

**Ministry of Education and Science of Ukraine
Odessa National University of Technology
Vinnytsia National Technical University
P.N. Platonov Institute of Computer Engineering, Automation,
Robotics and Programming**

**INFORMATION TECHNOLOGIES AND
AUTOMATION– 2025**

***PROCEEDINGS
OF THE XVIII INTERNATIONAL SCIENTIFIC AND PRACTICAL
CONFERENCE***



OCTOBER 30-31, 2025

Odesa

**Міністерство освіти і науки України
Одеський національний технологічний університет
Інститут комп'ютерної інженерії, автоматизації,
робототехніки та програмування ім.П.Н.Платонова**

**«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І
АВТОМАТИЗАЦІЯ – 2025»**

***МАТЕРІАЛИ
XVIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ***



30-31 ЖОВТНЯ 2025 р.

м.Одеса

Інформаційні технології і автоматизація – 2025 / Матеріали XVIII міжнародної науково-практичної конференції. Одеса, 30-31 жовтня 2025 р. - Одеса, Видавництво ОНТУ, 2025 р. – 1316 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області ІТ та автоматизації, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямками і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Головний редактор збірника Сергій Котлик

АВТЕНТИФІКАЦІЇ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ BLUETOOTH-З'ЄДНАНЬ. Білборін-Еррера О.М., Главчев М.І., Ігнат'єв К.І. Національний технічний університет «Харківський політехнічний інститут» (Україна)	
ПРОЕКТУВАННЯ ЕТАЛОННОЇ МОДЕЛІ КОМПАНІЇ-ПОСТАЧАЛЬНИКА ІТ-РІШЕНЬ. Бойченко В.І., Тройніна А.С., Рувінська В.М. Національний університет «Одеська Політехніка» (Україна)	658
ПРОЕКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ ФІНАНСАМИ ДЛЯ ФІЗИЧНОЇ ОСОБИ-ПІДПРИЄМЦЬ. Бородкіна І.Л. Бородкін Г.О. Український державний університет імені Михайла Драгоманова (Україна), Національний університет біоресурсів і природокористування України (Україна)	660
ВІДПОВІДНІСТЬ СТАНДАРТАМ ПРИ ПРОЄКТУВАННІ СЕРВЕРНОЇ ЧАСТИНИ ВЕБЗАСТОСУНКІВ. Браташ С.П. Національний університет «Львівська політехніка» (Україна)	664
ОПТИМІЗАЦІЯ ВЕБСИСТЕМИ ДЛЯ АВТОМАТИЗОВАНОГО БІЗНЕС-ПЛАНУВАННЯ БРЕНДУ ОДЯГУ. Брежнев О.С., Жульковська І.І., Жульковський О.О. Дніпровський державний технічний університет (Україна)	666
ІНТЕЛЕКТУАЛЬНА ТЕХНОЛОГІЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ЦИФРОВИХ ДВІЙНИКІВ ДЛЯ ДИСПЕТЧЕРІВ ЕКСТРЕНИХ СЛУЖБ. Бубенщиков Д.Є., Шаповалов С.П. Сумський державний університет (Україна)	668
ТЕЛЕГРАМ-БОТ ЯК ІНСТРУМЕНТ ОПЕРАТИВНОЇ ВЗАЄМОДІЇ ЗІ СЛУЖБОЮ ТЕХНІЧНОЇ ПІДТРИМКИ. Бур'ян С. С., Погореловська І. Д. Державний податковий університет (Україна)	670
РОЗРОБКА МЕТОДІВ ТА ПРОГРАМНИХ ЗАСОБІВ МОБІЛЬНОЇ СИСТЕМИ SMART-НОТАТОК. Бурбело С. М. ¹ , Коваленко О. О. ² , Саєцький Д. Р. ² ¹ Житомирський військовий інститут ім. С.П. Корольова, ² Вінницький національний технічний університет (Україна)	672
ПРОЄКТУВАННЯ ТА РОЗРОБКА МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ВІДМОВИСТІЙКОСТІ В МІКРОСЕРВІСНІЙ АРХІТЕКТУРІ НА ОСНОВІ ПАТЕРНУ CIRCUIT BREAKER. Ванда І. С. Харківський національний університет імені В. Н. Каразіна (Україна)	675
БЕЗПЕКА ТА ПРИВАТНІСТЬ У IOS-ДОДАТКАХ: ЯК ЗАБЕЗПЕЧИТИ ВІДПОВІДНІСТЬ ВИМОГАМ APPLE. Вдовенко Д.О., Сєдих О.Л. Національний університет харчових технологій (Україна)	677
РОЗРОБКА IOS-ЗАСТОСУНКУ "AI TRAVEL ASSISTANT" НА БАЗІ SWIFTUI ТА ШТУЧНОГО ІНТЕЛЕКТУ. Вдовенко Д.О., Сєдих О.Л. Національний університет харчових технологій (Україна)	679
МЕТОДИ РЕКОМЕНДАЦІЙНИХ СИСТЕМ ДЛЯ ВИБОРУ КОНДИТЕРСЬКИХ МАГАЗИНІВ. Виноградов М.Ю., Тітов С.В. Харківський національний університет радіоелектроніки (Україна)	681
АРХІТЕКТУРА ХМАРНОЇ СИСТЕМИ ДЛЯ ОБМІНУ ДАНИМИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ З ДЕРЖАВНИМИ СЛУЖБАМИ: ОСОБЛИВОСТІ ОПТИМІЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ Воробйов Р.Р. Державний університет інформаційно-комунікаційних технологій (Україна)	682
ІНТЕЛЕКТУАЛЬНА МОДЕЛЬ УПРАВЛІННЯ КОЛЕКЦІЯМИ В ХМАРНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ. В'юннік Ю.О. Інститут програмних систем Національної академії наук України (Україна)	684
ПІДХІД НА ОСНОВІ МОСК-ОБ'ЄКТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВАРІАБЕЛЬНОСТІ ПРОЦЕСІВ ТЕСТУВАННЯ СЕРВІС-ОРІЄНТОВАНИХ ПРОГРАМНИХ СИСТЕМ. Гамзаєв Р.О., Ткачук М.В. Харківський національний університет імені В.Н. Каразіна (Україна)	687
МОДЕЛЮВАННЯ ПОВЕДІНКОВИХ ПАТЕРНІВ КОРИСТУВАЧІВ У ЗАДАЧАХ ПІДВИЩЕННЯ ЯКОСТІ ІНТЕРФЕЙСІВ ІНФОРМАЦІЙНИХ СИСТЕМ. Гамор І.М. Інститут програмних систем Національної академії наук України (Україна)	690
ПРОГРАМНИЙ КОМПЛЕКС ДЛЯ КЕРУВАННЯ 2-DOF МЕХАНІЗМАМИ ПРОТЕЗІВ.	693

