АНОТАЦІЯ

Відповідно до мети дослідження робота присвячена дослідженню можливих кіберзагроз мобільних застосунків та розробці застосунку з використанням двухфакторної автентифікації під час авторизації облікових записів до застосунку. Було проведено аналіз технологій інструментів автентифікації та проаналізовано архітектуру безпеки мобільних платформ для розробки системи захисту для мобільного застосунку. Розглянуті вимоги до системи, проектування архітектури та реалізація необхідних заходів захисту. Виконано процес тестування та оцінки ефективності системи захисту. В результаті дослідженння реалізовано кросплатформений нативний застосунок з використанням двофакторної автентифікації під час авторизації облікових записів Google до застосунку зі безпечним з’єднанням між клієнтом та сервером, що в свою чергу збільшує безпеку передачі користувацьких даних під час авторизації та зменшує ризик витоку інформації.

ABSTRACT

According to the research objectives, the work is dedicated to investigating potential cyber threats to mobile applications and developing an application with two-factor authentication during the authorization of accounts. An analysis of authentication technology tools and a review of the security architecture of mobile platforms were conducted for the development of a protection system for the mobile application. The system requirements, architecture design, and implementation of necessary security measures were considered. Testing processes and the evaluation of the security system's effectiveness were carried out. As a result of the research, a cross-platform native application was implemented, utilizing two-factor authentication during the authorization of Google accounts within the application, ensuring a secure connection between the client and server. This, in turn, enhances the security of user data transmission during authorization and reduces the risk of information leakage.