'єктам, які захищають інформацію від неавторизованих суб'єктів, включаючи самого постачальника послуг. Другий вимагає обчислень, які враховують місцезнаходження користувачів як вхідні дані. Завдання полягає в тому, як виконати ці обчислення, не розкриваючи місцезнаходження користувачів. Основна ідея їхньої конструкції, що зберігає конфіденційність, полягає в тому, що лише суб'єкти в уповноваженій підмножині повинні мати можливість отримати ключ для розшифрування інформації про місцезнаходження. Вони показали, що їхні протоколи мають низькі накладні витрати та підходять для персональних мобільних пристроїв.

Метод шифрування на основі політик має перевагу в тому, що шифрування та контроль доступу об'єднані в один пакет. Він забезпечує шифрування не лише під час передачі, але й для зберігання. Таким чином, гарантується безпека всієї конфіденційної інформації, що передається. Схема шифрування також дозволяє нам реалізувати контроль доступу, оскільки лише ті, хто відповідає політиці, можуть розшифрувати та мати доступ до запису.

Користувачам не потрібно керувати власними ключами, а також немає потреби розподіляти ключі. Між цими двома варіантами не буде різниці у

взаємодії з користувачем. В обох випадках користувачі входять у систему та отримують доступ до документів, на які вони мають дозвіл.

Загальним недоліком будь-якої схеми шифрування є те, що записи зберігаються в зашифрованому вигляді. Ключі дешифрування повинні зберігатися протягом усього терміну дії запису. Алгоритм дешифрування також повинен бути доступним для відновлення оригінальних документів. Щоб забезпечити доступність обох, може знадобитися створити резервну копію ключів та алгоритму. В іншому випадку можна було б зберігати записи у зручному для читання форматі в фізично безпечному місці, не підключеному до мережі. Нам потрібно було б зберігати резервні копії записів у відкритому тексті незалежно від того, яка система використовувалася, через можливість збою обладнання.

1.7 Висновок до першого розділу

У розділі підкреслюється актуальність проблеми конфіденційності місцезнаходження у сучасних сервісах LBS, адже вони одночасно корисні для користувачів і небезпечні з точки зору приватності. Витік даних може призвести до злочинних дій або небажаного використання інформації рекламодавцями. Для захисту пропонуються методи анонімізації, використання агентів спотворення даних та підхід k-анонімності. Водночас існує потреба у зручних системах управління політиками конфіденційності, які дозволяють користувачам самостійно налаштовувати доступ до своїх даних. Запропонований прототип системи LPPM демонструє можливості автоматичного виявлення конфліктів політик та рекомендацій для користувачів. Ефективне управління конфіденційністю місцезнаходження є ключовим для безпеки та довіри до сучасних цифрових сервісів.

РОЗДІЛ 2. СИСТЕМА УПРАВЛІННЯ ПОЛІТИКОЮ КОНФІДЕНЦІЙНОСТІ МІСЦЕЗНАХОДЖЕННЯ

У цьому розділі спочатку буде представлено стислий, але виразний текст політики конфіденційності щодо місцезнаходження. Потім будуть описані алгоритми виявлення конфліктів політик та їх формування. Нарешті, буде пояснення системи рекомендацій щодо політик.

2.1 Визначення політики конфіденційності щодо місцезнаходження

Ця робота зосереджена на конфіденційності місцезнаходження, яку можна визначити як здатність запобігти отриманню іншими неавторизованими сторонами інформації про ваше поточне або минуле місцезнаходження. Політики можна розділити на три категорії: спеціалізовані, узагальнені та винятки. Ці три політики взаємодіють одна з одною, і результати визначають, чи користувач видимий для своїх зв'язків чи ні. Кожна з трьох основних політик працює дуже схожим чином, з кількома невеликими відмінностями.

Визначення 1. Нехай U1 – автор політики, нехай U2 – ціль політики. Нехай Pe – політика, де e – тип політики: спеціалізована, узагальнена або групова конфіденційність. Політика міститиме наступне: період часу Ttime, що складається з періоду в годинах, та діапазон днів; діапазон місцезнаходження, політику місцезнаходження, яка може включати місцезнаходження, місто, штат та країну.

До всіх трьох політик застосовуються кілька умов форматування. По-перше, цільовий користувач або зв'язок повинні бути частиною бази даних, перш ніж політика буде дійсною; аналогічно, користувач може створювати політики лише для людей зі свого списку зв'язків. Логіка цього правила полягає в тому, що якщо користувачі хочуть створити політику, вони повинні очікувати, що ця політика буде відображена. Крім того, якщо користувач дозволяє іншому користувачеві бачити його, він повинен мати певні зв'язки з

цим іншим користувачем. Ще одна поширена умова стосується часу; має пройти щонайменше 15 хвилин між часом початку та завершення будь-якої з дерев'яних політик. Передбачається, що для дійсності політики потрібна значна кількість. По-третє, для політики має бути повністю визначено місцезнаходження; тобто, якщо користувач вводить інформацію в поле штату, він також повинен надати інформацію для рядка країни, так само як штат має бути введено, якщо введено місто, і те саме стосується місцезнаходження та міста.

Спеціалізована політика.

Спеціалізовані політики є основним типом політик; вони вимагають зв'язку між творцем політики та цільовим користувачем. Після створення політики для цільового об'єкта, щоразу, коли цільовий об'єкт запитує список усіх видимих користувачів протягом відведеного для політики часу, автор відображається у звіті цільового об'єкта. Спеціалізовані поліси складаються з автора; цільової сторони; місця дії поліса, а також часу та дня дії поліса. Наприклад, якщо творець хоче повідомити цільову особу, що вона буде в банку в понеділок, він просто вводить місцезнаходження (банк, місто, штат і країну), цільову особу, час (час – час) і понеділок як дату початку, так і дату завершення.

Визначення 2. Нехай U_1 буде користувачем-творцем, а U_2 – індивідуальною цільовою платформою. Будь-яка політика, створена U_1 для U_2, P, міститиме період часу T_{time} та діапазон місцезнаходження RangeLocation. Протягом періоду часу T_{time} діапазон місцезнаходження RangeLocation буде повідомлятися U_2 як місцезнаходження U_1.

Узагальнена політика.

Узагальнені політики, з іншого боку, стосуються зв'язку між творцем політики та роллю відносин. Користувач може призначити кожному зі своїх партнерів одну з трьох ролей, кожна з яких достатньо загальна, щоб включати більшість його партнерів: родину, друзів та колег.

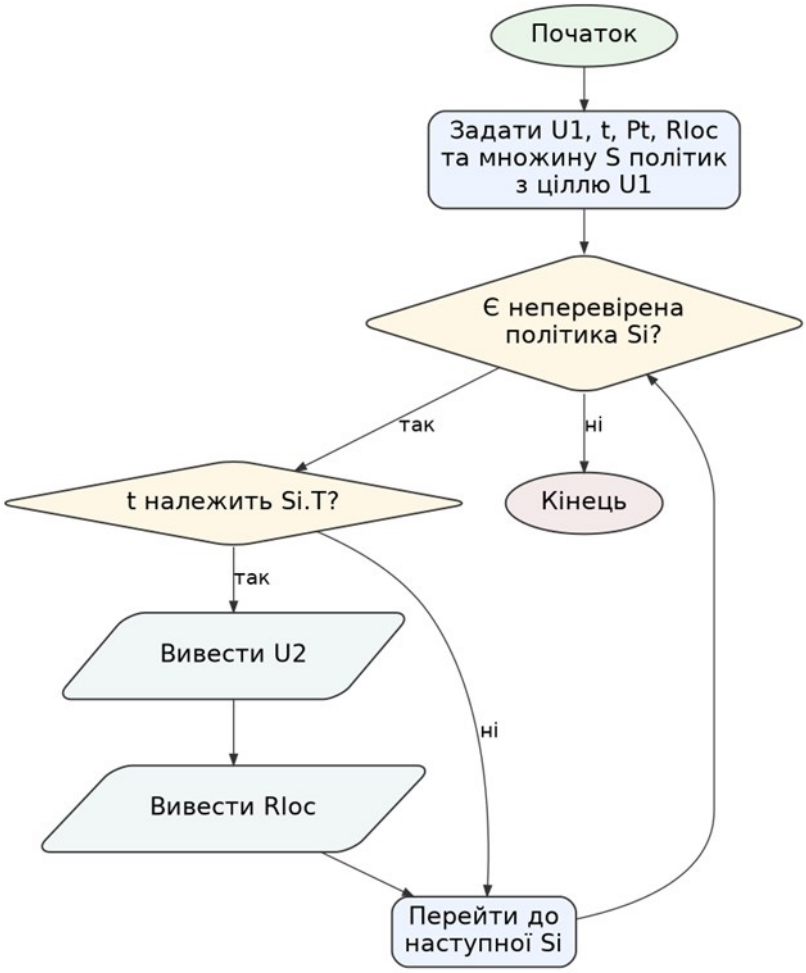

Рисунок 2.1 – Алгоритм перевірки наявності спеціалізованої політики

Кожен користувач у ролі зв'язку підпорядковується політиці, визначеній користувачем для цієї ролі. Як і спеціалізований поліс, узагальнений поліс складається з автора, періоду часу та місця розташування. Це відрізняється тим, що замість визначення конкретного користувача як цільового, творець обирає один із типів зв'язків для політик. Узагальнені політики також дозволяють користувачеві вказати рівень конфіденційності для політики. Наприклад, нехай U1 хоче повідомити своїм друзям, що він увесь цей тиждень у школі з 7:00 до 15:00. Тому він створює групову політику з часовим діапазоном з 7:00 до 15:00, з понеділка по п'ятницю. U_1 надсилає цю політику на перевірку, і якщо немає конфліктів політик, він рекомендує рівень конфіденційності для політики. Через середній часовий проміжок та дуже специфічне розташування, як буде

описано пізніше в груповій політиці конфіденційності, рівень конфіденційності політики встановлено на високий та вказано в базі даних.

Визначення 3. Нехай U_1 – користувач-творець, нехай Re – цільова роль, де e – роль (сім'я, друг або колега). Будь-яка політика p, створена U_1 для Re, P, міститиме період часу T_{time} та діапазон розташування RangeLocation. Протягом періоду часу T_{time} діапазон розташування RangeLocation буде передано U_2, де U_2 – це відношення U_1 у категорії e, як розташування U_1.

Політика винятків.

Винятки становлять доповнення до групових політик; вони виключають певного користувача з групової політики. Іншими словами, автор політики видаляє своє місцезнаходження з будь-яких звітів, які були б видимими для цільового користувача. Однак політики винятків також дуже схожі на окремі політики, оскільки їхня функція полягає в приховуванні інформації від конкретного користувача; вони не потребують визначення місцезнаходження. Можна налаштувати винятки, щоб дозволити автору політики приховувати своє місцезнаходження від певного користувача протягом частини або всього періоду групової політики. Вони також дозволяють політиці винятків перекривати дві або більше політик. Повертаючись до узагальненої політики, припустимо, що автор політики купує подарунок для одного з членів своєї родини, тому він може створити політику винятків для цієї особи..

Визначення 4. Нехай U_1 буде користувачем-творцем, а U_2 – індивідуальною цільовою особою. Будь-які винятки, e, створені U_1 для U_2, міститимуть період часу T_{time}. Якщо U_1 має узагальнене або групове визначення конфіденційності протягом часу T_{time}, місцезнаходження U_1 не буде повідомлено U_2, незалежно від цільової ролі визначення.

Політика конфіденційності групи.

Ця політика відрізняється від трьох інших тим, що вона є трьома політиками в одній. Цей тип політики дозволяє користувачеві відображати своє місцезнаходження всім користувачам, яким призначено певну роль, але обмежувати інформацію, доступну кожному користувачеві в даній ролі,

залежно від рівня конфіденційності. Політика конфіденційності групи містить автора, цільову роль, а також період часу та діапазон місцезнаходження для кожного з трьох рівнів конфіденційності.

