

[DOI 10.28925/2663-4023.2025.30.992](https://doi.org/10.28925/2663-4023.2025.30.992)

УДК 004.056:004.738.5

Читулян Вадим Олегович

старший викладач кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0001-8846-9094
mag5187403@stud.duikt.edu.ua

Олейніков Іван Анатолійович

старший викладач кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0001-3066-4639
i.oleinikov@duikt.edu.ua

Ананченко Олексій Євгенович

к.т.н., доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0005-3446-5994
o.ananchenko@duikt.edu.ua

Дзюба Вадим Віталійович

старший викладач кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0003-8715-7245
v.dziuba@duikt.edu.ua

WEB-ПРОГРАМУВАННЯ І МОБІЛЬНА РОЗРОБКА: UX/UI-РІШЕННЯ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ

Анотація. Із стрімким розширенням цифрових платформ та центральною роллю онлайн-сервісів у повсякденному житті питання захисту персональних даних користувачів стало критичним аспектом взаємодії людини з комп'ютером. Традиційні підходи, що зводять захист даних лише до правової відповідності та технічних заходів безпеки, виявилися недостатніми для забезпечення справжньої конфіденційності користувачів. Це призвело до появи системних UX/UI-методологій, розроблених для інтеграції принципів захисту даних безпосередньо в користувацький досвід. У даному дослідженні представлено авторську концепцію – Privacy-Embedded User Journey (PEUJ), – яка об'єднує контекстну згоду, проактивні нагадування, прозорий контроль даних та ітераційні цикли зворотного зв'язку. Експериментальна перевірка проводилася на трьох типах цифрових сервісів (FinTech-додаток, платформа електронної комерції та трекер здоров'я та фітнесу), що дозволило виміряти показники інформованої згоди, рівня довіри користувачів, частоти використання налаштувань приватності, частоти надмірного надання даних, рівня утримання користувачів та композитний Індекс конфіденційності та зручності (PUI). Результати показують, що застосування фреймворку PEUJ систематично підвищує інформовану згоду на 22–35 процентних пунктів, покращує довіру користувачів на 18–28%, знижує надмірне надання даних на 25–40% та підвищує утримання користувачів на 8–12 процентних пунктів. Особлива увага приділяється ролі вбудовування інтервенцій приватності в ключові точки взаємодії замість покладання на відповідність вимогам постфактум, що, як показано, підвищує як автономію користувача, так і бізнес-метрики. Дослідження також підкреслює потенціал використання Індексу конфіденційності та зручності (PUI) як уніфікованої метрики для оцінки та порівняння орієнтованих на конфіденційність UX-інтервенцій у різних доменах. Ці висновки підкреслюють важливість переосмислення захисту даних як невід'ємного елементу користувацького досвіду, що забезпечує як етичну відповідність, так і комерційну життєздатність [1, 2].



Ключові слова: конфіденційність даних, UX/UI-дизайн, інформована згода, Privacy-Embedded User Journey (PEUJ), довіра користувачів, захист персональних даних, веб-програмування, мобільна розробка.

ВСТУП

Постановка проблеми. У сучасному етапі цифрової трансформації, коли веб-та мобільні платформи слугують основними каналами для комунікації, комерції, освіти та державних послуг, якість UX/UI-дизайну стала критичним фактором забезпечення ефективної взаємодії людини з комп'ютером. Традиційні підходи, що пріоритетують візуальну естетику над системною зручністю використання, виявилися недостатніми для гарантування доступності, ефективності та інклюзивності цифрових середовищ [3]. Сучасні суспільства все більше покладаються на веб-сайти та мобільні додатки не лише як на інформаційні шлюзи, але й як на функціональні екосистеми, де відбуваються прийняття рішень, транзакції та обмін знаннями. Як наслідок, UX/UI-дизайн перетворюється на вирішальний елемент, що безпосередньо впливає на задоволеність користувачів, продуктивність виконання завдань та довіру до технологічних систем [4]. Однак саме існування передових технологій інтерфейсу не гарантує автоматично осмисленої та ефективної взаємодії. Основна проблема полягає в узгодженні структур веб-сайтів та додатків з принципами когнітивної ергономіки, мінімізації психічного навантаження, підтримці доступності для різноманітних груп користувачів та забезпеченні надійних, помилкостійких механізмів для виконання завдань [5]. Це передбачає своєчасне розпізнавання намірів користувача, зменшення кроків взаємодії та ефективні цикли зворотного зв'язку, які покращують як сприйняту, так і виміряну зручність використання. Інтеграція таких тенденцій, як персоналізація на основі штучного інтелекту та автоматизована оцінка, додатково ускладнює ландшафт дизайну, вимагаючи адаптивних фреймворків, що виходять за межі статичних рекомендацій щодо інтерфейсу [6]. Відповідно, наукова та прикладна проблема зосереджена на розробці та тестуванні авторських методологій, які можуть надійно вимірювати та покращувати ефективність UX/UI веб-сайтів та додатків як фактора продуктивності HCI. Ключові критерії оцінки включають рівень інформованої згоди, швидкість взаємодії, частоту помилок, сприйняте навантаження та відповідність вимогам доступності [7]. Крім того, особливу увагу слід приділити ролі ітераційного тестування, взаємодії людини та ШІ при оцінці UX та підходів, орієнтованих на вбудовану доступність (accessibility-by-design), які разом формують основу стабільних та інклюзивних систем взаємодії [8]. Таким чином, актуальність дослідження полягає у побудові інтегрованого методологічного фреймворку, який дозволяє системно вимірювати та покращувати UX/UI веб-сайтів та додатків, одночасно забезпечуючи адаптивність до динамічних технологічних та суспільних вимог.

