УДК 004.056:621.317.3

В. М. Буняк[1]
В. В. Лукічов[2]

ЗАХИСТ КОНФІДЕНЦІЙНОСТІ В СИСТЕМАХ РОЗУМНОГО ОБЛІКУ. ТЕХНОЛОГІЇ ДИФЕРЕНЦІЙНОЇ ПРИВАТНОСТІ ТА АГРЕГАЦІЇ ДАНИХ

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Анотація

У доповіді розглянуто питання захисту конфіденційності в системах розумного обліку із застосуванням сучасних технологій диференційної приватності та агрегації даних. Представлено аналіз переваг і обмежень цих підходів для забезпечення конфіденційності інформації користувачів, а також інтеграційних можливостей впровадження запропонованих технологій в існуючі системи автоматизованого обліку споживання ресурсів. Описано практичні кейси та результати експериментальних досліджень, що підтверджують ефективність запропонованих рішень у контексті економічних обмежень та високих вимог до захисту даних.

Ключові слова: розумний облік, диференційна приватність, агрегація даних, захист конфіденційності, кібербезпека.

Abstract

The report examines the issue of privacy protection in smart metering systems using modern technologies of differential privacy and data aggregation. An analysis of the advantages and limitations of these approaches to ensuring the confidentiality of user information is presented, as well as the integration possibilities of implementing the proposed technologies into existing automated resource consumption accounting systems. Practical cases and results of experimental studies are described, confirming the effectiveness of the proposed solutions in the context of economic constraints and high data protection requirements.

Keywords: smart accounting, differential privacy, data aggregation, privacy protection, cybersecurity.

Вступ

Сучасні системи розумного обліку, що використовуються в енергетиці та комунальному господарстві, забезпечують оперативний збір та аналіз даних, що дозволяє підвищити ефективність управління ресурсами. Проте широке впровадження цих технологій супроводжується зростанням ризиків витоку конфіденційної інформації, що може містити детальні дані про поведінку користувачів та їхні споживчі звички. Зростаюча кількість IoT-пристроїв створює додаткове навантаження на системи безпеки, що вимагає впровадження сучасних методів захисту даних [1].

Захист персональних даних набуває особливої актуальності в умовах високої інтеграції цифрових технологій у критичну інфраструктуру. Інформація, що надходить із систем розумного обліку, часто містить чутливі відомості, які можуть бути використані для аналізу соціально-економічних трендів, прогнозування поведінки споживачів, а також для потенційних кібератак. Саме тому забезпечення конфіденційності є пріоритетною задачею, яка потребує як технічних, так і організаційних заходів [2].

У даній доповіді пропонуються технології диференційної приватності та агрегації даних як ефективні інструменти для забезпечення захисту конфіденційної інформації в системах розумного обліку. Технологія диференційної приватності дозволяє шляхом додавання контрольованого шуму до початкових даних зберегти їх статистичну цінність, уникаючи можливості ідентифікації окремих користувачів. Агрегація даних, що полягає у групуванні окремих показників для отримання зведених статистичних даних, значно знижує ризик розкриття персональних даних.

Результати дослідження

Технологія диференційної приватності полягає у внесенні контрольованого шуму в початкові дані, що дозволяє зберегти статистичну цінність інформації, одночасно приховуючи індивідуальні відомості

користувачів. Цей підхід є особливо актуальним для систем розумного обліку, де зібрані дані можуть містити конфіденційну інформацію, що потребує додаткового рівня захисту. У таблиці 1 наведено приклади різних алгоритмічних рішень, які можна застосовувати для забезпечення диференційної приватності та агрегації даних у системах розумного обліку [3][4].

Досягнення ефективної диференційної приватності потребує впровадження математичних моделей, які забезпечують баланс між збереженням корисної інформації та зменшенням ймовірності ідентифікації окремих записів. У цьому контексті застосовуються алгоритми, що оптимізують параметри додавання шуму, зокрема, методи, які використовують ε-диференційність. Попередні дослідження показали, що правильна калібрування цього параметра є критичним для збереження якості даних у системах розумного обліку [3].

Таблиця 1. Приклади алгоритмічних рішень для забезпечення диференційної приватності та агрегації даних у системах розумного обліку

Назва алгоритму	Тип/Категорія	Опис
Механізм Лаплас	ε-диференційна приватність	Додає шум з розподілу Лапласа до результатів запитів, забезпечуючи математично строгий захист числових даних.
Гауссівський механізм	ε-диференційна приватність	Використовує нормальний (гауссівський) розподіл для додавання шуму, що дозволяє зберігати точність статистичних показників.
Експоненціальний механізм	ε-диференційна приватність	Обирає оптимальний вихід серед можливих результатів, зважуючи утилітарність, що зберігає корисність даних при захисті приватності.
Рандомізований відгук	Локальна диференційна приватність	Кожен користувач модифікує свої дані випадковим чином за встановленими ймовірнісними правилами, забезпечуючи захист на етапі збору.
Ієрархічна агрегація	Агрегація даних	Розбиває дані на декілька рівнів або груп із подальшим обчисленням агрегованих показників, що знижує ризик ідентифікації.

Технологія агрегації даних, яка передбачає групування окремих показників у зведені статистичні дані, допомагає суттєво знизити ризик розкриття особистої інформації. Завдяки агрегації даних можна отримати корисну аналітичну інформацію, яка відображає загальні тренди без можливості ідентифікації окремих користувачів. Цей підхід дозволяє оптимізувати обсяг оброблюваної інформації та мінімізувати вплив потенційних кібератак, пов’язаних із несанкціонованим доступом до індивідуальних даних.