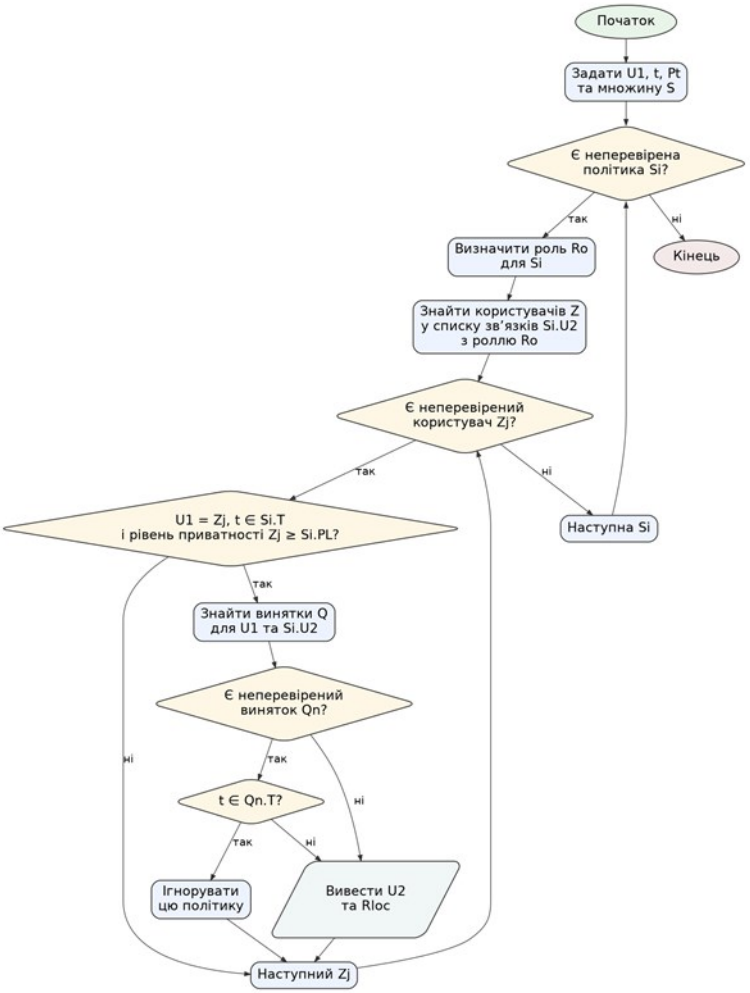

Рисунок 2.2 – Алгоритм перевірки узагальненої політики.

Наприклад, користувач1 хоче створити політику, щоб повідомити всім своїм друзям, що він буде в Монтані на вихідні, але він хоче повідомити лише своїм найближчим друзям, у якому місті він буде. Тому він встановлює цільову роль на друг і вводить період часу та діапазон місцезнаходження для кожного рівня конфіденційності.

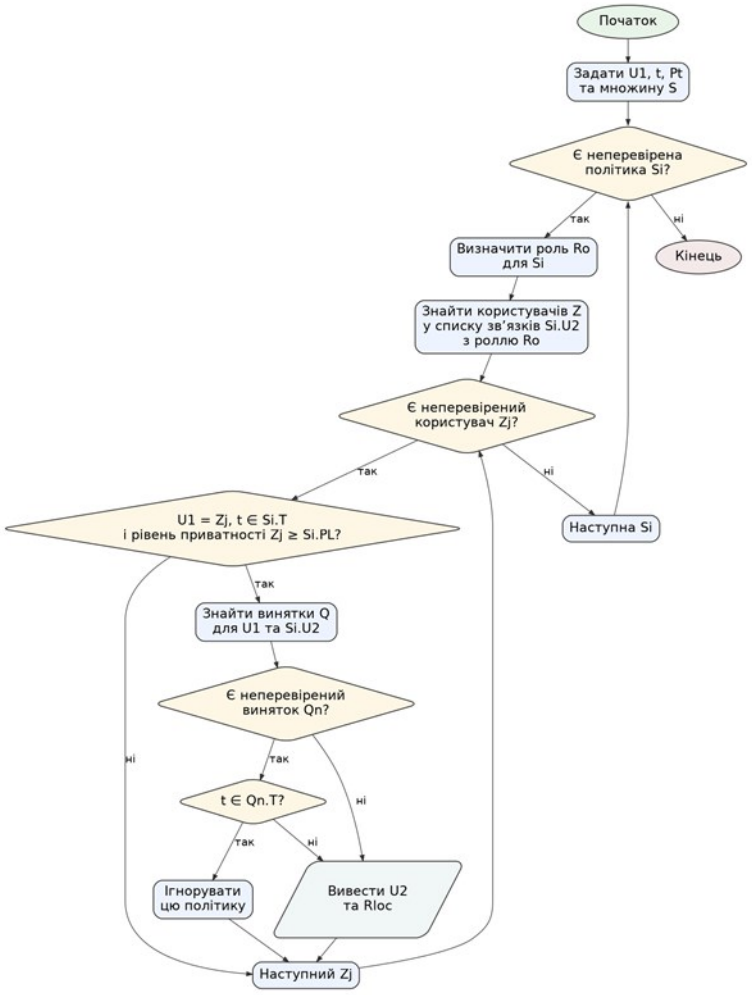

Рисунок 2.3 – Алгоритм перевірки політики конфіденційності групи.

2.2 Виявлення конфліктів політик

Усі форми конфлікту мають справу з подібними елементами та термінами. Основна ідея конфлікту полягає в тому, що Користувач1 не може перебувати в двох місцях одночасно; тому конфлікт може виникнути або в часі, або в місці розташування, або в обох. Рівні розташування базуються на ієрархії розташування, як показано на рис 2.4.

Місцезнаходження – це найточніший рівень, а країна – найменш конкретний. Рівень місцезнаходження, який має пріоритет, залежить від типу взаємодії.

Концепція подібного часу є складною, оскільки години мають бути визначені як циклічний час, а дні тижня – як лінійний. Нехай S_e – час початку

встановлених політик, S_n – час початку нової політики, а E_e та E_n – встановлені часи закінчення та новий час закінчення відповідно. Дві політики мають подібний час, якщо час початку або закінчення нової політики знаходиться між встановленим часом початку та часом закінчення, як показано на рис. 2.4.

Рисунок 2.4 -Ієрархія розташування для системи.

Дві політики також мають схожий час, якщо встановлений період однієї з них знаходиться між новими періодами часу, як показано на рис. 2.5.

Зрештою, через лінійну часову шкалу, якщо встановлений час завершення менший за встановлений час початку, нам потрібно перевірити, чи знаходиться новий час початку або новий час завершення між встановленим часом початку та однією секундою до півночі, 23:59:59 або північчю 00:00:00 та встановленим часом завершення, як показано на рис. 2.6.

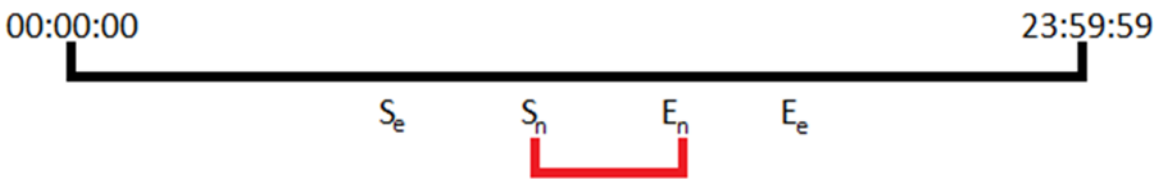

Рисунок 2.5 – Конфлікт часу. $(Se \leq Sn \leq Ee)$ OR $(Se \leq En \leq Ee)$

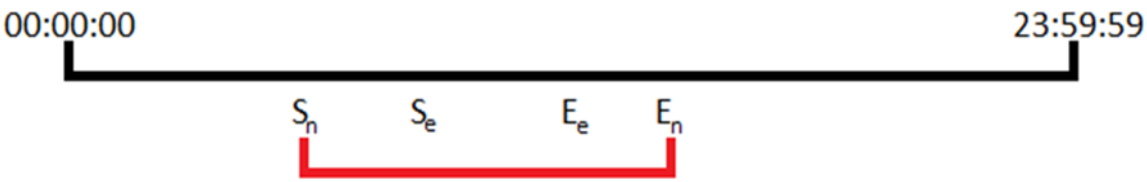

Рисунок 2.6 – Конфлікт часу. $(Sn \leq Se)\ AND\ (Ee \leq En)$

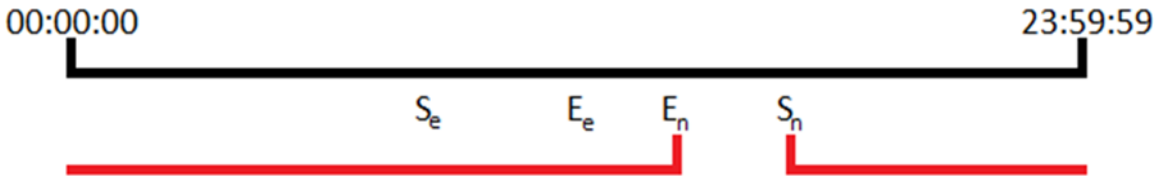

Рисунок 2.7 – Конфлікт кругової лінії часу.

$$(EE \leq SE)\ AND\ ((SE \leq (SN\ or\ EN) \leq 23:59:59)\ OR\ (00:00:00 \leq (SN\ or\ EN) \leq EE))$$

Типи конфліктів.

Політика від узагальненого до спеціалізованого.

Не всі узагальнені та спеціалізовані політики конфліктують. Конфлікт вимагає виконання певних умов. По-перше, має бути схожий діапазон часу та доби. Узагальнена політика конфліктуватиме зі встановленою спеціалізованою політикою, якщо вона має той самий рівень розташування або вищий. І навпаки, спеціалізоване визначення конфліктуватиме з групою, якщо її рівень розташування такий самий або нижчий, ніж встановлене узагальнене визначення. Наприклад, нехай U_1 встановив узагальнену політику середнього рівня, і нехай у користувача є три друга: U_h, U_m та U_l, які мають відповідно високий, середній та низький рівні конфіденційності. U_1 намагається створити для кожного зі своїх друзів політику, яка перетинається відповідно до встановленої групової політики. Виходячи з нашого припущення, встановлена узагальнена політика конфліктуватиме з політикою користувачів високого та середнього рівня, але оскільки U_l не може бачити узагальнену політику, вона не конфліктуватиме з узагальненою політикою; як показано на рисунку нижче. Однак, якщо узагальнену політику змінити на політику низького рівня, вона конфліктуватиме з усіма трьома користувачами, оскільки всі користувачі можуть бачити цю політику.

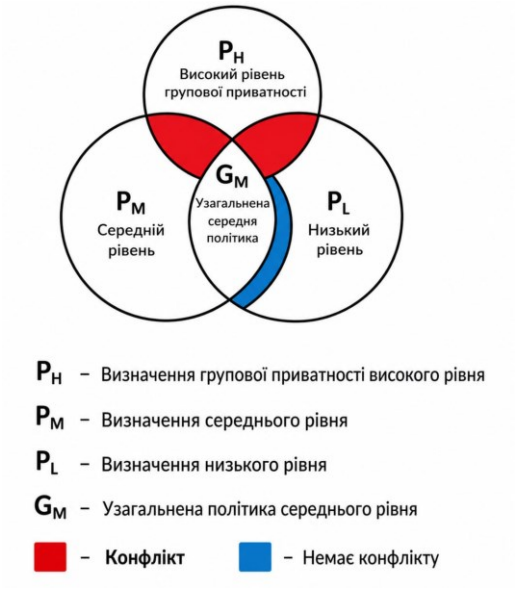

Рисунок 2.8 – Конфлікт між узагальненою та спеціалізованою політикою.