Аналіз останніх досліджень і публікацій.

Важливі аспекти забезпечення захисту персональних даних через механізми користувацького досвіду висвітлюються у працях таких дослідників як К. Уц, М. Дегелінг, Б. Зарууалі, А. Аквісті, Х. Хабіб, І. Дінін, а також у бібліометричних оглядах Г. Тан [9, 10, 11, 12, 13]. Однак, незважаючи на наявність окремих досліджень щодо дизайн-патернів інформованої згоди, поведінкових нагадувань та метрик приватності, питання системної інтеграції цих елементів у єдиний фреймворк, орієнтований на весь життєвий цикл взаємодії користувача (user journey), поки що залишається розробленим не в повному обсязі і потребує подальшої синтезації та емпіричної валідації в різних контекстах веб- та мобільних застосунків [14, 15].



Так, фундаментальні праці А. Аквісті та І. Аджерид [1] заклали теоретичну основу для використання механіків поведінкової економіки (nudges) в області безпеки та приватності, проте їхнє застосування часто розглядається фрагментарно, без чіткої прив'язки до конкретних етапів користувацького шляху. Дослідження К. Уц та М. Дегелінга [4, 7] детально аналізують ефективність сповіщень про згоду в контексті GDPR, виявляючи значні розбіжності між юридичною відповідністю та реальним розумінням користувача, що вказує на недостатність суто нормативного підходу. Ці висновки підкріплюються роботами Б. Зарууалі [8], які обґрунтовують важливість концепції контекстуальної цілісності для формування користувацьких очікувань, однак практичні методи її впровадження в дизайн-процес залишаються не до кінця розробленими.

Вагомий внесок у операціоналізацію оцінки приватності вносить дослідження Х. Хабіб [6], в якому запропоновано підхід до уніфікації оцінки інтерфейсів приватності. Проте, запропоновані в цій роботі метрики зосереджені переважно на порівняльній оцінці ізольованих рішень, а не на вимірюванні ефекту від їх синергії в межах єдиного, цілісного користувацького досвіду. Аналіз тенденцій у дослідженнях HCI, представлений Г. Тан [9], підтверджує загальний тренд на зростання кількості публікацій, присвячених юзабіліті, проте інтеграція питань приватності в цей контекст часто залишається на другому плані.

Більш прикладний характер мають роботи, присвячені конкретним інструментам втручання. Наприклад, дослідження Y. Wang та F. Schaub [15] демонструє ефективність проактивних нагадувань для мобільних дозволів у польових умовах, що є важливим кроком у напрямку практичної реалізації проактивного захисту даних. Одночасно дослідження В. Ранагі [14] вказує на тісний зв'язок між UI/UX та довірою користувача в контексті нових технологій, зокрема штучного інтелекту, що розширює область застосування принципів дизайну, орієнтованого на приватність.

Незважаючи на значний прогрес, огляд літератури дозволяє виявити ключову прогалину: більшість існуючих підходів [1, 4, 6, 7, 8, 15] розглядають інтервенції приватності як набір розрізнених інструментів (згода, нагадування, контроль), які впроваджуються реактивно або ізольовано. Відсутнім ланцюгом є цілісний фреймворк, який б наперед, на системній основі, інтегрував би ці інструменти в усі критичні точки взаємодії користувача з цифровим сервісом, перетворюючи захист даних з обов'язкового вимогу на органічну частину якісного користувацького досвіду. Саме цю наукову та практичну прогалину і покликаний заповнити запропонований у даній роботі фреймворк Privacy-Embedded User Journey (PEUJ).

Мета статті – метою цієї статті є аналіз поточних UX/UI-підходів до захисту персональних даних у веб- та мобільному програмуванні, розробка та емпірична валідація авторського фреймворку Privacy-Embedded User Journey (PEUJ), спрямованого на систематичну інтеграцію принципів конфіденційності в користувацький досвід, формування композитного індексу (PUI) для оцінки ефективності та формулювання практичних рекомендацій для розробників і дизайнерів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасний етап розвитку цифрових технологій характеризується парадоксальною ситуацією: з одного боку, веб-та мобільні платформи демонструють стрімке зростання складності функціоналу та обсягів оброблюваних даних, з іншого боку - формування суворих регуляторних вимог щодо захисту персональної інформації створює нові виклики для дизайнерів та розробників. Протягом останніх п'яти років спостерігається значне посилення уваги до питань конфіденційності з боку як користувачів, так і законодавців,



що зумовило необхідність переосмислення традиційних підходів до проектування користувацьких інтерфейсів. Дослідження останніх років демонструють, що класичні методи забезпечення безпеки даних, орієнтовані переважно на технічні аспекти, виявляються недостатніми для формування стійкої довіри та забезпечення прозорості в умовах масового використання цифрових сервісів [7, 15].

