УДК 004.056.55

Туржанська І.Д.

КРИПТОСИСТЕМА ПАЙЄ ЯК ІНСТРУМЕНТ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ У ФІНАНСОВИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У роботі досліджується проблема надмірного доступу бухгалтерів до конфіденційних фінансових даних працівників у традиційних облікових системах. Показано, що стандартні механізми розмежування доступу не забезпечують належного захисту персональних фінансових відомостей під час виконання агрегованих розрахунків. Запропоновано застосування криптосистеми Пайє для виконання бухгалтерських обчислень над зашифрованими даними без їх розкриття. Розроблено трирівневу архітектуру застосунку на мові Python із базою даних у форматі JSON, що реалізує розмежування прав між оператором введення даних, бухгалтером та адміністратором.

Ключові слова: захист персональних даних, гомоморфне шифрування, криптосистема Пайє, кібербезпека, бухгалтерський облік, фінансові технології.

Abstract

The paper investigates the problem of excessive access of accountants to confidential financial data of employees in traditional accounting systems. It is shown that standard access delimitation mechanisms do not provide adequate protection of personal financial information when performing aggregate calculations. The use of the Payer cryptosystem is proposed to perform accounting calculations on encrypted data without revealing them. A three-level architecture of the application in Python with a database in JSON format is developed, which implements the delimitation of rights between the data entry operator, accountant and administrator..

Keywords: personal data protection, homomorphic encryption, Paillier cryptosystem, cybersecurity, accounting, FinTech.

Вступ

Бухгалтерський облік є основою фінансового управління підприємства, а процес нарахування заробітної плати — одним із найчутливіших з погляду конфіденційності, оскільки передбачає роботу з персональними даними кожного співробітника [1]. На практиці більшість підприємств надає бухгалтерам прямий доступ до бази даних нарахувань, що дозволяє переглядати індивідуальні фінансові показники всіх працівників під час виконання рутинних операцій. Це суперечить вимогам Закону України «Про захист персональних даних» [2]. Сучасні бухгалтерські системи (M.E.Doc [3], BAS Бухгалтерія [4]) зберігають дані централізовано, що збільшує ризики компрометації персональної інформації, інсайдерського шахрайства та корпоративного шпигунства [5]. Метою дослідження є підвищення конфіденційності персональних фінансових даних у системах бухгалтерського обліку шляхом застосування гомоморфного шифрування Пайє, що унеможливлює доступ до індивідуальних нарахувань при збереженні повної функціональності обчислень.

Результати досліджень

Для того щоб зрозуміти вразливості, потрібно розуміти як саме нараховується заробітна плата. Відповідно до стандартів обліку [6, 7], процес нарахування складається з кількох етапів: нарахування основної ставки, додавання бонусів, а також вирахування податків (ПДФО - 18%, військовий збір - 1,5%, ЄСВ - 22%). З точки зору математики, усі бухгалтерські процеси зводяться до дій додавання та множення на коефіцієнти. Саме цей факт стає критерієм при виборі гомоморфної системи шифрування.

Проблема полягає в архітектурі традиційних облікових систем: при обчисленні загальної суми зарплат по фірмі, загального ПДФО або додавання бонусів працівнику програма надає бухгалтеру повний доступ до таблиці нарахувань, у якій видно всі фінансові дані кожного працівника. Хоча для роботи потрібен лише фінальний результат, співробітник бачить індивідуальні доходи кожного працівника. Крім того, під загрозою опиняється й інша конфіденційна інформація: компенсація за лікарняні, премії. Такий надмірний доступ суперечить нормам захисту персональних даних [2, 5].

Для вирішення даної проблеми запропоновано криптосистему Пайє - алгоритм гомоморфного шифрування, розроблений у 1999 році [7], що виконує математичні операції над шифротекстом без його розкриття [8]. Система використовує два ключі: публічний (n, g) - для шифрування, та приватний λ - для розшифрування лише довіреною особою.

Математична основа схеми [9, 10]: система генерує два великі прості числа p та q. На їх основі обчислюється модуль $n = p \cdot q$ та секретний параметр $\lambda = НСК(p - 1, q - 1)$. Формуються два ключі: публічний (n, g) та приватний λ. Шифрування значення m (суми зарплати) виконується за формулою:

$$c = g^m \cdot r^n \pmod{n^2},$$

де c - отриманий шифротекст, r - згенероване випадкове число. Наявність параметра r забезпечує генерацію різних шифротекстів навіть для однакових значень зарплати.

Розшифрування виконується власником приватного ключа за формулою [9]:

$$m = L(c^{\lambda} \bmod n^2) \cdot \mu \pmod{n}$$

Для бухгалтерського застосунку важливою є адитивна гомоморфність схеми [8, 9], що надає такі властивості:

1. Додавання зашифрованих сум: при множенні двох шифротекстів отримуємо зашифровану суму відкритих значень: $D(E(m_1) \cdot E(m_2) \bmod n^2) = m_1 + m_2$.

2. Множення на коефіцієнт: піднесення шифротексту до степеня k (наприклад, ставки податку) дає зашифрований добуток: $D(E(m)k \bmod n^2) = k \cdot m$.

Завдяки цим властивостям бухгалтер може підсумувати зашифровані нарахування всіх співробітників та обчислити податкові утримання, при цьому не маючи доступу до персональних даних.

