МАГІСТЕРСЬКА РОБОТА

МР. ІПм - 57.00.00.000 ПЗ

Група ІПм-24-3

Яковишин Богдан

2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Яковишин Богдан Тарасович

(прізвище, ім'я, по батькові)

УДК 004.9

(індекс)

МАГІСТЕРСЬКА РОБОТА

Методи та моделі ефективної анонімізації даних

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

Яковишин Б.Т.

(підпис, ініціали та прізвище здобувача освітнього ступеня)

Науковий керівник Романишин Тарас Любомирович, к.т.н., доцент

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

Допущено до захисту

Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Нормоконтроль

доц. Вовк Р.Б.

(посада) (підпис) (дата) (ініціали та прізвище)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Івано-Франківськ – 2025

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**

доц. В.В. Бандура

“ 04 ” вересня 2025 р.

ЗАВДАННЯ

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Яковишину Богдану Тарасовичу

(прізвище, ім’я, по-батькові)

1. Тема магістерської роботи “ Методи та моделі ефективної анонімізації даних ”
керівник проекту (роботи) Романишин Т.Л., к.т.н., доцент
затверджені наказом закладу вищої освіти від “ 05 ” листопада 2025 р. № 695/7

2. Строк подання студентом проекту (роботи) 15 грудня 2025 р.

3. Вихідні дані до проекту (роботи) Формальні моделі і методи побудови інформаційних технологій ефективної анонімізації даних

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

1. Аналіз предметної області забезпечення приватності та анонімізації даних
2. Концепції та процеси публікації даних із захистом конфіденційності
3. Алгоритми та моделі забезпечення ефективної анонімізації та конфіденційності даних
4. Імплементація методів та інструментів для процесів ефективної анонімізації даних

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

1. Огляд процесу публікації даних із захистом конфіденційності (рис. 1.1)
2. Традиційний процес анонімізації (рис. 1.2)
3. Ієрархії узагальнення значень для сімейного стану, віку та поштового індексу (рис. 1.3)
4. Ілюстрація роботи алгоритму kACTUS (рис. 1.4)
5. Графічна інтерпретація роботи алгоритму MDAV (рис. 1.5)

6. Консультанти розділів проекту (роботи)

Розділ	Консультант	Підпис, дата
Перевірка на плагіат	доц., к.т.н. Вовк Р.Б.	

7. Дата видачі завдання 04 вересня 2025 р.

Керівник _____
(підпис)

Завдання прийняв до виконання_____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назви етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір і вивчення літератури по темі магістерської роботи	15.09.2025	виконано
2	Аналіз предметної області забезпечення приватності та анонімізації даних	01.10.2025	виконано
3	Концепції та процеси публікації даних із захистом конфіденційності	17.10.2025	виконано
4	Алгоритми та моделі забезпечення ефективної анонімізації та конфіденційності даних	02.11.2025	виконано
5	Імплементація методів та інструментів для процесів ефективної анонімізації даних	19.11.2025	виконано
6	Експериментальна оцінка інструментів анонімізації на публічному наборі даних	02.12.2025	виконано
7	Затвердження пояснювальної записки роботи завідувачем кафедри	15.12.2025	виконано

Студент – магістр _____
(підпис)

Керівник роботи _____
(підпис)

АНОТАЦІЯ

Магістерська робота: 78 с., 18 рис., 9 табл., 38 джерел.

Тема: Методи та моделі ефективної анонімізації даних

Метою роботи є комплексне дослідження методів, моделей та інструментів анонімізації даних, а також розроблення підходів до їх ефективного застосування з урахуванням балансу між конфіденційністю та корисністю інформації.

Об'єктом дослідження є процеси забезпечення приватності під час публікації та обробки даних у інформаційних системах.

Предметом дослідження є методи, формальні моделі, алгоритми та інструментальні засоби анонімізації даних.

Результати дослідження

В роботі систематизовано сучасні методи та моделі анонімізації даних, обґрунтовано критерії вибору оптимальних моделей конфіденційності, визначено сильні та слабкі сторони поширених алгоритмів, проведено комплексне порівняння програмних засобів анонімізації з урахуванням реальних практик і міжнародних стандартів.

Висновок

Наукова новизна роботи полягає в інтеграційному підході до аналізу методів анонімізації, що охоплює взаємозв'язок між формальними моделями конфіденційності, алгоритмічними механізмами їх реалізації та практичними інструментами для забезпечення приватності.

АНОНІМІЗАЦІЯ ДАНИХ, ПРИВАТНІСТЬ, КОНФІДЕНЦІЙНІСТЬ, МІКРОАГРЕГАЦІЯ, АНОНІМІЗАЦІЙНІ АЛГОРИТМИ, КОРИСНІСТЬ ДАНИХ, ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ.

ABSTRACT

Master Thesis: 78 pp., 18 fig., 9 tab., 38 sources.

Topic: Methods and models of effective data anonymization

The method of the work is a comprehensive study of methods, models and tools of data anonymization, as well as developed approaches to their effective application, taking into account the balance between confidentiality and usefulness of information.

The object of the study is the processes of ensuring privacy during the publication and processing of data in information systems.

The subject of the study is methods, formal models, algorithms and tools for data anonymization.

Research results

The work systematizes modern methods and models of data anonymization, substantiates the criteria for choosing optimal confidentiality models, identifies the strengths and weaknesses of extended algorithms, and conducts a comprehensive comparison of software tools for anonymization, taking into account real practices and international standards.

Conclusion

The scientific novelty of the work lies in the integrative approach to the analysis of anonymization methods, which covers the relationship between formal confidentiality models, algorithmic mechanisms for their implementation and practical tools for ensuring privacy.

DATA ANONYMIZATION, PRIVACY, CONFIDENTIALITY, MICROAGGREGATION, ANONYMIZATION ALGORITHMS, DATA USEFULNESS, PERSONAL DATA PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

VGH - Value Generalization Hierarchy

QID - Quasi-Identifier

GSL - Generalization Semantic Level (метрика якості VGH)

GDPR - General Data Protection Regulation

OSSpal - Open Source Software Assessment Methodology

BRR - Business Readiness Rating

OSS - Open Source Software

DPO - Data Protection Officer

CSV - Comma Separated Values

ВСТУП

Актуальність теми.

Стрімке зростання обсягів даних, цифровізація суспільства та активне впровадження інформаційних систем у всі сфери життєдіяльності створюють нові можливості для аналізу інформації, проте одночасно формують низку критичних викликів, пов’язаних із забезпеченням приватності. Сучасні організації активно використовують персональні дані для аналітики, прогнозування та оптимізації бізнес-процесів, що збільшує цінність інформації, але також підвищує ризики витоку та зловживання. З огляду на це, проблема захисту конфіденційних даних набуває глобального та міждисциплінарного значення, оскільки зачіпає технологічні, правові, етичні та соціальні аспекти.

У світі, де дані стають стратегічним ресурсом, а їх безпечна обробка — критичною передумовою функціонування цифрових сервісів, особливо зростає потреба у використанні науково обґрунтованих методів анонімізації. Відомо, що навіть після видалення явних ідентифікаторів існує можливість повторної ідентифікації осіб на основі комбінацій квазіідентифікаторів. Це підтверджують численні практичні приклади деанонімізації, що демонструють недостатність традиційних механізмів захисту.

Актуальність проблеми посилюється тим, що сучасні атаки на приватність стають дедалі витонченішими, а обчислювальні можливості для здійснення повторної ідентифікації зростають. Крім того, законодавчі вимоги, зокрема GDPR, передбачають високі стандарти захисту персональних даних та накладають на організації суттєві обов’язки щодо мінімізації ризиків.

У цьому контексті формальні моделі приватності (k-анонімність, ℓ-різноманітність, t-близькість, диференціальна конфіденційність) та алгоритмічні механізми їх реалізації займають ключову роль. Однак, попри значний науковий прогрес, потреба у вдосконаленні методів анонімізації

залишається актуальною, адже існуючі підходи нерідко супроводжуються істотними втратами корисності даних або не забезпечують необхідного рівня захисту.

У зв’язку з цим особливого значення набувають практичні інструменти анонімізації, здатні реалізувати складні моделі конфіденційності та підтримувати різноманітні сценарії публікації даних. Крім того, важливим є об’єктивне порівняння ефективності таких інструментів, оцінка їх якості за міжнародними методологіями, а також експериментальне підтвердження їх працездатності на реальних наборах даних.

Представлена магістерська робота спрямована на комплексне дослідження методів і моделей анонімізації даних, аналіз їх теоретичної основи, алгоритмічних механізмів і практичних засобів реалізації, що дозволяє сформувати цілісне уявлення про сучасні підходи до забезпечення приватності в умовах відкритих інформаційних середовищ.

Актуальність дослідження зумовлена різким збільшенням обсягів персональних даних, що обробляються організаціями, їх постійною доступністю у цифровому середовищі та підвищенням рівня ризику їх неправомірного використання. У сучасних умовах дані містять не лише інформацію про соціально-демографічні характеристики осіб, але й поведінкові, медичні, фінансові та локаційні відомості, які можуть суттєво впливати на приватність людини. З іншого боку, аналітичні технології, включаючи методи машинного навчання, потребують якісних даних, що ускладнює завдання збереження корисності інформації при анонімізації.

Традиційні методи захисту конфіденційності, такі як видалення ідентифікаторів, вже не здатні забезпечити необхідний рівень безпеки, адже наявність квазіідентифікаторів та побічної інформації полегшує повторну ідентифікацію. З розвитком технологічних та статистичних методів аналізу підвищується ймовірність успішних атак навіть на «захищені» дані. Тому у світі зростає роль формальних моделей конфіденційності, які гарантують обмеження ризиків математично обґрунтованими методами.

На нормативному рівні актуальність підтверджується вимогами міжнародних стандартів та законодавства, зокрема GDPR, що встановлює високі вимоги до анонімізації даних і визначає необоротність процесу як обов'язкову умову. У цих умовах організації стикаються з необхідністю впровадження методів, які одночасно забезпечують приватність і дозволяють використовувати дані для аналітики.

Окремим актуальним аспектом є брак універсальних інструментів, здатних однаково ефективно працювати з різними типами даних та різними моделями конфіденційності. Також недостатньо дослідженою є проблема оцінювання якості анонімізованих даних, оскільки універсальних метрик корисності не існує, а актуальні підходи нерідко суперечать один одному.

Таким чином, актуальність роботи визначається поєднанням наукових, практичних і нормативних потреб: покращення методів анонімізації, забезпечення формальних гарантій конфіденційності, мінімізація втрат корисності та розвиток ефективних інструментів для практичного застосування.

Метою роботи є комплексне дослідження методів, моделей та інструментів анонімізації даних, а також розроблення підходів до їх ефективного застосування з урахуванням балансу між конфіденційністю та корисністю інформації.

Об'єктом дослідження є процеси забезпечення приватності під час публікації та обробки даних у інформаційних системах.

Предметом дослідження є методи, формальні моделі, алгоритми та інструментальні засоби анонімізації даних.

Завдання дослідження:

1. Проаналізувати сучасні виклики приватності та проблеми публікації даних.

2. Дослідити концепції та процеси забезпечення конфіденційності під час публікації даних.

3. Оглянути та класифікувати алгоритми анонімізації, включаючи детерміністичні та рандомізовані підходи.

4. Розглянути формальні моделі конфіденційності та оцінити їх застосовність у практичних сценаріях.

5. Дослідити апаратні й програмні засоби для анонімізації даних, зокрема ARX та Amnesia.

6. Виконати оцінювання інструментів анонімізації за методологією OSSpal.

Методи дослідження

У роботі використано такі методи:

- аналітичні методи для вивчення наукових джерел і нормативних документів;

- методи математичного моделювання для аналізу формальних моделей приватності;

- алгоритмічні методи для дослідження механізмів анонімізації;

- статистичні методи для оцінювання корисності та втрат інформації;

- експериментальні методи для практичного тестування інструментів анонімізації;

- порівняльний аналіз для визначення ефективності різних підходів та інструментів.

Наукова новизна отриманих результатів

Систематизовано сучасні моделі конфіденційності та алгоритми анонімізації з урахуванням їх переваг, обмежень і практичної застосовності. Узагальнено підходи до оцінки корисності даних, що дає змогу встановлювати оптимальний баланс між точністю та приватністю. Удосконалено підхід до порівняльного аналізу інструментів анонімізації через інтеграцію методології OSSpal та експериментальної оцінки.

Виявлено особливості впливу різних моделей конфіденційності на результати анонімізації даних залежно від структури та типів атрибутів.

Практичне застосування результатів

Отримані результати можуть бути використані у діяльності організацій, що працюють із персональними даними, для побудови політик анонімізації та впровадження моделей конфіденційності. Рекомендації щодо вибору інструментів ARX і Amnesia дозволяють оптимізувати процес анонімізації залежно від типів даних і бізнес-вимог. Методичні напрацювання можуть бути застосовані у сфері кібербезпеки, розробці інформаційних систем, аналітиці даних та забезпеченні відповідності регуляторним вимогам.

Структура магістерської роботи. Представлена робота складається зі вступу, трьох розділів та висновків. Загальний обсяг роботи становить 78 сторінок, і містить 18 рисунків, 9 таблицm, перелік використаних джерел із 38 позицій.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ ТА АНОНІМІЗАЦІЇ ДАНИХ

1.1. Виклики приватності та публікації даних

Глобальне генерування цифрових даних демонструє експоненційне зростання. Приблизно 75% цього обсягу складають персональні дані, які охоплюють такі атрибути, як фізичний стан, преференції, поведінкові патерни та геолокаційні дані індивідів. Ця тенденція зумовила підвищений інтерес з боку організацій (державних структур, науково-дослідних установ, комерційних корпорацій) до збору та аналізу цих даних. Метою є створення інноваційних бізнес-моделей або підвищення якості надання послуг. Як наслідок, виникає високий попит на обмін та публікацію персональних даних між різними суб'єктами (наприклад, міжвідомча взаємодія, співпраця з аутсорсинговими партнерами, публічний доступ), що мотивовано потенційною взаємною вигодою або законодавчими вимогами.

1.1.1. Проблема конфіденційності та захисту даних

Персональні дані часто містять чутливу інформацію (наприклад, медичні записи, релігійні переконання). Неконтрольоване розголошення цієї інформації може спричинити значну шкоду. Для індивідів це ризики дискримінації, стигматизації або крадіжки особистих даних. Для організацій — це загроза негативного публічного резонансу, фінансових санкцій або інших регуляторних обмежень.

Для мінімізації цих ризиків перед поширенням необхідна анонімізація персональних даних. Сфера публікації даних із захистом конфіденційності (Privacy-Preserving Data Publishing, PPDP) пропонує методології для оприлюднення даних, які забезпечують конфіденційність індивідів, зберігаючи при цьому достатню корисність даних для аналітичних цілей

(наприклад, навчання моделей data mining, виконання агрегованих запитів, функціонування систем підтримки прийняття рішень).

Незважаючи на значний прогрес у дослідженнях PPDP [6, 8], їхнє практичне впровадження залишається обмеженим. Видавці даних (суб'єкти, що займаються обміном даних — практики, дослідники, консультанти, які прагнуть безпечного та корисного поширення) переважно обмежуються методами деідентифікації (видалення прямих ідентифікаторів, як-от імена та унікальні номери) або застосуванням хеш-функцій.

Однак доведено, що ці стратегії недостатні для захисту наборів даних від атак розкриття. Можливість ре-ідентифікації індивідів зберігається шляхом комбінування опублікованих наборів даних або використання фонової інформації. Ре-ідентифікація часто досягається через зв'язування анонімізованих даних з ідентифікованими на основі квазі-ідентифікаторів (QID). QID — це атрибути (наприклад, стать, дата народження, поштовий індекс), які в сукупності корелюють з особою настільки, що дозволяють її унікальну ідентифікацію. Запобігання таким асоціаціям вимагає застосування процедур анонімізації саме до цих атрибутів.

1.1.2. Основні виклики для видавців даних. Анонімізація даних

Процес анонімізації даних є нетривіальним і пов'язаний з низкою проблем для видавців даних (надалі — користувачів).

1. Вибір та тестування алгоритмів анонімізації

Першочерговим завданням є вибір адекватного алгоритму анонімізації для санітарної обробки даних. Через зафіксовані випадки порушення конфіденційності у нібито анонімізованих даних існує необхідність у застосуванні більш надійних стратегій, які надають формальні гарантії захисту приватності.

Велика кількість доступних алгоритмів та обмежена інформація про їхню продуктивність ускладнюють узагальнення знань і визначення оптимального алгоритму для конкретних потреб.

Неефективна анонімізація є частим наслідком виконання процесу неекспертами. Малі та середні організації або незалежні консультанти часто позбавлені ресурсів для найму кваліфікованих експертів з конфіденційності. Хоча існують програмні інструменти, вони часто все ще вимагають високого рівня експертизи для коректного застосування алгоритмів та конфігурації їхніх параметрів. Критично важливим є широке тестування методів анонімізації на різноманітних наборах даних для оцінки їхньої надійності. Однак доступ до сирих персональних даних є суворо обмеженим. Публіковані дані, як правило, вже пройшли агрегацію чи анонімізацію, що знижує їхню цінність для тестування. Хоча поширеною є практика генерації синтетичних даних, більшість існуючих методів не відповідають специфічним вимогам PPDP для адекватного тестування.

2. Забезпечення якості та корисності даних

Інший ключовий виклик полягає у створенні анонімізованих даних високої якості, які зберігають бажану вимогу конфіденційності.

