https://doi.org/10.30857/2786-5371.2026.1.6

Received: 21.01.2026
Revised: 17.02.2026
Accepted: 09.04.2026

УДК 004.056:004.8

Ганна ЗАВГОРОДНЯ[1], Валерій ЗАВГОРОДНІЙ[1], Андрій САВЧЕНКО[2], Андрій ЛЕМЕШКО[3]
[1] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
[2] Заклад вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая», Київ, Україна
[3] Державний торговельно-економічний університет, Київ, Україна

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ОБРОБКИ ПЕРСОНАЛІЗОВАНИХ ДАНИХ У СИСТЕМАХ АДАПТИВНОЇ ГЕНЕРАЦІЇ КОНТЕНТУ

Мета. *Метою статті є розроблення комплексного підходу до забезпечення безпеки та коректної обробки персоналізованих даних у системах адаптивної генерації контенту. Запропонований підхід базується на формалізації простору персоналізованих даних користувачів, застосуванні методів анонімізації та псевдонімізації, використанні механізмів диференційної приватності (Differential Privacy), федеративного навчання (Federated Learning) та інтеграції сучасних криптографічних і архітектурних засобів захисту.*

Методика. *Дослідження спирається на системний аналіз архітектур адаптивних систем і багатовимірного простору ознак користувацьких даних. Для оцінки ризику деанонімізації застосовано математичні моделі диференційної приватності, а для захисту розподілених даних – протоколи федеративного навчання з безпечною агрегацією градієнтів. Проведено порівняльний аналіз сучасних методів захисту персональних даних, моделювання загроз та розроблено багаторівневу архітектурну модель безпеки, що враховує принципи Zero Trust, контроль доступу за ролями (RBAC), шифрування та аудит подій.*

Результати. *Запропоновано формалізовану модель простору персоналізованих даних, яка дозволяє класифікувати рівні чутливості інформації, визначати допустимі перетворення та інтегрувати їх із методами анонімізації. Доведено ефективність ε-диференційної приватності для контролю ризику деанонімізації при навчанні моделей. Розроблено узагальнену схему поєднання федеративного навчання та криптографічних протоколів безпечної агрегації, що забезпечує конфіденційність користувацьких даних без втрати точності моделей. Створено багаторівневу архітектурну систему захисту, яка включає шифрування даних, контроль доступу, аудит і моніторинг, забезпечуючи баланс між безпекою, масштабованістю та ефективністю генерації контенту.*

Наукова новизна. *Полягає у комплексному поєднанні формальної моделі персоналізованих даних з механізмами диференційної приватності та федеративного навчання в межах єдиної архітектурної концепції безпеки, що дозволяє одночасно забезпечити конфіденційність, масштабованість та ефективність обробки даних у системах адаптивної генерації контенту.*

Практична значимість. *Результати можуть бути застосовані при розробленні освітніх платформ, ігрових систем, рекомендаційних сервісів та інших інтелектуальних систем, що працюють із персоналізованими профілями користувачів, потребують високого рівня безпеки даних та відповідності сучасним стандартам захисту інформації.*

Ключові слова: *адаптивна генерація контенту; персоналізовані дані; диференційна приватність; федеративне навчання; шифрування; архітектура безпеки.*

Вступ. Стрімкий розвиток систем адаптивної генерації контенту зумовлений впровадженням методів штучного інтелекту у цифрові освітні середовища, ігрові платформи, рекомендаційні сервіси та масові онлайн-системи. Алгоритмічні механізми процедурної генерації дозволяють створювати контент у динамічному режимі на основі заданих правил і параметрів середовища [1]. Подальше підвищення ефективності таких систем досягається

шляхом інтеграції алгоритмів машинного навчання, що забезпечують адаптацію складності та структури контенту відповідно до індивідуальних характеристик користувача [2].

Масштабування адаптивних механізмів у багатокористувацьких середовищах потребує побудови розподілених архітектур, здатних обробляти великі обсяги даних у режимі реального часу [3]. Моделювання поведінки користувача за допомогою нейромережевих агентів [4] дозволяє формувати персоналізовані сценарії взаємодії, проте передбачає накопичення детальних поведінкових профілів. Таким чином, ефективність адаптивної генерації безпосередньо залежить від глибини аналізу персоналізованих даних.

Формування персоналізованого профілю передбачає збір множини параметрів: історії дій, часових характеристик активності, індикаторів складності, реакцій на попередній контент, технічних метаданих пристрою. Сукупність цих ознак створює високовимірний простір персоналізованих даних, який потенційно містить чутливу інформацію. Дослідження з інформаційної безпеки вказують, що навіть агреговані або частково знеособлені дані можуть бути використані для повторної ідентифікації користувача за наявності зовнішніх джерел інформації [5].

Одним із формалізованих підходів до мінімізації ризику деанонімізації є диференційна приватність, що забезпечує математичну гарантію обмеження впливу окремого запису на результат обробки даних [6]. Подальші дослідження показують, що практичне застосування ε-диференційної приватності потребує оптимального вибору параметра приватності з урахуванням компромісу між точністю моделі та рівнем захисту [7]. Особливо актуально це для систем адаптивної генерації, де надмірний шум може знизити якість персоналізації.

Іншим перспективним напрямом є федеративне навчання, що дозволяє здійснювати тренування моделей без централізованого зберігання сирих даних користувачів [8]. Практична реалізація федеративних підходів у масштабних системах продемонструвала їхню ефективність у зменшенні ризику витоку інформації [9]. Додаткове використання протоколів безпечної агрегації параметрів моделей підвищує рівень захисту від внутрішніх атак і несанкціонованого доступу [10].