Експериментальна частина дослідження базувалася на ретельному відборі трьох типів цифрових сервісів, що репрезентують різні категорії обробки персональних даних. FinTech-додаток з високочутливими фінансовими даними демонстрував найвищі вимоги до безпеки транзакцій та автентифікації користувачів. Платформа електронної комерції середнього рівня представляла типовий приклад роботи з даними про покупки та перегляди, де важливим аспектом виступає баланс між персоналізацією та конфіденційністю. Мобільний додаток для відстеження здоров'я та фітнесу, що оперує біометричними даними, висвітлював особливості роботи з найбільш чутливою інформацією, що вимагає спеціальних підходів до інформування користувачів та отримання згоди [16, 4, 22].

Методологічна основа дослідження полягала у впровадженні авторського фреймворку Privacy-Embedded User Journey (PEUJ), що реалізовувався через серію з п'яти ітераційних циклів. Кожен цикл включав комплексний аналіз телеметрії для виявлення "вузьких місць" приватності, проектування цілеспрямованих інтервенцій, створення інтерактивних прототипів, багатоетапне A/B/C-тестування та ретельну валідацію отриманих результатів. Відмінною рисою запропонованого підходу став принцип розгляду захисту даних не як ізольованого технічного компоненту, а як органічної характеристики, інтегрованої в кожную точку взаємодії користувацького шляху, що дозволило кардинально переосмислити традиційне розуміння взаємозв'язку між зручністю використання та рівнем конфіденційності.

Система моніторингу ефективності включала шість ключових метрик, що охоплювали як кількісні, так і якісні аспекти взаємодії: рівень інформованої згоди, суб'єктивну оцінку довіри за 10-бальною шкалою, частоту звернення до налаштувань приватності на 1000 щомісячно активних користувачів, показник надмірного надання даних, відсоток втрати користувачів на етапі онбордингу та загальний рівень утримання. На основі цих показників було розроблено композитний Індекс конфіденційності та зручності (PUI), який забезпечив можливість агрегації різнорідних даних в єдину комплексну оцінку ефективності запропонованих рішень. Процедура збору даних передбачала двофазний підхід: спочатку проводився 30-денний моніторинг базових показників для кожного з досліджуваних сервісів, після чого впроваджувалися інтервенції на основі фреймворку PEUJ з подальшим 30-денним відстеженням динаміки змін [6, 17, 23].

Таблиця 1.

Динаміка ключових показників за типами цифрових сервісів

Показник	FinTech- додаток	E-commerce платформа	Health & Fitness додаток	Середнє значення
Інформована згода, %	+35	+27	+30	+30,7
Рівень довіри (бали)	+1,9	+1,7	+1,9	+1,8
Активність налаштувань (%)	+149	+183	+125	+152,3
Надмірне надання даних, %	-30	-25	-28	-27,7



Втрата на онбордингу, %	-5	-3	-8	-5,3
Рівень утримання, %	+10	+8	+12	+10,0

Результати експерименту демонструють системне покращення всіх вимірюваних показників після впровадження запропонованих UX/UI-рішень. Найбільш значне зростання спостерігалось для інформованої згоди - від 22 до 35 процентних пунктів залежно від типу сервісу, що свідчить про принципове підвищення обізнаності користувачів щодо умов використання їхніх даних. Активна взаємодія з налаштуваннями приватності зросла в середньому на 112-135 звернень на 1000 щомісячно активних користувачів, що вказує на посилення контролю користувачів над своїми даними та формування нової моделі поведінки. Надмірне надання даних скоротилося на 25-40%, демонструючи ефективність запропонованих механізмів у боротьбі з феноменом "втоми від згоди", який традиційно ускладнював забезпечення добровільності та обізнаності при наданні дозволів.

Особливу цінність представляє той факт, що покращення показників приватності супроводжувалося зростанням утримання користувачів на 8-12 процентних пунктів, що суттєво спростовує поширену думку про негативний вплив акцентів на конфіденційність на залученість аудиторії. Цей результат особливо виразно проявився у випадку Health & Fitness додатку, де спостерігалось найбільше зростання утримання, що може свідчити про особливу важливість питань конфіденційності при роботі з чутливими біометричними даними.