Корисність даних - це збереження достовірності та інформаційної цінності оригінальних даних після анонімізації є критичним для більшості застосувань, оскільки це безпосередньо впливає на точність результатів аналізу.

Ключову роль у цьому контексті відіграють VGHs (Value Generalization Hierarchies) — деревоподібні структури, які живлять алгоритми анонімізації, засновані на узагальненні. Вони визначають набір трансформацій, яким можуть піддаватися значення атрибута, і, отже, мають бути точно визначені. Традиційно VGHs створюються та оцінюються вручну користувачами на основі їхніх знань та досвіду. Цей ітеративний процес може генерувати множину кандидатів VGHs для кожного атрибута, і вибір остаточного VGH значно впливає на корисність анонімізованих даних. Суб'єктивна та неформальна оцінка якості VGHs може призвести до неправильної класифікації або внутрішньої неузгодженості, що суттєво знижує якість анонімізованого результату. Залучення інженерів знань може зробити процес

дорогим через його трудомісткість та обмежену доступність експертів. Рішення щодо якості VGHs часто відображає суб'єктивну інтерпретацію домену однією особою.

Необхідність створення окремої VGH для кожного атрибута QID, а також потреба в ручній адаптації VGHs при зміні вхідних даних робить процес обтяжливим. Ця проблема посилюється для великих VGHs або в сценаріях постійно змінних даних (наприклад, потокові дані). Хоча запропоновані підходи до автоматичного створення VGHs [5, 9], більшість з них орієнтовані виключно на числові атрибути (створення інтервалів за розподілом даних). Методи для категоріальних даних залишаються рідкісними, оскільки числові підходи ігнорують їхню внутрішню семантику (ключовий фактор для збереження цінності). Створення категоріальних VGHs вимагає вирішення додаткових складнощів, таких як усунення багатозначності слів та визначення змістовних міток для кластеризованих концепцій.

Завдання, пов'язані з вибором, тестуванням методів анонімізації, а також створенням та оцінкою VGHs, є складними, а поточні практики неефективними. Це зумовлено високою потребою в експертних знаннях та значними ручними зусиллями, що робить процеси високо схильними до помилок і трудомісткими.

1.2. Основні концепції та виклики в публікації даних із захистом конфіденційності

Цей розділ присвячений критичному огляду фундаментальних концепцій сфери PPDP, включно з основними підходами до захисту даних, релевантними нормативними актами, наслідками порушення конфіденційності, а також метриками корисності та конфіденційності, необхідними для подальшого аналізу. Додатково розглянуто концепції семантичної подібності, які застосовуються в цій роботі.

1.2.1. Захист даних

Сучасні технологічні парадигми, зокрема великі дані та Інтернет речей (IoT), призвели до появи нових викликів у сфері приватності індивідів. Зростання кількості випадків зловживання персональними даними стимулювало розробку різноманітних підходів, спрямованих на забезпечення конфіденційності при збереженні можливості вторинного використання даних.

Поширеним інструментом для захисту приватної інформації є угоди про нерозголошення (Non-Disclosure Agreements, NDAs), які регламентують використання та зберігання чутливих даних. Хоча NDAs можуть бути ефективними для захисту корпоративної власності та інтелектуальної власності, вони не забезпечують гарантій від недбалої втрати чутливих даних або їхнього несанкціонованого доступу. Крім того, застосування NDAs вимагає рівня довіри, який є непрактично високим у багатьох сценаріях обміну даними.

Іншим загальноприйнятим підходом до захисту конфіденційності при поширенні даних є деідентифікація (de-identification). Цей метод передбачає видалення всіх явних ідентифікаторів перед публікацією персональної інформації.

Цей підхід часто імплементується у нормативно-правових актах щодо захисту даних, які розробляються урядами різних країн. Ці регуляторні механізми визначають захист особистої ідентифікаційної інформації (Personally Identifiable Information, PII), обмежуючи типи даних, які можуть бути оприлюднені відповідно до юридичних стандартів.

Наприклад, положення "безпечної гавані" (safe harbor) Закону США про переносність та підзвітність медичного страхування (HIPAA) [8] визначає набір із 18 високодиференційованих атрибутів, які повинні бути видалені з медичних даних перед їх публікацією. До цих атрибутів належать імена, ідентифікаційні номери, електронні адреси та географічна інформація.

Однак, незважаючи на те, що такий підхід забезпечує початковий рівень захисту, дані, що залишаються, є вразливими. У багатьох випадках вони можуть бути використані для ре-ідентифікації індивідів шляхом зв'язування з загальнодоступними джерелами даних або через аналіз унікальних характеристик у опублікованому наборі даних.

1.2.2. Приклад деанонімізації наборів даних користувачів

Незважаючи на зусилля із застосування анонімізації та обмеження типів даних, які підлягають публікації, було зафіксовано декілька резонансних випадків деанонімізації опублікованих наборів даних. Наведені нижче приклади демонструють, що просте видалення прямих ідентифікаторів або виконання поверхневих трансформацій даних є недостатнім для захисту конфіденційності, а також ілюструють складнощі розробки та застосування ефективних методів PPDP.

1. Інцидент з Губернатором Массачусетсу (1997) [17].

Комісія з групового страхування (GIC) Массачусетсу опублікувала медичні записи 100 000 державних службовців, попередньо видаливши всі прямі ідентифікатори. Дані все ще містили квазі-ідентифікатори (QID), такі як дата народження, стать та поштовий індекс.

Атака. Користувач зміг повторно ідентифікувати запис губернатора Массачусетсу, зв'язавши медичний набір даних із придбаною копією списку реєстрації виборців. Виявилося, що 87% населення США можуть бути унікально ідентифіковані за комбінацією поштового індексу, дати народження та статі. Цей випадок є класичною демонстрацією атаки зв'язування записів (record linkage attack), де зовнішня інформація використовується для деанонімізації.

2. Набір даних AOL (2006) [8].

AOL опублікувала "анонімізований" файл із мільйонами пошукових запитів від 650 000 користувачів, замінивши ідентифікатори користувачів випадковими псевдонімами.

Атака. Незабаром після публікації багато користувачів були ідентифіковані. Журналісти New York Times відстежили конкретного користувача, ґрунтуючись на семантичному вмісті її пошукових запитів та інших джерелах інформації (назва міста, прізвище, вік).

Це порушення конфіденційності сталося через неврахування розсіяних джерел інформації та семантичної цінності самих пошукових запитів, що дозволило провести атаку на основі вмісту.

3. Netflix Prize (2008) [9].

Netflix опублікувала 100 мільйонів оцінок фільмів від 480 000 користувачів, видаливши особисту інформацію та замінивши ідентифікатори користувачів псевдонімами. Дослідники деанонімізували набір даних, показавши, що за допомогою зовнішньої інформації (наприклад, оцінок, публічно доступних на IMDb) та невеликої кількості знань про оцінки підписника можна легко ідентифікувати його запис у даних.

Це підкреслило вразливість перед атаками, що використовують зовнішні, нечутливі, але корельовані дані для зв'язування.

4. Дані таксі Нью-Йорка (2014) [10].

Був опублікований набір даних про поїздки на таксі, що містив час, місце посадки/висадки, суму оплати та анонімізовані номери ліцензій та медальйонів водіїв. Схема анонімізації полягала у застосуванні хеш-функції MD5.

Розробник програмного забезпечення зміг деанонімізувати всі записи менш ніж за дві години. Оскільки номери ліцензій та медальйонів мали передбачувану структуру, він запустив ітерації всіх можливих вхідних даних через той самий алгоритм MD5 і порівняв вихідні хеші з тими, що були в опублікованому наборі.

Ця атака стала можливою через використання неефективного та криптографічно слабкого механізму анонімізації (незворотного хешування) для структурованих вхідних даних, що дозволило провести атаку за словником або повним перебором (brute-force attack).

1.2.3. Семантична подібність, заходи конфіденційності та корисності

Для повного розуміння методів PPDP необхідно розглянути метрики оцінки конфіденційності та корисності даних, а також концепції семантичної подібності.

В контексті цієї роботи, поняття семантичної подібності відноситься до методів кількісної оцінки міри, в якій два терміни, вирази або об'єкти даних мають спільне значення або контекстну спорідненість. Це особливо важливо для атрибутів із категоріальними значеннями, де узагальнення має зберігати внутрішню логіку даних.

Заходи конфіденційності - це формальні гарантії, що кількісно оцінюють ступінь захисту осіб від атак розкриття. До них належать такі моделі, як k-анонімність, ℓ-різноманітність та диференційна приватність.

Заходи корисності - це метрики, що оцінюють ступінь, у якому анонімізований набір даних зберігає інформаційну цінність оригінальних даних для конкретних аналітичних завдань (наприклад, точність класифікації, мінімізація втрати інформації, збереження кореляцій).

1.3. Концепції та процеси публікації даних із захистом конфіденційності

Публікація даних із захистом конфіденційності (PPDP) – це наукова дисципліна, яка фокусується на розробці методів та інструментарію для оприлюднення анонімізованих наборів даних. Мета полягає у збереженні корисності даних для різних аналітичних завдань при одночасному захисті конфіденційності осіб, представлених у цих наборах, шляхом запобігання їхній повторній ідентифікації.

1.3.1. Типовий сценарій публікації даних із захистом конфіденційності

Типовий сценарій PPDP охоплює кілька фаз обробки даних:

1. Збір даних - активне агрегування значних обсягів персональних даних.

2. Потреба в публікації. Видавці даних (наприклад, лікарні, школи, роздрібні мережі) часто потребують обміну цими даними з третіми сторонами для досліджень, комерціалізації чи аутсорсингу.

3. Анонімізація. Оскільки дані можуть містити чутливу інформацію, вони повинні бути анонімізовані перед поширенням для захисту приватності, зберігаючи при цьому максимальну корисність для подальшого аналізу.

4. Поширення та використання. Опубліковані анонімізовані дані використовуються різними одержувачами (аутсорсингові партнери, дослідники, широка публіка), рівень довіри до яких може варіюватися.

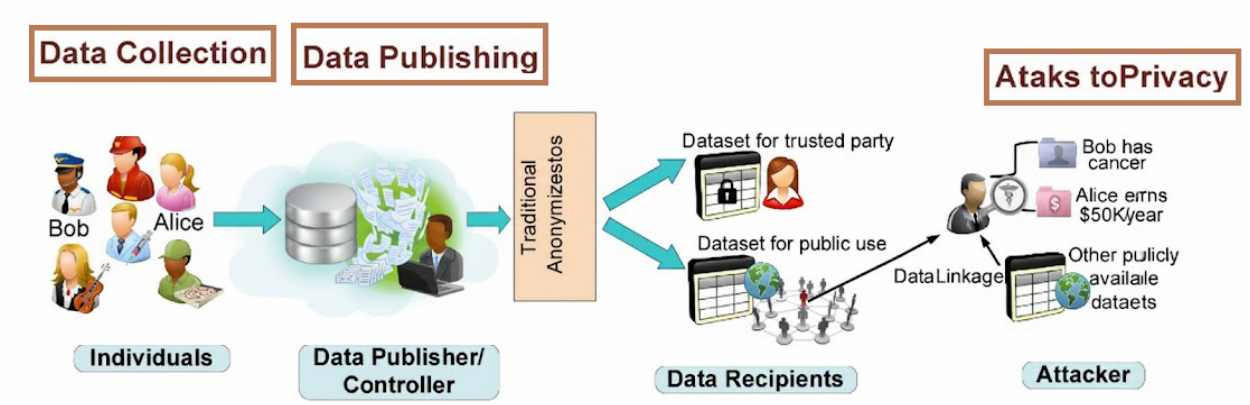

Рис. 1.1. Огляд процесу публікації даних із захистом конфіденційності

Ключовим припущенням моделі PPDP є потенційна присутність серед одержувачів зловмисників, які можуть мати намір розкрити чутливу інформацію. Таким чином, основна мета PPDP-методів полягає в запобіганні атакам на конфіденційність шляхом публікації безпечних, але функціональних даних.

Важливою передумовою PPDP є створення наборів даних із високою корисністю для різноманітних завдань, оскільки всі потенційні сценарії використання (наприклад, у рамках ініціатив відкритих даних) зазвичай невідомі.

У базовій формі PPDP, таблиця мікроданих (неагрегована інформація про окремих осіб) складається з кортежів, де кожен кортеж відповідає запису, пов'язаному з особою, та визначеному над набором атрибутів. Атрибути класифікуються на чотири категорії:

- ідентифікатори (IDs) - атрибути, які явно ідентифікують осіб (наприклад, ім'я, унікальні ID-номери).

- квазі-ідентифікатори (QIDs) - атрибути, які потенційно можуть спричинити повторну ідентифікацію при комбінуванні із зовнішньою інформацією (наприклад, професія, національність).

- чутливі атрибути (SAs) - атрибути, що містять чутливу інформацію про осіб (наприклад, діагноз, зарплата).

- нечутливі атрибути (NSAs) - атрибути, розголошення яких не створює проблем конфіденційності.

1.3.2. Традиційний процес анонімізації

Традиційний процес анонімізації даних у PPDP є ітеративним і складається з низки послідовних кроків. На рисунку 1.2 зображено поширену практику анонімізації.

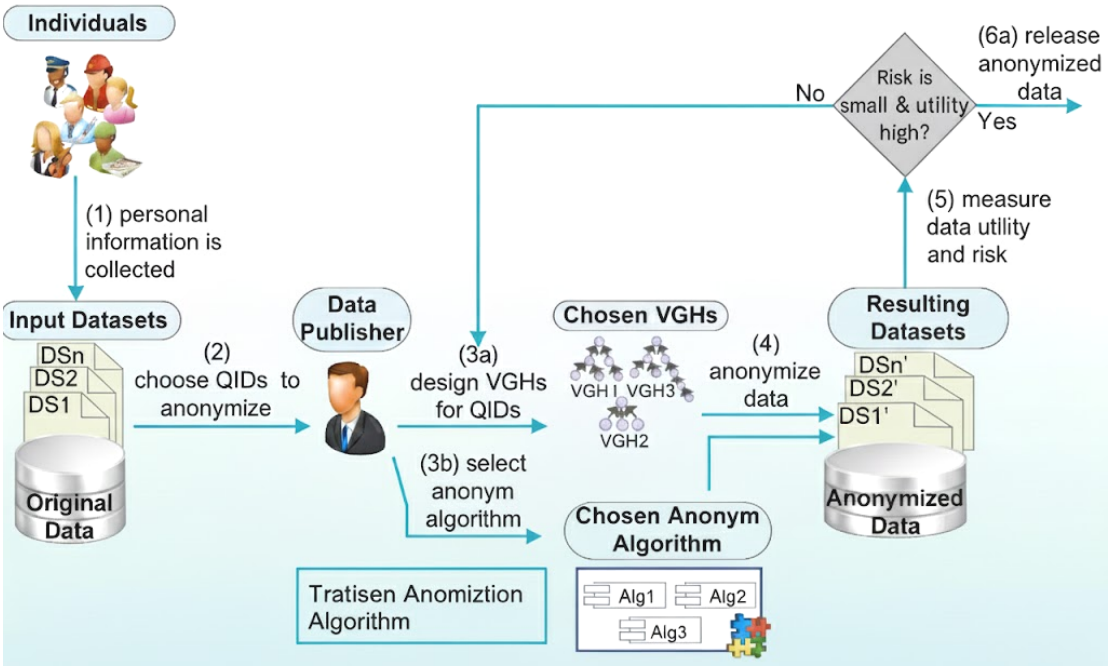

Рис. 1.2. Традиційний процес анонімізації

1. Збір та класифікація атрибутів.

Видавець даних (організація або незалежний консультант) збирає інформацію. Атрибути набору даних класифікуються на IDs, QIDs, SAs та NSAs. З метою захисту IDs видаляються, а вибрані QIDs підлягають анонімізації/санітарній обробці.

2. Критичні рішення щодо анонімізації (вибір моделі та алгоритму).

Користувач приймає два ключові рішення, які визначають якість кінцевих даних. Успішність цих рішень залежить від експертного розуміння методів анонімізації та моделювання предметної області.

2.1. Створення ієрархій узагальнення значень (VGHs). Для кожного QID-атрибута користувач вручну створює набір кандидатів VGH для моделювання домену. Оцінка якості VGH проводиться користувачем суб'єктивно на основі знань та досвіду. Це є трудомістким та схильним до помилок процесом.

2.2. Вибір алгоритму анонімізації. Користувач обирає відповідний алгоритм анонімізації на основі бізнес-випадку. Різні алгоритми використовують різні операції санітарної обробки, що впливає на якість даних, розмір простору пошуку та рівень захисту конфіденційності.

3. Застосування анонімізації.

Вибраний алгоритм та VGH (у випадках, коли застосовується узагальнення) використовуються для анонімізації даних. Часто застосовується критерій конфіденційності (наприклад, k-анонімність) як умова зупинки, забезпечуючи, щоб санітарна обробка тривала, доки не буде задоволено заданий параметр захисту.

4. Оцінка та компроміс.

Оцінюється якість отриманих даних (порівняно з оригіналом або за точністю аналітичних завдань), а також ризик розголошення (якщо не було надано критерію конфіденційності).

Оцінюється компроміс між корисністю даних (точністю аналізу) та конфіденційністю (кількістю інформації, яку може отримати зловмисник).

Якщо корисність є достатньо високою, а ризик розкриття мінімальним, дані публікуються. В іншому випадку ініціюється новий ітераційний цикл анонімізації (починаючи з кроку 2), де конфігурації анонімізації, включно з моделюванням VGH, можуть бути адаптовані відповідно до цілей користувача.