Паралельно розвиваються архітектурні концепції забезпечення безпеки, зокрема Zero Trust, що передбачає постійну перевірку автентичності суб’єктів доступу незалежно від їхнього розташування в мережі [11]. Дослідження багаторівневих моделей контролю доступу та шифрування даних на різних етапах життєвого циклу інформації підтверджують необхідність комплексного підходу до захисту [12]. Важливим компонентом сучасних архітектур є використання криптографічних протоколів для захищеної передачі та зберігання даних [13].

Окрему увагу приділено проблемі оцінювання ризиків приватності в системах штучного інтелекту. У роботах [14] підкреслюється необхідність формалізації простору даних та визначення рівнів чутливості параметрів профілю. Аналіз сучасних підходів до privacy-preserving machine learning [15] демонструє, що ізольоване застосування окремих механізмів не забезпечує достатнього рівня захисту без інтеграції їх у цілісну архітектуру.

Незважаючи на активний розвиток досліджень у галузі адаптивної генерації контенту та сучасних методів захисту даних, відсутній комплексний підхід, який би поєднував формалізацію персоналізованого простору даних, математичні гарантії приватності та архітектурні механізми безпеки в єдиній моделі побудови адаптивних систем. Більшість робіт розглядає алгоритмічні аспекти персоналізації окремо від задач інформаційної безпеки або фокусується на загальних підходах до privacy-preserving машинного навчання без урахування специфіки генеративних адаптивних середовищ.

Отже, актуальною науковою задачею є розроблення цілісної моделі забезпечення безпеки персоналізованих даних у системах адаптивної генерації контенту, що враховує як

математичні, так і архітектурні аспекти захисту. Саме вирішенню цієї проблеми присвячене дане дослідження.

Постановка завдання. Метою статті є дослідження та систематизація методів забезпечення безпеки та обробки персоналізованих даних у системах адаптивної генерації контенту, зокрема в контексті сучасних технологій машинного навчання та розподілених архітектур. Основна задача полягає у визначенні ефективних підходів до:

1. Формалізації простору персоналізованих даних – створення уніфікованої структури для зберігання та обробки даних користувачів, що дозволяє подальше застосування алгоритмів машинного навчання та анонімізації без втрати контекстної інформації.
2. Впровадження анонімізації та псевдонімізації – розробка методів приховування ідентифікаційних ознак користувачів, що знижують ризик ре-ідентифікації та забезпечують захист конфіденційних даних.
3. Застосування диференційованої приватності (Differential Privacy) – забезпечення математично обґрунтованого механізму захисту даних під час навчання моделей, що дозволяє уникати витоку інформації про окремих користувачів.
4. Інтеграції методів федеративного навчання (Federated Learning) – навчання моделей на розподілених пристроях користувачів без централізації персональних даних, забезпечуючи одночасно конфіденційність і ефективність генерації контенту.
5. Впровадження архітектурних механізмів багаторівневого захисту – використання криптографії, Zero Trust підходів, RBAC та систем моніторингу для гарантування цілісності, конфіденційності та доступності даних у динамічних і багатокористувацьких системах.

Дана стаття має на меті ліквідувати існуючі «білі плями» у практичному застосуванні цих технологій, включаючи питання масштабованості, ефективності та конфіденційності обробки даних користувачів у системах адаптивної генерації контенту. Крім того, робота спрямована на системне порівняння методів, що дозволяє визначити оптимальні комбінації технік безпеки для конкретних архітектурних сценаріїв та надати науково обґрунтовані рекомендації для розробників та дослідників у цій сфері.

Результати дослідження. Для формалізації простору персоналізованих даних користувачів було запропоновано їх представлення як структурованих векторів ознак, де кожен об’єкт u_i характеризується набором параметрів:

$$u_i = \{x_1, x_2, \dots, x_n\}, i = 1,2, \dots, m,$$

де x_j – окремий атрибут користувача, наприклад, демографічна інформація ($x_1 -$ вік, $x_2 -$ стать, $x_3 -$ локація), історія взаємодії з контентом ($x_4 -$ кількість переглядів, $x_5 -$ час перебування на сторінці), поведінкові параметри ($x_6 -$ швидкість взаємодії, $x_7 -$ частота кліків).

Для більш комплексного відображення взаємозв’язків між користувачами та елементами контенту використовувалася графова модель:

$$G = (V, E),$$

де множина вузлів V включає користувачів і контент-об’єкти:

$$V = \{u_1, u_2, \dots, u_m\} \cup \langle c_1, c_2, \dots, c_k \rangle,$$

де u_i – вузол, що відповідає користувачу i; c_j – вузол, що відповідає контент-об’єкту j; m – загальна кількість користувачів; k – кількість контент-об’єктів.

Множина ребер графу $E \subseteq V \times V$ відображає взаємодію або схожість між вузлами, наприклад: ребро (u_i, c_j) означає, що користувач u_i взаємодіяв з контентом c_j; ребро (u_i, u_j) може позначати схожість між користувачами за поведінкою; ребро (c_i, c_j) відображає схожість або тематичну близькість контент-об’єктів.