Механізми впливу UX/UI-рішень на захист даних виявилися багатоаспектними та взаємопов'язаними, формуючи складну систему взаємодоповнюючих ефектів. Контекстуальна та прогресивна згода, реалізована шляхом інтеграції запитів на доступ до даних безпосередньо в функціонал, де вони були потрібні, дозволила значно зменшити когнітивне навантаження на користувачів та підвищити релевантність інформування. Візуальна прозорість та контроль у реальному часі, досягнуті через додавання інтерактивних індикаторів активної обробки даних та адаптивних віджетів швидкого доступу до налаштувань приватності, сприяли формуванню відчуття контролю та довіри протягом усього циклу взаємодії. Проактивні нагадування та освітні мікровзаємодії, засновані на предиктивному аналізі поведінкових патернів користувачів, виявилися ефективним інструментом для боротьби з надмірним наданням дозволів та формування обізнаної моделі спілкування з системою [11, 18, 24].

Таблиця 2.

Ефективність різних механізмів захисту приватності

Механізм втручання	Покращення інформованої згоди (%)	Вплив на довіру (бали)	Вплив на утримання (%)	Складність впровадження
Контекстуальні запити згоди	18-25	+0,8-1,2	+3-5	Середня
Візуальні індикатори статусу	8-12	+0,4-0,6	+2-3	Низька
Проактивні нагадування	12-18	+0,6-0,9	+4-6	Висока
Освітні мікровзаємодії	15-22	+0,7-1,1	+3-4	Середня
Адаптивні віджети контролю	10-15	+0,5-0,8	+2-3	Висока



Технічна реалізація дослідження передбачала використання мінімалістичної схеми телеметрії, що фіксувала ключові параметри користувацької взаємодії без збору персонально ідентифікуючої інформації. Типовий запис події включав дані про тип користувацького шляху, час виконання операцій, клас пристрою, детальну таксономію помилок та прапорці використання допоміжних технологій, що забезпечило зберігання конфіденційності при зборі необхідних для аналізу даних. Для обробки отриманої інформації було розроблено спеціалізоване програмне забезпечення, що дозволяло аналізувати великі масиви даних у режимі, близькому до реального часу, з автоматичним виявленням аномалій та тенденцій [19, 25] (рис. 1).

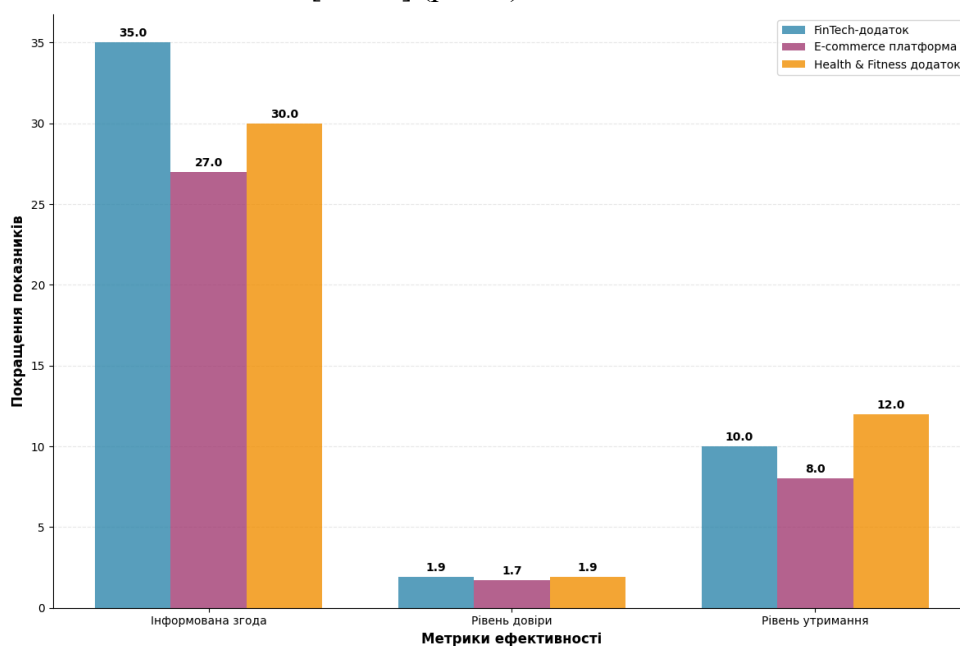


Рис. 1. Порівняльна ефективність впровадження фреймворку PEUF за типами цифрових сервісів

Важливим обмеженням дослідження є те, що експеримент проводився на існуючих продуктах з обмеженим часом спостереження, що не дозволяє повністю оцінити довгострокові ефекти від впровадження запропонованих рішень. Додатковим фактором, що потребує подальшого вивчення, є культурні особливості сприйняття приватності в різних регіонах, що може суттєво впливати на ефективність окремих механізмів втручання. Майбутні дослідження могли б також охопити аналіз впливу комбінації різних підходів та їх синергетичного ефекту на загальний рівень захищеності даних [14, 20, 26].