PPDP має спільні риси з іншими дослідницькими галузями, такими як захист конфіденційності в Data Mining (PPDM), статистичний контроль розголошення (SDC) та шифрування даних (DE), проте між ними існують суттєві відмінності.

PPDP і PPDM. PPDM зосереджується на результатах конкретного завдання Data Mining, де рішення тісно пов'язані з цим завданням. PPDP, навпаки, є незалежною від завдання і фокусується на публікації наборів даних, корисних для множинних аналітичних цілей. Крім того, в PPDP видавець даних не обов'язково повинен бути експертом у Data Mining.

PPDP і SDC. SDC переважно орієнтований на публікацію табличних статистик (агрегованих даних). Методи SDC часто не зберігають достовірність на рівні записів, використовуючи збурення та шум для збереження статистичних властивостей. SDC оцінює загрози після санітарної обробки шляхом вимірювання ризику. PPDP, навпаки, покладається на a priori моделі конфіденційності, які надають формальні гарантії захисту, враховуючи атаки на основі фонових знань та виведення чутливих атрибутів.

PPDP і DE. Шифрування (DE) перетворює дані в нечитабельний формат, доступний лише довіреним та авторизованим одержувачам через ключ. Хоча DE підходить для захисту даних під час передачі/зберігання, воно значно обмежує подальшу обробку/обчислення даних, хоча гомоморфне шифрування є предметом активних досліджень. Анонімізація (PPDP) трансформує дані так, щоб захистити конфіденційність, зберігаючи їхню семантику. Це дозволяє безпечно обмінюватися даними з багатьма сторонами, зберігаючи їхню гнучкість для виконання будь-якого необхідного аналізу.

1.4. Детерміністичні та рандомізовані підходи механізмів анонімізації

Анонімізація табличних даних реалізується шляхом застосування послідовності операцій, які зазвичай орієнтовані на квазі-ідентифікатори (QID), з метою досягнення заздалегідь визначеного критерію конфіденційності. Ці операції можуть бути класифіковані на детерміністичні та рандомізовані механізми. Детерміністичні механізми є доцільними, коли основною метою є збереження правдивості даних. Правдивість даних означає, що кожен опублікований запис відповідає реально існуючій особі в оригінальному наборі даних [12].

Приклади детерміністичних механізмів включають:

- Бакетизація (Bucketization), також відома як анатомізація.
- Узагальнення (Generalization).
- Придушення (Suppression).

Рандомізовані механізми не зберігають правдивість даних. Вони вводять стохастичні елементи для захисту конфіденційності.

Приклади рандомізованих механізмів включають:

- Мікроагрегація;
- Випадкове збурення;
- Адитивний шум;
- Обмін даними.

Оскільки подальший аналіз у цій роботі ґрунтується на алгоритмах узагальнення та придушення, наступні підрозділи присвячені детальному опису цих операцій.

Операції узагальнення та придушення набули значного поширення в науковій літературі [14, 16].

Придушення полягає у заміні частини оригінальних даних спеціальним символом (наприклад, "*"). Це слугує індикатором того, що конкретне значення не розголошується, ефективно приховуючи його.

Узагальнення передбачає заміну оригінальних значень атрибута менш точними, але семантично узгодженими значеннями. Основна ідея полягає у зменшенні специфічності оригінальних даних, що, у свою чергу, знижує ймовірність повторної ідентифікації осіб у опублікованих наборах даних. Наприклад, спеціальність "онколог" може бути узагальнена до загальнішого терміну "лікар" для захисту професійної приватності особи.

Ієрархії узагальнення значень (Value Generalization Hierarchies, VGHs) є обов'язковою передумовою для алгоритмів, заснованих на узагальненні. VGHs є деревоподібними структурами, які керують процесом анонімізації, визначаючи набір допустимих трансформацій для атрибута. Приклади VGH показані на рисунку 1.3.

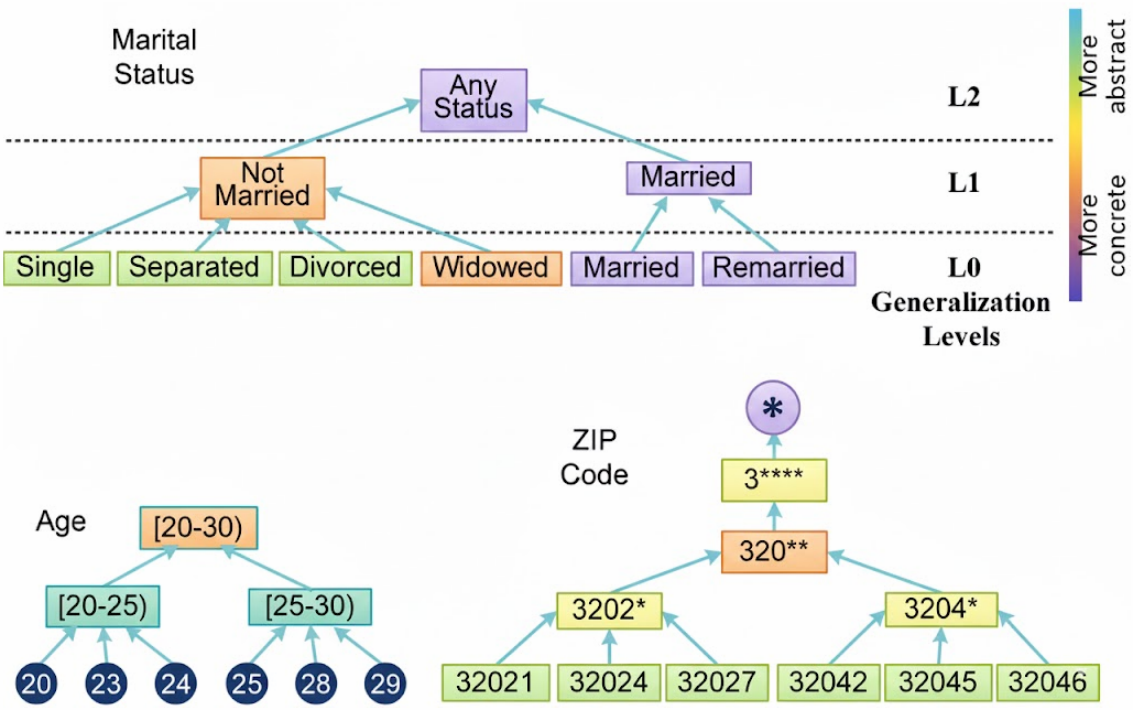

Рис. 1.3. Ієрархії узагальнення значень для сімейного стану, віку та поштового індексу

Листові вузли (L0) відповідають фактичним значенням атрибута у вихідному наборі даних. Предкові вузли (L1 до кореня) відповідають кандидатним значенням, які використовуються для узагальнень. Більш

загальні терміни розташовані на вищих рівнях VGH, а більш спеціалізовані терміни знаходяться на нижчих рівнях VGH.

Узагальнення може бути реалізовано за допомогою глобальної (узагальнення всього домену) або локальної схеми.

Локальне узагальнення це коли до записів можуть бути застосовані різні рівні гранулярності узагальнення, навіть якщо вони мають однакові вихідні значення атрибутів. Глобальне узагальнення - до всіх екземплярів атрибута застосовується однакове узагальнення, забезпечуючи, щоб вони мали однакове узагальнене значення.

Глобальне узагальнення поділяється на одновимірне узагальнення: кожен атрибут у групі QID розглядається незалежно і багатовимірне узагальнення – домен узагальнення визначається як добуток доменів окремих QID-атрибутів (узагальнення n-векторів).

Виконаємо ілюстрація анонімізації на основі узагальнення. Для цього розглянемо вихідну таблицю 2.1 (кримінальні записи), де: ідентифікатор (ID) - ім'я, квазі-ідентифікатори (QID) - сімейний стан, вік, поштовий індекс, чутливий атрибут (SA): злочин.

Таблиця 1.1.

Приклад вихідної таблиці із даними до анонімізації

Ім'я (ID)	**Сімейний стан (QID)**	**Вік (QID)**	**Поштовий індекс (QID)**	**Злочин (SA)**
Особа А	Одружений	32	12345	Крадіжка
Особа Б	Розлучений	45	12347	Напад
Особа В	Вдовець	61	12341	Шахрайство
...	...	...	...	...

Таблиця 1.2 демонструє 3-анонімну версію таблиці 1.1, що гарантує, що кожен кортеж належить до еквівалентного класу принаймні з трьома записами, які мають однакові значення QID.

Для досягнення 3-анонімності були застосовані такі трансформації:

1. Видалення ідентифікатора: атрибут ім'я було видалено.

2. Одновимірне узагальнення QID:

- сімейний стан - замінено менш специфічними, але семантично узгодженими описами (наприклад, "Одружений", "Розлучений" → "Одружений/Повторно одружений").

- вік - замінено діапазонами значень (наприклад, 30-40).

- поштовий індекс - остання цифра була замінена на символ придушення ("*"), узагальнюючи домен.

Таблиця 1.2.

Приклад таблиці із даними після анонімізації

Сімейний стан (QID)	**Вік (QID)**	**Поштовий індекс (QID)**	**Злочин (SA)**
Одружений/Повторно одружений	30 - 40	1234*	Крадіжка
Одружений/Повторно одружений	30 - 40	1234*	Напад
Одружений/Повторно одружений	30 - 40	1234*	Шахрайство
...	...	...	...

У цьому прикладі перші три записи тепер складають один еквівалентний клас і, отже, є 3-анонімними, що ускладнює асоціацію QID-значень із конкретним чутливим атрибутом.

Висновки до розділу

У першому розділі було встановлено, що проблема збереження приватності даних є однією з ключових у сучасних інформаційних системах. Детальний аналіз предметної області показав, що публікація даних супроводжується численними ризиками, пов’язаними з витоком конфіденційної інформації. Розглянуті виклики підтверджують, що традиційні заходи безпеки не забезпечують достатнього рівня захисту без

застосування спеціалізованих методів анонімізації. Було з’ясовано, що навіть після видалення явних ідентифікаторів дані можуть бути повторно зіставлені завдяки квазіідентифікаторам. Приклади деанонімізації реальних наборів даних демонструють вразливість інформації в умовах сучасних аналітичних можливостей. Проаналізовано концепції семантичної подібності та їхній вплив на збереження корисності анонімізованих даних. Розділ показав, що процес публікації даних із захистом конфіденційності є складним багатокроковим сценарієм, який потребує ретельного планування. Традиційний процес анонімізації описано як комбінацію операцій генералізації, приховування та модифікації атрибутів. Особливу увагу приділено детерміністичним та рандомізованим підходам, які істотно відрізняються за рівнем стійкості до повторної ідентифікації. Висновки розділу свідчать, що формування ефективної стратегії анонімізації потребує поєднання різних технічних, статистичних та аналітичних методів для забезпечення збалансованості між приватністю та корисністю даних.

РОЗДІЛ 2. АЛГОРИТМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОЇ АНОНІМІЗАЦІЇ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ

2.1. Огляд алгоритмів анонімізації

У науковій літературі представлено значну кількість алгоритмів анонімізації, розроблених у різних напрямках галузі захисту даних. Ці методи можна класифікувати за основними механізмами, які вони використовують, зокрема, узагальненням та мікроагрегацією.

2.1.1. Алгоритми, базовані на узагальненні

Ця група методів використовує операції узагальнення та придушення для забезпечення формальних гарантій конфіденційності, часто прагнучи мінімізувати втрату корисності, зокрема для завдань класифікації.

Генетичний алгоритм для збереження класифікаційної інформації [22]. Запропоновано підхід, що використовує генетичний алгоритм для оптимізації процесу анонімізації з метою максимального збереження класифікаційної точності в опублікованих даних.

Ітеративний алгоритм узагальнення "Знизу Вгору". Представлено ітеративний алгоритм, який виконує узагальнення, починаючи з найбільш специфічного рівня, і прагне досягти мінімальної k-анонімізації (мінімальної втрати інформації при задоволенні вимоги k-анонімності) для збереження класифікаційних властивостей.

Спеціалізація "Зверху Вниз" - алгоритм ініціює процес із найбільш узагальненого стану таблиці та послідовно спеціалізує її на основі певної метрики пошуку, забезпечуючи мінімальну k-анонімізацію.

k-Optimize [11] - метод, що пропонує оптимальну анонімність шляхом використання узагальнення піддерева та придушення записів із застосуванням технік обрізання (pruning) для ефективного пошуку.

2.1.2. Основні концепції та принцип роботи алгоритму kACTUS

kACTUS - алгоритм k-анонімізації, який фокусується на захисті конфіденційності в задачах класифікації з використанням механізму багатовимірного придушення.

kACTUS – це алгоритм анонімізації, розроблений для забезпечення k-анонімності наборів даних, зокрема, орієнтований на захист конфіденційності в задачах класифікації (classification tasks). Він досягає цієї мети шляхом комбінування кластеризації записів із застосуванням багатовимірного придушення (Multi-Dimensional Suppression).

Основна ідея полягає в тому, що для набору даних, який буде використовуватися для навчання класифікатора (де є атрибути-предиктори, які можуть бути квазі-ідентифікаторами, QID, та цільовий атрибут), необхідно мінімізувати втрату інформації, забезпечуючи, щоб кожен запис належав до еквівалентного класу розміром не менше k.

Основні концепції та принцип роботи

- k-Анонімність гарантує, що для кожного запису в анонімізованій таблиці існує щонайменше $k-1$ інших записів, які мають ідентичні значення квазі-ідентифікаторів (QID).

- кластеризація (Grouping). kACTUS групує записи в таблиці, щоб сформувати ці еквівалентні класи. Кожен клас (кластер) повинен мати розмір $\geq k$.

На відміну від простого одновимірного узагальнення, kACTUS застосовує придушення на рівні кластера та багатовимірних комбінацій атрибутів. Це означає, що замість заміни значень на узагальнені діапазони, як у традиційному узагальненні, він може придушити (замінити на '*') певні атрибути в межах кластера, щоб досягти k-анонімності. Придушення може застосовуватися до всієї групи, якщо жодна форма узагальнення не може зберегти k-анонімність або якщо кластер містить занадто багато унікальних чутливих значень.

kACTUS працює ітеративно, слідуючи приблизно таким крокам:

- початкова кластеризація. Набір даних спочатку розбивається на початкові кластери розміром не менше k. Це зазвичай робиться на основі метрики подібності між записами (наприклад, використовуючи відстань між значеннями QID).

- оцінка конфіденційності. Для кожного кластера перевіряється умова k-анонімності. Оскільки kACTUS орієнтований на класифікацію, він також може враховувати додаткові вимоги приватності, такі як ℓ-різноманітність для захисту чутливих атрибутів (SA), хоча його основна мета — k-анонімність.

- мінімальне придушення. Для кластерів, які не задовольняють умову k-анонімності або мають проблеми з різноманітністю чутливих атрибутів (якщо враховується ℓ-різноманітність), застосовується мінімальна кількість придушень QID-атрибутів у цьому кластері. Мета — знайти оптимальний набір атрибутів для придушення, щоб клас став k-анонімним, при цьому максимізуючи збереження інформації (корисності).

- визначення придушених областей. На відміну від звичайного узагальнення, яке замінює значення на діапазони, kACTUS визначає, які атрибути в межах кластера повинні бути замінені на символ придушення ("*"), щоб зробити всі записи в цьому кластері нерозрізненними за QID-атрибутами.

- ітеративна оптимізація. Процес кластеризації та придушення повторюється, щоб гарантувати, що кожен запис набору даних належить до принаймні одного k-анонімного еквівалентного класу, мінімізуючи загальну втрату інформації.

Основна перевага kACTUS полягає в його здатності краще зберігати корисність даних для завдань класифікації порівняно з традиційними методами узагальнення. Кластеризація допомагає групувати подібні записи. Застосовуючи придушення лише до необхідних атрибутів у межах кластера, kACTUS часто досягає кращого балансу між приватністю та точністю моделі класифікації, оскільки менше інформації втрачається через надмірне

узагальнення. Придушення є локальним до кластера, що дозволяє більш точно контролювати втрату інформації порівняно з глобальним узагальненням.