Тестування продемонструвало, що комбінований режим роботи ModifiedCB забезпечує найвищу ефективність у високо-навантажених середовищах. Однією з головних переваг цього режиму є автоматичний перехід до асинхронного каналу зв'язку, що зменшує негативний вплив збоїв на загальну роботу системи. Бібліотека також демонструє високу стійкість до перевантаження окремих компонентів і підтримує доступність навіть у разі частих помилок або великих обсягів запитів. Порівняльний аналіз із популярним рішенням Polly показав, що, попри високу швидкість обробки запитів, стійкість цього інструменту до збоїв є обмеженою.

Список використаної літератури

- [1] S. Newman, Building Microservices. Sebastopol, CA, USA: O'Reilly Media, 2015. 280 p.
- [2] M. T. Nygard, Release It!: Design and Deploy Production-Ready Software. Nashville, TN, USA: Pragmatic Bookshelf, 2007. 350 p.
- [3] “Circuit Breaker Pattern (Design Patterns for Microservices),” Medium. [Online]. Available: <https://medium.com/geekculture/design-patterns-for-microservices-circuit-breaker-pattern-276249ffab33>. [Accessed: 17-Oct-2025].
- [4] “Meet Polly: The .NET resilience library,” Polly. [Online]. Available: <https://www.pollydocs.org/>. [Accessed: 17-Oct-2025].

УДК 004.05

БЕЗПЕКА ТА ПРИВАТНІСТЬ У IOS-ДОДАТКАХ: ЯК ЗАБЕЗПЕЧИТИ ВІДПОВІДНІСТЬ ВИМОГАМ APPLE

Вдовенко Д.О., Сєдих О.Л.

(dmitryvdvnk@gmail.com, olgased@ukr.net)

Національний університет харчових технологій (Україна)

У статті розглянуто актуальні аспекти забезпечення безпеки та конфіденційності в iOS-додатках відповідно до вимог Apple. Проаналізовано ключові інструменти та правила, які повинні враховувати розробники: політику AppTrackingTransparency (ATT), механізми контролю доступу до чутливих ресурсів (камера, мікрофон, геолокація), оформлення пояснень у файлі Info.plist, а також "етикетки конфіденційності" (Privacy Nutrition Labels). Окрему увагу приділено використанню локального зберігання даних через Keychain та Secure Enclave для підвищення захисту користувацької інформації. Виконання цих вимог забезпечує схвалення додатку під час модерації в App Store, підвищує рівень довіри користувачів та сприяє формуванню позитивної репутації розробника.