Комбінування технологій диференційної приватності та агрегації даних створює синергічний ефект, який забезпечує оптимальний рівень захисту при збереженні високої точності отриманих показників [5]. Експериментальний аналіз показав, що використання спільного підходу дозволяє суттєво знизити ймовірність витоку конфіденційної інформації, зберігаючи при цьому можливість проводити точну аналітику споживання ресурсів [1]. У таблиці 2 порівнює основні алгоритмічні підходи для забезпечення диференційної приватності та агрегації даних у системах розумного обліку. Ця таблиця ілюструє ключові параметри налаштування, вплив на точність даних, а також переваги та обмеження кожного підходу, що дозволяє вибрати оптимальне рішення для конкретних умов застосування [2][4].

Таблиця 2. Порівняльна характеристика основних алгоритмічних підходів

Назва алгоритму	Параметри / Рівень шуму	Вплив на точність даних	Переваги	Обмеження
Механізм Лаплас	Параметр ε (чим менше ε – більше шуму)	Залежить від вибраного ε; менше ε – вищий рівень захисту, але зниження точності даних	Простота реалізації, математично строгий захист даних	При низькому ε може суттєво погіршувати точність результатів
Гауссівський механізм	Стандартне відхилення σ	Забезпечує збереження точності для даних із нормальним розподілом; варіювання рівня шуму залежить від σ	Підтримує точність статистичних показників для даних з нормальним розподілом	Менш ефективний для даних з асиметричним розподілом
Експоненціальний механізм	Оптимізація утилітарності	Балансує між точністю та приватністю, вибираючи оптимальний вихід	Забезпечує високий рівень корисності вихідних даних	Складність налаштування та розрахунку утилітарності
Рандомізований відгук	Локальні ймовірнісні параметри	Захищає дані на рівні користувача, але може знизити точність окремих записів	Забезпечує приватність вже на етапі збору даних	Можливе зниження точності індивідуальних відповідей
Ієрархічна агрегація	Рівні агрегації (групування даних)	Зберігає точність агрегованих показників, знижуючи ризик ідентифікації	Ефективно знижує ризик розкриття даних, оптимізує обсяг обробки даних	Можлива втрата детальної інформації на нижчих рівнях агрегації

Інтеграція запропонованих технологій у існуючі системи розумного обліку відкриває широкі перспективи для підвищення загальної кібербезпеки енергетичної інфраструктури. Подальші дослідження спрямовані на оптимізацію алгоритмів та розробку адаптивних систем моніторингу, які зможуть

автоматично реагувати на потенційні загрози. Це дозволить не лише знизити ризики витоку даних, а й забезпечити безперебійну роботу критичних систем, що є важливим чинником конкурентоспроможності в умовах швидкого розвитку IoT-технологій.

Висновки

Запропонований підхід до захисту конфіденційності в системах розумного обліку, який базується на застосуванні технологій диференційної приватності та агрегації даних, демонструє високий потенціал для зниження ризиків витоку чутливої інформації. Це дозволяє ефективно захищати персональні дані користувачів, мінімізуючи можливість їх ідентифікації при збереженні статистичної цінності даних [5]. Системи розумного обліку, що працюють на базі запропонованого підходу, забезпечують покращення якості обробки даних, що є особливо важливим у контексті енергетичної інфраструктури, де достовірність показників має критичне значення для управління ресурсами.

Використання сучасних алгоритмічних рішень сприяє розробці адаптивних систем моніторингу, здатних автоматично реагувати на потенційні загрози та аномальну активність. Це забезпечує не лише підвищення рівня безпеки, але й оптимізацію операційних витрат, що є ключовим фактором конкурентоспроможності в умовах швидкого розвитку цифрових технологій.

Подальші дослідження мають бути спрямовані на оптимізацію алгоритмів та адаптацію технологій до умов високої конкуренції та економічних обмежень, що сприятиме підвищенню стійкості критичної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Fang, Y., Misra, S., & Christin, N. (2019). Privacy-Preserving Data Aggregation in Smart Grid: Differential Privacy Approaches. IEEE Transactions on Smart Grid, 10(2), 1214–1223.
2. Li, F., Luo, B., & Liu, P. (2019). Smart Grid Data Privacy: Challenges and Solutions. IEEE Communications Surveys & Tutorials, 21(3), 2765–2789.
3. Zhou, X., Li, J., & Wu, X. (2020). A Differential Privacy Approach for Smart Meter Data Aggregation. IEEE Access, 8, 102345–102355.
4. Sharma, A., Gupta, P., & Singh, R. (2021). Differential Privacy Techniques in IoT-Enabled Smart Metering Systems: A Review. Journal of Network and Computer Applications, 178, 102943.
5. Kumar, S., & Patel, D. (2022). Enhancing Consumer Privacy in Smart Metering via Data Aggregation and Differential Privacy. IEEE Internet of Things Journal, 9(5), 3456–3465.

Буняк Віталій Михайлович — студент групи 125-23а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vetalbunjak@gmail.com

Лукічов Віталій Володимирович — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Buniak Vitalii M. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vetalbunjak@gmail.com

Lukichov Vitalii V. — Cand. Sc. (Eng), Assistant Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia