

OPPORTUNITIES FOR MOBILE APPLICATIONS IN SUPPORTING STUDENT EDUCATIONAL ACTIVITIES DURING WARTIME

Natalia Bobro,
Ph.D, Doctor of Philosophy,
Director of the digital department
of the European University,
director of the “NooLab & AI”
scientific laboratory of the European University
European University

The study of mobile applications’ potential to support the educational process for students during wartime is especially relevant given the rapid transformations in Ukraine’s higher education system following the full-scale Russian invasion in 2022. This attack led to widespread infrastructure damage, forced displacement of students and educators, and the disruption of traditional education methods. War and associated security threats have catalyzed significant changes within higher education. As a response to these challenges, universities have pivoted to distance learning, resulting in a substantial increase in the use of mobile applications as the primary means to ensure the continuity of the educational process in conditions of limited access to traditional educational resources.

The potential of mobile applications within educational settings is an active area of interdisciplinary research among both domestic and international scholars. Y.O. Kolodinska and D.O. Gudakov, for instance, explore stages of user interface design, a crucial element in developing mobile applications for students [1]. O. Skliarenko et al. examine the role of digital interactive learning technologies as a core component of contemporary education [2]. Additionally, O.O. Khomenko, M.V. Paustovska, and I.A. Onyshchuk in their study analyze the impact of interactive technologies on higher education students’ learning and development [3]. Notably, prominent Ukrainian researcher C. Yahodzinsky highlights the need for interpreting convergence as a strategic innovation in response to social modernization [4].

This research highlights the wide range of issues associated with mobile applications in education, underscoring the growing role of digital tools in shaping the modern higher education landscape.

Modern mobile applications operate on a client-server architecture, where the mobile interface is provided on the client side, while data storage and processing are managed on the server side. This setup enables efficient management of educational resources, knowledge assessments, and student performance tracking. An analysis of existing mobile applications reveals their high adaptability to crisis situations, supporting continuity in education even when stable internet access is unavailable. By distributing mobile applications through platforms like Google Play and the App Store, students can easily access software that facilitates interaction with their institution’s electronic learning systems.

While the use of mobile applications in education is essential for maintaining learning continuity in unstable environments, it brings new challenges. Data privacy and cybersecurity have become particularly pressing concerns, as the active use of digital technologies during wartime introduces additional risks to educational data security. This situation underscores the need for developing and implementing effective protection measures.

For instance, mobile applications handle various types of confidential information, including the personal data of students, teachers, and staff, as well as details about the educational process. This data is processed on institutional servers, which are key elements of the infrastructure of electronic educational systems. These servers manage data storage, processing, and synchronization across mobile clients, enabling remote access to learning materials, assessments, and consultations. This infrastructure enhances the flexibility of the educational process, especially in situations where traditional educational resources are limited due to military operations.

To safeguard against information security threats, employing a mobile device manager (MDM) is advisable. An MDM enforces basic personal data security policies by configuring the settings and operational modes of users' mobile devices. Key configurable parameters include:

- equipment settings (e.g., permissions for Bluetooth, NFC, etc.);
- password settings (including requirements for length and complexity);
- encryption settings;
- browser settings (e.g., disabling cookies, blocking JavaScript);
- allowed and prohibited applications;
- compliance policies (e.g., required OS version) [5, pp. 36–37].

In the event of a threat to the physical integrity of a user's mobile device, the program can delete confidential information from the device. Additionally, it may implement measures such as clearing secret codes, remote locking, or providing antivirus support. The mobile device management process can be illustrated in the sequence shown in Fig. 1.

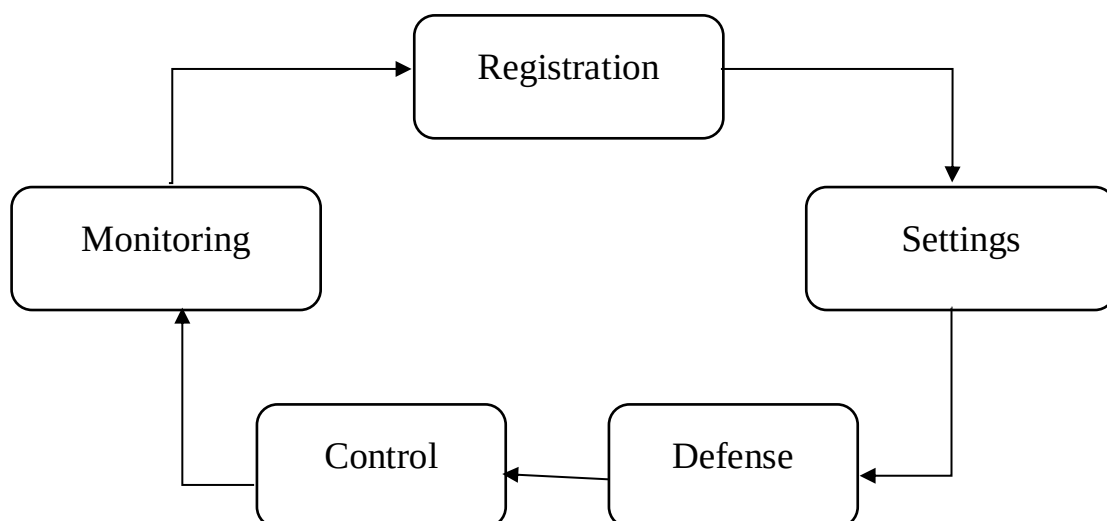


Fig. 1. Mobile Device Management Process Using Typical MDM Solutions

A Mobile Application Manager (MAM) can also be employed to protect against information security threats. This class of security tools provides a subset of mobile device management functions. The program facilitates data distribution and management while regulating the life cycle of specific mobile applications. MAM ensures the security of tools used for device authentication and may also include diagnostic functions such as remote login, report generation, and troubleshooting. Notably, specialized MAM implementations operate as standalone components within mobile applications, as they do not integrate with MDM solutions.

It is important to note that, in organizing the protection of information resources within an educational organization against threats targeting vulnerabilities in mobile access services to educational information systems, the use of Identification and Access Management (IAM) tools is also advisable. This class of information security tools is employed to implement authentication and authorization while creating a unified security profile for all users in a mobile solution. IAM facilitates a consistent approach to security across all mobile services and allows for the integration of corporate user authentication systems into mobile solutions. When used in conjunction with Mobile Device Management (MDM), IAM enables users to access multiple mobile devices configured with the same access level. Additionally, the IAM system ensures data synchronization between multiple devices and users.

Thus, mobile applications are essential for ensuring the continuity of the educational process during wartime when traditional teaching methods are either impossible or limited. They not only enhance flexibility in accessing educational materials but also provide tools for monitoring progress and fostering interactive engagement between teachers and students. However, for these solutions to function effectively, it is crucial to address aspects of cybersecurity and the protection of confidential information, which become particularly critical in times of conflict.

Список використаних джерел

1. Колодинська Я.О., Гудаков Д.О. Етапи проектування користувацького інтерфейсу. Науковий вісник, 2023. 1, 61-66. DOI: <https://doi.org/978-966-301-265-0/1.2023.61>.
2. Скляренко О.В., Ягодзінський С.М., Ніколаєвський О.Ю., Невзоров А.В. Цифрові інтерактивні технології навчання як невід’ємна складова сучасного освітнього процесу. Інноваційна педагогіка, 2024. 68 (2), 2024, 51-55. DOI: <https://doi.org/10.32782/2663-6085/2024/68.2.51>.
3. Хоменко О. О., Паустовська М. В., Онищук І. А. Вплив інтерактивних технологій на процес навчання і розвиток здобувачів вищої освіти. Наукові інновації та передові технології, 2024. 5(33), 1222-1231. DOI: [https://doi.org/10.52058/2786-5274-2024-5\(33\)-1222-1231](https://doi.org/10.52058/2786-5274-2024-5(33)-1222-1231).
4. Yahodzinskyi S. Anthropomorphic information networks and converging technologies: challenge to humanity (vs), step forward? Artificial intelligence, 2023. 1, с. 29-35. DOI: <https://doi.org/10.15407/jai2023.01.029>.
5. Бобро Н. С. Цифрова трансформація освітніх систем. Ефективна економіка, 2024. 1, 36-41. DOI: <https://doi.org/10.32702/2307-2105.2024.1.36>.