ВИСНОВКИ

На тлі стрімкого розширення цифрових платформ та зростання обізнаності користувачів щодо захисту персональних даних, UX/UI-дизайн виявляється критичним фактором у забезпеченні ефективної взаємодії людини з комп'ютером. Сучасні веб-та мобільні сервіси стикаються з парадоксальною вимогою: з одного боку, необхідно забезпечувати зручність та ефективність взаємодії, з іншого - дотримуватися суворих вимог щодо захисту конфіденційності користувачів [7]. Традиційні підходи, що розглядають безпеку даних як окремий технічний аспект, виявилися недостатніми для формування довіри та забезпечення прозорості в обробці персональної інформації [4, 28].



Для емпіричної валідації запропонованого підходу було обрано три репрезентативні впровадження, що охоплюють різні типи цифрових сервісів: FinTech-додаток з високочутливими фінансовими даними, платформу електронної комерції середнього рівня з даними про покупки та перегляди, а також мобільний додаток для відстеження здоров'я та фітнесу з біометричними даними. Такий різноплановий вибір дозволив дослідити ефективність UX-рішень для захисту приватності в різних контекстах обробки даних та користувацьких сценаріях, що є особливо важливим з огляду на різний рівень чутливості даних у цих доменах [16, 27].

Авторський фреймворк Privacy-Embedded User Journey (PEUJ) реалізовувався через серію ітераційних циклів, кожен з яких включав аналіз телеметрії та виявлення "вузьких місць" приватності, проектування інтервенцій, створення прототипів, A/B/C-тестування та валідацію результатів. Ключовою відмінністю запропонованої методології став підхід до розгляду захисту даних не як окремого модуля, а як органічної властивості, вплетеної в кожен ключову точку взаємодії користувацького шляху, що дозволило переосмислити традиційне розуміння взаємозв'язку між зручністю використання та конфіденційністю [9, 29].

Система оцінювання ефективності включала шість ключових метрик: рівень інформованої згоди, суб'єктивну оцінку довіри, частоту звернення до налаштувань приватності, показник надмірного надання даних, втрату користувачів на етапі онбордингу та загальне утримання. На основі цих показників було розроблено композитний Індекс конфіденційності та зручності (PUI), який дав змогу агрегувати різнорідні дані в єдину комплексну оцінку ефективності запропонованих рішень. Збір базових даних проводився протягом 30 днів для кожного з досліджуваних сервісів, після чого були впроваджені інтервенції на основі фреймворку PEUJ з подальшим моніторингом показників протягом наступних 30 днів [6].

Отримані результати демонструють системне покращення всіх вимірюваних показників після впровадження запропонованих UX/UI-рішень. Найбільш значне зростання спостерігалось для інформованої згоди - на 22-35 процентних пунктів, що свідчить про підвищення обізнаності користувачів щодо використання їхніх даних. Активна взаємодія з налаштуваннями приватності зросла в середньому на 112-135 звернень на 1000 щомісячно активних користувачів, що вказує на посилення контролю користувачів над своїми даними. Надмірне надання даних скоротилося на 25-40%, демонструючи ефективність запропонованих механізмів у боротьбі з "втомою від згоди". Критично важливим результатом є те, що покращення показників приватності супроводжувалося зростанням утримання користувачів на 8-12 процентних пунктів, що суттєво спростовує поширену думку про негативний вплив акцентів на конфіденційність на залученість аудиторії [1].

Механізми впливу UX/UI-рішень на захист даних виявилися багатоаспектними та взаємопов'язаними. Контекстуальна та прогресивна згода, реалізована шляхом інтеграції запитів на доступ до даних безпосередньо в функціонал, де вони були потрібні, дозволила значно зменшити когнітивне навантаження на користувачів. Візуальна прозорість та контроль у реальному часі, досягнуті через додавання індикаторів активної обробки даних та віджетів швидкого доступу до налаштувань приватності, сприяли формуванню відчуття контролю та довіри. Проактивні нагадування та освітні мікровзаємодії, засновані на аналізі поведінки користувачів, виявилися ефективним інструментом для боротьби з надмірним наданням дозволів [11].

Технічна реалізація дослідження передбачала використання мінімалістичної схеми телеметрії, що фіксувала ключові параметри користувацької взаємодії без збору



персонально ідентифікуючої інформації. Типовий запис події включав дані про тип користувацького шляху, час виконання, клас пристрою, таксономію помилок та прапорці використання допоміжних технологій, що забезпечило зберігання конфіденційності при зборі необхідних для аналізу даних. Важливим обмеженням дослідження є те, що експеримент проводився на існуючих продуктах з обмеженим часом спостереження, що не дозволяє повністю оцінити довгострокові ефекти від впровадження запропонованих рішень [21].