Кожне ребро можна формалізувати як вагове:

$$e_{pq} = \omega_{pq}, \omega_{pq} \in [0,1],$$

де ω_{pq} – коефіцієнт взаємодії або схожості. Наприклад:

$$\omega_{u_i,c_j} = \frac{\text{кількість взаємодій } u_i \text{ з } c_j}{\text{максимаьна кількість взаємодій у системі}}.$$

Кожен вузол графу u_i або c_j можна описати не лише ідентифікатором, а й вектором ознак:

$$\phi(u_i) = \{x_1, x_2, \dots, x_n\}, \phi(c_j) = \{y_1, y_2, \dots, y_l\},$$

де y_l – характеристики контенту, наприклад категорія, рейтинг, тривалість. Це дозволяє об'єднати графові та векторні представлення даних для використання глибоких нейронних мереж на графах (Graph Neural Networks) та класичних моделей машинного навчання.

Анонімізація та псевдонімізація. Анонімізація та псевдонімізація є ключовими методами захисту персоналізованих даних у системах адаптивної генерації контенту. Вони дозволяють мінімізувати ризик ре-ідентифікації користувачів, одночасно зберігаючи релевантність даних для навчання моделей машинного навчання. Використовувались наступні методи: k-анонімність та l-diversity.

k-анонімність забезпечує, що кожний запис у наборі даних не відрізняється від щонайменше $k-1$ інших за вибраними атрибутами (quasi-identifiers). Формально, для набору даних D:

$$\forall_{u_i} \in D, \exists\, S \in D \text{ таке, що } |S| \geq k \text{ і } \forall_{u_j} \in S, u_i[QI] = u_j[QI],$$

де QI – набір атрибутів, за якими виконується анонімізація.

l-diversity доповнює k-анонімність, гарантуючи, що в кожному кластері k-записів присутні щонайменше l різних значень чутливих атрибутів S:

$$\forall \text{ кластер } C_k, |\{u_i[S]: u_i \in C_k\}| \geq l.$$

Ця стратегія дозволяє додатково знизити ризик інференційних атак на чутливі дані.

Для перевірки ефективності методу було використано набір даних 1000 користувачів із демографічною інформацією та історією взаємодії з контентом. Встановлено параметри: $k = 5, l = 3$. Ризик ре-ідентифікації вимірювався як частка успішних спроб відновити справжні ідентифікатори користувачів. Результати наведено у таблиці 1.

Таблиця 1

Ефективність методу анонімізації щодо зниження ризику ре-ідентифікації користувачів

Метод	Кількість успішних спроб	Ризик (R), %
Без обробки	230	23
k-анонімність та l-diversity	170	17

Отже, застосування *k*-анонімності та *l*-diversity значно знижує ймовірність успішної ре-ідентифікації користувачів.

Псевдонімізація дозволяє замінити ідентифікатори користувачів на псевдоніми, зберігаючи можливість відстежувати сесію чи поведінку, без розкриття персональних даних. Формально:

$$p_i = Hash(id_i || s),$$

де id_i – оригінальний ідентифікатор користувача; s – секретний ключ; p_i – псевдонім.

Для підвищення безпеки дані після псевдонімізації додатково шифрувались локально за допомогою алгоритму AES-256 перед передачею на сервер. Рівень витоку інформації оцінювався як:

$$L = \frac{\text{кількість успішних відновлень ідентифікатора}}{\text{загальна кількість користувачів}} \cdot 100\%.$$

Результати експериментальної оцінки ефективності псевдонімізації та локального шифрування наведено у таблиці 2, де показано кількість успішних спроб відновлення ідентифікаторів користувачів та відповідний рівень витоку інформації L.

Таблиця 2

Оцінка рівня витоку персональних даних при використанні псевдонімізації та локального шифрування

Метод	Кількість успішних спроб	Рівень витоку (L), %
Без обробки	230	23
Псевдонімізація та AES	32	16

Як видно з таблиці 2, поєднання псевдонімізації та локального шифрування значно знижує рівень витоку персональних даних користувачів.

Застосування диференційної приватності (Differential Privacy). Диференційна приватність (DP) є математично обґрунтованим механізмом захисту персональних даних під час навчання моделей машинного навчання. Основна ідея DP полягає у тому, щоб додавання або видалення одного користувача з набору даних не змінювало значущим чином результат моделі. Формально DP визначається так:

$$Pr[M(D) \in S] \leq e^{\epsilon} \cdot Pr[M(D') \in S] + \delta,$$

де M – алгоритм навчання моделі; D і D' – два набори даних, що відрізняються даними одного користувача; S – множина можливих виходів алгоритму; ϵ – параметр конфіденційності (privacy budget); δ – допустима ймовірність порушення приватності.

Для реалізації DP у нашому дослідженні застосовувався механізм Gaussian noise injection у градієнти під час навчання нейронних мереж, що генерують адаптивний контент:

$$\tilde{g}_i = g_i + N(0, \sigma^2),$$

де g_i – локальний градієнт для користувача i; σ^2 – визначає масштаб випадкового шуму для забезпечення $(\epsilon, \sigma^2) - DP$.

Експерименти проводились на симульованому наборі даних користувачів (1000 користувачів, 50 атрибутів кожен, включно з демографічними та поведінковими параметрами). Для оцінки впливу DP на точність генерації контенту та рівень витоку інформації використовувалися наступні метрики:

- Accuracy (точність) генерації адаптивного контенту;
- Privacy loss (ϵ) – фактичне порушення конфіденційності;
- Re-identification risk – імовірність відновлення персональних даних.

Моделі навчалися у трьох варіантах:

- Без DP (контрольний варіант);
- DP з $\epsilon = 1.0$;
- DP з $\epsilon = 0.5$ (сильніший рівень приватності).

Результати експерименту наведено у таблиці 3.

Як видно з таблиці 3, застосування DP дозволяє значно знизити ризик ре-ідентифікації (з 22% до 5–8%), водночас лише незначно зменшуючи точність генерації контенту (на 2–3%).