Вступ. У сучасному цифровому середовищі питання захисту персональних даних користувачів набувають особливої актуальності. Apple, як один із лідерів технологічної індустрії, приділяє значну увагу безпеці та конфіденційності, впроваджуючи суворі вимоги до мобільних застосунків, що публікуються в App Store. Для розробників це означає необхідність дотримання низки правил: використання механізму *AppTrackingTransparency*, обмеження доступу до чутливих даних, а також чіткого інформування користувача про мету їхнього збору. Розуміння та виконання цих вимог є обов'язковою умовою для створення успішних застосунків, які відповідають очікуванням користувачів та політиці Apple.

Основна частина. Однією з ключових вимог є дотримання політики *AppTrackingTransparency* (ATT) — фреймворку, запровадженого в iOS 14.5. ATT зобов'язує розробників отримувати явний дозвіл користувача перед тим, як відстежувати його активність у сторонніх застосунках або на вебсайтах. Без такої згоди доступ до ідентифікатора пристрою (IDFA) заборонено, що суттєво вплинуло на підходи до інтеграції рекламних SDK та аналітики й змусило компанії переглядати стратегії монетизації. Особливого контролю потребує доступ до чутливих системних ресурсів — камери, мікрофона, геолокації, контактів або фото. Для кожного з таких доступів розробник має додати пояснення в *Info.plist* (наприклад, *NSCameraUsageDescription*, *NSLocationWhenInUseUsageDescription*), чітко вказавши мету його

використання. Некоректне або відсутнє пояснення може стати підставою для відхилення застосунку під час модерації App Store. З виходом iOS 15 Apple посилила контроль за роботою з фоновими даними. Наприклад, при запиті доступу до геопозиції у режимі *Always* користувач отримує додаткове системне повідомлення та може обмежити або повністю заборонити такий доступ. Це зобов'язує розробників ретельно планувати сценарії використання додатку, запитуючи лише ті права, які є критично необхідними.

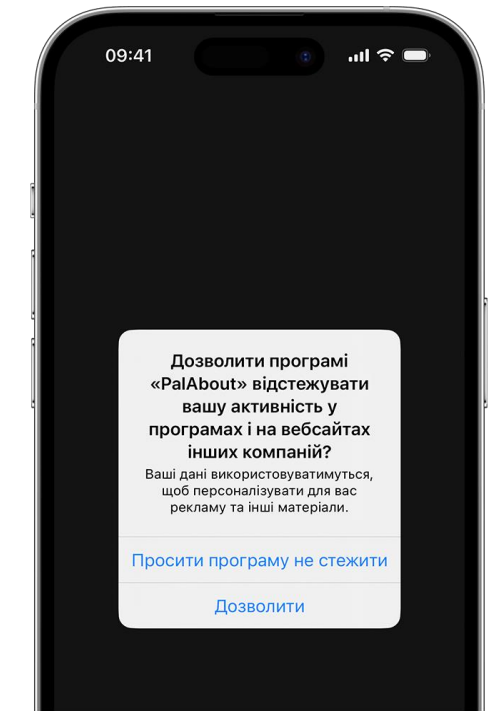


Рисунок 1 – Приклад запити щодо відстеження активності

Для підвищення прозорості Apple запровадила *Privacy Nutrition Labels* — так звані "етикетки конфіденційності", що відображаються на сторінці застосунку в App Store. Розробник повинен вказати типи даних, які збираються, мету їхнього використання (аналітика, персоналізація, реклама) та інформацію про можливу передачу третім сторонам. Неправдиві або неповні дані можуть призвести до видалення застосунку з App Store.

Важливим аспектом також є впровадження локального зберігання даних без передачі інформації на зовнішні сервери, коли це можливо. Apple підтримує використання *Keychain* для безпечного збереження паролів і токенів доступу та *Secure Enclave* для роботи з біометричними даними [1, 2].

Висновки. Безпека та конфіденційність користувачів є фундаментом сучасної розробки iOS-додатків. Apple надає розробникам чіткий набір інструментів і вимог, дотримання яких є обов'язковим для публікації застосунку в App Store. Виконання політики *AppTrackingTransparency*, коректне обґрунтування доступів до чутливих ресурсів, заповнення "етикеток конфіденційності" та застосування безпечних механізмів зберігання даних дають змогу створювати застосунки, яким довіряють користувачі. Розробники, що приділяють належну увагу цим аспектам, отримують не лише схвалення модерації, але й підвищують рівень лояльності своєї аудиторії, що є ключовим чинником успіху на сучасному ринку мобільних технологій.

Список використаної літератури

- [1] “Якщо програма робить запит щодо відстеження вашої активності,” Служба підтримки Apple (UA). [Online]. Available: <https://support.apple.com/uk-ua/102420> [Accessed: September 25, 2025].
- [2] “App Tracking Transparency,” Apple Developer Documentation. [Online]. Available: <https://developer.apple.com/documentation/apptackingtransparency> [Accessed: September 25, 2025].