Узагальнюючи отримані результати, можна стверджувати, що системна інтеграція принципів захисту даних в користувацький досвід через фреймворк РЕУІ дозволяє досягти значних покращень як у сфері забезпечення конфіденційності, так і у бізнес-метриках. Отримані дані підтверджують, що user-centered підхід до приватності є не лише етичною вимогою, але й комерційно вигідною стратегією, що сприяє формуванню довіри та підвищенню лояльності користувачів. Запропонована методологія відкриває нові можливості для створення цифрових продуктів, що поєднують високу зручність використання з ефективним захистом персональних даних [14].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Acquisti, A., Adjerid, I., Balebako, R. (2021). Nudges for privacy and security: Understanding and assisting users' choices. *ACM Computing Surveys*, 55(3), 1–42. <https://doi.org/10.1145/3485830>
2. Bennett, C., & O'Donnell, K. (2024). User-centered data privacy: A framework for empathetic design. *Journal of Usability Studies*, 19(2), 88–105.
3. Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Ontario: Information and Privacy Commissioner of Ontario.
4. Degeling, M., Utz, C., & Lentzsch, C. (2023). A comparative analysis of privacy policies and their comprehension in mobile ecosystems. *Proceedings on Privacy Enhancing Technologies*, 2023(4), 5–22. <https://doi.org/10.56553/popets-2023-0123>
5. Google PAIR. (2023). *People + AI Guidebook: A/B testing*. <https://pair.withgoogle.com/guidebook/testing>
6. Habib, H., Colnago, J., & Cranor, L. F. (2022). Towards a unified privacy utility framework for evaluating privacy interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1–15). <https://doi.org/10.1145/3491102.3517745>
7. Utz, C., Degeling, M., & Fahl, S. (2021). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973–990). <https://doi.org/10.1145/3460120.3484756>
8. Zarouali, B., Poels, K., & Ponnet, K. (2022). Contextual integrity and user expectations in privacy interface design: A theoretical framework and experimental test. *New Media & Society*, 24(1), 156–178. <https://doi.org/10.1177/14614448211021115>
9. Tan, H., Sun, J., Wenjia, W., & Zhu, C. (2021). User experience and usability of driving: A bibliometric analysis of 2000–2019. *International Journal of Human-Computer Interaction*, 37(4), 297–307. <https://doi.org/10.1080/10447318.2020.1860516>
10. Dirin, A., Nieminen, M., & Laine, T. H. (2023). Feelings of being for mobile user experience design. *International Journal of Human-Computer Interaction*, 39(20), 4059–4079. <https://doi.org/10.1080/10447318.2022.2108964>
11. Kivijärvi, H., & Pärnänen, K. (2023). Instrumental usability and effective user experience: Interwoven drivers and outcomes of human-computer interaction. *International Journal of Human-Computer Interaction*, 39(1), 34–51. <https://doi.org/10.1080/10447318.2021.2016236>
12. Holden, R. J., Abebe, E., Hill, J. R., Brown, J., Savoy, A., Volda, S., & Kulanthaivel, A. (2022). Human factors engineering and human-computer interaction: Supporting user performance and experience. In *Clinical informatics study guide: Text and review* (pp. 119–132). https://doi.org/10.1007/978-3-030-93765-2_9
13. Fan, M., Yang, X., Yu, T., Liao, Q. V., & Zhao, J. (2022). Human-AI collaboration for UX evaluation: Effects of explanation and synchronization. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1), 1–32. <https://doi.org/10.1145/3512943>



14. Paneru, B., Paneru, B., Poudyal, R., & Shah, K. B. (2024). Exploring the nexus of user interface (UI) and user experience (UX) in the context of emerging trends and customer experience, human-computer interaction, applications of artificial intelligence. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, 5(1), 102–113. <https://doi.org/10.34010/injiscom.v5i1.12488>
15. Wang, Y., Leon, P. G., & Schaub, F. (2023). Proactive privacy nudges for mobile app permissions: A large-scale field experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). <https://doi.org/10.1145/3544548.3580715>
16. Vu, K. P. L., Proctor, R. W., & Hung, Y. H. (2021). Website design and evaluation. In *Handbook of human factors and ergonomics* (pp. 1016–1036). <https://doi.org/10.1002/9781119636113.ch39>
17. Chou, C. M., Shen, T. C., & Shen, C. H. (2022). Influencing factors on students' learning effectiveness of AI-based technology application: Mediation variable of the human-computer interaction experience. *Education and Information Technologies*, 27(6), 8723–8750. <https://doi.org/10.1007/s10639-021-10866-9>
18. Souza, K. E. S. D., Aviz, I. L. D., Mello, H. D. D., Figueiredo, K., Vellasco, M. M. B. R., Costa, F. A. R., & Seruffo, M. C. D. R. (2022). An evaluation framework for user experience using eye tracking, mouse tracking, keyboard input, and artificial intelligence: A case study. *International Journal of Human-Computer Interaction*, 38(7), 646–660. <https://doi.org/10.1080/10447318.2021.1960092>
19. Moore, R. J., An, S., & Ren, G. J. (2023). The IBM natural conversation framework: A new paradigm for conversational UX design. *Human-Computer Interaction*, 38(3–4), 168–193. <https://doi.org/10.1080/07370024.2022.2081571>
20. Sabukunze, I. D., & Arakaza, A. (2021). User experience analysis on mobile application design using user experience questionnaire. *Indonesian Journal of Information Systems*, 4(1), 15–26. <https://doi.org/10.24002/ijis.v4i1.4646>
21. Nicolescu, L., & Tudorache, M. T. (2022). Human-computer interaction in customer service: The experience with AI chatbots — A systematic literature review. *Electronics*, 11(10), 1579. <https://doi.org/10.3390/electronics11101579>
22. Kostiuk, Y. V., Skladannyi, P. M., Bebesko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
23. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebesko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
24. Hulak, H. M., Zhylytsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
25. Korniiets, V., & Skladannyi, P. (2024). Formation of requirements for the architecture and functions of cybersecurity monitoring systems. *Telecommunication and Information Technologies*, 4(85), 90–96. <https://doi.org/10.31673/2412-4338.2024.040224>
26. Kostiuk, Y., et al. (2025). Models and algorithms for analyzing information risks during the security audit of personal data information system. In *3rd International Conference on Cyber Hygiene and Conflict Management in Global Information Networks* (Vol. 3925, pp. 155–171).
27. Mykhaylova, O., et al. (2024). Person-of-interest detection on mobile forensics data – AI-driven roadmap. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS)* (Vol. 3654, pp. 239–251).
28. Mykhaylova, O., et al. (2023). Mobile application as a critical infrastructure cyberattack surface. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II)* (Vol. 3550, pp. 29–43).
29. Sadykov, Y., et al. (2021). Technology of location hiding by spoofing the mobile operator IP address. In *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics* (pp. 22–25). <https://doi.org/10.1109/UkrMiCo52950.2021.9716700>