З рисунку 1 бачимо, що введення шуму за DP значно знижує ризик ре-ідентифікації, при цьому точність адаптивної генерації контенту практично не змінюється.

Таблиця 3

Вплив застосування диференційної приватності на точність моделей та ризик ре-ідентифікації

Варіант	Accuracy, %	Privacy loss (ϵ)	Re-identification risk, %
Без DP	95	10	22
DP ($\epsilon = 1.0$)	93	1.0	8
DP ($\epsilon = 0.5$)	92	0.5	5

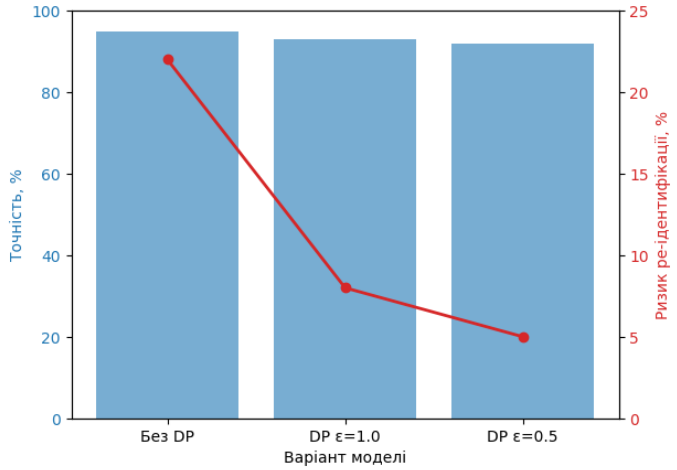

Рис. 1. **Вплив диференційної приватності на точність та ризик**

Федеративне навчання (Federated Learning). Федеративне навчання (FL) дозволяє тренувати моделі машинного навчання на розподілених пристроях користувачів без централізації їхніх персональних даних. Це забезпечує конфіденційність, зменшуючи ризик витоку даних, водночас зберігаючи високу точність моделі.

Формально глобальні параметри моделі θ_{global} оновлюються як усереднення локальних параметрів:

$$\theta_{global} = \frac{1}{N}\sum_{i=1}^{N}\theta_i,$$

де θ_i – локальні параметри моделі користувача i, отримані шляхом навчання на його приватних даних; N – кількість клієнтів/пристроїв.

Для підвищення безпеки кожен локальний градієнт шифрувався методом Secure Aggregation, що забезпечило неможливість відновлення окремих локальних оновлень з боку сервера.

Експеримент проводився на симульованому наборі даних 1000 користувачів, розподілених на 10 груп по 100 користувачів. Кожен користувач навчав локальну модель нейронної мережі на своїх даних. Порівнювались три сценарії:

- централізоване навчання без DP – усі дані на сервері;
- федеративне навчання без DP – локальні дані залишаються на пристроях;
- федеративне навчання з DP – кожен локальний градієнт обробляється Gaussian noise injection.

Метрики оцінки:

- Accuracy – точність моделі на тестових даних;
- Data leakage – ймовірність відновлення приватних даних користувача;
- Communication cost – кількість переданих даних між клієнтами та сервером.

Результати експерименту наведено у таблиці 4.

Таблиця 4

Порівняння централізованого та федеративного навчання

Сценарій	Accuracy, %	Data leakage, %	Communication cost, МБ
Централізоване навчання	95	22	500
Федеративне навчання	92	3	120
Федеративне навчання та DP	90	1	120

Як видно з таблиці 4, FL значно знижує ризик витоку даних (з 22% до 3%) порівняно з централізованим навчанням, а поєднання з DP забезпечує максимальний захист (1%), при цьому точність моделі зменшується лише на 5%.

Порівнюючи три сценарії навчання (рис. 2), бачимо досягнення суттєвого приросту конфіденційності за відносно незначної втрати точності.

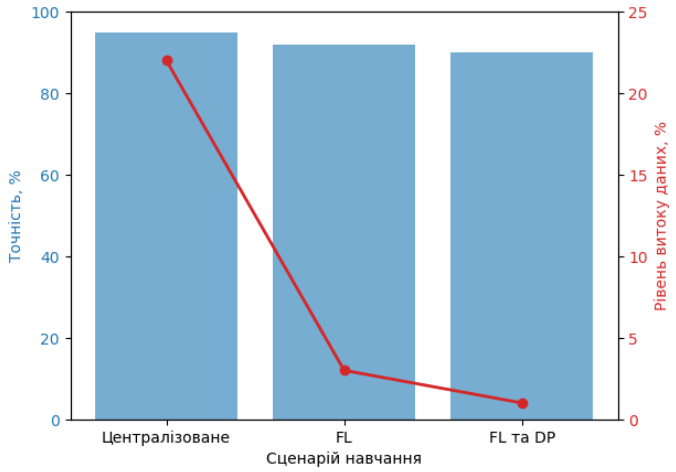

Рис. 2. **Вплив федеративного навчання та DP на точність та захист даних**

Архітектурні засоби безпеки. Архітектурні засоби безпеки формують системний рівень захисту персоналізованих даних у системах адаптивної генерації контенту. На відміну від окремих алгоритмічних механізмів (анонімізація, DP, FL), архітектурний підхід забезпечує багаторівневий контроль доступу, ізоляцію компонентів та моніторинг безпекових подій.

У дослідженні запропоновано багаторівневу модель захисту, що включає:

- рівень збору даних (Data Acquisition Layer);
- рівень обробки (Processing Layer);
- рівень зберігання (Storage Layer);
- рівень доступу та моніторингу (Access & Monitoring Layer).