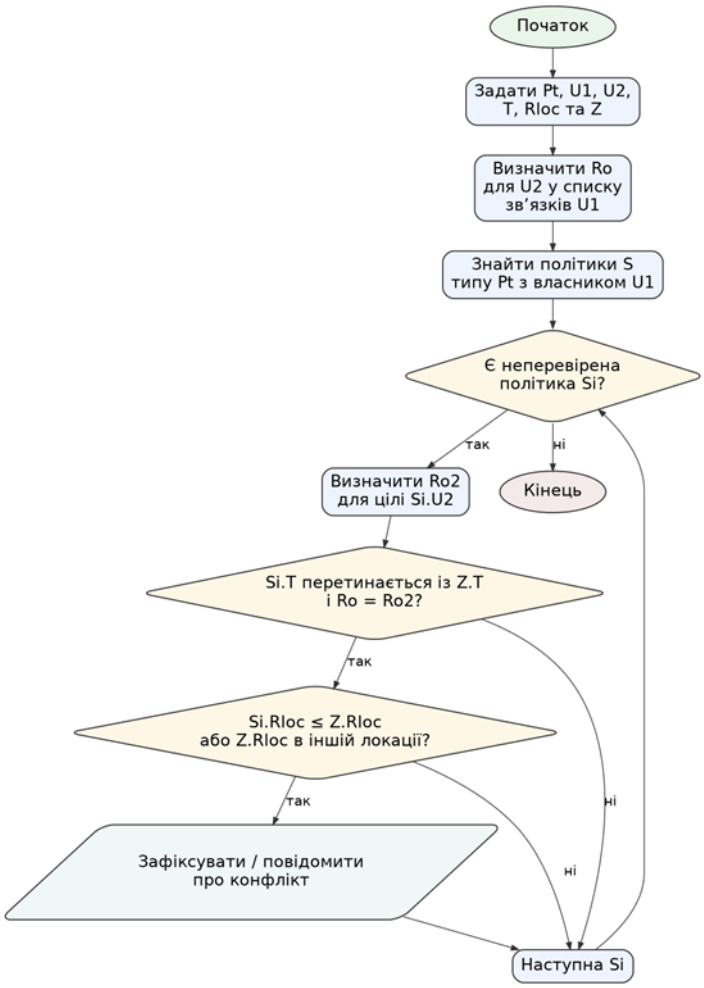

Рисунок 2.9 – Алгоритм конфлікту від узагальненої до спеціалізованої політик.

Політика «від узагальнених до виняткових».

Узагальнені політики та політики винятків не конфліктують між собою, оскільки останні є частиною перших. Іншими словами, винятки використовуються разом із узагальненими політиками і тому повинні мати можливість перетинатися одна з одною.

Інший спосіб розглядати винятки – це як підмножину будь-яких узагальнених політик, що виникають одночасно. Як підмножину узагальнених політик, як показано на рисунку нижче.

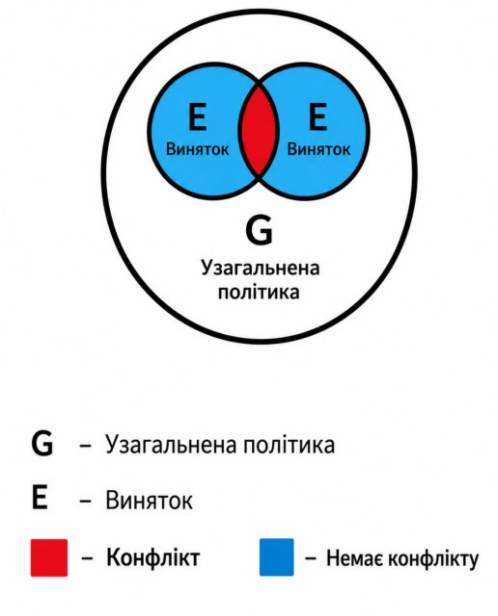

Рисунок 2.10 – Перекриття між узагальненою політикою та політикою винятків.

Політика «спеціалізований-виняток».

Оскільки спеціалізована політика робить користувача видимим, а політики винятків фактично роблять протилежне, будь-яке перекриття між ними вважається конфліктом. Користувач1 не може вимагати, щоб він був одночасно видимим і невидимим.

Політика конфіденційності групи в узагальненому вигляді

Групова політика конфіденційності – це, по суті, три групові політики, об’єднані в одну політику. Таким чином, конфлікт між узагальненою політикою

та груповою політикою конфіденційності може існувати між будь-якою з трьох групових політик окремо та узагальненою політикою.

Якщо будь-який з моментів часу конфліктує, то обидві політики конфліктують одна з одною; див. рис. 2.7.

Групова конфіденційність з винятком.

Політики винятків взаємодіють із політиками конфіденційності групи так само, як вони взаємодіють із груповими політиками.

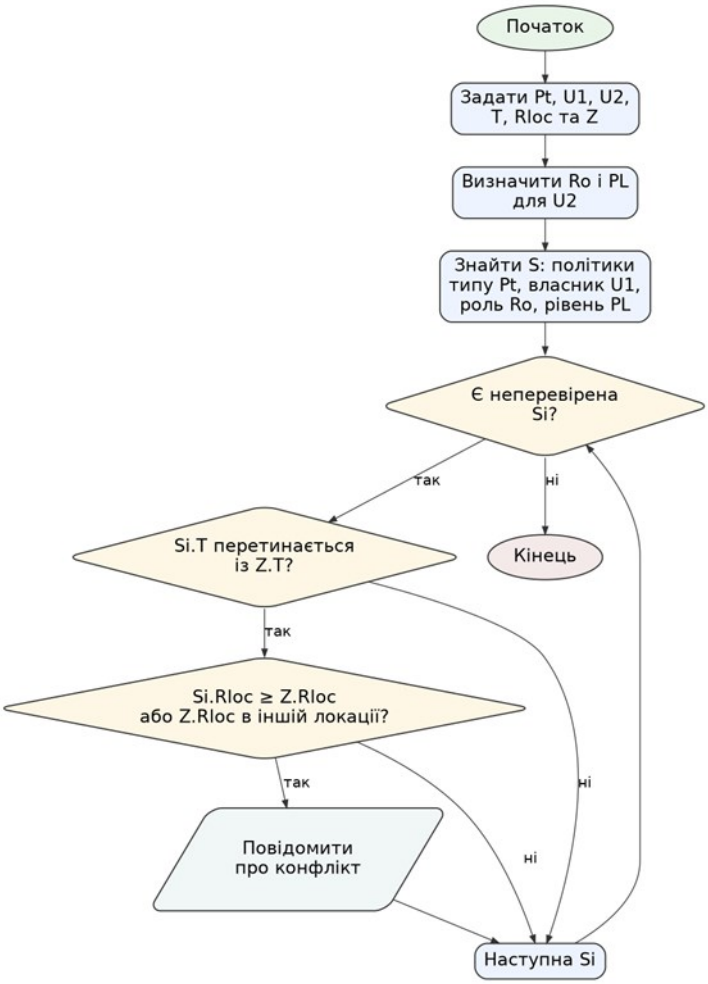

Рисунок 2.11 – Алгоритм вирішення конфліктів, спеціалізований на груповій політиці конфіденційності.

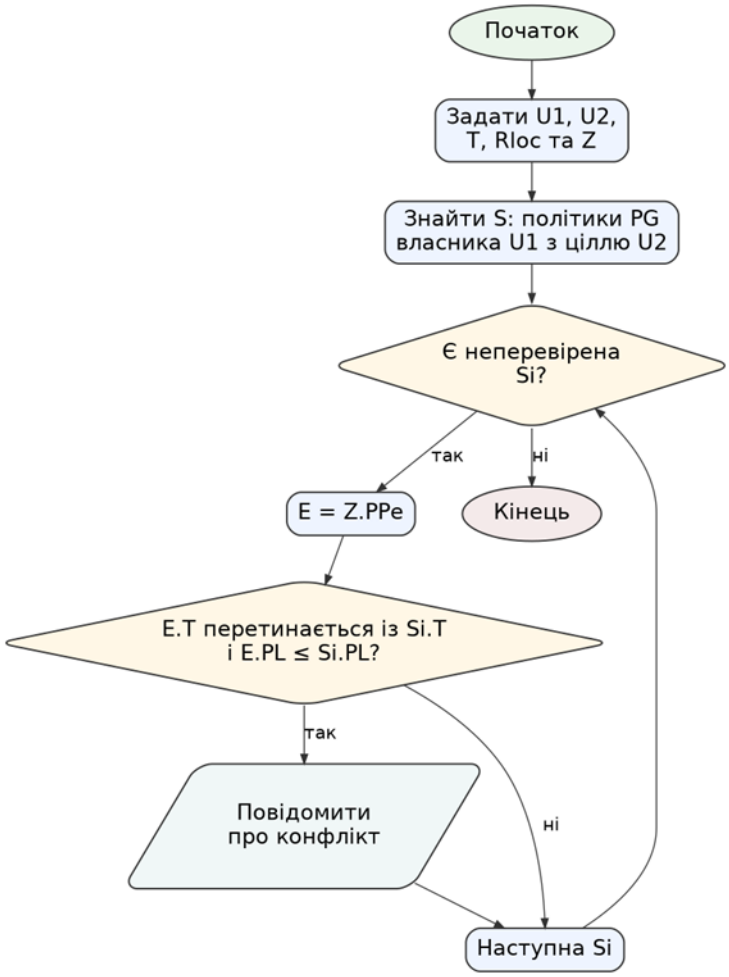

Рисунок 2.12 – Алгоритм політики конфіденційності групи алгоритмів конфліктів узагальнений

Винятки не можуть конфліктувати з політиками конфіденційності групи, оскільки вони використовуються з такими сторонами.

Групова конфіденційність для спеціалістів.

На відміну від узагальненого визначення, спеціалізовані визначення не конфліктуватимуть з усім визначенням конфіденційності групи, а з індивідуальною політикою, яка відповідає рівню конфіденційності цільового користувача. Візьмемо, наприклад, що приклад, описаний для визначення конфіденційності групи, був впроваджений.

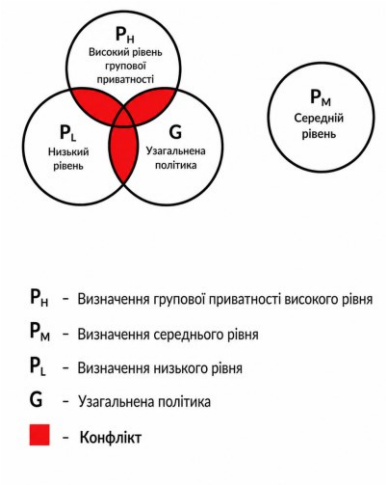

Рисунок 2.13 – Конфлікт між узагальненою та груповою політикою конфіденційності.

Якщо автор політики конфіденційності групи, Користувач1, захоче створити індивідуальну політику для друга з низьким рівнем конфіденційності о 4:30 ранку – 5:30 ранку в понеділок для вестибюля готелю, нова індивідуальна політика конфліктуватиме з нижчим рівнем політики конфіденційності групи, але якщо день тижня буде змінено на неділю, це конфліктуватиме із частинами політики середнього та високого рівнів. Однак, навіть якщо ми зробили, оскільки цільовий друг є користувачем низького рівня, ці дві політики не конфліктують, і політику можна встановити, як показано на рис. 2.14.

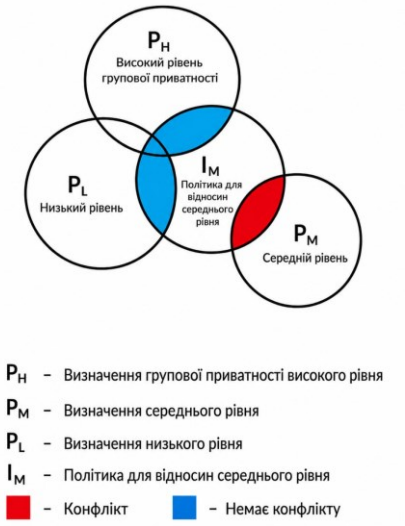

Рисунок 2.14 – Конфлікт між груповою конфіденційністю та спеціалізованим.