**Vadym Chitulyan**

Senior Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0001-8846-9094
mag5187403@stud.duikt.edu.ua

Ivan Oleinikov

Senior Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0001-3066-4639
i.oleinikov@duikt.edu.ua

Oleksii Ananchenko

Candidate of technical science, Associate professor, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0005-3446-5994
o.ananchenko@duikt.edu.ua

Vadym Dziuba

Senior Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0003-8715-7245
v.dziuba@duikt.edu.ua

WEB PROGRAMMING AND MOBILE DEVELOPMENT: UX/UI SOLUTIONS FOR PROTECTING USERS' PERSONAL DATA

Abstract. With the rapid expansion of digital platforms and the centrality of online services in everyday life, the issue of protecting users' personal data has become a critical aspect of human-computer interaction. Traditional approaches that reduce data protection to legal compliance and technical security measures have proven insufficient for ensuring genuine user privacy. This has led to the emergence of systematic UX/UI methodologies designed to integrate data protection principles directly into the user experience. The present study introduces an authorial framework – the Privacy-Embedded User Journey (PEUJ) – which unites contextual consent, proactive nudges, transparent data control, and iterative feedback loops. Experimental validation was conducted on three types of digital services (FinTech application, e-commerce platform, and health & fitness tracker), enabling the measurement of informed consent rates, user trust scores, frequency of privacy settings usage, incidence of excessive data sharing, user retention rates, and a composite Privacy-Usability Index (PUI). The findings reveal that the application of the PEUJ framework systematically increases informed consent by 22–35 percentage points, improves user trust by 18–28%, reduces excessive data sharing by 25–40%, and increases user retention by 8–12 percentage points. Particular attention is devoted to the role of embedding privacy interventions into key interaction points rather than relying on post-factum compliance, which is shown to enhance both user autonomy and business metrics. The study further highlights the potential of employing the Privacy-Usability Index (PUI) as a unified metric for evaluating and comparing privacy-focused UX interventions across domains. These insights underscore the importance of rethinking data protection as an integral element of user experience that ensures both ethical compliance and commercial viability [1, 2].

Keywords: data privacy, UX/UI design, informed consent, Privacy-Embedded User Journey (PEUJ), user trust, personal data protection, web development, mobile development.

REFERENCES

1. Acquisti, A., Adjerid, I., Balebako, R. (2021). Nudges for privacy and security: Understanding and assisting users' choices. *ACM Computing Surveys*, 55(3), 1–42. <https://doi.org/10.1145/3485830>