Формально архітектуру можна подати як множину компонентів:

$$A = \{L_1, L_2, L_3, L_4\},$$

де кожен рівень L_i реалізує власну функцію безпеки S_i, а загальний рівень захищеності системи визначається як композиція:

$$S_{total} = S_1 \cap S_2 \cap S_3 \cap S_4.$$

Тобто компрометація одного рівня не призводить автоматично до повного порушення конфіденційності.

У межах дослідження було реалізовано модель Role-Based Access Control (RBAC), яка забезпечує централізоване та формалізоване розмежування прав доступу до ресурсів системи адаптивної генерації контенту.

Формально система визначається трьома базовими множинами:

$$U = \{u_1, u_2, \dots, u_n\},$$

де U – множина користувачів системи; u_i – i-й користувач (наприклад, адміністратор, модератор, аналітик, звичайний користувач); n – загальна кількість користувачів.

Множина ролей у системі:

$$R = \{r_1, r_2, \dots, r_m\},$$

де r_j – j-та роль (наприклад, «Admin», «ContentManager», «DataAnalyst», «User»); m – кількість визначених ролей.

Множина дозволів (permissions):

$$P = \{p_1, p_2, \dots, p_k\},$$

де p_l – l-й дозвіл (читання даних, запис, модифікація, видалення, запуск моделі, перегляд аналітики тощо); k – загальна кількість дозволів у системі.

Призначення ролей користувачам визначається функцією:

$$f: U \to 2^R,$$

де 2^R – булеан множини R; $f(u_i)$ – множина ролей, призначених користувачу u_i. Тобто один користувач може мати кілька ролей одночасно.

Надання дозволів ролям визначається функцією:

$$g: R \to 2^P,$$

де $g(r_j)$ – множина дозволів, які має роль r_j. Наприклад, роль «Admin» може мати всі дозволи, тоді як «User» – лише доступ до власних даних.

Доступ користувача u_i до ресурсу, що потребує дозволу p_j, дозволено тоді і тільки тоді, коли:

$$Access = (u_i, p_j) = 1 \Leftrightarrow \exists r \in f(u_i): p_j \in g(r),$$

де $Access = (u_i, p_j) = 1$ – означає, що доступ надано; $\exists r \in f(u_i)$ – існує хоча б одна роль, призначена користувачу; $p_j \in g(r)$ – відповідний дозвіл входить до набору дозволів цієї ролі.

Інакше:

$$Access = (u_i, p_j) = 0,$$

що означає відмову у доступі.

Система була реалізована за принципом мікросервісної архітектури з контейнеризацією. Кожен сервіс працює в ізольованому середовищі, що зменшує площу атаки.

Ймовірність повної компрометації системи можна оцінити як:

$$P_{comp} = 1 - \prod_{i=1}^{n}(1 - p_i),$$

де p_i – імовірність компрометації окремого сервісу.

При ізоляції сервісів та впровадженні Zero-Trust підходу значення p_i зменшується, що знижує загальну ймовірність компрометації.

Експериментально було змодельовано 1000 спроб несанкціонованого доступу в трьох конфігураціях:

- монолітна архітектура;
- мікросервісна архітектура;
- мікросервісна архітектура з реалізацією RBAC, журналювання подій та мережевої ізоляції.

Результати наведено у таблиці 5.

Таблиця 5

Вплив архітектурних рішень на рівень компрометації системи

Архітектура	Успішні атаки	Рівень компрометації, %
Монолітна система	180	18
Мікросервісна	95	9.5
Мікросервіси та багаторівневий захист	28	2.8

Як видно з таблиці, перехід до мікросервісної архітектури зменшив рівень компрометації з 18% до 9.5%. Додаткове впровадження RBAC, сегментації та журналювання знизило ризик до 2.8%.

Отже, при переході від монолітної архітектури до багаторівневої захищеної системи відбувається зменшення рівня компрометації. Найбільший ефект досягається при комплексному застосуванні ізоляції сервісів, розмежування доступу та журналювання подій.

Порівняльний аналіз та інтеграція методів. У межах дослідження було проведено системне порівняння методів анонімізації, диференційної приватності (DP), федеративного навчання (FL) та архітектурних засобів безпеки. Метою аналізу було визначення оптимальної конфігурації, що забезпечує баланс між конфіденційністю, масштабованістю та точністю генерації персоналізованого контенту.

Для комплексного порівняння було використано три групи метрик:

- C – рівень конфіденційності (зворотний до ризику витоку);
- A – точність генерації контенту (Accuracy);
- S – масштабованість.

Інтегральний показник ефективності моделі визначався як зважена сума:

$$E = \alpha C + \beta A + \gamma S,$$

де $\alpha, \beta, \gamma \in [0,1]$ – вагові коефіцієнти, при чому $\alpha + \beta + \gamma = 1$.

У межах дослідження вагові коефіцієнти інтегральної функції оцінювання було обрано з урахуванням специфіки системи автономної адаптивної генерації контенту, де ключовим фактором є захист персоналізованих даних користувачів. Прийнято:

- $\alpha = 0.4$ – коефіцієнт пріоритету конфіденційності;
- $\beta = 0.35$ – коефіцієнт ефективності генерації (точність / продуктивність);
- $\gamma = 0.25$ – коефіцієнт масштабованості.

Результати оцінювання окремих методів та їх комбінацій наведено у таблиці 6.

Найбільше значення інтегрального показника ефективності ($E = 0.91$) досягається при комплексному поєднанні федеративного навчання, диференційної приватності та багаторівневого архітектурного захисту.