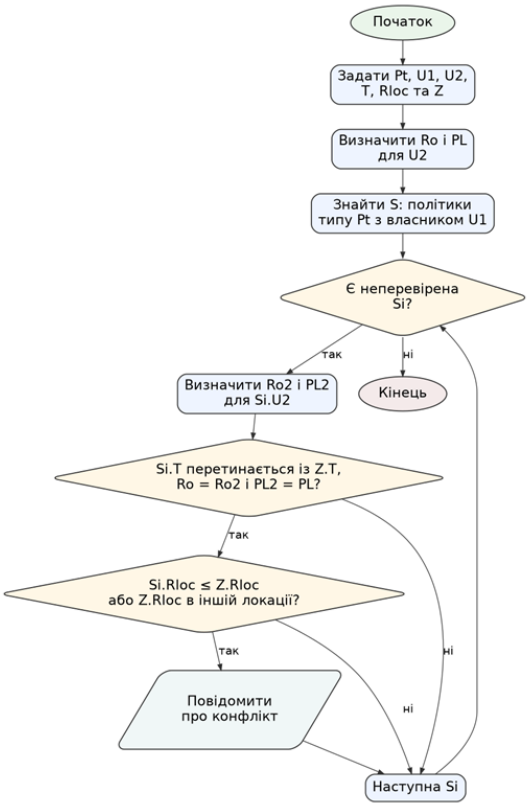

Рисунок 2.15 – Група алгоритмів конфліктів – Політика конфіденційності відповідно до Спеціалізованої політики

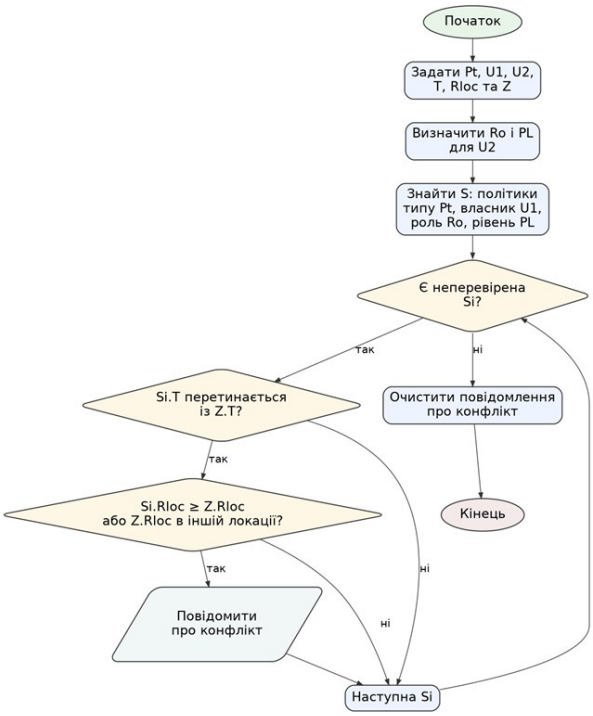

Рисунок 2.16 – Алгоритм вирішення конфліктів, спеціалізований на груповій політиці конфіденційності

Структура алгоритму виявлення конфлікту політик.

Під час перевірки місцезнаходження інших користувачів система спочатку розрізняє три типи видимих визначень. Таблиці для кожного типу політик запитуються окремо з бази даних. Політики розділяються за цільовими користувачами та ролями, після розділення політик вони вибираються на основі того, чи належить вибраний користувач до групи поточної політики. Потім політики вибираються, якщо вони знаходяться в межах часу вибору політик. Нарешті, політики порівнюються зі встановленими винятками, якщо вони конфліктують, то конфліктуюча політика не витягується.

2.3 Склад політики

Вставка політики.

Вставка політики в систему означає створення нової політики, яка буде вставлена в базу даних. Це найчастіше використовувана функція програми, яка дозволяє додавати нові політики. Спочатку політики надсилаються, потім перевіряються на дійсність, потім перевіряються на відповідність встановленим політикам для підтвердження або спростування конфліктів, і, нарешті, якщо політика дійсна, вона вставляється в базу даних..

Зміна політики.

Модифікація політики – це більш-менш зміна встановлених політик відповідно до умов конфлікту. Подібно до вставки, користувач повторно надсилає політики, які, у свою чергу, перевіряються на дійсність, порівнюються з іншими встановленими політиками та, нарешті, повторно надсилаються до бази даних..

Видалення політики.

Видалення політики є простим. Коли запитується видалення політики, спочатку перевіряється, чи має вона кілька визначень, тобто кілька періодів часу..Якщо існує кілька визначень, видаляється лише запитуване визначення, з іншого боку, якщо існує лише одне визначення, видаляється вся політика..

Об'єднання політик.

Коли встановлена політика об’єднується з новою політикою, новий часовий діапазон політики додається до існуючої політики, що дозволяє впроваджувати політику кілька разів. Стандартні умови для таких дій прості: дві політики повинні мати спільного цільового користувача, автора та місцезнаходження, і вони не повинні перетинатися в часі. Однак для кожного з чотирьох визначень політики є додаткові умови. Для спеціалізованих та узагальнених визначень додаткових умов немає, якщо вищезазначені умови виконано, і автор бажає об’єднати політику, вони об’єднаються.

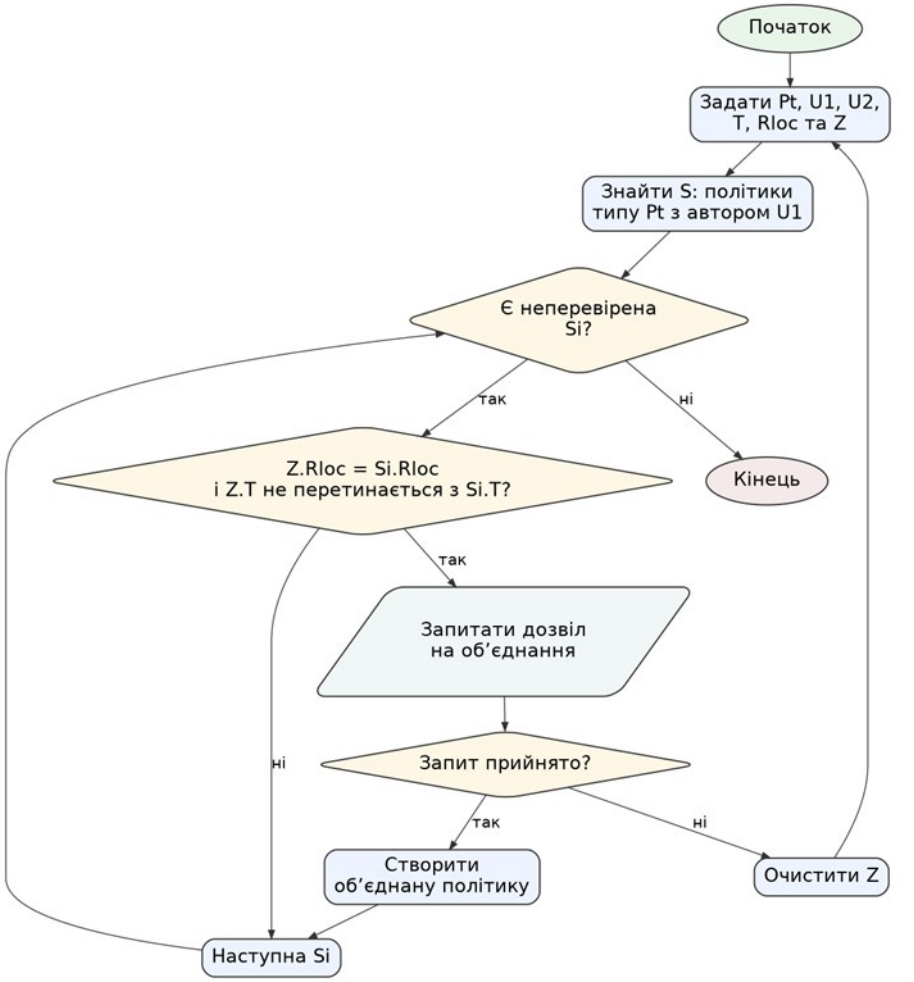

Рисунок 2.17 – Алгоритм політики об'єднання

Винятки не мають умов об’єднання, оскільки винятки не можуть бути об’єднані, оскільки вони не мають інформації для показу користувачеві.

Визначення конфіденційності групи дещо відрізняються, щоб об’єднання було можливим для політики конфіденційності групи, вищезазначені умови мають бути виконані для всіх трьох політик.

2.4 Система політичних рекомендацій

Система рекомендацій щодо політик генеруватиме рекомендовані політики на основі основних вимог користувачів, щоб зменшити навантаження на них. Далі ми спочатку визначимо поняття рівня конфіденційності, а потім представимо наш алгоритм рекомендацій.

Визначення рівнів конфіденційності політики.

Коли користувач створює нову групову політику, йому рекомендується рівень конфіденційності для цієї політики. Цей рівень конфіденційності визначає, яким категоріям зв'язків у ролі дозволено бачити політику. Видимість базується на ієрархії рівнів, де висока конфіденційність знаходиться зверху, а низька – знизу. Будь-який користувач на рівні конфіденційності групової політики або з високим може бачити політику, тобто політику низького рівня можуть переглядати всі три рівні, друзі високого та середнього рівнів можуть бачити політику середнього рівня, і лише друзі високого рівня можуть бачити політику високого рівня. Рівні конфіденційності для групових політик базуються на обчисленому числі, яке створюється за допомогою алгоритму на основі діапазону місцезнаходження та періоду часу. Користувач вказує в окремому вікні вагу місцезнаходження, тобто вагу політики рівня місцезнаходження, наприклад, встановлюючи вагу політики рівня міста на 15, а рівня місцезнаходження на 0. Вага за замовчуванням для кожного рівня місцезнаходження: 0 для місцезнаходження, 20 для міста, 55 для штату та 90 для країни, оскільки кожен рівень є більш узагальненим, ніж наступний. Вага місця розташування віднімається від ваги часу, яка може бути від 0 до 100, для обчислення рівня конфіденційності, як показано нижче

$$Privacy\ Level = \frac{|S_{time} - E_{time}|^{.613}}{7 - |S_{day} - E_{day}|} * 100 - Location\ Weight$$

S_{time}– це час початку дії полісних годин;

E_{time}– це кінцевий час для годин дії політики;

S_{day} – час початку дії поліса$

E_{day} – час закінчення дії поліса. Де часова шкала для дня починається о суботу = 6, а закінчується о неділю = 0.

Формула для часу влаштована таким чином, що вона відповідає декартовій траєкторії, подібній до y= √x, де y – різниця в часі, а x – різниця в днях. Але співвідношення між двома різницями повинні дорівнювати одиниці, коли вони досягають максимуму, тобто $23 = 7^{1/x}$ і розв'язання задачі щодо x призводить до x, що дорівнює 0,613. Потім це співвідношення помножте на 100, щоб перетворити десятковий дріб у відсоток. Після знаходження ваги конфіденційності, якщо вага знаходиться між граничними значеннями для трьох рівнів конфіденційності, цей рівень конфіденційності рекомендується. Якщо вага знаходиться між 100 і 71, це високий рівень, якщо між 70 і 24 – середній, а будь-що 23 або нижче – це низький рівень політики.

Граничні значення базуються на порушеній політиці та вазі загальних сценаріїв політик. Наприклад, загальна політика низького рівня становить 4 години та 4 дні, а політика державного рівня, тому її вага становить $(4^{613}/ (7-3)) * 100 – 55 \approx 3$, а загальний середній рівень – 8 годин, один день, а вага політики міського рівня – $(8^{613}/ (7-0)) * 100 – 20 \approx 31$. Але ми також хочемо, щоб політика була розподілена таким чином, щоб більшість із неї були політиками низького рівня, і щоб політик середнього рівня було більше, ніж високого рівня. Таким чином, діапазон середнього рівня потрібно розширити, щоб відсотковий розподіл становив 62,5% політик низького рівня, 23% політик середнього рівня та 14,5% політик високого рівня.

Вагові коефіцієнти розташування за замовчуванням для чотирьох рівнів розташування: розташування, місто, штат та країна; були визначені на основі

оцінок, а не на основі математичного проекту. Вага для кожного рівня розташування не обов'язково має бути дуже точною, оскільки значення за замовчуванням слід використовувати лише як рекомендацію. Таким чином, оцінки досить приблизні: розташування дорівнює нулю, оскільки воно має бути найлегшим, а країна має бути найважчою. Тому, щоб спростити ситуацію, значення за замовчуванням дорівнює 100. Оскільки рівень штату має бути приблизно між рівнем розташування та країною, розташування має бути набагато ближчим до країни, тому встановлення рівня штату на п'ятдесят п'ять призводить до того, що рівень буде ближчим до рівня країни та приблизно посередині спектру. Нарешті, рівень міста має бути між рівнем штату п'ятдесят п'ять та рівнем розташування нуль і ближчим до легшого рівня розташування, тому я оцінив вагу рівня міста як двадцять. Причина великої різниці між містом і штатом полягає в тому, що існує велика різниця між міською територією та територією штату, тому між двома рівнями розташування має бути велика різниця.