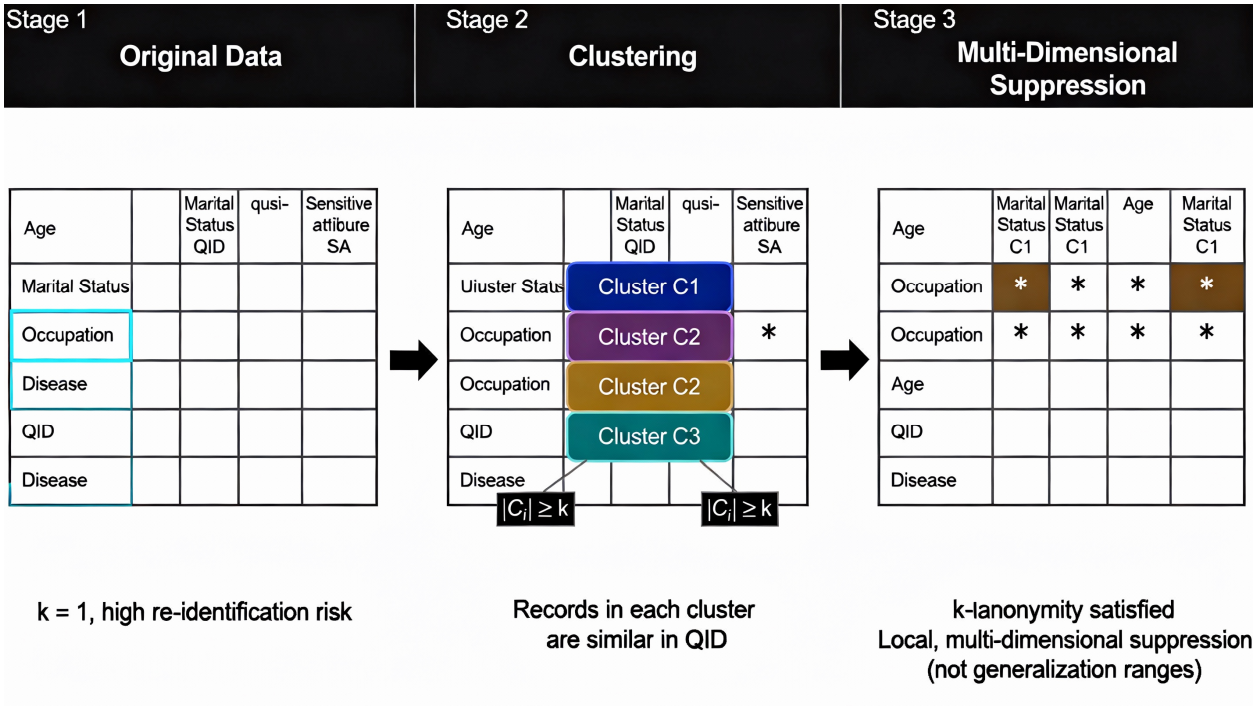

Рис. 2.1. Ілюстрація роботи алгоритму kACTUS

2.1.3. Алгоритми, базовані на мікроагрегації

Ця категорія алгоритмів реалізує анонімізацію шляхом кластеризації записів та заміни значень у кожному кластері їхнім агрегованим представленням (наприклад, середнім значенням).

Метод максимальної відстані до середнього вектора (MDAV - Maximum Distance to Average Vector) - один із найбільш репрезентативних методів, що використовує критерій максимальної відстані для формування кластерів з метою мікроагрегації.

Багатовимірна мікроагрегація фіксованого розміру - техніка, яка формує кластери строго фіксованого розміру у багатовимірному просторі.

Розбиття мінімального остовного дерева (Minimum Spanning Tree Partitioning) - метод, що використовує мінімальне остовне дерево для ефективного розбиття даних на кластери, мінімізуючи втрату корисності.

MDAV-Універсальний та MDAV змінного розміру [24] - Модифікації оригінального MDAV, які адаптують його для універсального застосування або дозволяють використання кластерів змінного розміру.

Більш детально розглянемо метод максимальної відстані до середнього вектора (MDAV - Maximum Distance to Average Vector).

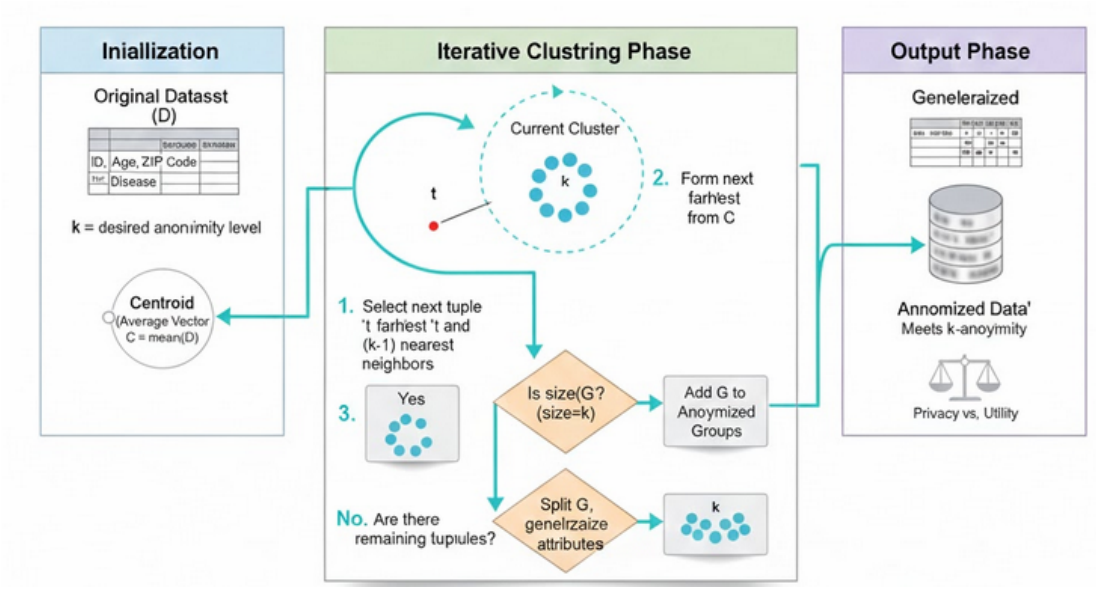

Рис. 2.2. Графічна інтерпретація роботи алгоритму MDAV

Рисунок 2.2 ілюструє роботу алгоритму анонімізації, який використовує підхід ітеративної кластеризації для досягнення бажаного рівня k-анонімності. Цей алгоритм є варіацією методів, орієнтованих на кластеризацію та узагальнення, а саме MDAV, де записи групуються для подальшої анонімізації.

Опис роботи алгоритму розділено на три основні фази: ініціалізація, фаза ітеративної кластеризації та фаза виводу.

1. Фаза ініціалізації

На цьому етапі визначаються початкові параметри та обчислюються ключові показники:

- оригінальний набір даних (d): вхідна таблиця мікро даних, яка містить ідентифікатори (ID), квазі-ідентифікатори (QID, наприклад, Age, ZIP Code) та чутливі атрибути (SA, наприклад, Disease).

- бажаний рівень анонімності (k): визначається мінімальна кількість записів, які повинні бути нерозрізненними за QID у кожному анонімізованому класі.

- центроїд (c): обчислюється як середній вектор (Mean Vector) усього набору даних D. Цей центроїд використовується як опорна точка для початку процесу кластеризації.

2. Фаза ітеративної кластеризації

Цей етап є основним і повторюється, доки всі записи не будуть згруповані та анонімізовані. На кожній ітерації формується новий кластер:

- вибір початкового запису та кластера. Спочатку обирається кортеж t, який є найвіддаленішим (farthest) від поточного центроїда C. Навколо цього запису t обираються (k−1) найближчих сусідів (nearest neighbors). Це формує потенційний кластер (групу) G початковим розміром k.

- формування наступної групи. Визначається запис, який є найвіддаленішим від щойно сформованого кластера $C_{current}$ (або t) для ініціалізації формування наступного кластера в подальшій ітерації.

- перевірка та обробка кластера. Система перевіряє, чи відповідає розмір сформованої групи G мінімальному рівню анонімності k (Is size(G) ≥k?). Якщо розмір групи ≥k, група G додається до списку анонімізованих груп, і процес переходить до наступної ітерації. Якщо розмір групи <k, перевіряється, чи залишилися ще необроблені кортежі (tuples) у наборі даних. Якщо залишилися кортежі, відбувається розбиття групи (G) (Split G). Це може включати узагальнення атрибутів та переформування кластерів до задоволення умови k (або повторне включення до набору необроблених даних). Якщо не залишилося кортежів, процес завершується, і дані переходять до фази виводу.

3. Фаза виводу

Цей етап фіналізує анонімізацію. Згруповані кластери G піддаються узагальненню (або іншим формам санітарної обробки), де значення QID замінюються на менш специфічні значення (наприклад, діапазони) для всіх

записів у кластері, щоб вони стали ідентичними. Отриманий набір даних задовольняє умові k-анонімності. На цьому етапі відбувається оцінка компромісу між досягнутим рівнем конфіденційності (Privacy) та збереженою корисністю (Utility) даних.

2.2. Формальні моделі захисту конфіденційності

Ключовим припущенням у сфері публікації даних із захистом конфіденційності (PPDP) є те, що обмін анонімізованими даними відбувається у ворожому середовищі, де серед одержувачів можуть бути присутні зловмисники. Отже, для забезпечення формальних гарантій захисту анонімізованих даних у літературі розроблено низку моделей конфіденційності, які враховують різні сценарії атак та рівні фонових знань зловмисника.

Алгоритми PPDP застосовуються разом із моделлю конфіденційності для надання формальних гарантій захисту. Оскільки кожна окрема модель може бути вразливою до специфічних атак, поширеною практикою є комбінування цих моделей для посилення захисту.

Репрезентативними моделями є:

- k-анонімність;
- ℓ-різноманітність;
- t-близькість;
- диференціальна конфіденційність (ε-конфіденційність)/

Далі наведено детальний огляд цих моделей.

2.2.1. Модель k-анонімність

k-анонімність [16, 17] є фундаментальною моделлю, на основі якої було розроблено більшість наступних розширень для анонімізації мікроданих. Мета - запобігання атакам зв'язування записів, при яких

зловмисник, маючи фонові знання про квазі-ідентифікатори (QID) жертви, може унікально ідентифікувати її запис у опублікованому наборі даних.

Модель вимагає модифікації QID-атрибутів (переважно шляхом узагальнення та придушення) таким чином, щоб створити класи еквівалентності (Equivalence Classes, EQ). Кожен запис у опублікованій таблиці повинен бути нерозрізненним від принаймні k−1 інших записів у межах свого EQ.

Наприклад, таблиця 1.2 є 3-анонімною версією таблиці 1.1, де кожен кортеж має щонайменше два інші кортежі з ідентичними значеннями QID.

Обмеження:

- проблема дублікатів: k-анонімність припускає, що кожен запис відповідає окремій особі. Якщо в наборі даних присутні дублікати записів, фактична кількість власників записів може бути меншою за k. Це вирішується розширенням (x,y)-анонімність, яке гарантує, що кожна група x відповідає щонайменше k окремим особам.

- атака зв'язування атрибутів: якщо всі записи в EQ мають подібні значення чутливого атрибута (SA), зловмисник може вивести SA жертви без точної ре-ідентифікації її запису. Це стало поштовхом до розробки подальших моделей.

2.2.2. Модель ℓ-різноманітність

Модель ℓ-різноманітність [27] була запроваджена для протидії атаці зв'язування атрибутів. Мета - гарантувати, що в кожному класі еквівалентності (EQ) є достатня різноманітність чутливих значень, щоб запобігти виведенню SA.

Модель вимагає, щоб кожен EQ містив принаймні ℓ "добре представлених" чутливих значень. Існують різні варіації принципу ℓ-різноманітності, включаючи різноманітність різних ℓ (distinct ℓ-diversity) (найпростіша, вимагає ℓ різних значень SA), ентропійну ℓ-різноманітність та рекурсивну ℓ-різноманітність.

Обмеження:

- навіть якщо значення SA є різними в EQ, вони можуть бути семантично подібними. Це все ще дозволяє зловмиснику робити висновки про категорію чутливої інформації.

- у випадках, коли загальний розподіл SA є сильно перекошеним, ℓ-різноманітність може не запобігти атакам зв'язування атрибутів, оскільки зловмисник може вивести SA з високою ймовірністю.

2.2.3. Модель t-близькість

Модель t-близькість була розроблена для усунення проблем атак перекосу та атак подібності, притаманних ℓ-різноманітності. Мета - забезпечити, щоб розподіл чутливого атрибута в кожному EQ був близьким до його розподілу в загальній таблиці (вихідному наборі даних).

Таблиця задовольняє t-близькість, якщо відстань (зазвичай вимірюється через метрики, такі як відстань Землероба – Earth Mover's Distance) між розподілом значень SA в EQ та розподілом SA у всій таблиці не перевищує порогового значення t.

Обмеження:

- Забезпечення відповідності даних цьому критерію може значно погіршити корисність даних.

- Модель не має гнучкості для визначення різних рівнів захисту для різних чутливих значень.

2.2.4. Диференціальна конфіденційність

Диференціальна конфіденційність надає найсуворіші гарантії захисту, оскільки вона не робить жодних припущень щодо фонових знань зловмисника. Мета - гарантувати, що видалення або додавання одного запису в базі даних несуттєво впливає на результат будь-якого аналізу. Це гарантує, що анонімізований вихід нечутливий (до параметра ε) до модифікацій вхідної бази даних.

Для двох баз даних, що відрізняються лише одним записом, алгоритм, який задовольняє диференціальну конфіденційність, повинен забезпечувати рандомізовані виходи, які є майже ідентично розподіленими на обох наборах даних. Початково модель була запропонована для інтерактивного сценарію, де видавець додає шум (наприклад, за допомогою механізму Лапласа) до відповідей на запити (наприклад, до статистичної бази даних), замість публікації самого набору даних.

Обмеження:

- застосовність моделі все ще обмежена у сценаріях, які вимагають прямої роботи з даними, таких як PPDP. Вона більш підходить для відповідей на запити та обчислення статистики, де дані не публікуються.

- хоча модель є надійною, вона може погіршити корисність анонімізованих даних, щоб зберегти сувору гарантію конфіденційності.

Серед обговорених моделей k-анонімність залишається фундаментальним принципом конфіденційності через її концептуальну простоту та практичну прийнятність. На відміну від більш обмежувальних моделей (наприклад, ентропійна ℓ-різноманітність) або важкодосяжних для деяких сценаріїв (наприклад, t-близькість), k-анонімність дозволяє загальну публікацію даних з розумною корисністю. Це робить її широко прийнятою в реальних системах та доменах, таких як охорона здоров'я, Data Mining, тощо.

Незважаючи на вразливість до деяких атак, k-анонімність продовжує становити основу для нових методів анонімізації та вдосконалених моделей конфіденційності в різних контекстах (наприклад, соціальні мережі, сервіси на основі місцезнаходження).

2.3. Метрики оцінки корисності анонімізованих даних

Вигоди від використання анонімізованих даних критично залежать від їхньої якості, яка систематично оцінюється шляхом вимірювання корисності, що залишилася після процесу анонімізації (або, іншими словами, втрати

інформації, що відбулася). Метрики корисності класифікуються на незалежні від завдання (task-independent) та залежні від завдання (task-dependent).

2.3.1. Метрики, незалежні від завдання (загального призначення)

Ці метрики оцінюють якість анонімізованих даних (T*) на основі рівня спотворення (синтаксичного або семантичного), якому піддалися оригінальні дані (T). Вони застосовуються, коли кінцеве використання опублікованих даних невідоме. Вони переважно складаються із загальних мір та мір, заснованих на відстані.

Узагальнена втрата інформації (GenILoss) - це метрика яка кількісно визначає штраф, спричинений узагальненням конкретного атрибута, шляхом обчислення частки значень домену, які були узагальнені.

Вона оцінює, наскільки менш точним є узагальнене значення порівняно з оригінальним.

Принцип роботи наступний. Комірки даних, що представляють більший діапазон значень (наприклад, "не одружений" як інтервал [неодружений – вдовець]), вважаються менш точними, ніж ті, що представляють менший діапазон.

$$\text{GenILoss}(T^*) = \frac{1}{|T| \cdot n} \times \sum_{i=1}^{n} \sum_{j=1}^{|T|} \frac{U_{ij} - L_{ij}}{U_i - L_i}$$

де:

$|T|$ — кількість записів, n — кількість атрибутів.

$[L_i, U_i]$ — нижня та верхня межі домену атрибута i.

$[L_{ij}, U_{ij}]$ — нижня та верхня межі узагальненого інтервалу для комірки (i,j).

Діапазон: 0 (немає узагальнення) до 1 (максимальне узагальнення).

Для розрахунку штрафу категоріальні значення відображаються на числові значення на основі їхньої ієрархії узагальнення (VGH).

Метрика розрізнюваності (Distinguishability Metric, DM) – метрика що вимірює, наскільки запис є невідмінним від інших, призначаючи штраф, пропорційний розміру класу еквівалентності (EQ), до якого він належить.

Принцип: більші EQ вказують на більшу втрату інформації; отже, бажаними є нижчі значення DM. Для k-анонімізованого EQ розмір штрафу дорівнює ∣EQ∣2. Якщо запис придушений, штраф дорівнює ∣T∣.

$$\mathrm{DM}(T^*) = \sum_{\forall EQs,\ \text{s.t. } |EQ| \geq k} |EQ|^2 + \sum_{\forall \text{suppressed } EQs,\ \text{s.t. } |EQ| < k} |T| \cdot |EQ|$$

Метрика середнього розміру класу еквівалентності (CAVG) - це метрика яка оцінює, наскільки процес створення EQ наближається до ідеального випадку, де кожен запис узагальнюється в EQ, що містить рівно k записів. Мета — мінімізувати штраф. Значення 1 вказує на ідеальну анонімізацію, де ∣EQ∣=k.

$$C_{AVG}(T^*) = \frac{|T|}{|\mathrm{EQs}| \cdot k}$$

де ∣EQs∣ — загальна кількість створених EQ.

Семантична втрата інформації (SemILoss) - метрика що вимірює, наскільки семантично анонімізовані значення відрізняються від оригінальних у середньому. Застосовується лише до категоріальних атрибутів. ип: Використовує метрику семантичної відстані (sdist) для кількісної оцінки семантичних змін.

$$\mathrm{SemILoss}(T^*) = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} \mathrm{sdist}(x_{ij}, x_{ij}^*)}{n \cdot m}$$

де x_{ij} — оригінальне значення, x_{ij}^* — анонімізоване значення.