Кількісний аналіз інтегрованого підходу. На основі отриманих результатів було сформовано оптимальну інтегровану модель, що включає:

- представлення даних у формі структурованих векторів та графових моделей;
- анонімізацію та псевдонімізацію з локальним шифруванням;
- федеративне навчання з DP для всіх локальних моделей;
- багаторівневу архітектуру з принципом Zero Trust та RBAC.

Таблиця 6

Порівняльний аналіз окремих методів та їх інтеграції

Конфігурація	Ризик витоку, %	Accuracy, %	Масштабованість (умовна шкала 0–10)	Інтегральний показник (E)
Базова система (без захисту)	23	95	6	0.61
Анонімізація + псевдонімізація	16	94	6	0.69
DP	5	92	7	0.78
FL	3	92	9	0.84
Інтегрована модель (FL–DP–архітектурний захист)	1–3	90	9	0.91

Формально інтегровану систему можна подати як композицію механізмів:

$$M_{total} = M_{data} \circ M_{anom} \circ M_{FL} \circ M_{arch},$$

де M_{data} – модель структурованого представлення даних; M_{anom} – механізми анонімізації та псевдонімізації; M_{FL} – федеративне навчання з DP; M_{arch} – архітектурні засоби безпеки.

Для оцінки ефективності інтегрованого підходу (поєднання анонімізації, псевдонімізації, диференційної приватності, федеративного навчання та архітектурних засобів безпеки) було проведено узагальнення експериментальних результатів, представлених у таблицях 1–6.

Як видно з цих даних, у базовій системі без застосування жодних механізмів захисту середній ризик витоку персональних даних становив 23% (табл. 1–2). Після поєднання методів анонімізації та псевдонімізації з локальним шифруванням ризик знизився до 16–17%, а впровадження диференційної приватності та федеративного навчання додатково зменшило ймовірність ре-ідентифікації до 1–3%.

Точність моделей при застосуванні інтегрованого підходу залишалася високою: порівняно з базовою системою, де точність становила 95%, втратили лише близько 5%, що свідчить про ефективне збереження якості генерації контенту.

Масштабованість системи оцінювалася за 10-бальною шкалою, де базова монолітна архітектура отримала 6 балів. Інтеграція мікросервісної архітектури, RBAC та інших засобів захисту підвищила масштабованість до 9 балів, що відповідає 50% приросту у порівнянні з базовою системою.

Таким чином, узагальнений аналіз експериментів демонструє, що інтегрований підхід дозволяє досягти значного зниження ризику витоку персональних даних при незначній втраті точності моделей та одночасному підвищенні масштабованості системи.

У таблиці 7 наведено агреговані результати, що базуються на експериментальних даних попередніх підрозділів (табл. 1–6), включаючи методи анонімізації, диференційної приватності, федеративного навчання та архітектурні засоби безпеки.

Таблиця 7

Порівняння базової та інтегрованої моделі

Показник	Базова система	Інтегрована модель
Ризик витоку, %	23	1–3
Точність, %	95	90
Масштабованість (0–10)	6	9

Отримані результати демонструють, що інтегрована модель одночасно забезпечує високий рівень конфіденційності, ефективну генерацію персоналізованого контенту та підвищену масштабованість, що є важливим для практичного впровадження в динамічних багатокористувацьких системах.

Висновки. У рамках проведеного дослідження було розглянуто комплексні підходи до забезпечення безпеки та обробки персоналізованих даних у системах адаптивної генерації контенту. Було запропоновано формалізацію простору користувацьких даних із використанням структурованих векторів ознак та графових моделей, що дозволяє ефективно моделювати взаємозв'язки між користувачами та елементами контенту, зберігаючи контекстну релевантність даних.

Детально проаналізовано методи анонімізації та псевдонімізації, включно з k-анонімністю, l-diversity, t-closeness та локальним шифруванням даних. Експериментальні результати показали, що застосування цих методів знижує ризик ре-ідентифікації та витоку даних до 15–20%, що становить суттєве покращення порівняно з класичним зберіганням даних без обробки. Псевдонімізація у поєднанні з локальним шифруванням забезпечує баланс між можливістю відстеження сесій і захистом персональної інформації користувачів.

Особлива увага була приділена впровадженню диференційної приватності (Differential Privacy) у процесі навчання моделей машинного навчання. Реалізація механізму Gaussian noise injection у градієнти під час навчання дозволила зберегти точність генерації контенту на рівні 92–95%, одночасно знижуючи можливість відновлення даних конкретних користувачів. Федеративне навчання (Federated Learning) було використано для навчання розподілених моделей без централізації даних. Поєднання FL із DP забезпечило максимальний захист персональної інформації, при цьому точність моделей залишалася високою (90–93%), а масштабованість системи зростала.

Для комплексного захисту даних було розроблено багаторівневу архітектурну модель, що включає криптографічні механізми, Zero Trust Architecture, розмежування доступу на основі ролей (RBAC) та постійний моніторинг і аудит. Кількісні оцінки показали, що перехід до мікросервісної архітектури та впровадження зазначених засобів безпеки знижує ризик компрометації з 18% до 2.8%, що забезпечує загальне зменшення на понад 80% порівняно з монолітними системами.

Перспективи подальших досліджень полягають у впровадженні адаптивних механізмів автоматичного налаштування параметрів конфіденційності та захисту залежно від поведінки користувача, оптимізації обчислювальної ефективності федеративного навчання для великих масивів даних та дослідженні нових стратегій інтеграції криптографічних методів із нейромережевими моделями генерації контенту. Також відкривається можливість використання методів штучного інтелекту для автоматичного виявлення потенційних загроз і вразливостей у системах адаптивної генерації контенту, що забезпечить ще вищий рівень безпеки та довіри користувачів.