Алгоритм рекомендацій щодо політики.

Рекомендація щодо політики працює наступним чином. Щоразу, коли політика вставляється в систему, її рівень конфіденційності обчислюється та зберігається. Потім, коли користувач хоче створити нову політику, він може повідомити системі, яку саме політику він хоче. Наприклад, користувач може вказати, що він хоче призначити політику конфіденційності середнього рівня своєму новому другу Бобу. На запит користувача система здійснить пошук серед існуючих політик та знайде політики із середнім рівнем конфіденційності. Серед отриманих політик політика, яка містить аналогічну роль Боба, буде повернута користувачеві як рекомендована політика. Користувач може або прийняти рекомендовану політику як таку, або змінити її. Таким чином, користувачам більше не потрібно щоразу створювати нові політики.

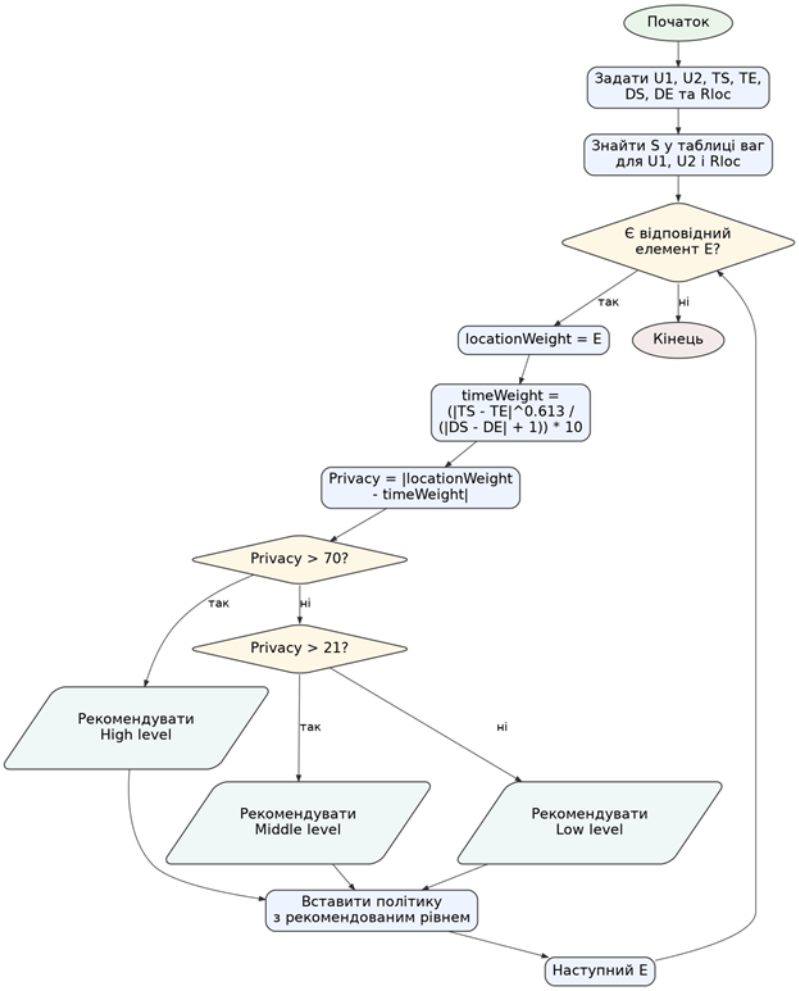

Рисунок 2.18 – Рекомендовані політики

2.5 Висновок до другого розділу

Система управління політикою конфіденційності місцезнаходження базується на чотирьох типах політик: спеціалізованих, узагальнених, винятків та групових. Кожна політика визначає часові рамки та діапазон місцезнаходження, а також рівень доступу для конкретних користувачів чи ролей. Важливим елементом є механізм виявлення конфліктів, який перевіряє перетини у часі та просторі, адже користувач не може бути одночасно у двох місцях. Система підтримує операції вставки, зміни, видалення та об’єднання політик, що забезпечує гнучке управління конфіденційністю. Політики винятків діють як доповнення до узагальнених і групових політик, дозволяючи приховати інформацію від окремих користувачів.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ СИСТЕМИ

Системну модель було реалізовано за допомогою Microsoft Access, цей вибір забезпечує легкість доступу, але призводить до втрати деяких функцій безпеки. Максимальний розмір файлу бази даних Access становить два гігабайти. Окрім максимального розміру, існує також максимальна кількість об'єктів, які можуть знаходитися у файлі бази даних протягом заданого часу. 32 768 об'єктів можуть бути частиною бази даних у будь-який момент часу. Нарешті, це місткість користувачів, які можуть одночасно перебувати в потоці, яка становить 255, але, як і розмір файлу, базу даних можна розділити на розподілену мережу баз даних, що фактично збільшує обмеження кількості одночасних користувачів.

Система була реалізована на основі двох мов програмування: Visual Basic та SQL.

Visual Basic.

Оскільки для цього експерименту потрібна була лише модель для тестування, Visual Basic був прийнятною мовою програмування. Використовуючи Visual Basic, ми змогли створити необхідні поля введення та вікна для програми без додаткової роботи, що дало б більше часу для внутрішньої роботи програми. Visual Basic дозволив мені швидко створити макет інтерфейсу, а потім швидко та лаконічно додати необхідний базовий код. Також розглядався Visual Basic, оскільки я мав досвід, необхідний для підключення інтерфейсу користувача до фонової бази даних у SQL.

Функція Visual Basic у програмі полягала здебільшого у створенні користувацького інтерфейсу. Інтерфейс мав бути простим, зручним для користувача та коректно працювати. Інтерфейс мав направляти користувача до правильної політики та відображати політики, які користувач уже створив. Іншою функцією Visual Basic була взаємодія з базою даних.

Використовуючи SQL та дані, що надаються у Visual Basic, оцініть, чи конфліктує політика з встановленими політиками.

Структурована мова запитів SQL.

Планувалося використовувати в проєкті з самого початку, оскільки він оптимізований для операторів select, а також для створення та модифікації як таблиць, так і кортежів у використаній базі даних. Microsoft Access SQL було обрано через простоту використання. Хоча його важко захистити, і він не рекомендується для повноцінної системи, він був адекватним для цього експерименту та пропонував додаткову перевагу графічного інтерфейсу користувача, завдяки чому таблиці та бази даних можна було легко створювати, а кортежі можна було досить швидко змінювати.

Основною функцією SQL у проекті було виконання зв'язків з базою даних, що надсилаються Visual Basic. Оскільки SQL оптимізовано для вибору кортежів з таблиць з використанням різних форм умов, це дуже важливо для функціонування алгоритмів конфліктів, оскільки конфлікти дуже специфічні та стосуються чотирьох типів політик та їхньої взаємодії один з одним.

У наступному розділі система оцінюється як з точки зору ефективності, так і результативності.

3.1 Розробка інтерфейсу користувача для налаштування політик

Інтерфейс користувача розроблено зручним та простим для користувача. Усі функції користувача зібрані в одному місці, щоб користувач міг легко та швидко змінювати потрібні дії. Усі функції згруповані за їхнім впливом. Інтерфейс спрощений для легкого розуміння.

Головне вікно.

Головне вікно працює як центр для всіх процесів, які користувач бажає виконувати, воно містить доступ до додавання, зміни та видалення як політик, так і зв'язків. У вікні стану відображається ім'я користувача, а у великій області вікна відображаються політики, які користувачі, що зареєстровані в системі,

мають у системі цільову роль або користувача, місцезнаходження та час початку/закінчення політики, як показано на рис. 3.1.

Якщо користувач хоче побачити, де знаходяться інші користувачі, він повинен натиснути кнопку «Переглянути зв’язки», щоб відкрити список видимих зв’язків. Винятки відокремлені від трьох інших типів визначення політик для ясності, а натискання вікна винятків відкриває окреме вікно, яке дозволяє користувачам додавати, видаляти та змінювати винятки

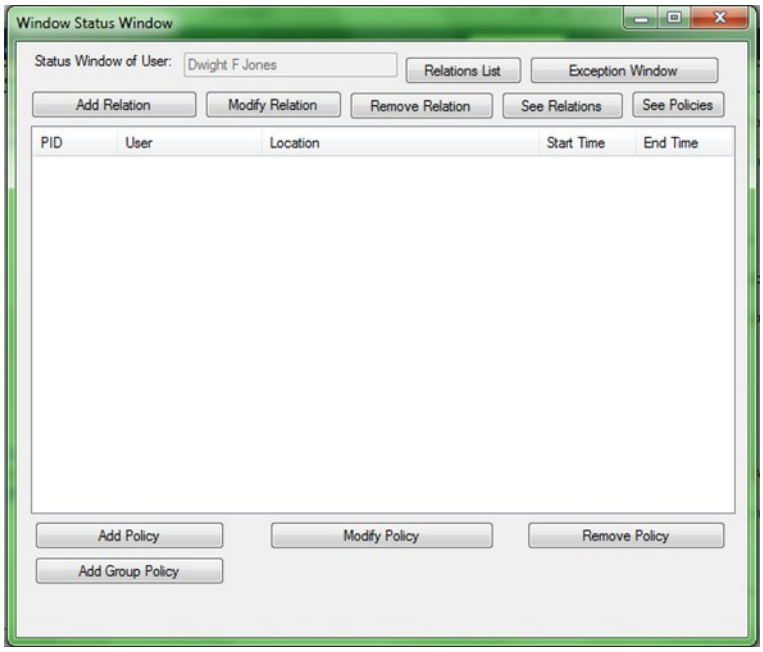

Рисунок 3.1 – Головне вікно системи

Додавання спеціалізованої або узагальненої політики.

Натискання кнопки «Додати політику» відкриває друге вікно, і введіть ідентифікатор користувача в перше текстове поле. Другий рядок містить випадаючий список, який містить список усіх користувачів зі списком родинних зв'язків. Це дозволяє зручно для користувача орієнтуватися на певного користувача, не запам'ятовуючи його ідентифікатор. На рисунку 4.2 показано, як діапазон розташування розділено на текстові поля для кращого розуміння того, що потрібно ввести. Час початку та час завершення подаються у вигляді пари числових символів вгору та вниз, що дозволяє користувачеві вибрати час. Нарешті, день тижня відображається у випадаючому вікні для

легкого вибору. Додавання групових політик не сильно відрізняється від індивідуальних політик, окрім того, що замість цільового користувача є цільова роль.

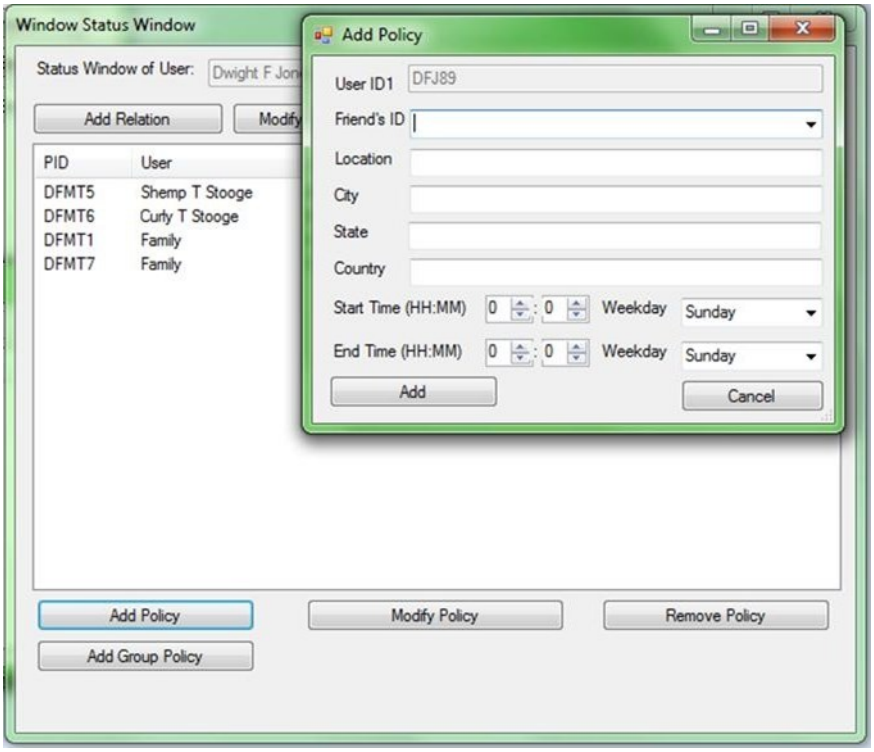

Рисунок 3.2 – Додавання спеціалізованої та узагальненої політики

Додавання політик конфіденційності групи.

