

ПРОБЛЕМАТИКА БЕЗПЕЧНОГО ДИЗАЙНУ НА ПРИКЛАДІ ДОДАТКУ GREEN GUARD

Носок Н.С.

Кафедра твердотільної електроніки та інформаційної безпеки,
ДВНЗ «Ужгородський національний університет»,
Україна

E-mail: nikolettanosok@ukr.net

Abstract

The Green Guard application enables real-time ecological monitoring with IoT and drone technologies, providing environmental insights. It's including Security by Design (SbD) principles to support data protection across system layers. At the same time, Privacy by Design (PbD) promotes ethical data handling practices that highlight user consent and minimize data collection to what is absolutely necessary. These foundational principles flow through into the application's UI/UX, so that security and privacy into the core of user interactions. Certain mechanisms for secure data management are implemented through multi-layered controls and audit-ready systems, effectively in preventing unauthorized access, and it has been well received by users. The Green Guard solution represents the realization of SbD and PbD principles applied in a practical way, and is an example for future-based, secure, and user-centric solutions in environmental monitoring technologies.

У сучасних умовах екологічний моніторинг вимагає не лише своєчасного доступу до достовірної інформації, а й створення гнучких, адаптивних інструментів, здатних у реальному часі збирати, обробляти та аналізувати великі обсяги даних. Поєднання технологій Інтернету речей (IoT), розумного дому, концепції Smart City та безпілотних літальних апаратів відкриває можливість розробити масштабовану екологічну платформу для міста Ужгород, водночас забезпечивши дослідження її складової кібербезпеки. Попри стрімкий розвиток інфраструктури розумних міст, найбільша увага здебільшого зосереджується на цифровізації послуг, електрифікації та оптимізації транспортних потоків, тоді як питання екологічної безпеки залишаються недостатньо опрацьованими, хоча їх значущість постійно зростає.

Використання AI, IoT та IIoT технологій дає змогу не лише фіксувати зміни довкілля, але й прогнозувати потенційні ризики та завчасно інформувати населення про небезпеки. Проте ефективність подібних систем і рівень довіри до них неможливі без належного рівня кіберзахисту – особливо на рівні користувацького інтерфейсу (UI) та взаємодії користувача з системою (UX). Тому етап дизайну сьогодні має розглядатися не лише як питання зручності, а як активний механізм інформаційної безпеки та формування довіри між користувачем і платформою.

У ході роботи було проаналізовано чотири реальні платформи моніторингу повітря – SaveEcoBot, Luftdaten, EcoCity та Atmosfera – з позиції кібербезпеки, приватності та реалізації принципів Security by Design і Privacy by Design. Дослідження показало, що всі сервіси загалом використовують базові механізми захисту, зокрема HTTPS, однак значною проблемою залишається відсутність прозорого й зрозумілого користувацького інтерфейсу щодо збору та обробки даних. Загальним висновком є те, що сучасні еко-платформи приділяють увагу технічним аспектам безпеки, але в більшості випадків не забезпечують достатньої прозорості для користувача, не надають пояснень щодо збору даних.

Ключовою основою для створення безпечних інтерфейсів є концепція Security by Design (SbD), яка передбачає впровадження механізмів захисту ще на етапі архітектурного планування. У контексті Green Guard це означає побудову багаторівневої системи, у якій кожен компонент – від IoT-сенсорів і дронів до хмарної інфраструктури й мобільного додатку – отримує лише мінімально необхідний набір даних.

Не менш важливою є концепція Privacy by Design (PbD), яка ставить у центр уваги захист приватності та прозорість обробки даних. У межах Green Guard вона реалізована через мінімізацію

збору персональних даних, обробку інформації лише зі згоди користувача, можливість повного керування дозволами та зрозумілі пояснення, навіщо саме система потребує певні дані. PbD у цьому контексті інтегрується у сам UI/UX – безпека сприймається не як обмеження, а як частина зручної та роз’яснювальної взаємодії.

У підсумку дослідження, кібербезпека в UI/UX-дизайні Green Guard є фундаментальною складовою системи та визначає її надійність, ефективність і рівень довіри. Комбінування принципів SbD і PbD дозволяє створити платформу, стійку до атак і водночас зрозумілу для користувача. Вже на етапі аналізу визначаються критичні дані й потенційні ризики, а під час проєктування розробляються безпечні сценарії взаємодії, логічна навігація та прозорі механізми контролю даних. Такий підхід формує повний цикл інформаційного захисту – від сенсора до інтерфейсу – перетворюючи Green Guard на інноваційний приклад “екологічно безпечного” дизайну.

Література

1. Goyal, V., & Kumar, A. (2023). *Artificial Intelligence for IoT*. Springer Nature.
2. Cisco. (n.d.). *Cisco Cybersecurity Reports*. Retrieved from https://www.cisco.com/c/uk_ua/products/security/securityreports.html#~download-th
3. Piasecki, S., Urquhart, L., & McAuley, D. (2021). Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *ScienceDirect*. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0267364921000157>
4. Bertino, E., Sandhu, R., & Paci, F. (2020). *Security and Privacy Issues in Smart Homes: An Overview*. Springer.
5. Del-Real, C., De Busser, E., & van den Berg, B. (2022). Shielding software systems: A comparison of Security by Design and Privacy by Design based on a systematic literature review. *International Journal of Information Security*, 21, 543–567.