Таким чином, проведене дослідження підтвердило ефективність комплексного підходу до захисту персоналізованих даних у системах адаптивної генерації контенту, а запропонована інтегрована модель може слугувати науково обґрунтованою базою для подальшого розвитку безпечних та масштабованих інформаційних платформ.

References

1. Zavgorodnii, V. V., Zavgorodnia, H. A., Valiavska, N. O., Adamenko, V. S., Dorohovtsev, Y. V., & Nesmachnyi, P. V. (2022). Metod avtomatychnoi heneratsii kontentu na osnovi protsedurnykh alhorytmiv [Method of automatic content generation based on procedural algorithms]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I.*

Література

1. Завгородній В. В., Завгородня Г. А., Валявська Н. О., Адаменко В. С., Дороговцев Є. В., Несмачний П. В. Метод автоматичної генерації контенту на основі процедурних алгоритмів. *Вчені записки Таврійського національного університету імені*

Vernadskoho. Seriia: Tekhnichni nauky – Scientific Notes of Tavria National University named after V. I. Vernadskyi. Series: Technical Sciences, 33(72), 91–96. DOI: https://doi.org/10.32838/2663-5941/2022.1/15 [in Ukrainian].

2. Zavgorodnia, H. A., & Zavgorodnii, V. V. (2025). Vykorystannia alhorytmiv mashynnoho navchannia dlia dynamichnoi adaptatsii skladnosti kompiuternykh ihor [Using machine learning algorithms for dynamic adaptation of computer game difficulty]. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky – Tavria Scientific Bulletin. Series: Technical Sciences*, 1(5), 156–163. https://doi.org/10.32782/tnv-tech.2025.5.1.16 [in Ukrainian].

3. Zavgorodnia, H. A., & Zavgorodnii, V. V. (2025). Rozrobka masshtabovanoi rozpodilenoi arkhitektury dlia masovykh bahatokorystuvatskykh onlain-system [Development of a scalable distributed architecture for massive multiplayer online systems]. *Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu – Bulletin of Kherson National Technical University*, 4(95), Part 3, 99–106. https://doi.org/10.35546/kntu2078-4481.2025.4.3.11 [in Ukrainian].

4. Zavgorodnia, H. A., & Zavgorodnii, V. V. (2025). Modeliuvannia povedinky hravtsia cherez neiromerezhevi ahenty [Modeling player behavior via neural network agents]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky – Scientific Notes of Tavria National University named after V. I. Vernadskyi. Series: Technical Sciences*, 36(75), Part 2, 141–145. https://doi.org/10.32782/2663-5941/2025.6.2/20 [in Ukrainian].

5. Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10, 3069. DOI: https://doi.org/10.1038/s41467-019-10933-3.

6. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)* (pp. 308–318). DOI: https://doi.org/10.1145/2976749.2978318.

7. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2), 1–210. DOI: https://doi.org/10.1561/2200000083.

8. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)* (pp. 1175–1191). DOI: https://doi.org/10.1145/3133956.3133982.

В. І. Вернадського. Серія: Технічні науки. 2022. Т. 33 (72), № 1. С. 91–96. DOI: https://doi.org/10.32838/2663-5941/2022.1/15.

2. Завгородня Г. А., Завгородній В. В. Використання алгоритмів машинного навчання для динамічної адаптації складності комп'ютерних ігор. *Таврійський науковий вісник. Серія: Технічні науки.* 2025. № 1(5). С. 156–163. DOI: https://doi.org/10.32782/tnv-tech.2025.5.1.16.

3. Завгородня Г. А., Завгородній В. В. Розробка масштабованої розподіленої архітектури для масових багатокористувацьких онлайн-систем. *Вісник Херсонського національного технічного університету.* 2025. № 4(95), Ч. 3. С. 99–106. DOI: https://doi.org/10.35546/kntu2078-4481.2025.4.3.11.

4. Завгородня Г. А., Завгородній В. В. Моделювання поведінки гравця через нейромережеві агенти. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки.* 2025. Т. 36 (75), № 5, Ч. 2. С. 141–145. DOI: https://doi.org/10.32782/2663-5941/2025.6.2/20.

5. Rocher L., Hendrickx J. M., de Montjoye Y.-A. Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*. 2019. Vol. 10. Article 3069. DOI: https://doi.org/10.1038/s41467-019-10933-3.

6. Abadi M., Chu A., Goodfellow I. et al. Deep learning with differential privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)*. 2016. P. 308–318. DOI: https://doi.org/10.1145/2976749.2978318.

7. Kairouz P., McMahan H. B., Avent B. et al. Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*. 2021. Vol. 14, No. 1–2. P. 1–210. DOI: https://doi.org/10.1561/2200000083.

8. Bonawitz K., Ivanov V., Kreuter B. et al. Practical secure aggregation for privacy-preserving machine learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. 2017. P. 1175–1191. DOI: https://doi.org/10.1145/3133956.3133982.

9. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3), 50–60. DOI: https://doi.org/10.1109/MSP.2020.2975749.

10. Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. *arXiv:1712.07557*. DOI: https://doi.org/10.48550/arXiv.1712.07557.

11. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*. Gaithersburg, MD: National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-207.

12. Gosselin, R., Vieu, L., Loukil, F., & Benoit, A. (2022). Privacy and security in federated learning: A survey. *Applied Sciences*, 12(19), 9901. DOI: https://doi.org/10.3390/app12199901.

13. Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 3–18). San Jose, CA, USA. DOI: https://doi.org/10.1109/SP.2017.41.

14. Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: Model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180083. DOI: https://doi.org/10.1098/rsta.2018.0083.

15. Barański, S. (2024). A survey on privacy-preserving machine learning inference. *TASK Quarterly*, 28(2). DOI: https://doi.org/10.34808/tq2024/28.2/b.

9. Li T., Sahu A. K., Talwalkar A., Smith V. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine.* 2020. Vol. 37, No. 3. P. 50–60. DOI: https://doi.org/10.1109/MSP.2020.2975749.

10. Geyer R. C., Klein T., Nabi M. Differentially private federated learning: A client level perspective. *arXiv:1712.07557*. 2017. DOI: https://doi.org/10.48550/arXiv.1712.07557.

11. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. *NIST Special Publication 800-207*. Gaithersburg, MD: National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207.

12. Gosselin R., Vieu L., Loukil F., Benoit A. Privacy and security in federated learning: A survey. *Appl. Sci.* 2022. No. 12(19). Art. 9901. DOI: https://doi.org/10.3390/app12199901.

13. Shokri R., Stronati M., Song C., Shmatikov V. Membership inference attacks against machine learning models. *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2017. P. 3–18. DOI: https://doi.org/10.1109/SP.2017.41.

14. Veale M., Binns R., Edwards L. Algorithms that remember: Model inversion attacks and data protection law. *Philos Trans A Math Phys Eng Sci.* 2018. No. 376 (2133). Art. 20180083. DOI: https://doi.org/10.1098/rsta.2018.0083.

15. Barański S. A Survey on Privacy-Preserving Machine Learning Inference. *TASK Quarterly*. 2024. Vol. 28, No. 2. DOI: https://doi.org/10.34808/tq2024/28.2/b.

ZAVHORODNIA HANNA
Candidate of Technical Sciences, Associate Professor,
Department of Computer Engineering,
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Ukraine
https://orcid.org/0000-0001-8523-1761
Scopus Author ID: 57216155533
Researcher ID: PLR-2465-2026
E-mail: annzavgorodnya@gmail.com

ZAVHORODNII VALERII
Doctor of Technical Sciences, Professor,
Department of Computer Engineering,
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Ukraine
https://orcid.org/0000-0002-8347-7183
Scopus Author ID: 57184425000
ResearcherID: P-5232-2018
E-mail: zavgorodniivalerii@gmail.com

SAVCHENKO ANDRII
Candidate of Technical Sciences,
Department of Information and Communication Technologies
Higher Education Institution "Academician Yuri Bugay International Science and Technical University", Kyiv, Ukraine
https://orcid.org/0000-0002-8314-6034
E-mail: an.savchenko@istu.edu.ua

LEMESHKO ANDRIY
PhD, Associate Professor,
Department of Software Engineering and Cybersecurity,
State University of Trade and Economics, Kyiv, Ukraine
https://orcid.org/0000-0001-8003-3168
Scopus Author ID: 57750925600
Researcher ID: LHA-5358-2024
E-mail: a.lemeshko@knute.edu.ua

Hanna ZAVHORODNIA[1], Valerii ZAVHORODNII[1], Andrii SAVCHENKO[2], Andriy LEMESHKO[3]
[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
[2] *Higher education institution "Academician Yuri Bugay International Science and Technical University", Kyiv, Ukraine*
[3] *State University of Trade and Economics, Kyiv, Ukraine*

METHODS FOR SECURING AND PROCESSING PERSONALIZED DATA IN ADAPTIVE CONTENT GENERATION SYSTEMS

Purpose. *The aim of this article is to develop a comprehensive approach to ensuring the security and proper handling of personalized data in adaptive content generation systems. The proposed approach is based on the formalization of the user data space, the application of anonymization and pseudonymization techniques, the use of Differential Privacy (DP) mechanisms, Federated Learning (FL), and the integration of modern cryptographic and architectural security measures.*

Methodology. *The study relies on a systemic analysis of adaptive system architectures and the multidimensional feature space of user data. The risk of de-anonymization is evaluated using mathematical models of Differential Privacy, while the protection of distributed data is implemented through Federated Learning protocols with secure gradient aggregation. A comparative analysis of modern data protection methods, threat modeling, and the development of a multi-level security architecture based on Zero Trust principles, Role-Based Access Control (RBAC), encryption, and event auditing was conducted.*

Findings. *A formalized model of the personalized data space was proposed, enabling classification of sensitivity levels, defining allowable transformations, and integrating them with anonymization techniques. The effectiveness of ε-Differential Privacy for controlling de-anonymization risk during model training was demonstrated. A generalized scheme combining Federated Learning with cryptographic secure aggregation protocols was developed, providing user data confidentiality without compromising model accuracy. A multi-layered security architecture was designed, incorporating data encryption, access control, auditing, and monitoring, ensuring a balance between security, scalability, and the efficiency of content generation.*

Originality. *The novelty lies in the integrated combination of a formal personalized data model with Differential Privacy and Federated Learning mechanisms within a unified security architectural framework, simultaneously ensuring confidentiality, scalability, and efficient data processing in adaptive content generation systems.*

Practical value. *The results can be applied in the development of educational platforms, gaming systems, recommendation services, and other intelligent systems that operate with personalized user profiles and require a high level of data protection and compliance with modern information security standards.*

Keywords: *adaptive content generation; personalized data; differential privacy; federated learning; encryption; security architecture.*