Натискання кнопки «Політика конфіденційності» призводить до переходу до групової політики конфіденційності рис. 3.3. Як і у випадку з груповою та індивідуальною політикою, політика починається з ідентифікатора автора та цільової ролі, але елементи звідси змінюються. Три кнопки під цільовою роллю – це окремі політики для кожного рівня конфіденційності. Користувач натискає та вводить кожен рівень, а потім натискає «Додати», щоб закрити вікно. Після додавання інформації для кожного рівня, натискання «Додати» в головному вікні додає цю політику до політик користувача. Перед додаванням політики до бази даних система рекомендує рівень конфіденційності для політики, що відкриває вікно з рекомендованим рівнем та трьома кнопками, по одній для

кожного рівня. Після вибору потрібного рівня політика остаточно встановлюється в базу даних.

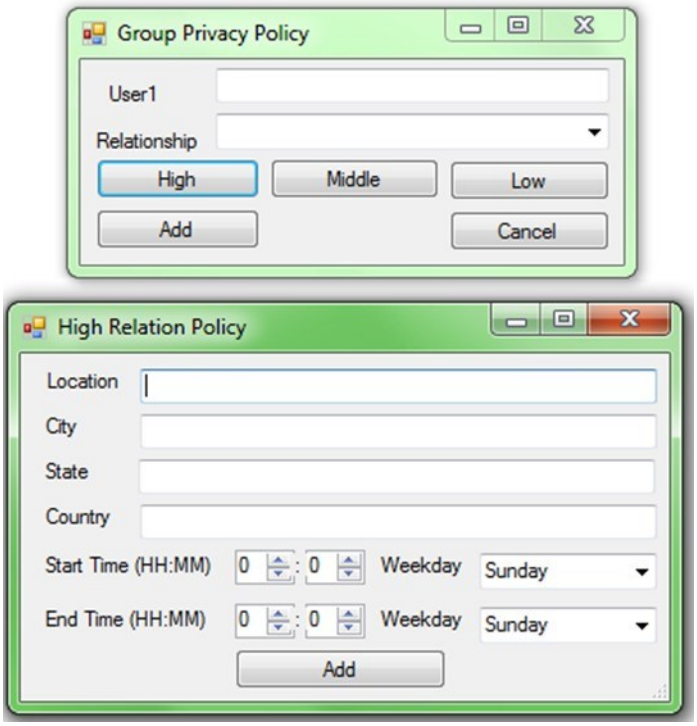

Рисунок 3.3 – Додавання політики конфіденційності групи

Зміна політик.

Вибравши встановлену політику, а потім натиснувши «Змінити політику», ви відкриєте вікно зміни політики. Кожне вікно виглядає дуже схоже на відповідну політику додавання, за винятком того, що поля введення заповнюються раніше введеними даними, як показано на рисунку 4.4..Зміна будь-якої інформації в цьому вікні призведе до зміни інформації про встановлену політику.

Видалення політик.

Видалити дуже просто, спочатку потрібно виділити встановлену політику та натиснути «Видалити політику». З’явиться діалогове вікно підтвердження. Натискання кнопки «Так» видалить встановлену політику, а натискання кнопки «Ні» поверне користувача до головного вікна стану. Після натискання кнопки

«Так» головне вікно політики знову відкриється, показуючи, що політику було видалено.

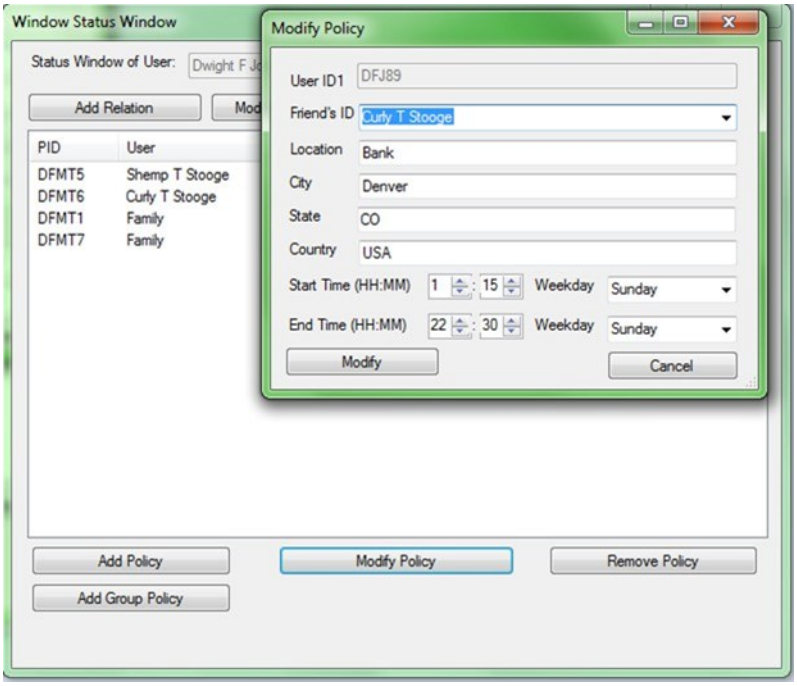

Рисунок 3.4 – Зміна політики

Вікно винятків.

Клацання на вікні винятків відкриває вікно стану винятків. Виняток відокремлено від трьох інших політик, щоб чіткіше розмежувати їх. Окрім розділення, немає жодної суттєвої різниці у зовнішньому вигляді. Це вікно містить опції для винятків: додавання, змінення та видалення. Під час відкриття вікна воно заповнюється встановленими винятками. Як і головне вікно, велика область посередині вікна винятків є вікном політики. У цій області відображаються встановлені винятки, що показують ідентифікатор політики, користувача, на якого спрямований виняток, а також час початку та завершення винятку. Закриття вікна відкриває головне вікно стану, як показано на рис. 3.5.

Функція зв'язку.

Функції зв'язків не є важливою частиною системи, але потрібні для визначення політик. Список зв'язків відображає зв'язки користувача та роль, до

якої він належить. Додавання, зміна та видалення друга дуже схоже на те, як це робиться з визначенням політики рис. 3.6.

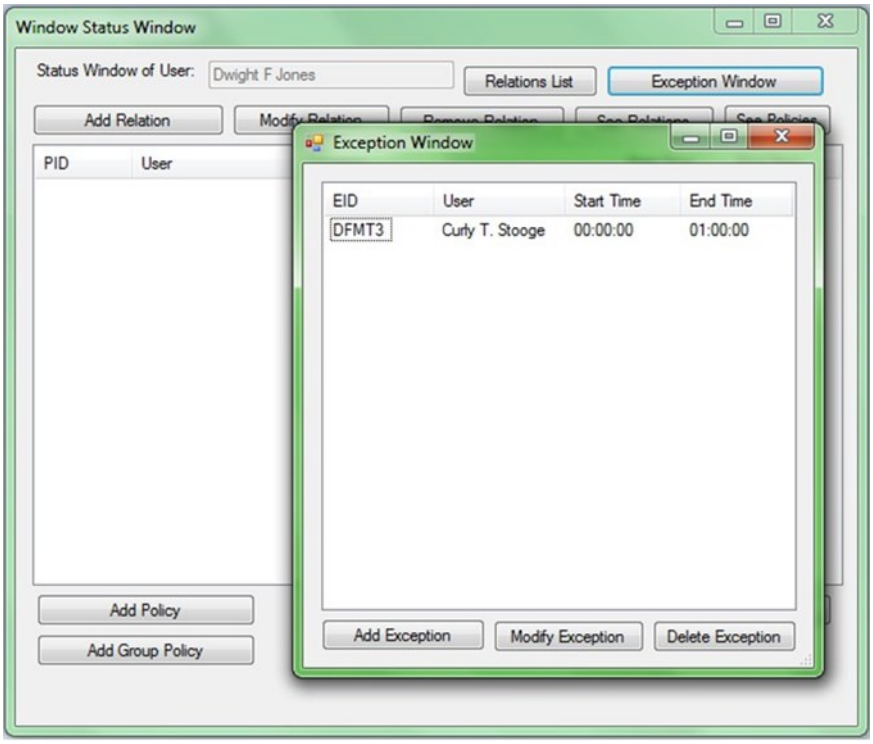

Рисунок 3.5 – Вікно створення політики винятків

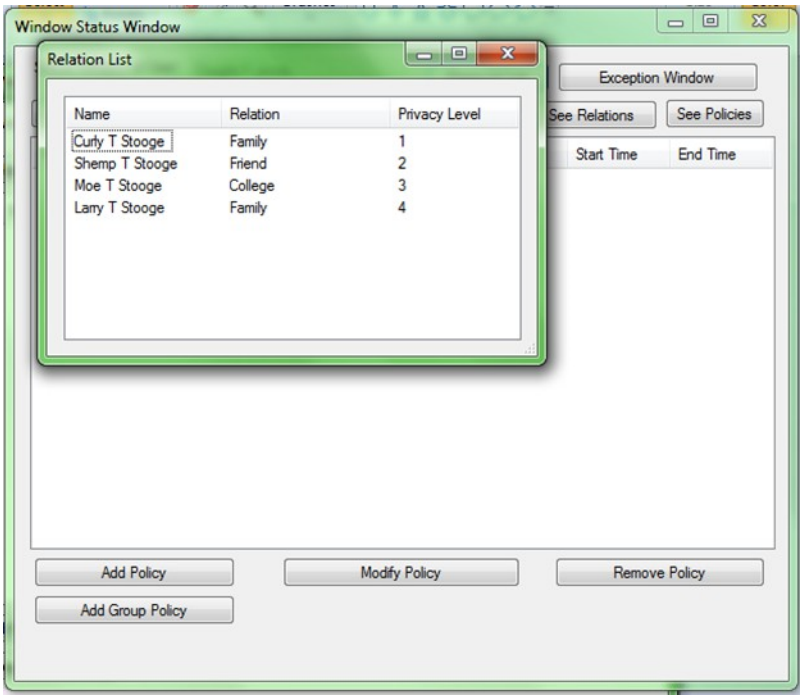

Рисунок 3.6 – Вікно стосунків

3.2 Ефективність використання системи

Оскільки час виконання дії залежить від швидкості Visual Basic, SQL, швидкості з'єднання та багатьох інших факторів, фіксоване вимірювання часу отримати неможливо. Таким чином, оцінка часової складності у нотації великого О повинна дати корисне вимірювання часу. Перш ніж детальніше обговорити час виконання функції main, є кілька фактів, які потрібно спочатку встановити. Один з них – це складність основних функцій SQL, вставки та вибору.

Вибір кортежу або кортежів з таблиці може мати один із двох рівнів складності, залежно від того, чи індексована база даних. Якщо таблиця налаштована на індексацію за своїм первинним числовим ключем, її складність становить порядку O(log(n)), з іншого боку, якщо таблиця не індексована, її складність стає порядку O(n). Що стосується вставки в базу даних, індексована база даних має складність вставки $O(\log(n_2))$, оскільки таблицю потрібно шукати, а кортеж, який потрібно вставити, потрібно оцінити, куди його розмістити. З іншого боку, для неіндексованої таблиці потрібно лише додати новий кортеж у кінець таблиці, що робить складність O(1). По-друге, це тип бази даних, яка буде використовуватися, тобто чи буде база даних індексованою, чи неіндексованою. Хоча індексована база даних зменшує час, витрачений на вибір інформації з таблиць, час її вставки набагато вищий, ніж для неіндексованої вставки. З цієї причини модель є неіндексованою.