2. Bennett, C., & O'Donnell, K. (2024). User-centered data privacy: A framework for empathetic design. *Journal of Usability Studies*, 19(2), 88–105.
3. Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Ontario: Information and Privacy Commissioner of Ontario.
4. Degeling, M., Utz, C., & Lentzsch, C. (2023). A comparative analysis of privacy policies and their comprehension in mobile ecosystems. *Proceedings on Privacy Enhancing Technologies*, 2023(4), 5–22. <https://doi.org/10.56553/popets-2023-0123>
5. Google PAIR. (2023). *People + AI Guidebook: A/B testing*. <https://pair.withgoogle.com/guidebook/testing>
6. Habib, H., Colnago, J., & Cranor, L. F. (2022). Towards a unified privacy utility framework for evaluating privacy interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1–15). <https://doi.org/10.1145/3491102.3517745>
7. Utz, C., Degeling, M., & Fahl, S. (2021). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973–990). <https://doi.org/10.1145/3460120.3484756>
8. Zarouali, B., Poels, K., & Ponnet, K. (2022). Contextual integrity and user expectations in privacy interface design: A theoretical framework and experimental test. *New Media & Society*, 24(1), 156–178. <https://doi.org/10.1177/14614448211021115>
9. Tan, H., Sun, J., Wenjia, W., & Zhu, C. (2021). User experience and usability of driving: A bibliometric analysis of 2000–2019. *International Journal of Human-Computer Interaction*, 37(4), 297–307. <https://doi.org/10.1080/10447318.2020.1860516>
10. Dirin, A., Nieminen, M., & Laine, T. H. (2023). Feelings of being for mobile user experience design. *International Journal of Human-Computer Interaction*, 39(20), 4059–4079. <https://doi.org/10.1080/10447318.2022.2108964>
11. Kivijärvi, H., & Pärnänen, K. (2023). Instrumental usability and effective user experience: Interwoven drivers and outcomes of human-computer interaction. *International Journal of Human-Computer Interaction*, 39(1), 34–51. <https://doi.org/10.1080/10447318.2021.2016236>
12. Holden, R. J., Abebe, E., Hill, J. R., Brown, J., Savoy, A., Volda, S., & Kulanthaivel, A. (2022). Human factors engineering and human-computer interaction: Supporting user performance and experience. In *Clinical informatics study guide: Text and review* (pp. 119–132). https://doi.org/10.1007/978-3-030-93765-2_9
13. Fan, M., Yang, X., Yu, T., Liao, Q. V., & Zhao, J. (2022). Human-AI collaboration for UX evaluation: Effects of explanation and synchronization. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1), 1–32. <https://doi.org/10.1145/3512943>
14. Paneru, B., Paneru, B., Poudyal, R., & Shah, K. B. (2024). Exploring the nexus of user interface (UI) and user experience (UX) in the context of emerging trends and customer experience, human-computer interaction, applications of artificial intelligence. *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, 5(1), 102–113. <https://doi.org/10.34010/injiscom.v5i1.12488>
15. Wang, Y., Leon, P. G., & Schaub, F. (2023). Proactive privacy nudges for mobile app permissions: A large-scale field experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). <https://doi.org/10.1145/3544548.3580715>
16. Vu, K. P. L., Proctor, R. W., & Hung, Y. H. (2021). Website design and evaluation. In *Handbook of human factors and ergonomics* (pp. 1016–1036). <https://doi.org/10.1002/9781119636113.ch39>
17. Chou, C. M., Shen, T. C., & Shen, C. H. (2022). Influencing factors on students' learning effectiveness of AI-based technology application: Mediation variable of the human-computer interaction experience. *Education and Information Technologies*, 27(6), 8723–8750. <https://doi.org/10.1007/s10639-021-10866-9>
18. Souza, K. E. S. D., Aviz, I. L. D., Mello, H. D. D., Figueiredo, K., Vellasco, M. M. B. R., Costa, F. A. R., & Seruffo, M. C. D. R. (2022). An evaluation framework for user experience using eye tracking, mouse tracking, keyboard input, and artificial intelligence: A case study. *International Journal of Human-Computer Interaction*, 38(7), 646–660. <https://doi.org/10.1080/10447318.2021.1960092>
19. Moore, R. J., An, S., & Ren, G. J. (2023). The IBM natural conversation framework: A new paradigm for conversational UX design. *Human-Computer Interaction*, 38(3–4), 168–193. <https://doi.org/10.1080/07370024.2022.2081571>
20. Sabukunze, I. D., & Arakaza, A. (2021). User experience analysis on mobile application design using user experience questionnaire. *Indonesian Journal of Information Systems*, 4(1), 15–26. <https://doi.org/10.24002/ijis.v4i1.4646>
21. Nicolescu, L., & Tudorache, M. T. (2022). Human-computer interaction in customer service: The experience with AI chatbots — A systematic literature review. *Electronics*, 11(10), 1579. <https://doi.org/10.3390/electronics11101579>



22. Kostiuk, Y. V., Skladannyi, P. M., Bebashko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
23. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebashko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
24. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
25. Korniiets, V., & Skladannyi, P. (2024). Formation of requirements for the architecture and functions of cybersecurity monitoring systems. *Telecommunication and Information Technologies*, 4(85), 90–96. <https://doi.org/10.31673/2412-4338.2024.040224>
26. Kostiuk, Y., et al. (2025). Models and algorithms for analyzing information risks during the security audit of personal data information system. In *3rd International Conference on Cyber Hygiene and Conflict Management in Global Information Networks* (Vol. 3925, pp. 155–171).
27. Mykhaylova, O., et al. (2024). Person-of-interest detection on mobile forensics data – AI-driven roadmap. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS)* (Vol. 3654, pp. 239–251).
28. Mykhaylova, O., et al. (2023). Mobile application as a critical infrastructure cyberattack surface. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II)* (Vol. 3550, pp. 29–43).
29. Sadykov, Y., et al. (2021). Technology of location hiding by spoofing the mobile operator IP address. In *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics* (pp. 22–25). <https://doi.org/10.1109/UkrMiCo52950.2021.9716700>