Семантична сума квадратів помилок (SSE) визначається як сума квадратів відстаней між кожним елементом кластера та їхнім відповідним центроїдом. Нижче значення SSE вказує на вищу внутрішньогрупову однорідність і меншу втрату інформації внаслідок анонімізації.

$$\mathrm{SSE}(T^*) = \sum_{i=1}^{n} \left(\frac{\sum_{j=1}^{m} \mathrm{sdist}(x_{ij}, x_{ij}^*)}{m} \right)^2$$

Як і SemILoss, SSE застосовується лише до категоріальних атрибутів і залежить від метрики sdist.

2.3.2. Метрики, залежні від завдання (спеціального призначення)

Ці метрики оцінюють якість анонімізованих даних на основі точності (accuracy), яку вони забезпечують для конкретного сценарію застосування, наприклад, кластеризація, відповіді на агреговані запити, видобування асоціативних правил або навчання класифікаторів.

Узгодженість кластеризації даних (Data Clustering Consistency) оцінює якість анонімізованих даних шляхом порівняння подібності між кластерами, отриманими з оригінальних даних c(T), та кластерами, отриманими з анонімізованих даних c(T*).

Процедура наступна:

1. Застосувати метод кластеризації c до оригінального набору T для отримання розбиття A=c(T).

2. Застосувати той самий метод c до анонімізованого набору T* для отримання розбиття B=c(T*).

3. Порівняти подібність між розбиттями A та B.

Чим більше c(T*) подібний до c(T), тим менша втрата інформації, що дозволяє визначити оптимальну конфігурацію анонімізації.

Метрики парної узгодженості (Pairwise Consistency Metrics) оцінюють, чи кожна пара записів (точок даних) кластеризується разом або розділяється однаково в розбиттях A та B. Вони базуються на матриці невідповідностей.

Для цих метрик вищі значення кращі (від 0 до 1).

Індекс Ренда (RAB) - представляє співвідношення узгодженості як між збігами, так і між незбігами.

$$\mathcal{R}_{AB} = \frac{a+d}{a+b+c+d}$$

Коефіцієнт Воллеса (W) представляє умовну ймовірність.

$$\mathcal{W}_I(A,B) = \frac{a}{a+b} \quad \text{та} \quad \mathcal{W}_{II}(A,B) = \frac{a}{a+c}$$

WI — ймовірність того, що пара, що згрупована в A, також згрупована в B. WII — ймовірність того, що пара, що згрупована в B, також згрупована в A.

Метрики на основі ентропії використовують поняття теорії інформації для вимірювання кількості інформації, яку ділять розбиття кластерів.

Нормалізована взаємна інформація (NMI):

$$NMI_{AB} = \frac{2 \cdot I(A,B)}{H(A)+H(B)}$$

Взаємна інформація (I(A,B)) вимірює узгодженість між двома розбиттями.

$$I(A,B) = \sum_{i=1}^{R}\sum_{j=1}^{Q} \frac{n_{ij}}{N} \log \frac{n_{ij}/N}{n_i n_j / N^2}$$

де R і Q — кількість кластерів у A і B, n_{ij} — кількість спільних записів між кластерами $C_i \in A$ і $C_j \in B$.

Ентропія H(A) обчислюється, використовуючи частотні підрахунки як наближення ймовірностей.

$$H(A) = -\sum_{i=1}^{R} \frac{n_i}{N} \log \frac{n_i}{N}$$

де n_i — кількість записів у кластері $Ci \in A$.

Діапазон NMI: Від 0 до 1 і більші значення NMI вказують на більшу подібність між розбиттями.

2.4. Огляд програмних засобів та інструментів для анонімізації даних із захистом конфіденційності

Значна частина наукових досліджень спрямована на розробку програмних інструментів та прототипів, які надають єдиний фреймворк для оцінки та порівняння алгоритмів анонімізації. Нижче представлено огляд відомих некомерційних та дослідницьких інструментів.

TIAMAT (Tool for Interactive Analysis of Microdata Anonymization Techniques) є візуальним інструментом, призначеним для інтерактивного аналізу методів анонімізації мікроданих. Допомагає користувачам оцінювати переваги (точність) та витрати (накладні витрати) існуючих алгоритмів k-анонімізації. Підтримує редагування ієрархій узагальнення значень (VGHs), що використовуються для QID-атрибутів.

Використовує загальну метрику впевненості та метрику класифікації. Вихідний код та сам інструмент не є публічно доступними.

CAT (Cornell Anonymization Toolkit) — це дослідницький прототип, створений для демонстрації нових підходів до анонімізації. Реалізує лише алгоритм Incognito з моделями ℓ-різноманітності та t-близькості. Не призначений для великомасштабних реальних застосувань, оскільки всі дані зберігаються в основній пам'яті. Як додаткова функціональність включає аналізатор ризиків для оцінки ризику розголошення анонімізованих даних на основі фонових знань зловмисника про визначений користувачем набір QID.

UTD Anonymization Toolbox – це інструмент, орієнтований на дослідників. Не має графічного інтерфейсу користувача (GUI); налаштування параметрів здійснюється вручну через XML-файл. Не реалізує інформаційні метрики для оцінки якості отриманих наборів даних. Його вихідний код є публічно доступним, що дозволяє дослідникам розширювати функціональність або розробляти нові механізми захисту конфіденційності.

SECRETA - це система для оцінки та порівняння алгоритмів анонімізації реляційних та транзакційних даних. Надає графічний інтерфейс користувача (GUI) для налаштування параметрів алгоритмів, візуалізації та зберігання результатів тестування. Підтримує дев'ять алгоритмів, включаючи Incognito, Cluster та Top-down для реляційних даних, а також COAT та PCTA для транзакційних даних. Інструмент та його вихідний код не є публічно доступними.

ARX є зрілим, публічно доступним інструментом анонімізації даних. Інтерфейс підтримує чотири різні графічні перспективи для налаштування процесу анонімізації, включаючи завантаження даних, налаштування параметрів конфіденційності, дослідження простору рішень, оцінку корисності та аналіз ризиків.

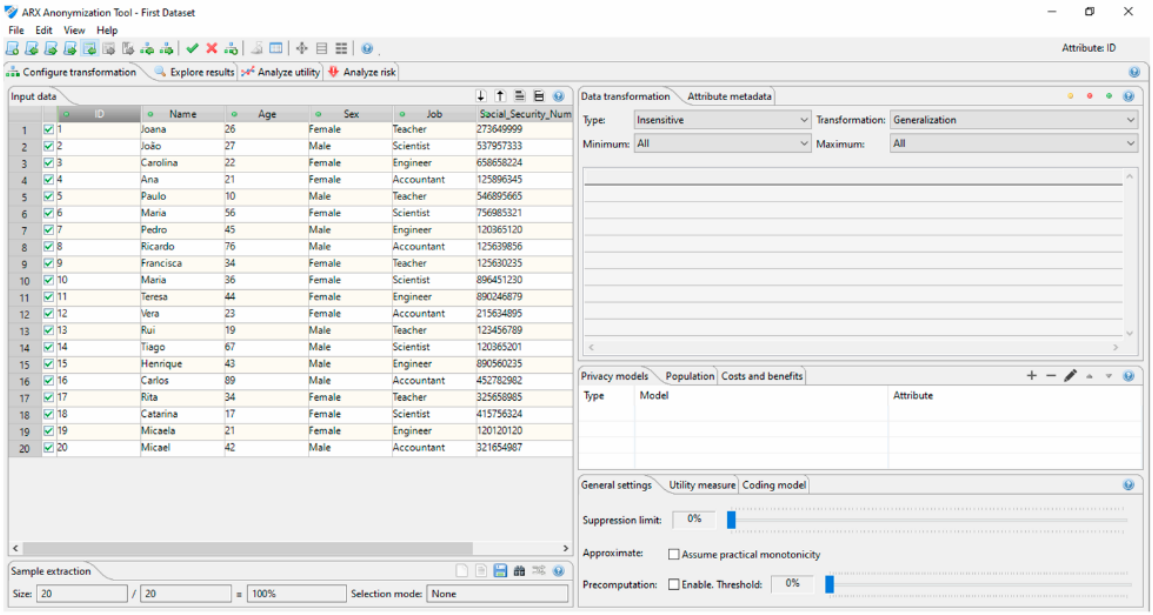

Рис. 2.3. Інтерфейс ARX

Підтримує багато варіантів алгоритму Flash (глобально оптимальний алгоритм). Оскільки вихідний код є публічно доступним, ARX може бути використаний для реалізації нових методів. Підтримує k-анонімність, всі варіанти ℓ-різноманітності, два варіанти t-близькості та δ-наявність.

У галузі статистичного контролю розголошення (SDC), яка тісно пов'язана з PPDP, статистичними агентствами ЄС широко використовуються два відкритих інструменти:

- μ-Argus - програмне забезпечення з відкритим кодом, що реалізує різні методи SDC для санітарної обробки мікроданих (наприклад, мікроагрегація, PRAM, обмін рангами, синтетичні дані). Включає модуль для аналізу ризиків.

- sdcMicro - пакет з відкритим кодом для статистичного програмного забезпечення R. Включає всі методи, реалізовані в μ-Argus, а також додаткові нові.

Обидва інструменти SDC вимагають від користувача глибоких знань про реалізовані механізми SDC для їх ефективного застосування. Хоча всі ці інструменти є цінними та сприяють прийняттю обґрунтованих рішень при публікації даних, загальною проблемою залишається високий рівень експертизи, необхідний користувачам для ефективного застосування алгоритмів анонімізації та коректного налаштування їх параметрів.

Висновки до розділу

Другий розділ продемонстрував, що сучасні алгоритми анонімізації значно відрізняються за підходами, складністю та якістю забезпечення конфіденційності. Детальний огляд алгоритмів показав, що різні методи створені для різних типів даних та різних рівнів ризику повторної ідентифікації. Алгоритм kACTUS виявився прикладом оптимізованого підходу до досягнення k-анонімності за рахунок гнучкого вибору схем генералізації. Алгоритми мікроагрегації продемонстрували високу

ефективність при роботі з числовими атрибутами, забезпечуючи мінімальні втрати інформації. У розділі докладно розглянуто формальні моделі конфіденційності, які задали методологічну основу сучасних систем анонімізації. Моделі k-анонімності, ℓ-різноманітності та t-близькості описано як послідовне ускладнення підходів до захисту даних, що усувають обмеження попередніх моделей. Особливе місце займає концепція диференціальної конфіденційності, яка гарантує математично підтверджений рівень захисту незалежно від зовнішніх даних. Проаналізовані метрики корисності показали важливість кількісної оцінки втрат інформації при застосуванні методів анонімізації.

РОЗДІЛ 3. ІМПЛЕМЕНТАЦІЯ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ ПРОЦЕСІВ ЕФЕКТИВНОЇ АНОНІМІЗАЦІЇ ДАНИХ

3.1. Анонімізація даних як імператив захисту персональної інформації

Обсяг даних, доступних у цифровому середовищі, демонструє експоненційне зростання в останні роки. Персональні дані є критично важливим ресурсом, що використовується державними установами, комерційними організаціями та приватними суб'єктами у широкому спектрі застосувань, включаючи маркетингові стратегії, медичні та наукові дослідження, а також прогнозування майбутніх тенденцій.

Проте, ключовою проблемою є потенційне включення до цих наборів даних конфіденційної інформації, що може призвести до ідентифікації особи та її нецільового використання. Такі атрибути, як адреса, вік, номер банківського рахунку та інша чутлива інформація, вимагають належного захисту від несанкціонованого розкриття. Суспільний консенсус підкреслює неприпустимість публічного доступу до особистих даних без явної згоди, з огляду на ризики зловживань.

Для забезпечення конфіденційності суб'єктів даних їхня особиста інформація повинна бути прихована або модифікована перед публікацією чи обробкою в мережі. Ця дія є превентивним заходом проти таких загроз, як крадіжка особистих даних та фінансове вимагання.

Анонімізація даних є необхідною процедурою для організацій, які збирають та зберігають персональні дані для прямої діяльності або для публікації з метою непрямого використання (дослідження, маркетинг, охорона здоров'я). У випадках, коли дані містять конфіденційну інформацію, їх компрометація створює значні загрози конфіденційності. Отже, анонімізація забезпечує модифікацію вихідних даних з метою приховування

або зміни конфіденційної інформації, що запобігає її розкриттю, водночас зберігаючи можливість використання даних для аналітичних цілей.

Кінцевим результатом цього процесу є менш точний набір даних, у якому ідентифікація особи за анонімізованими даними стає неможливою. Одним із критичних аспектів анонімізації є втрата корисності даних. Необхідно ретельно контролювати кількість застосовуваних методів та алгоритмів, а також частоту їх застосування до набору даних. Надмірне застосування методів може призвести до неприйнятної втрати корисності, роблячи анонімізований набір даних непридатним для цільового використання.

Анонімізація визначається як процес шифрування або видалення даних, що дозволяють встановити особу, з наборів даних, щоб особу більше не можна було ідентифікувати прямо чи опосередковано. Анонімізовані дані перестають вважатися персональними даними, оскільки їхня повторна ідентифікація неможлива, і, відповідно, GDPR до них більше не застосовується. Псевдонімізація визначається як обробка персональних даних у такий спосіб, що персональні дані більше не можуть бути віднесені до конкретного суб'єкта даних без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо і підлягає технічним та організаційним заходам для забезпечення того, щоб персональні дані не були віднесені до ідентифікованої або такої, яку можна ідентифікувати, особи.

У межах даної роботи підтверджено, що анонімізація даних є критично важливою технікою для захисту персональних даних від зловмисників. Тому в цьому розділі здійснено оцінку інструментів анонімізаціїз відкритим вихідним кодом, зосередившись на найбільш популярних рішеннях: ARX Data Anonymization та Amnesia. Оцінка інструментів проводилася за допомогою методології OSSpal та на публічному реальному наборі даних.

Методологія OSSpal призначена для оцінки програмного забезпечення з відкритим вихідним кодом. Вона використовує набір категорій, включаючи

функціональність, операційні характеристики, підтримку, документацію, технологічні атрибути, спільноту та процес розробки.

3.2. Архітектура та функціональні можливості інструментів забезпечення анонімізації даних

3.2.1. Інструмент ARX Data Anonymization

ARX Data Anonymization є вільно доступним інструментом з відкритим вихідним кодом, який активно використовується в комерційних платформах аналізу великих даних, дослідницьких проєктах, для обміну даними клінічних випробувань та в освітніх цілях, забезпечуючи анонімізацію чутливих персональних даних.

Інструмент ARX реалізує широкий спектр алгоритмів захисту конфіденційності, що охоплюють як фундаментальні, так і передові моделі:

- моделі анонімності - k-анонімність та k-карта (k-Map).

- моделі різноманітності та близькості - ℓ-різноманітність (ℓ-Diversity) та t-близькість (t-Closeness).

- розширені моделі захисту - δ-розкриття приватності, β-подібність та γ-присутність.

- посилена конфіденційність - (ε,δ) - диференційна приватність.

Крім того, ARX підтримує різноманітні техніки перетворення даних:

- схеми глобального та локального перетворення, випадкова вибірка.

- узагальнення, мікроагрегація, кодування верхнього та нижнього рівнів, категоризація.

- придушення записів, атрибутів та комірок.

Інтерфейс інструменту ARX Data Anonymization Tool представлено на рисунку 2.3. Процес анонімізації вимагає від користувача виконання низки послідовних кроків:

1. Створення нового проєкту та завантаження цільового набору даних. Інструмент не накладає обмежень на розмір набору даних.

2. Призначення типу для кожного атрибута (стовпця). Підтримуються такі типи: неконфіденційні, конфіденційні, квазіідентифікуючі та ідентифікуючі.

3. Зв'язування відповідної моделі конфіденційності (одного із зазначених вище алгоритмів) з кожним конфіденційним атрибутом.

4. Створення або завантаження ієрархій узагальнення для кожного з решти атрибутів.

5. Після виконання всіх попередніх кроків запускається процес анонімізації вихідного набору даних.

Результати анонімізації відображаються у вкладці "Explore results". Інструмент представляє користувачеві різні рішення для анонімізації, кожне з яких демонструє різний рівень узагальнення для конфіденційних атрибутів. Користувач повинен обрати найбільш прийнятне рішення та застосувати його до вихідного набору даних. У вкладці "Analysis utility" відображається фінальний анонімізований набір даних разом із відповідними статистичними показниками. Анонімізований набір даних може бути завантажений у форматі CSV.

3.2.2. Інструмент Amnesia

Amnesia є інструментом з відкритим вихідним кодом, який відповідає рекомендаціям GDPR і підтримує методи псевдоанонімізації. Інструмент вирізняється високою зручністю використання та гнучкістю, що робить його доступним для широкого кола користувачів. Amnesia гарантує, що анонімізована інформація не може бути зв′язана з оригінальним набором даних, і прагне мінімізувати зниження якості інформації (втрату корисності), зберігаючи при цьому придатність даних до використання.

Подібно до ARX Data Anonymization, Amnesia інтегрує алгоритми захисту конфіденційності:

- k-анонімність (k-anonymity);

- km-анонімність (km-anonymity)/

Amnesia доступна для використання як онлайн-інструмент, так і для завантаження на робочий стіл. Для ознайомлення користувачів інструмент також надає набір навчальних даних. Інтерфейс інструменту Amnesia представлено на рисунку 3.1.