Оцінка часової складності моделі базується на основній дії системи: аналіз конфліктів, перегляд політик інших користувачів і, нарешті, перевірка власних політик. Нам не потрібно оцінювати всі завдання, оскільки оцінки у великій нотації О базуються на найважливіших аспектах систем. Перша основна дія, з якою зіткнеться користувач, – це перевірка та відображення політик. Це найпростіша основна дія системи, оскільки вона виконує лише оператор вибору умови. Оскільки це просто оператор вибору умови, складність оператора просто O(n). Є три таблиці для перевірки під час пошуку всіх

політик, індивідуальних політик, групових політик та групової політики конфіденційності. Таким чином, оскільки є три перевірки, базова складність стає O(3n).

Далі йде пошук видимих користувачів. Це складна дія, оскільки кожна з трьох політик видимості має свою власну складність. Індивідуальна політика є прямим вибором, що робить її складністю O(n). Групова політика має порядок O(nm). Це пов'язано з тим, як виконується пошук групової політики. Нехай n – кількість політик у таблицях групових політик, а m – кількість людей у таблиці зв'язків. Для кожної групової політики n необхідно перевірити весь зв'язок m, що робить складність O(nm). Групова політика конфіденційності дуже схожа на групову політику, за винятком того, що вона по суті складається з трьох групових політик. Таким чином, кожну групову політику конфіденційності потрібно перевірити тричі, по одній для кожної підполітики, що робить її складність O((3n)m). Поєднуючи складності O((3m+1)nm + n) та відкидаючи n для спрощення порядку, ми оцінюємо складність як O((3m+1)nm). Останньою важливою дією є аналіз конфліктів. Перевірка конфліктів варіюється між чотирма визначеннями політик. Середня кількість перевірок для кожної політики становить приблизно три. Кожна перевірка сама по собі є простим пошуком, що робить її порядком O(3n).

3.3 Висновок до третього розділу

У розділі була реалізована системна модель на базі Microsoft Access, що забезпечило простоту використання, але водночас обмежило рівень безпеки та масштабованості.

Для роботи застосовано Visual Basic (створення інтерфейсу та взаємодія з базою даних) та SQL (обробка запитів і перевірка конфліктів політик).

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером

У сучасному світі все більше людей проводять значну частину свого робочого часу за комп'ютером, що призводить до ряду ергономічних проблем, які негативно впливають на безпеку та здоров'я людей. Неправильна позиція тіла, незручне розташування робочого місця, тривале сидіння та напружена робота з клавіатурою та мишею спричиняють м'язове напруження, біль у спині та напругу очей, що викликає дискомфорт та незручності.

Розташування робочого місця відіграє важливу роль у забезпеченні безпеки та здоров'я під час роботи за комп'ютером. Оптимальна висота столу та стільця є ключовим фактором для забезпечення комфорту і підтримки правильної позиції тіла. Стіл належної висоту, щоб лікті могли спокійно розташовуватися на клавіатурі, а стопи – на підлозі. Стілець обладнаний підтримкою для спини та належними регульованими підлокітниками. Клавіатура розташована на рівні ліктів, монітор – належним чином вирівняний перед очима, а миша – в зоні доступу для зап'ястя.

Правильне розташування робочого місця сприяє уникненню незручностей та проблем зі здоров'ям. Ергономічні пристрої підтримки є корисними для забезпечення комфорту та запобігання напрузі м'язів. Використання регульованих підлокітників та підставок для зап'ястя допомагає знизити напругу на м'язах і запобігти незручностям. Оптимальне розташування робочого місця повинне враховувати індивідуальні особливості користувача та забезпечувати комфортні умови для роботи.

Правильна позиція тіла та рухи є ключовими факторами для забезпечення комфорту та запобігання напрузі м'язів та незручностям.

Важливо пам'ятати про правильну позицію спини та уникати підгорблення або надмірного нахилу голови під час тривалої роботи за

комп'ютером. Регулярні перерви для розтяжки та руху є важливими для підтримання здоров'я. Прості фізичні вправи, такі як розтягування шиї, плечей, рук і ніг, допомагають зняти напругу з м'язів та покращити кровообіг. Регулярні перерви дозволяють розслабитися і зберегти енергію для продуктивної роботи. Очі є одними з найбільш вразливих органів під час роботи за комп'ютером. Постійне спрямування погляду на екран призводить до напруження та втому очей.

Для зменшення негативного впливу необхідно використовувати екрани з антиблисковим покриттям, яке знижує відблиск та рефлексію світла. Також важливо налаштовувати яскравість та контрастність екрану для комфортного сприйняття. Щоб зменшити напругу на очі, необхідно робити перерви для відпочинку, фокусуючись на далеких предметах або виконуючи вправи для розслаблення очей.

Використання неправильної клавіатури та миші призводить до м'язового напруження і тунельного синдрому. Важливо використовувати ергономічні клавіатури та миші з додатковою підтримкою для зап'ястя та комфортною формою. Правильна позиція рук та зап'ястя під час роботи з ними має велике значення. Регулярні перерви для розтяжки рук та масажу зап'ястя допомагають уникнути негативних наслідків від тривалого використання клавіатури та миші. Розглядаючи ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером, варто зазначити, що їх вирішення є ключовим для забезпечення безпеки та здоров'я під час роботи.

Дотримання принципів ергономіки, налагодження робочого місця, правильна позиція тіла та виконання фізичних вправ сприяють покращенню безпеки та створенню здорового робочого середовища. Застосування ергономічних пристроїв підтримки, таких як регульовані підлокітники та підставки для зап'ястя, також сприяє комфорту та попередженню незручностей. Загальною метою є створення безпечного та здорового робочого середовища для людей, які працюють за комп'ютером та виконують дослідження захищеності веб сервісу електронного навчання Atutor, що забезпечує

збереження здоров'я та підвищення продуктивності працівників, сприяє запобіганню травмам та ергономічним проблемам, а також сприяє загальному комфорту та задоволенню від роботи.

Додатково, важливо зазначити, що належна освітленість приміщення також є важливим фактором, який впливає на комфорт та здоров'я під час роботи за комп'ютером. Потрібно забезпечити достатнє природне або штучне освітлення, яке не перевантажує очі. Розміщення робочого місця біля вікна або використання належної освітлювальної техніки допомагає забезпечити оптимальні умови освітлення.

Важливо також уникати відблисків на екрані, розташовуючи монітор під правильним кутом до джерел світла. Безпека та конфіденційність інформації також є важливим аспектом при роботі за комп'ютером. Важливо зберігати конфіденційні дані та захищати їх від несанкціонованого доступу. Використання паролів, шифрування даних та регулярне оновлення програмного забезпечення допомагає забезпечити безпеку інформації.

Крім того, необхідно усвідомлювати потенційні загрози з боку шкідливих програм та фішингових атак і приймати заходи для їх запобігання, такі як використання антивірусного програмного забезпечення та обережне відкривання електронних листів та посилань. Регулярне навчання та свідомість про важливість ергономіки та безпеки при роботі за комп'ютером є важливими.

Працівники повинні мати бути проінформовані про правильні методи роботи, виконання пауз і фізичних вправ, а також процедур безпеки. Організації можуть проводити навчання та інформаційні тренінги, щоб підвищити свідомість та забезпечити правильну поведінку під час роботи за комп'ютером.

Враховуючи всі ці аспекти, створення комфортного, безпечного та здорового робочого середовища є важливим завданням як для працівників, так і для роботодавців. Захист здоров'я та добробуту працівників при роботі за комп'ютером не тільки покращує їхню якість життя, але й сприяє збільшенню

продуктивності та задоволення від роботи, що має позитивний вплив на всю організацію.

4.2 Організація безпечної роботи електроустаткування задіяного при роботі системи електронного навчання

Безпечна робота електроустаткування є ключовим елементом для забезпечення стабільної та безперебійної роботи системи електронного навчання. Це включає в себе правильне проектування, встановлення, експлуатацію та обслуговування електроустаткування. Дотримання стандартів і правил охорони праці допомагає мінімізувати ризики електричних ударів, пожеж та інших небезпек.

Перед встановленням електроустаткування необхідно ретельно оцінити його відповідність вимогам системи електронного навчання. Вибір обладнання повинен базуватися на таких критеріях: надійність та безпека: обладнання має відповідати стандартам якості та безпеки, мати сертифікати відповідності та бути розрахованим на довготривалу експлуатацію; відповідність технічним вимогам: обладнання повинно підтримувати необхідні технічні параметри, такі як напруга, потужність, тип з'єднання тощо; сумісність з іншими компонентами: всі компоненти системи повинні бути сумісні між собою, щоб уникнути збоїв та небезпек при експлуатації/

Під час встановлення необхідно дотримуватися таких заходів безпеки:

правильне заземлення: всі пристрої повинні бути заземлені відповідно до норм, щоб уникнути накопичення статичної електрики та можливості удару струмом; використання захисних пристроїв: встановлення автоматичних вимикачів, пристроїв захисного вимкнення (ПЗВ) та інших захисних засобів є обов’язковим для забезпечення безпеки; професійний монтаж: монтаж повинен виконуватися кваліфікованими спеціалістами з дотриманням всіх норм і правил/

Для забезпечення безпечної експлуатації електроустаткування слід дотримуватися таких рекомендацій: регулярний контроль та технічне обслуговування: обладнання повинно регулярно перевірятися на наявність зношення, перегріву, пошкоджень проводів та інших дефектів. Технічне обслуговування повинно проводитися відповідно до інструкцій виробника; контроль температурного режиму: устаткування не повинно перегріватися. Необхідно забезпечити достатню вентиляцію та уникати розташування пристроїв поблизу джерел тепла; правильне використання: обладнання має використовуватися тільки за призначенням, з дотриманням інструкцій та рекомендацій виробника.

При обслуговуванні та ремонті електроустаткування необхідно дотримуватися таких заходів безпеки: відключення живлення: перед проведенням будь-яких робіт обладнання має бути відключене від джерела живлення; використання засобів індивідуального захисту (ЗІЗ): спеціалісти повинні використовувати відповідні ЗІЗ, такі як діелектричні рукавички, килимки, інструменти з ізоляційними покриттями; дотримання процедур: всі ремонтні роботи повинні проводитися відповідно до технічних інструкцій та нормативних документів;

Управління ризиками та навчання персоналу є невід'ємною частиною забезпечення безпеки електроустаткування: ідентифікація ризиків: постійний аналіз можливих ризиків та їх мінімізація є ключовим аспектом безпеки. Для цього проводяться регулярні оцінки стану обладнання та аналіз умов експлуатації; навчання та інструктажі: персонал повинен проходити регулярні навчання та інструктажі з питань безпечної роботи з електроустаткуванням. Це включає як базові знання, так і спеціальні навички для роботи з конкретними видами обладнання; розробка та впровадження процедур безпеки: необхідно розробити детальні інструкції та процедури з безпеки, які повинні бути доступними для всіх працівників та регулярно оновлюватися. Таким чином, організація безпечної роботи електроустаткування задіяного при роботі системи електронного навчання вимагає комплексного підходу, що включає

вибір надійного обладнання, правильне його встановлення, регулярне технічне обслуговування, навчання персоналу та управління ризиками. Дотримання цих заходів дозволяє забезпечити стабільну та безпечну роботу системи, що є критично важливим для ефективного функціонування освітнього процесу.

4.3 Висновок до четвертого розділу

Ергономічні умови роботи є критично важливими для збереження здоров’я працівників, адже правильна організація робочого місця, регулярні перерви та використання спеціальних пристроїв значно знижують ризики травм і перевтоми.

Безпечна експлуатація електроустаткування потребує комплексного підходу: вибору сертифікованого обладнання, професійного монтажу, регулярного технічного обслуговування та навчання персоналу.

ВИСНОВКИ

У роботі представлено систему управління політикою конфіденційності на основі місцезнаходження. Вона має три основні функції. По-перше, вона допомагає складати політики конфіденційності на основі місцезнаходження для користувачів, які підписані на послуги на основі місцезнаходження. По-друге, вона автоматично виявляє конфлікт політик щоразу, коли відбувається оновлення політики. Таким чином, управління політиками стає простим завданням для користувачів. По-третє, вона також надає важливу функцію – рекомендації щодо політик. Користувачам не потрібно створювати нові політики для кожного нового друга. Натомість система генеруватиме рекомендовані політики на основі існуючих політик конфіденційності для аналогічної групи користувачів. Загалом, кінцевою метою запропонованої нами системи є полегшення навантаження на кінцевих користувачів під час управління їхніми налаштуваннями конфіденційності, щоб вони могли повною мірою користуватися перевагами LBS. Прототип системи був оцінений як з точки зору ефективності, так і результативності.

ПЕРЕЛІК ДЖЕРЕЛ

1 Jiang H., Li J., Zhao P., Zeng F., Xiao Z., Iyengar A. Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey // ACM Computing Surveys. 2021. Vol. 54, No. 1. Article 4. DOI: 10.1145/3423165.

2 Kim J.W., Edemacu K., Kim J.S., Chung Y.D., Jang B. Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey // Journal of Network and Computer Applications. 2022. Vol. 200. Article 103315. DOI: 10.1016/j.jnca.2021.103315.

3 Kim J.W., Edemacu K., Kim J.S., Chung Y.D., Jang B. A Survey of Differential Privacy-Based Techniques and Their Applicability to Location-Based Services // Computers & Security. 2021. Vol. 111. Article 102464. DOI: 10.1016/j.cose.2021.102464.

4 Zhang S., Li M., Liang W., Sandor V.K.A., Li X. A Survey of Dummy-Based Location Privacy Protection Techniques for Location-Based Services // Sensors. 2022. Vol. 22, No. 16. Article 6141. DOI: 10.3390/s22166141.

5 Wang B. et al. An Efficient Differential Privacy-Based Method for Location Privacy Protection in Location-Based Services // Sensors. 2023. Vol. 23, No. 11. Article 5219. DOI: 10.3390/s23115219.

6 Rasheed H. et al. Preserving location-query privacy in location-based services // Security and Privacy. 2024. DOI: 10.1002/spy2.412.

7 Schmidtke H.R. Location-aware systems or location-based services: a survey with applications to COVID-19 contact tracking // Journal of Reliable Intelligent Environments. 2020. DOI: 10.1007/s40860-020-00111-4.

8 Georgiadou Y., de By R.A., Kounadi O. Location Privacy in the Wake of the GDPR // ISPRS International Journal of Geo-Information. 2019. Vol. 8, No. 3. Article 157. DOI: 10.3390/ijgi8030157.

9 European Data Protection Board. Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 2.0, adopted 9 March 2021.

10 Javed Y. et al. A Systematic Review of Privacy Policy Literature // ACM Computing Surveys. 2024. Vol. 57, No. 2. Article 45. DOI: 10.1145/3698393.

11 Hosseini H., Utz C., Degeling M., Hupperich T. A Bilingual Longitudinal Analysis of Privacy Policies Measuring the Impacts of the GDPR and the CCPA/CPRA // Proceedings on Privacy Enhancing Technologies. 2024. No. 2. P. 434–463. DOI: 10.56553/popets-2024-0058.

12 Esteves B. et al. Analysis of ontologies and policy languages to represent information flows in GDPR // Semantic Web. 2024. DOI: 10.3233/SW-223009.

13 Porcelli L. et al. A User-Centered Privacy Policy Management System for Supporting Informed Privacy Decisions // Computers. 2024. Vol. 13, No. 2. Article 43. DOI: 10.3390/computers13020043.

14 Del-Real C., De Busser E., van den Berg B. A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies // International Review of Law, Computers & Technology. 2025. DOI: 10.1080/13600869.2025.2457227.

15 Hewage U.H.W.A., Sinha R., Naeem M.A. Privacy-preserving data mining techniques and their impact on data mining accuracy: a systematic literature review // Artificial Intelligence Review. 2023. Vol. 56. P. 10427–10464. DOI: 10.1007/s10462-023-10425-3.

16 Majeed A., Lee S. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey // IEEE Access. 2021. Vol. 9. P. 8512–8545. DOI: 10.1109/ACCESS.2020.3045700.

17 De Capitani di Vimercati S., Foresti S., Livraga G., Samarati P. k-Anonymity: From Theory to Applications // Transactions on Data Privacy. 2023. Vol. 16, No. 1. P. 25–49.

18 Ge Y.-F., Wang H., Cao J., Zhang Y., Jiang X. Privacy-preserving data publishing: an information-driven distributed genetic algorithm // World Wide Web. 2024. Vol. 27. DOI: 10.1007/s11280-024-01241-y.

19 Han X., Yang Y., Wu J. Hybrid Obscuring for Privacy-Preserving Data Publishing // IEEE Transactions on Knowledge and Data Engineering. 2024. DOI: 10.1109/TKDE.2023.3331568.

20 Su B. et al. K-Anonymity Privacy Protection Algorithm for Multi-Dimensional Data against Skewness and Similarity Attacks // Sensors. 2023. Vol. 23, No. 3. Article 1554. DOI: 10.3390/s23031554.

21 Qian J., Jiang H., Yu Y., Wang H., Miao D. Multi-level personalized k-anonymity privacy-preserving model based on sequential three-way decisions // Expert Systems with Applications. 2024. Vol. 239. Article 122343. DOI: 10.1016/j.eswa.2023.122343.

22 Li B., He K., Sun G. Local Generalization and Bucketization Technique for Personalized Privacy Preservation. 2020. arXiv:2008.11016.

23 Yang D., Qu B., Cudré-Mauroux P. Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation // IEEE Transactions on Knowledge and Data Engineering. 2019. Vol. 31, No. 3. P. 507–520. DOI: 10.1109/TKDE.2018.2840974.

24 Shen H. et al. A Privacy-Preserving Trajectory Publishing Method Based on k-Anonymity and the Similarity of Sub-Trajectories. 2023.

25 Jiang N., Zhai Y., Wang Y., Yin X., Yang S., Xu P. Location Privacy Protection for the Internet of Things with Edge Computing Based on Clustering K-Anonymity // Sensors. 2024. Vol. 24, No. 18. Article 6153. DOI: 10.3390/s24186153.

26 Zhang G. et al. Location Privacy Protection in Edge Computing: Co-Design of Differential Privacy and Offloading Mode // Electronics. 2024. Vol. 13, No. 13. Article 2668. DOI: 10.3390/electronics13132668.

27 Al Muhander B., Wiese J., Rana O., Perera C. Interactive Privacy Management: Toward Enhancing Privacy Awareness and Control in Internet of Things // ACM Computing Surveys. 2023. DOI: 10.1145/3600096.

28 Pinto G.P. et al. A Systematic Review on Privacy-Aware IoT Personal Data Stores // Sensors. 2024. Vol. 24, No. 7. Article 2197. DOI: 10.3390/s24072197.

29 Kayes A.S.M. et al. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues // Sensors. 2020. Vol. 20, No. 9. Article 2464. DOI: 10.3390/s20092464.

30 Ullah I. et al. Location Privacy Schemes in Vehicular Networks: Taxonomy, Comparative Analysis, Design Challenges, and Future Opportunities // ACM Computing Surveys. 2025. Vol. 57, No. 6. Article 160. DOI: 10.1145/3711681.

31 Benarous L. et al. A Review of Pseudonym Change Strategies for Location Privacy in Vehicular Networks // ACM Computing Surveys. 2025. DOI: 10.1145/3718736.

32 Babaghayou M. et al. A Safety-Aware Location Privacy-Preserving IoV Scheme with Road Congestion Estimation. 2023.

33 Ma B. et al. Location Privacy Threats and Protections in 6G Vehicular Networks: A Comprehensive Review. 2023. arXiv:2305.04503.

34 Choudhury O. et al. Anonymizing Data for Privacy-Preserving Federated Learning. 2020. arXiv:2002.09096.

35 Fu J. et al. Differentially Private Federated Learning: A Systematic Review. 2024. arXiv:2405.08299.

36 Garrido G.M. et al. Lessons Learned: Surveying the Practicality of Differential Privacy // Proceedings on Privacy Enhancing Technologies. 2023.

37 Cummings R., Sarathy J. Centering Policy and Practice: Research Gaps around Usable Differential Privacy. 2024. arXiv:2406.12103.

38 Aloufi O.F. et al. An Agent-Based System for Location Privacy Protection in Location-Based Services // ISPRS International Journal of Geo-Information. 2025.

39 Kim J.W. et al. Efficiently Supporting Online Privacy-Preserving Data Publishing // Applied Sciences. 2021. Vol. 11, No. 22. Article 10740. DOI: 10.3390/app112210740.

40 Partovi A., Zheng W., Jung T., Lin H. Ensuring Privacy in Location-Based Services: A Model-based Approach. 2020. arXiv:2002.10055.

41 Fryz M., Mlynko B. Determination of the characteristic function of discrete-time conditional linear random process and its application // Scientific Journal of TNTU. 2023. Vol. 109, № 1. P. 16–23.

42 M. Fryz and B. Mlynko, “Property Analysis of Conditional Linear Random Process as a Mathematical Model of Cyclostationary Signal,” in Proceedings of the 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), 2022, vol. 3309, pp. 77–82. Available: https://ceur-ws.org/Vol-3309/short2.pdf

43 Бабак В.П., Куц Ю.В., Мислович М.В., Фриз М.Є., Щербак Л.М. Об’єктно-орієнтована ідентифікація стохастичних шумових сигналів. Київ: Наукова думка, 2024. 240 с. https://doi.org/10.15407/978-966-00-1883-9.

44 V. Babak, A. Zaporozhets, Y. Kuts, M. Fryz, L. Scherbak. Noise signals: Modelling and Analyses. Cham: Springer Nature Switzerland, 2025. 222 p. DOI: https://doi.org/10.1007/978-3-031-71093-3

45 Бабак В.П., Марченко Б.Г., Фриз М.Є. Теорія ймовірностей, випадкові процеси та математична статистика. – К.: Техніка, 2004. – 288 с.

46 M. Fryz, S. Kharchenko, and L. Scherbak, “Ergodicity and Mixing of Conditional Linear Random Processes in the Problems of Information Signal Modelling and Analysis,” in 3rd International Workshop on Information Technologies: Theoretical and Applied Problems, ITTAP 2023, 2023, vol. 3628, pp. 306 – 314.

47 Fryz M., Mlynko B. Property analysis of multivariate conditional linear random processes in the problems of mathematical modelling of signals // Technol. Audit Prod. Reserv. 2022. Vol. 3, No 2(65). P. 29–32.

48 Шимчук, Г. В., Назаревич, О. Б., Литвиненко, Я. В., Готович, В. А., Никитюк, В. В., & Боднарчук, І. О. (2025). Грід-системи та технології хмарних обчислень. Навчальний посібник для здобувачів освітнього рівня «магістр» спеціальностей: F3 «Комп'ютерні науки», F6 «Інформаційні системи та технології».

49 Leshchyshyn, Y., Scherbak, L., Nazarevych, O., Gotovych, V., Tymkiv, P., & Shymchuk, G. (2019, May). Multicomponent Model of the Heart Rate Variability Change-point. In 2019 IEEE XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH) (pp. 110-113). IEEE.

50 Lytvynenko, I., Lupenko, S., Nazarevych, O., Shymchuk, G., & Hotovych, V. (2021, September). Mathematical model of gas consumption process in the form of cyclic random process. In 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT) (Vol. 1, pp. 232-235). IEEE.

51 Lytvynenko, I., Lupenko, S., Kunanets, N., Nazarevych, O., Shymchuk, G., & Hotovych, V. (2021). Simulation of gas consumption process based on the mathematical model in the form of cyclic random process considering the scale factors. In 1st International Workshop on Information Technologies: Theoretical and Applied Problems, ITTAP (Vol. 2021).

52 Шимчук Г., Голотенко О., Небесний Р., Готович В. Застосування мови Scala у системах паралельних і хмарних обчислень. Наука і техніка сьогодні. 2026. № 4(58). С. 4794–4807. DOI: 10.52058/2786-6025-2026-4(58)-4794-4807.

53 Шевченко Н., Шимчук Г., Готович В., Голотенко О., Литвиненко С., Петрошук М. Математична модель для прогнозування змін у бездротових сенсорних мережах. Наука і техніка сьогодні. 2026. № 4(58). С. 4767–4782. DOI: 10.52058/2786-6025-2026-4(58)-4767-4782.