Розроблена архітектура застосунку реалізує дані властивості через три модулі з чітко розмежованими правами доступу, схему яких наведено на рис. 1.

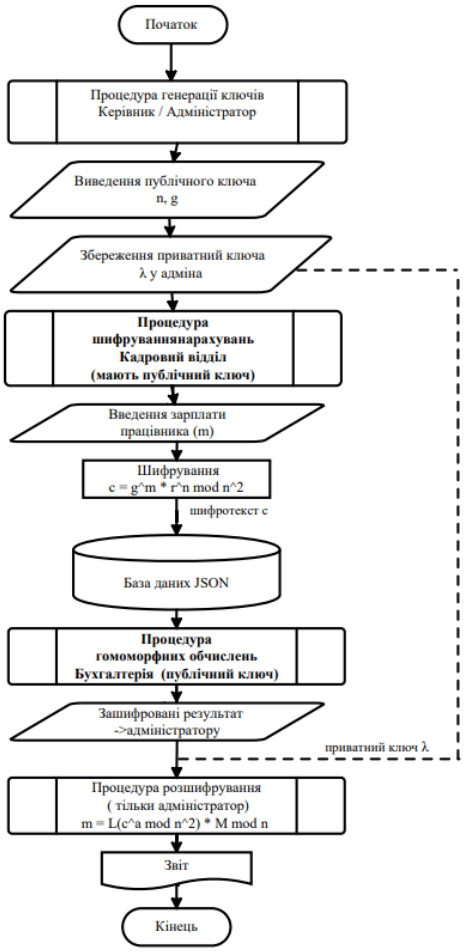

Рисунок 1 — Схема роботи застосунку

Як видно з рис. 1, архітектура системи базується на трьох ізольованих модулях. Процедура генерації ключів, яку виконує адміністратор, є довіреним вузлом системи: вона відповідає за створення

ключів Пайє, локальне збереження приватного ключа λ та передачу публічного ключа (n, g) іншим учасникам. Процедура шифрування нарахувань, яку виконує кадровий оператор, використовує публічний ключ для шифрування індивідуальних нарахувань працівників і записує отримані шифротексти у базу даних JSON. Процедура гомоморфних обчислень, яку виконує бухгалтерія, взаємодіє виключно із зашифрованим масивом, де — гомоморфно перемножує шифротексти для розрахунку фонду оплати праці або зводить до степеня для обчислення. Зашифрований результат повертається адміністратору, який за допомогою приватного ключа виконує процедуру розшифрування і отримує фінальний звіт.

Висновки

Традиційні системи бухгалтерського обліку створюють вразливість щодо отримання повного доступу до персональних фінансових даних працівників, хоча для виконання обов'язків достатньо лише агрегованих результатів. Це суперечить нормам захисту персональних даних та створює ризики витоку конфіденційної інформації. Запропоноване рішення на основі криптосистеми Paillier усуває дану проблему завдяки гомоморфній властивості. Бухгалтер виконує всі необхідні обчислення над зашифрованими даними, не маючи прямого доступу до конфіденційної інформації. Розроблена трирівнева архітектура з чітким розмежуванням прав між оператором, бухгалтером та адміністратором підтверджує практичну придатність запропонованого підходу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996-14 (дата звернення 03.03.2026)

2.Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення 03.03.2026)

3. Компанія «M.E.Doc». Програмний комплекс M.E.Doc — електронна звітність та документообіг. URL: https://medoc.ua/ (дата звернення 03.03.2026)

4. Компанія «БАС». BAS Бухгалтерія — програма для ведення бухгалтерського обліку. URL: https://www.bas-soft.eu/ (дата звернення 03.03.2026)

5. Чумаченко М. Г. та ін. Бухгалтерський облік : підручник. Київ : КНЕУ, 2004. 657 с.

6. Ткаченко Н. М. Бухгалтерський фінансовий облік, оподаткування і звітність : підручник. 7-ме вид. Київ : Алерта, 2016. 928 с.

7. Голов С. Ф. Бухгалтерський облік в Україні : монографія. Київ : Центр учбової літератури, 2007. 522 с.

8. Acar A., Aksu H., Uluagac A. S., Conti M. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Computing Surveys*. 2018. Vol. 51, No. 4. URL: https://dl.acm.org/doi/10.1145/3214303 (last accessed: 03.03.2026)

9. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *Advances in Cryptology — EUROCRYPT 1999*. Berlin : Springer, 1999. P. 223–238. URL: https://doi.org/10.1007/3-540-48910-X_16 (last accessed: 03.03.2026)

10. Kupcova E., Pleva M., Khavan V., Drutarovsky M. A Comparative Study of Partially, Somewhat, and Fully Homomorphic Encryption in Modern Cryptographic Libraries. *Electronics*. 2025. Vol. 14, No. 23. URL: https://doi.org/10.3390/electronics14234753 (last accessed: 03.03.2026)

Туржанська Ірина Дмитрівна - студентка групи 2БС-22Б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: turzhanskayaryna@gmail.com

Науковий керівник***: Баришев Юрій Володимирович*** – к.т.н., доцент кафедри захисту інформації, Вінницткий національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Iryna Turzhanska - student of group 2BS-22B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: turzhanskayaryna@gmail.com

Scientific supervisor: ***Yurii Baryshev*** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Ukraine, yuriy.baryshev@vntu.edu.ua