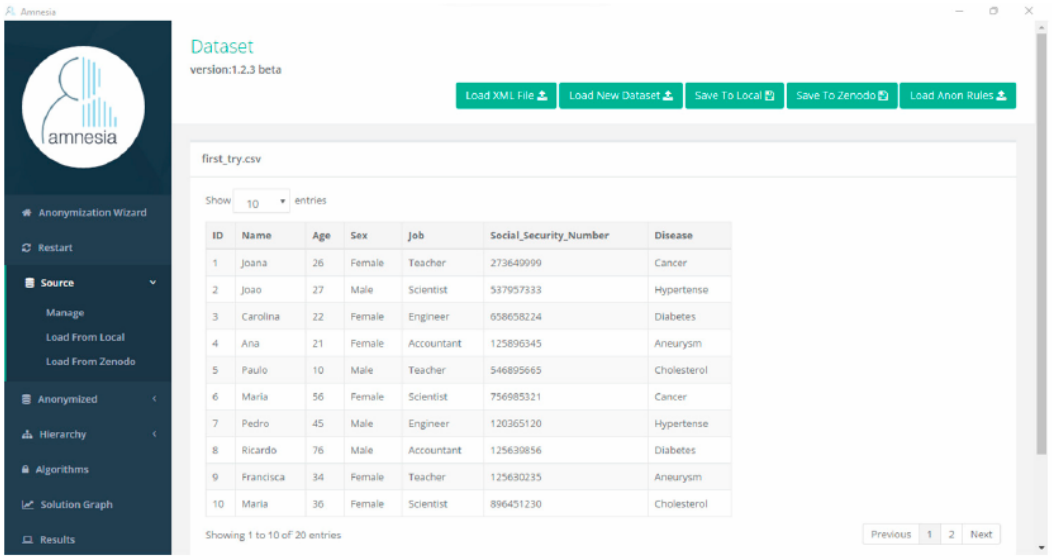

Рис. 3.1. Інтерфейс інструменту анонімізації даних Amnesia

Процес анонімізації в Amnesia складається з таких кроків:

1. Початковим кроком є завантаження набору даних. Однак, інструмент має значне обмеження розміру і підтримує набори даних обсягом лише до 4МБ.

2. Після завантаження даних користувач скеровується до створення ієрархій узагальнення. Ієрархії можуть бути створені для всіх або лише для квазіідентифікуючих атрибутів.

3. Наступний крок передбачає зв'язування ієрархій з відповідними атрибутами та вибір алгоритму анонімізації, а також визначення значення змінної k (рівня анонімності). Хоча в документації згадуються два алгоритми, інтерфейс відображає лише один — під назвою Flash. Таким чином, користувач може визначити лише значення для k при використанні єдиного доступного алгоритму.

Після налаштування параметрів інструмент генерує графік рішень (solution graph). Цей графік відображає велику кількість потенційних рішень з відмінностями у рівнях узагальнення для квазіідентифікуючих та конфіденційних атрибутів. Рішення поділяються на безпечні (safe) та небезпечні (unsafe). Небезпечні рішення — це ті, які порушують умову застосування k-анонімності для деяких записів. Хоча інструмент зазначає, що ці рішення можуть бути перетворені на безпечні шляхом придушення, спроба виконання цієї дії постійно викликає помилку.

Велика кількість рішень, представлених у графіку, ускладнює його інтерпретацію, роблячи його заплутаним для користувача. Фінальний етап передбачає вибір найбільш підходящого рішення, після чого відображається анонімізований набір даних. Інструмент дозволяє завантажити анонімізований набір даних у форматі CSV.

3.3. Методологія оцінки програмного забезпечення з відкритим кодом OSSpal

Методологія OSSpal була розроблена в рамках проєкту Business Readiness Rating (BRR), а її основна мета — об'єктивна оцінка інструментів із відкритим вихідним кодом (Open Source Software, OSS) за допомогою структурованого набору категорій, що сприяє користувачам та організаціям у виборі найбільш придатного програмного забезпечення.

Оцінка програмного забезпечення за методологією OSSpal базується на семи ключових категоріях:

1. Функціональність - оцінка відповідності програмного забезпечення вимогам користувача.

2. Операційні характеристики програмного забезпечення - оцінка надійності, безпеки, продуктивності, юзабіліті (простота використання, встановлення, конфігурації, підтримки та розгортання) та наявності коректного користувацького інтерфейсу.

3. Оцінка якості спільнотної або комерційної підтримки, а також наявність навчальних ресурсів.

4. Оцінка адекватності та якості наявної документації для ефективного використання інструменту.

5. Оцінка якості архітектури, портативності, розширюваності, відкритості, легкості інтеграції, а також якості коду, дизайну та тестування.

6. Вимірювання активності спільноти та сприйняття компонента в цій спільноті.

7. Оцінка професіоналізму на етапі розробки та організації проєкту.

Процес оцінки OSSpal для всіх категорій, окрім «Функціональності», складається з чотирьох послідовних фаз, що показано в таблиці 3.1.

Таблиця 3.1.

Фази оцінки

Фаза	**Опис**
I. Ідентифікація	Вибір компонентів програмного забезпечення та визначення критеріїв для оцінки
II. Призначення ваг	Призначення вагових коефіцієнтів (у відсотках, сумарно 100%) для критеріїв. Встановлення пріоритетного ранжування для вимірювань у межах кожної категорії.
III. Збір даних та ранжування	Збір даних та присвоєння оцінки (від 1 до 5) кожному вимірюванню, де: **1** — неприйнятно; **2** — погано; **3** — прийнятно; **4** — дуже добре; **5** — відмінно.
IV. Фінальний розрахунок	Розрахунок кінцевого балу OSSpal.

Категорія «Функціональність» оцінюється за відмінною процедурою:

1. Вибір та оцінка характеристик. Обираються характеристики для оцінки, і кожній присвоюється бал від 1 до 3 (1 — менш важлива; 2 — важлива; 3 — найбільш важлива).

2. Початкові результати стандартизуються за шкалою від 1 до 5 на основі наступних відсоткових діапазонів:

<65% : Бал = 1 (Неприйнятно)

65% – 80% : Бал = 2 (Погано)

80% – 90% : Бал = 3 (Прийнятно)

90% – 96% : Бал = 4 (Дуже добре)

96% – 100% : Бал = 5 (Відмінно)

Для призначення відсоткового вагового коефіцієнта кожній категорії необхідне розуміння її значущості. У контексті оцінки інструментів анонімізації даних були визначені наступні відсоткові ваги (таблиця 3.2):

Таблиця 3.2.

Відсоткові ваги

Категорія	Відсоток	Обґрунтування (ключові аспекти)
Функціональність	**30%**	Найвищий відсоток, оскільки критично важливо, щоб програмне забезпечення повністю відповідало потребам користувача
Операційні характеристики ПЗ	**20%**	Висока важливість. Наявність графічного інтерфейсу користувача (GUI) є обов'язковою вимогою через складність предметної області (анонімізації), а також важлива легкість експлуатації інструменту.
Атрибути технології ПЗ	**15%**	Важливість забезпечення безпомилковості та повноти програмного забезпечення (якість коду, архітектури та дизайну).
Документація	**10%**	Критично важлива для інструментів, особливо без GUI, оскільки якісна документація необхідна для досягнення очікуваних результатів.
Процес розробки	**10%**	Важливий показник професіоналізму та організації проєкту. (Також враховується вимога GDPR про ведення контролером записів про обробку даних).
Підтримка та послуги	**10%**	Для інструментів із відкритим кодом очікування високого рівня прямої підтримки від розробників зазвичай нижче.
Спільнота та адаптація	**5%**	Найнижчий відсоток. Значущість цієї категорії менша порівняно з такими факторами, як якість документації та функціональність.

Категорія «Функціональність» класифікується та оцінюється за допомогою специфічних характеристик, наведених у таблиці 3.3.

Таблиця 3.3.

Відсоткові ваги

Характеристики	Вага (1-3)	Обґрунтування
Застосування алгоритмів (Algorithm application)	3	Основна характеристика; оцінює легкість застосування алгоритму до набору даних.
Процес анонімізації (Anonymization process)	3	Основна характеристика; інструмент не повинен ускладнювати і без того складний процес анонімізації.
Кількість алгоритмів (Number of algorithms)	2	Робить інструмент більш повним та гнучким
Візуалізація анонімізованих даних (Anonymized data visualization)	1	Важлива для перевірки якості анонімізації та оцінки метрик. Складність візуалізації ускладнює інтерпретацію результатів.

Оцінка інструментів передбачає присвоєння значення від 1 до 5 для кожної з цих характеристик у категорії «Функціональність», а також для всіх інших категорій.

3.4. Оцінка інструментів анонімізації даних за методологією OSSpal

У цьому розділі представлена кількісна оцінка двох популярних інструментів із відкритим вихідним кодом для анонімізації даних — ARX Data Anonymization Tool та Amnesia — із застосуванням багатовимірної методології OSSpal.

Інструмент ARX Data Anonymization був визнаний відносно простим у використанні завдяки наявності графічного інтерфейсу користувача (GUI), що полегшує завантаження та анонімізацію наборів даних.

Ключові проблеми, виявлені під час оцінювання, включають:

- невідповідність значків довідки останній версії інструменту, що ускладнює отримання користувачами необхідних інструкцій.

- недостатня чіткість документації і складність розуміння необхідних дій у деяких модулях через недостатню чіткість документації.

Характеристики функціональності та присвоєні їм значення представлені в таблиці 3.4.

Таблиця 3.4.

Ваги і значення характеристик функціональності для ARX

Характеристики	**Вага**	**Значення (1-5)**
Кількість алгоритмів	2	2
Візуалізація анонімізованих даних	1	1
Застосування алгоритмів	3	3
Процес анонімізації	3	0
Сума ваг	9	6

Проведемо обґрунтування значень.

Кількість алгоритмів (значення 2) - інструмент має широкий вибір алгоритмів, проте він обмежує користувача у виборі бажаного алгоритму, пропонуючи лише ті, що вже пов'язані з конфіденційними атрибутами.

Візуалізація анонімізованих даних (значення 1) - результати анонімізації відображаються у таблиці поруч із вихідним набором даних, що значно спрощує порівняння обох версій.

Застосування алгоритмів (значення 3) до конфіденційних атрибутів є простим; інструмент також надає гнучкі варіанти для створення ієрархій залежно від типу атрибута.

Процес анонімізації (значення 0) може бути надмірно інформаційно насиченим та заплутаним, замість того, щоб спрощувати роботу користувача із системою.

Нормалізація сумарного балу за шкалою 1 – 5:

$$96 \times 100 \approx 66.7\%$$

Відповідно до шкали OSSpal (65% – 80%), бал для категорії Функціональність становить 215.

Загальний бал розраховується шляхом множення оцінки категорії на її відсотковий ваговий коефіцієнт.

Таблиця 3.5.

Фінальний результат оцінки ARX

Категорія	Оцінка (1-5)	Вага	Внесок (оцінка × вага)
Функціональність	2	30%	2 x 0.30 = 0.6
Операційні характеристики ПЗ	5	20%	5 x 0.20 = 1.0
Підтримка та послуги	4	10%	4 x 0.10 = 0.4
Документація	3	10%	3 x 0.10 = 0.3
Атрибути технології ПЗ	4	15%	4 x 0.15 = 0.6
Спільнота та адаптація	4	5%	4 x 0.05 = 0.2
Процес розробки	0	10%	0 x 0.10 = 0.0
Загальний Бал	3.1		

Загальний результат для ARX Data Anonymization Tool становить 3.1 з 5, що класифікується між прийнятно (3) та дуже добре (4). Високий бал (5) за операційні характеристики обумовлений чудовим GUI та легкістю встановлення/використання. Відсутність запису даних контролера призводить до нульового балу за процес розробки.

Інструмент Amnesia також не є складним у використанні. Основний недолік полягає у значних затримках під час виконання анонімізації, навіть для невеликих наборів даних.

Характеристики функціональності та присвоєні їм значення представлені в таблиці 3.6.

Таблиця 3.6.

Ваги і значення характеристик функціональності для Amnesia

Характеристики	Вага	Значення (1-5)
Кількість алгоритмів	2	0
Візуалізація анонімізованих даних	1	1
Застосування алгоритмів	3	0
Процес анонімізації	3	3
Сума ваг	9	4

Проведемо обґрунтування значень.

Кількість алгоритмів (значення 0) - інструмент пропонує обмежену кількість алгоритмів, що обмежує вибір користувача.

Візуалізація анонімізованих даних (значення 1) - графік рішень є надто великим і заплутаним, що ускладнює вибір оптимального результату. Проте, анонімізований набір даних після вибору рішення візуалізується.

Застосування алгоритмів - значення 0 надано через обмежену пропозицію алгоритмів інструментом.

Процес анонімізації (значення 3) - хоча процес може бути тривалим, він є відносно простим для виконання, і результати досягаються.

Нормалізація сумарного балу:

$$94 \times 100 \approx 44.4\%$$

Відповідно до шкали OSSpal (менше 65%), бал для категорії функціональність становить 142.

Фінальний результат оцінки Amnesia подано в таблиці 3.7.

Таблиця 3.7.

Фінальний результат оцінки Amnesia

Категорія	**Оцінка (1-5)**	**Вага**	**Внесок (оцінка × вага)**
Функціональність	1	30%	1 x 0.30 = 0.3
Операційні характеристики ПЗ	4	20%	4 x 0.20 = 0.8
Підтримка та послуги	4	10%	4 x 0.10 = 0.4
Документація	3	10%	3 x 0.10 = 0.3
Атрибути технології ПЗ	4	15%	3 x 0.15 = 0.45
Спільнота та адаптація	4	5%	4 x 0.05 = 0.2
Процес розробки	0	10%	0 x 0.10 = 0.0
Загальний Бал	2.45		

Загальний результат для Amnesia становить 2.45 з 5. Високий бал за операційні характеристики (4) отримано завдяки наявності GUI та простоті використання, незважаючи на повільність процесу анонімізації.

Порівняння результатів оцінки інструментів представлено в таблиці 3.8 та візуалізовано на діаграмі Ківіата (рис. 3.2).

Таблиця 3.8.

Порівняльні оцінки

Категорії	ARX Data Anonymization	Amnesia
Функціональність	0.6	0.3
Операційні характеристики ПЗ	1.0	0.8
Підтримка та послуги	0.4	0.4
Документація	0.3	0.3
Атрибути технології ПЗ	0.6	0.45
Спільнота та адаптація	0.2	0.2
Процес розробки	0.0	0.0
Всього	**3.1**	**2.45**

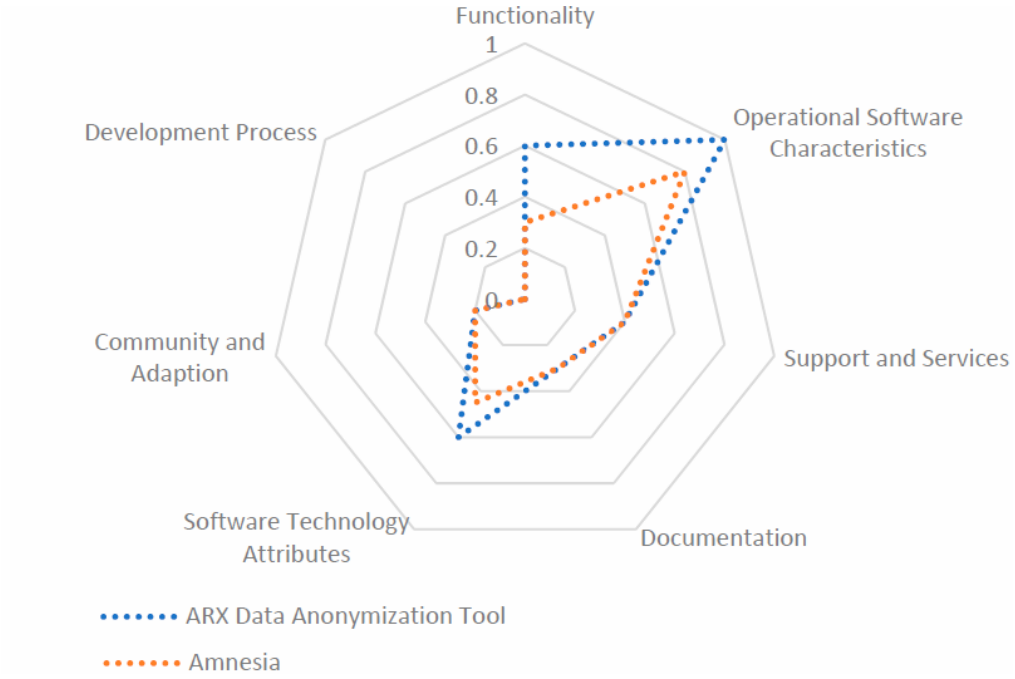

Рис. 3.2. Діаграма візуалізації результатів

Згідно з методологією OSSpal, ARX Data Anonymization Tool демонструє кращу оцінку (3.1) порівняно з Amnesia (2.45). Цей результат підтверджує, що ARX є одним із найбільш комплексних та широко використовуваних інструментів у галузі анонімізації даних.

3.5. Експериментальна оцінка інструментів анонімізації на публічному наборі даних

У цьому розділі представлена експериментальна оцінка інструментів ARX Data Anonymization Tool та Amnesia із застосуванням одного реального публічного набору даних Pfizer Vaccine Tweets Dataset. Цей набір містить актуальні твіти, пов'язані з вакцинами Pfizer та BioNTech. Набір даних має обсяг 3 488 606 байтів і містить 11 021 запис, складається з 16 атрибутів, включаючи id, username, userlocation, userdescription, дату, текст, хештеги та інше.

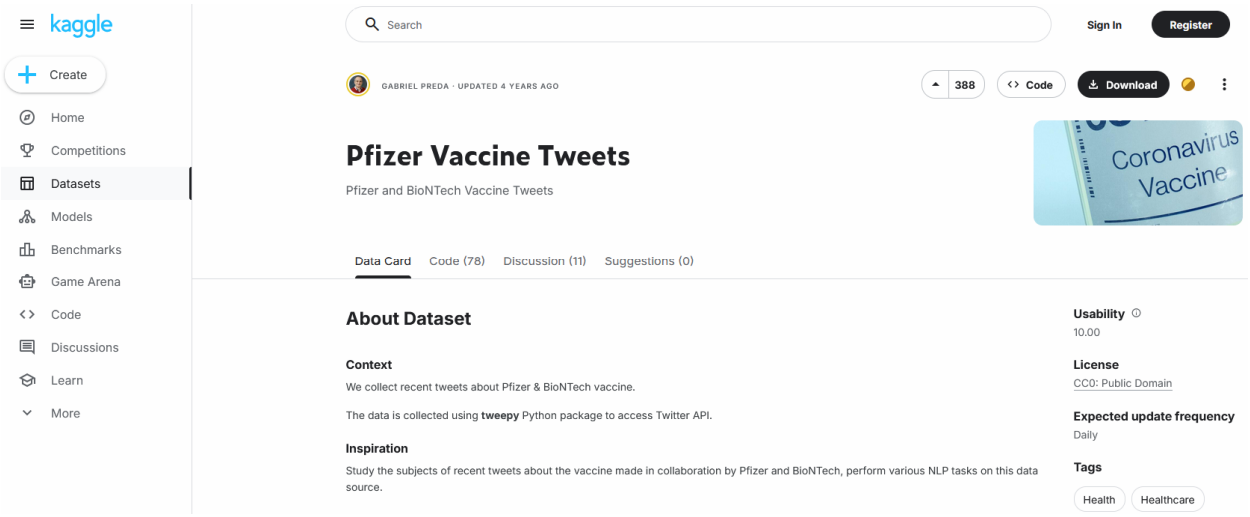

Рис. 3.3. Опис набору даних

Класифікація атрибутів, необхідна для процесу анонімізації, наведена в таблиці 3.9.

Таблиця 3.9.

Класифікація атрибутів для процесу анонімізації

Атрибут	Тип атрибута
id	Конфіденційний
username	Ідентифікатор
userlocation	Квазіідентифікатор
userdescription	Квазіідентифікатор
Решта 12 атрибутів	Неконфіденційний

3.5.1. Анонімізація набору даних за допомогою ARX Data Anonymization

У цьому розділі описується процедура впровадження та анонімізації набору даних у ARX Data Anonymization.

Конфігурація процесу наступна:

1. Файл у форматі CSV було завантажено з розділювачем — крапка з комою. Після верифікації типів даних набір було успішно імпортовано.

2. Встановлення моделі приватності - типи атрибутів були обрані згідно з таблицею 3.9. Для конфіденційного атрибута (`id`) інструмент обрав множину моделей: l-Diversity, t-Closeness, Disclosure privacy та beta-Likeness. Було обрано модель l-Diversity зі значенням 5. Це значення визначено як відповідне для збереження корисності даних, враховуючи їхній розмір (рис. 3.5).

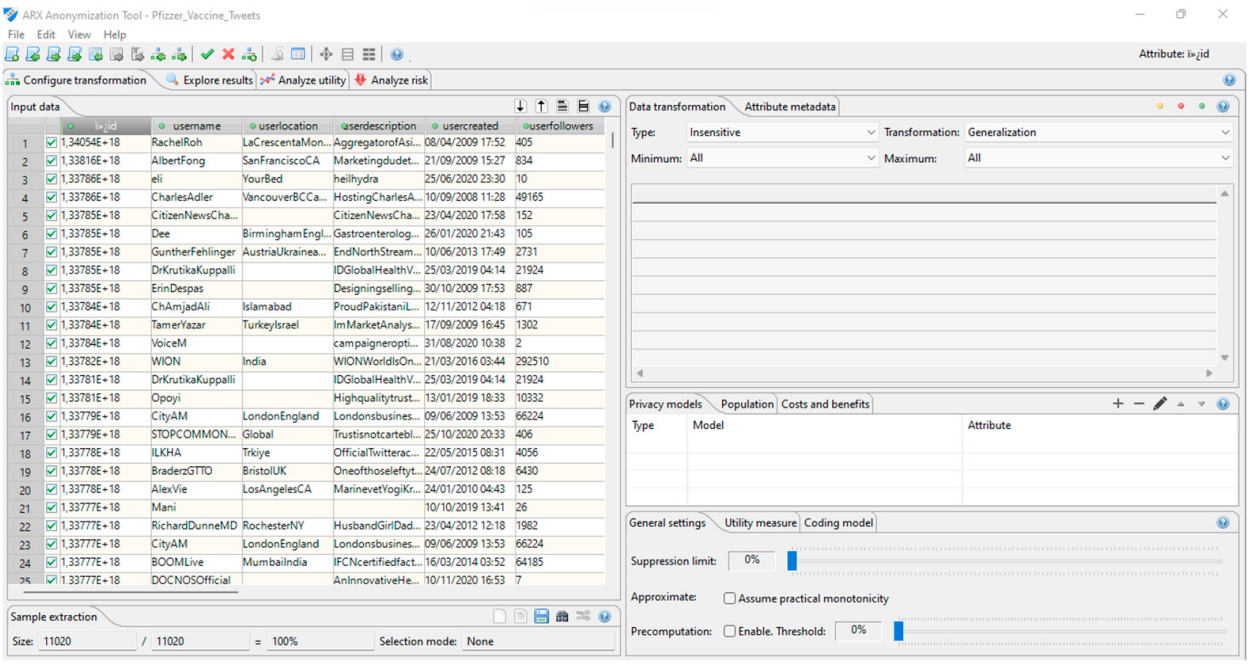

Рис. 3.4. Завантажений набір даних засобами ARX

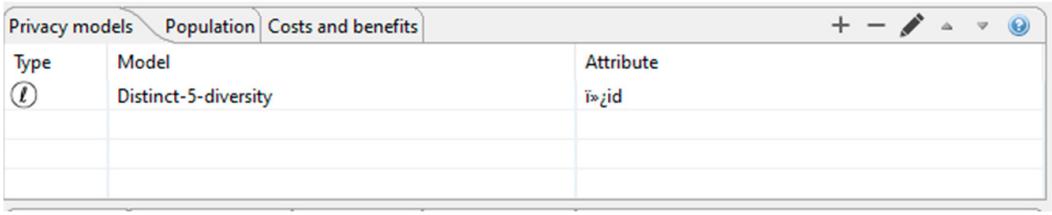

Рис. 3.5. Модель конфіденційності

3. Створення ієрархій узагальнення (VGHs). Ієрархії були створені для ідентифікуючих та квазіідентифікуючих атрибутів.

Атрибут username (ідентифікатор): обрано тип маскування із символом *. Маскування було застосовано для приховування текстової інформації. Максимальна кількість символів встановлена на 6 для порівнянності з Amnesia.

Зі збільшенням рівня ієрархії до значення атрибута додається маскуючий символ. Кількість рівнів ієрархії дорівнює кількості символів у найбільшому значенні атрибута. На останньому рівні найбільше значення має бути повністю замінене маскуючими символами.

Атрибути userlocation та userdescription (Квазіідентифікатори). Ієрархії створені за тим же принципом маскування, оскільки вони є текстовими атрибутами.

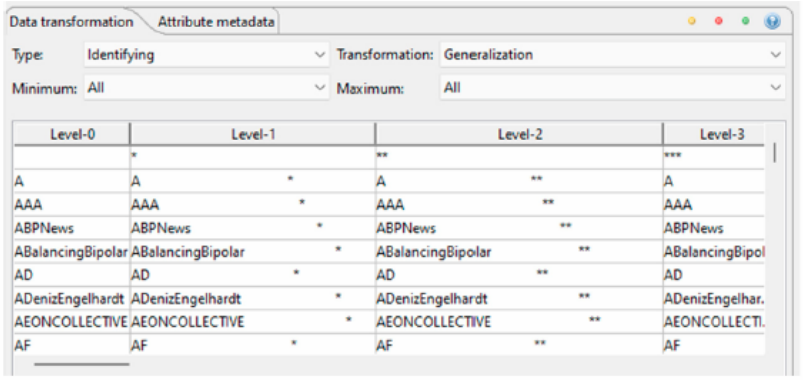

Рис. 3.6. Ієрархія username

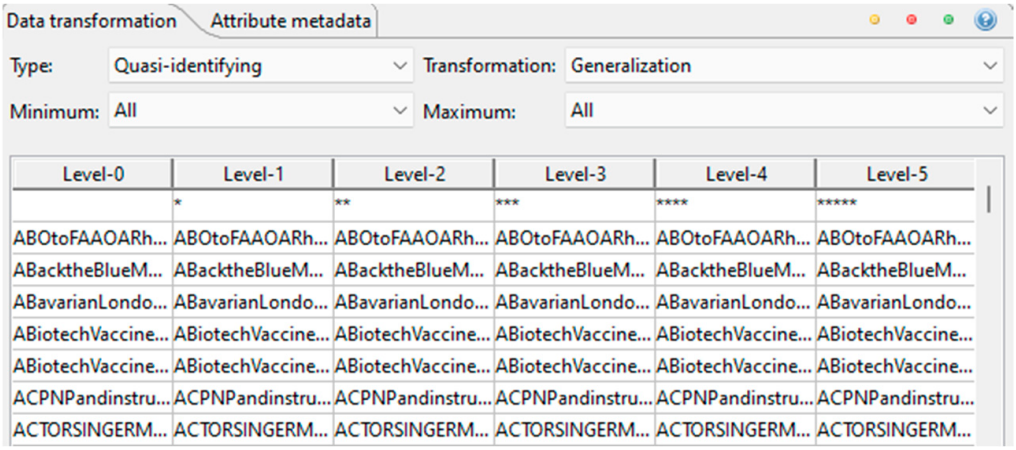

Рис. 3.7. Ієрархія userdescription

Після конфігурації моделі та ієрархій було виконано анонімізацію. ARX повернув лише один набір рішень у графіку рішень. Значення 85 та 146 відповідають рівням ієрархії, до яких були узагальнені атрибути `userlocation` та `userdescription` відповідно.

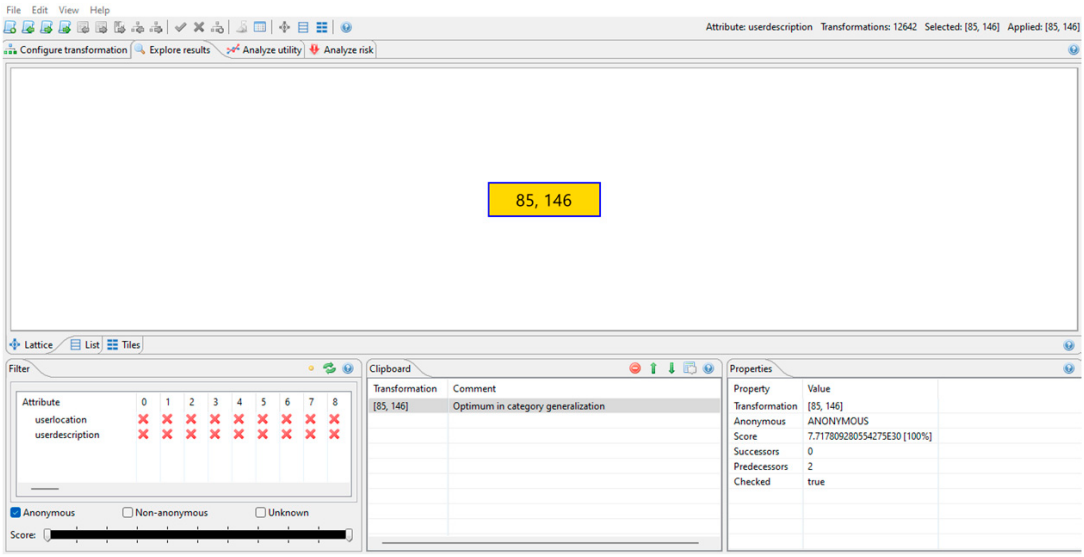

Рис. 3.8. Анонімізований графік рішень

Усі квазіідентифікуючі атрибути були анонімізовані до найвищих рівнів ієрархії, що еквівалентно 100% анонімізації (всі символи замінені маскуючими символами). Після цього анонімізований набір даних був доступний для завантаження у форматі CSV.

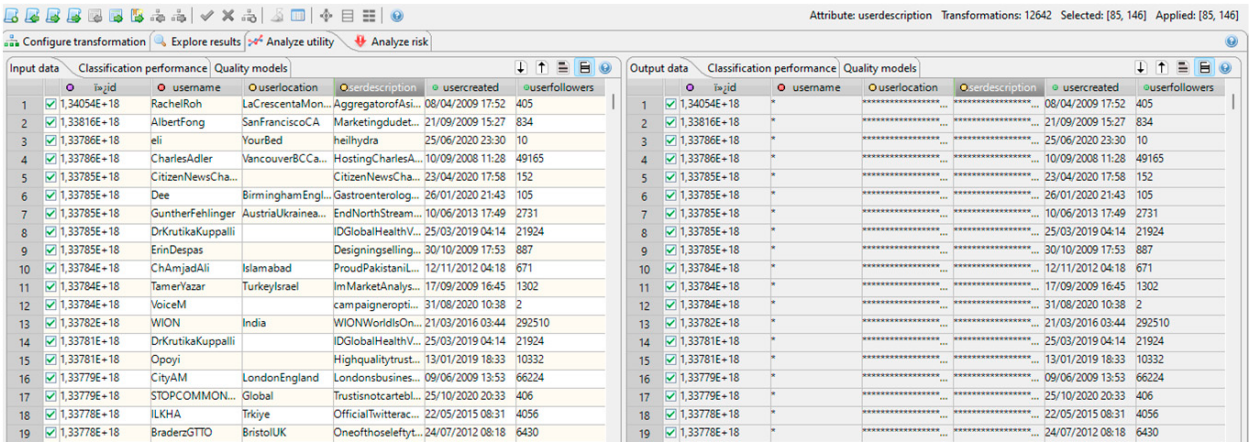

Рис. 3.9. Результат процесу анонімізації

3.5.2. Анонімізація набору даних за допомогою Amnesia

Процес анонімізації у Amnesia має значні відмінності.

1. Створення ієрархій

Атрибут username обрано тип на основі маскування. Довжина встановлена на рівні 6. Принцип маскування в Amnesia наступний: інструмент залишає перший символ незмінним і замінює решту маскуючим символом. Таким чином, модифіковані значення завжди мають 6 символів (перша літера + п'ять спеціальних символів).

Атрибут id (конфіденційний). Оскільки це ціле число, обрано тип діапазон (Range) для категоріального розділення значень. Крок узагальнення був визначений як 10^{16}. Атрибути userlocation та userdescription були оброблені аналогічно username (маскування першого символу та заміна решти на *).

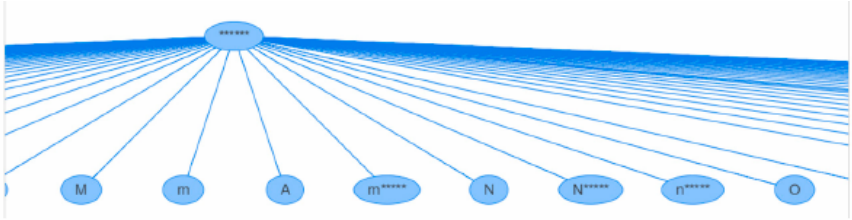

Рис. 3.10. Ієрархія username

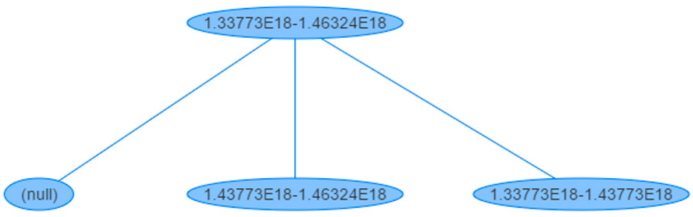

Рис. 3.11. Ієрархія id

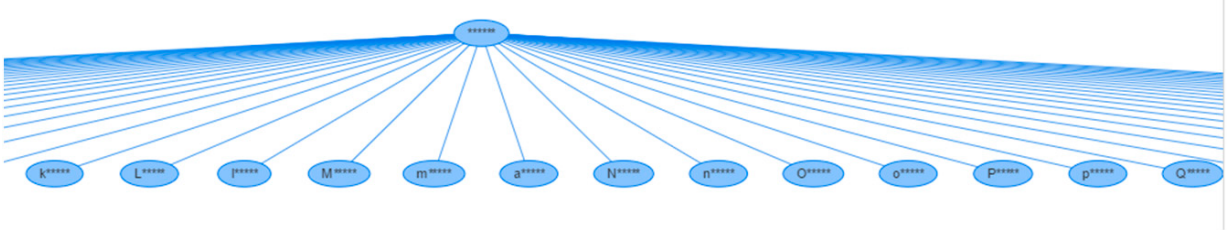

Рис. 3.12. Ієрархія userdescription

Незважаючи на документацію, Amnesia відображає лише алгоритм "Flash". Значення k було встановлено на 5 для порівнянності з ℓ=5 в ARX.

Отриманий графік виявився дуже заплутаним. Він містив безпечні (Safe) (сині вузли) та небезпечні (Unsafe) (червоні вузли) рішення.

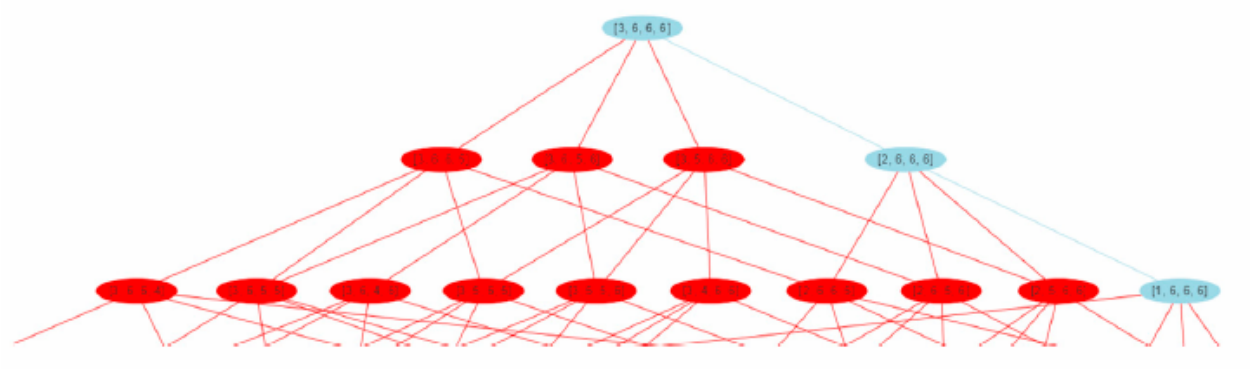

Рис. 3.13. Фрагмент графу рішень

Небезпечні рішення порушують гарантію k-анонімності для деяких записів. Хоча інструмент пропонує функцію "Suppression" для перетворення їх на безпечні, ця функція постійно генерувала помилку.

Anonymized Dataset

Show 10 entries

id	username	userlocation	userdescription	usercreated	userfollowers	userfriends	userfavourites
1.33773E18-1.46324E18	******	******	******	08/04/2009 17:52	405	1692	3247
1.33773E18-1.46324E18	******	******	******	21/09/2009 15:27	834	666	178
1.33773E18-1.46324E18	******	******	******	25/06/2020 23:30	10	88	155
1.33773E18-1.46324E18	******	******	******	10/09/2008 11:28	49165	3933	21853
1.33773E18-1.46324E18	******	******	******	23/04/2020 17:58	152	580	1473
1.33773E18-1.46324E18	******	******	******	26/01/2020 21:43	105	108	106
1.33773E18-1.46324E18	******	******	******	10/06/2013 17:49	2731	5001	69344
1.33773E18-1.46324E18	******	******	******	25/03/2019 04:14	21924	593	7815
1.33773E18-1.46324E18	******	******	******	30/10/2009 17:53	887	1515	9639

Рис. 3.14. Результат процесу анонімізації

Було отримано лише три безпечні рішення, що відображають рівні узагальнення для атрибутів [id,username,userlocation,userdescription]:

[3,6,6,6]: id узагальнено до рівня 3, інші атрибути — до рівня 6.

[2,6,6,6]: id узагальнено до рівня 2, інші атрибути — до рівня 6.

[1,6,6,6]: id узагальнено до рівня 1, інші атрибути — до рівня 6.

Отже, варіація між безпечними рішеннями стосується лише конфіденційного атрибута id (який не змінюється в результаті анонімізації), тоді як квазіідентифікуючі атрибути завжди анонімізуються до одного й того ж рівня 6. Це пояснює, чому ARX також повертає одне, найповніше рішення для квазіідентифікуючих атрибутів. В таблиці 3.10 представлено результати експерименту.

Таблиця 3.10.

Результат дослідження інструментів анонімізації

Характеристика	**ARX Data Anonymization**	**Amnesia**
Час виконання	Результат відображено негайно	Анонімізація зайняла 8 хвилин, відображення графіка — понад 5 хвилин
Складність рішень	Повернуто одне, чітке рішення; графік простий для інтерпретації.	Повернуто численні рішення (безпечні/небезпечні); графік є дуже заплутаним.
Проблеми конфіденційності	Не виявлено рішень, що порушують модель приватності.	Відображення небезпечних рішень, які порушують k-анонімність, ускладнює вибір.

Враховуючи значний розмір набору даних, спостерігається суттєва різниця у часі виконання між інструментами, де ARX працює значно швидше. Крім того, наявність небезпечних рішень та заплутаність графіка Amnesia значно ускладнює практичне використання інструменту для великих наборів даних.

За результатами проведеного аналізу та експериментальної оцінки, інструментом, рекомендованим для практичного застосування в анонімізації даних, є ARX Data Anonymization Tool1. Його перевага полягає у високій

стійкості до обмежень щодо розміру набору даних та складності структури елементів, а також у чіткості представлення фінального рішення.

Висновки до розділу

Третій розділ підтвердив, що практична реалізація анонімізації даних є не менш важливою, ніж теоретичні моделі та алгоритмічні процедури. У розділі було доведено, що інструменти анонімізації відіграють ключову роль у забезпеченні можливості коректної та ефективної обробки персональних даних. Аналіз архітектури інструментів ARX та Amnesia показав суттєві відмінності у рівні гнучкості, масштабованості та функціональних можливостей. Інструмент ARX продемонстрував ширший спектр моделей конфіденційності та багатші засоби контролю за втратою корисності. Натомість Amnesia виявилася ефективним рішенням для більш швидкої обробки даних та простоти інтеграції в робочі процеси. Методологія OSSpal дозволила провести об’єктивну оцінку програмних засобів та визначити ключові індикатори їхньої якості. Експериментальна частина засвідчила, що результати анонімізації можуть істотно різнитися залежно від вибраного інструменту та конфігурації моделей конфіденційності. Було встановлено, що ARX забезпечує точніше управління ризиками повторної ідентифікації, тоді як Amnesia демонструє стабільні та передбачувані результати при стандартних параметрах. Розділ доводить необхідність комплексного підходу до вибору інструментів, який враховує обсяги даних, типи атрибутів та цілі аналізу. Загалом проведене дослідження підтверджує, що практична ефективність анонімізації залежить від гармонійного поєднання методів, моделей та інструментальних засобів, адаптованих під конкретні умови застосування.

Отже, в цьому розділі представлено імплементації методів та інструментів для процесів ефективної анонімізації даних. За результатами анонімізації тестового набору даних зроблено висновок, що ARX Data

Anonymization є рекомендованим інструментом. Хоча інструмент Amnesia спрощує процес анонімізації, він виявив певні помилки, а представлені рішення є неповними та заплутаними.

ВИСНОВКИ

Магістерська робота, присвячена дослідженню методів, моделей та інструментів ефективної анонімізації даних, дає змогу комплексно оцінити сучасний стан проблематики збереження приватності в умовах стрімкого зростання обсягів даних, відкритості інформаційних потоків та підвищених вимог до захисту персональних даних. У роботі здійснено системний аналіз теоретичних підходів, формальних моделей, алгоритмів анонімізації та програмних засобів, що дозволило сформувати цілісну картину сучасних технологій приватності, а також провести їх експериментальну оцінку на реальних наборах даних.

На основі аналізу предметної області встановлено, що питання приватності в публікації даних є багатовимірною проблемою, що поєднує технічні, правові та етичні аспекти. Сучасні виклики, зокрема ризики деанонімізації, зростання кількості відкритих наборів даних та розвиток аналітичних технологій, зумовлюють необхідність удосконалення механізмів захисту конфіденційної інформації.

Дослідження демонструє, що традиційні підходи до анонімізації — видалення ідентифікаторів, генералізація, супресія — уже недостатні для гарантування приватності в умовах сучасних загроз. Показані практичні приклади деанонімізації доводять високу вразливість даних навіть після їх первинної обробки, що підтверджує актуальність формальних моделей конфіденційності.

У роботі обґрунтовано, що процес публікації даних із захистом приватності має розглядатися як повноцінний життєвий цикл, що охоплює аналіз ризиків, вибір моделі конфіденційності, застосування механізмів анонімізації, перевірку корисності та пост-аналіз потенційних векторів атак. Особлива увага приділена систематизації детерміністичних і рандомізованих підходів, що відрізняються рівнем стійкості та впливом на якість даних.

У другому розділі проведено ґрунтовний аналіз провідних моделей забезпечення конфіденційності, серед яких: k-анонімність як базова модель групового приховування; ℓ-різноманітність, що додатково враховує різноманітність чутливих атрибутів; t-близькість, яка мінімізує інформаційні втрати; диференціальна конфіденційність, що гарантує математично обґрунтовану стійкість проти широкого спектра атак.

Робота демонструє, що жодна з моделей не є універсальною; застосування конкретного підходу залежить від структури даних, типів чутливої інформації та вимог кінцевих користувачів. Виявлено тенденцію до посилення ролі рандомізованих методів, зокрема механізмів диференціальної конфіденційності, які забезпечують більш формальний рівень захисту.

Проаналізовані алгоритми анонімізації — включно з мікроагрегаційними підходами та алгоритмом kACTUS — дозволили визначити їхні ключові переваги та обмеження. Зокрема, мікроагрегація забезпечує мінімальні втрати корисності даних за умови правильної кластеризації, тоді як kACTUS оптимізує анонімізацію завдяки селективній генералізації квазіідентифікаторів.

У роботі поглиблено розглянуто метрики оцінки корисності даних, що є критично важливими для досягнення балансу між приватністю та якістю аналізу. Було встановлено, що найбільш релевантним підходом є комбінування загальних та специфічних до задачі метрик, що дозволяє оцінювати як збереження статистичних властивостей, так і продуктивність моделей машинного навчання на анонімізованих даних.

У третьому розділі проведено аналіз сучасних інструментів анонімізації даних, таких як ARX Data Anonymization та Amnesia, що широко застосовуються в академічних і промислових контекстах. На основі дослідження їх архітектури та функціональних можливостей встановлено, що ARX пропонує розширені механізми генералізації та моделювання ризиків, тоді як Amnesia забезпечує високу продуктивність і зручність взаємодії з великими наборами даних.

Для об'єктивної оцінки даних інструментів використано міжнародну методологію OSSpal, яка дозволяє систематично порівнювати програмне забезпечення за функціональністю, гнучкістю, надійністю та активністю спільноти. Застосування методології продемонструвало, що ARX має більш зрілу та комплексну екосистему, тоді як Amnesia вирізняється стабільністю та простотою інтеграції у більшості сценаріїв обробки персональних даних.

Експериментальна частина роботи підтвердила ефективність обох інструментів у контексті реальних даних:

ARX продемонстрував кращі можливості оптимізації моделей конфіденційності та контролю за втратами інформації;

Amnesia — більш збалансований показник швидкодії та якості анонімізації для наборів даних середнього розміру.

Порівняння результатів дає підстави стверджувати, що вибір інструменту повинен здійснюватися залежно від вимог до точності моделей, допустимого рівня втрат корисності та обсягів вхідних даних.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Beck, K., and Fowler, M. “Improving Agile Software Practices Through Continuous Refactoring.” Journal of Systems and Software, Berlin: Springer, 2019, pp. 45–59.
2. Cohn, M. “Adaptive Planning Strategies for Agile Teams.” International Journal of Project Management, Oxford: Elsevier, 2020, pp. 101–118.
3. Sanchez, D., and Müller, R. “Evaluating Agile Project Success Factors in Distributed Teams.” IEEE Transactions on Engineering Management, New York: IEEE Press, 2021, pp. 233–247.
4. Johnson, P., and White, A. “Agile-Based Methodological Enhancements for Large-Scale Projects.” Proceedings of the 15th International Conference on Software Engineering Advances, Paris: IEEE, 2020, pp. 77–86.
5. Thomas, R., and Li, S. “Comparative Analysis of Agile and Waterfall in Modern IT Projects.” Software Quality Journal, London: Springer, 2019, pp. 301–318.
6. Kim, J., and Park, H. “Model-Driven Engineering Using UML for Complex System Design.” Information and Software Technology, Amsterdam: Elsevier, 2021, pp. 150–166.
7. Horvat, A., and Guttman, S. “Enhancing UML-Based Software Modeling Through Automated Transformations.” Journal of Object Technology, Zurich: JOT Press, 2020, pp. 44–58.
8. Müller, T. “UML Sequence Diagram Optimization Techniques.” ACM SIGSOFT Conference on Software Engineering, New York: ACM, 2021, pp. 211–219.
9. Brown, E., and Taylor, P. “Advanced Paradigm Modeling Techniques for Software Systems.” International Journal of Computer Applications, London: IET Press, 2022, pp. 89–104.

10. Wang, Y., and Zhao, H. “Hybrid UML-Driven Modeling Frameworks in Distributed Architectures.” Journal of Software Engineering Research and Development, Berlin: Springer, 2019, pp. 122–137.
11. Roberts, L., and Singh, A. “Implementing Interactive Learning Environments Using Web Technologies.” Computers & Education, Oxford: Elsevier, 2020, pp. 55–71.
12. Martins, J., and Silva, T. “Adaptive Learning Management Systems for Higher Education.” Educational Technology & Society, New York: IEEE, 2021, pp. 118–131.
13. Patterson, G. “Gamification in E-Learning Platforms: A Systematic Review.” British Journal of Educational Technology, London: Wiley, 2022, pp. 599–617.
14. Yu, W., and Kaur, S. “User Interaction Models in Online Learning Systems.” International Journal of Human–Computer Studies, Amsterdam: Elsevier, 2019, pp. 87–103.
15. Chen, X. “Design Patterns for Interactive Educational Interfaces.” ACM Symposium on User Interface Software and Technology, New York: ACM, 2020, pp. 244–252.
16. Smith, R. “Project Tracking and Monitoring Systems in Modern Software Teams.” IEEE Software, New York: IEEE, 2021, pp. 33–48.
17. Patel, K., and Rao, V. “AI-Assisted Project Management Tools: Efficiency and Limitations.” Journal of Information Technology Management, Toronto: IGI Global, 2022, pp. 201–219.
18. Hamilton, D. “Integration of Agile Tools and Cloud-Based Project Tracking Platforms.” International Journal of Cloud Computing, London: Inderscience, 2020, pp. 79–95.
19. Curtis, M. “Workflow Optimization in Educational Project Tracking Systems.” Journal of Learning Analytics, New York: SoLAR, 2022, pp. 50–64.

20. Novak, P. “Dashboard Design Principles for Academic Project Monitoring Tools.” Interactions Journal, New York: ACM, 2021, pp. 110–124.
21. Lee, H., and Choi, B. “Usability Evaluation Methods for Interactive Educational Software.” Human–Computer Interaction Journal, London: Taylor & Francis, 2019, pp. 221–239.
22. Gomes, F. “Interface Modernization Approaches for Web-Based Learning Systems.” International Conference on Web Engineering, Berlin: Springer, 2021, pp. 291–304.
23. Andersson, K. “Responsive UI Architectures for High-Load Educational Platforms.” Journal of Web Engineering, Tokyo: Rinton Press, 2022, pp. 88–102.
24. Prasad, M. “Cognitive Load Reduction in Interactive Online Environments.” Computers in Human Behavior, Amsterdam: Elsevier, 2020, pp. 507–521.
25. Lopez, R., and Grant, T. “User Experience Metrics for System Evaluation in Educational Contexts.” International Journal of UX Studies, London: Elsevier, 2021, pp. 155–172.
26. Ortega, J. “Model Transformation Techniques from Paradigm to UML.” Model-Driven Engineering Conference (MODELS), Montreal: IEEE, 2022, pp. 99–115.
27. Fischer, L. “Formal Verification of UML Models in Complex Systems.” Journal of Formal Methods in System Design, Berlin: Springer, 2020, pp. 181–196.
28. Verma, S., and Kapoor, A. “Graph-Based Algorithms for UML Diagram Generation.” International Journal of Computing, London: Wiley, 2021, pp. 70–84.
29. Hudson, D. “Automated Code Generation from UML Models in Educational Platforms.” Software Engineering Education and Training Conference, New York: IEEE, 2020, pp. 144–157.

30. Rafiei, M. “Scalable Architecture Modeling Approaches for Enterprise Software.” Enterprise Information Systems Journal, London: Taylor & Francis, 2021, pp. 200–217.
31. Stewart, J. “Evaluating the Effectiveness of Interactive Learning Environments in STEM.” Journal of Educational Computing Research, Thousand Oaks: SAGE, 2022, pp. 301–320.
32. Oliveira, D. “Adaptive Content Delivery in E-Learning Systems Based on User Behavior.” IEEE Transactions on Learning Technologies, New York: IEEE, 2019, pp. 95–109.
33. Harris, P. “Cloud-Infrastructure Solutions for Scalable Educational Platforms.” ACM Cloud Computing Symposium, New York: ACM, 2021, pp. 187–198.
34. Takahashi, K. “Security and Privacy Considerations in Interactive Learning Systems.” Information Security Journal, London: Taylor & Francis, 2020, pp. 220–235.
35. Mensah, S. “Collaborative Learning Models Supported by Web Technologies.” International Journal of E-Learning, Norfolk: AACE, 2021, pp. 45–62.
36. Zhang, Q. “Performance Evaluation of Real-Time Educational Applications.” Journal of Network and Computer Applications, Amsterdam: Elsevier, 2019, pp. 178–195.
37. Carver, L. “Data-Driven Personalization Mechanisms in Learning Platforms.” Artificial Intelligence in Education Conference, Cham: Springer, 2022, pp. 64–79.
38. Rivera, A. “Design of Modular Architectures for Educational Software Systems.” Software Architecture Conference (ECSA), Paris: ACM, 2021, pp. 211–226.