**РЕФЕРАТ**

**Актуальність теми.** Мобільні пристрої є невід'ємною частиною повсякденного життя людства. Від соціальних мереж до банківських транзакцій мобільні пристрої користуються довірою мільйонів людей по ​​всьому світі. В той же час існує тенденція зростання кількість шкідливого програмного забезпечення, котра є актуальною для всіх популярних мобільних платформ.

На даний момент операційна система Android є найпоширенішою мобільною платформою у світі. Відповідно до цього факту, на ній щороку розгортається незліченна кількість зловмисних застосунків, що мають на меті нашкодити роботі пристрою та отримати доступ до конфіденційних даних користувача. Виходячи з вище зазначеної інформації, проблема виявлення таких додатків є вкрай актуальною на сьогоднішній день і саме тому потребує нових ідей та підходів.

**Об’єктом дослідження** є виявлення зловмисного програмного забезпечення в операційній системі Android базуючись на методі статичного аналізу програмного забезпечення.

**Предметом дослідження** є програмне забезпечення, що реалізовує запропонований спосіб виявлення зловмисного програмного забезпечення в застосунку операційної системи Android.

**Мета роботи:** дослідити методологію виявлення шкідливого програмного забезпечення та метод статичного аналізу зокрема; проаналізувати архітектуру та засоби безпеки операційної системи Android, розробити та реалізувати алгоритм для виявлення зловмисного програмного забезпечення шляхом статичного аналізу застосунку в операційній системі Android.

**Наукова новизна** полягає в наступному: запропоновано гнучкий спосіб виявлення шкідливого програмного забезпечення на основі статичного аналізу застосунку в операційній системі Android та реалізовано програму, котра використовує вище зазначений спосіб.

**Практична цінність** отриманих в роботі результатів полягає в тому, що запропонований спосіб дає змогу більш ефективно в плані гнучкості та детальності отриманої інформації проводити аналіз застосунків на предмет наявності ознак зловмисного програмного забезпечення в рамках операційної системи Android. Розроблене програмне забезпечення дає можливість аналізувати додатки та запобігти потраплянню зловмисних програм на персональний мобільний пристрій.

**Апробація роботи.** Основні положення і результати роботи були представлені та обговорювались на XIV науковій конференції магістрантів та аспірантів «Прикладна математика та комп’ютинг» ПМК-2021 (Київ, 17-19 листопада 2021 р.), на LXVII міжнародній науково-практичній конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» (Тернопіль, 12 травня 2022 р.) та на міжнародній мультидисциплінарній науковій інтернет-конференції «Світ наукових досліджень. Випуск 18» (м.Тернопіль (Україна) - м.Переворськ (Польща), 20-21 квітня 2023 року).

**Структура та обсяг роботи.** Магістерська дисертація складається з вступу, п’ятьох розділів та висновків.

*У вступі* подано загальну характеристику роботи, зроблено оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі досліджень, показано наукову новизну і практичну цінність роботи.

*У першому розділі* більш детально розглянуто постановку проблеми, проведено аналіз існуючих рішень та інструментів для аналізу безпеки мобільних додатків, визначено основні вимоги до програмного забезпечення та виявлено певні закономірності у розробці програм, що базуються на статичному аналізі, для виявлення зловмисного програмного забезпечення в операційній системі Android. Запропоновано власний підхід до вирішення зазначеної проблеми.

*У другому розділі* розглянуто архітектуру та модель безпеки операційної системи Android з метою кращого розуміння існуючих механізмів та способу їх використання у виявленні зловмисного програмного забезпечення.

У *третьому розділі* розглянуто методики та стратегії статичного аналізу програмного забезпечення, їхні переваги та недоліки, а також вказано, наскільки зазначені методи можуть сприяти виявленню потенційних проблем з безпекою в мобільних додатках для ОС Android. Окрім того, розібрано алгоритм аналізу додатків в цій системі та представлено послідовність етапів цього процесу.

*У четвертому розділі* наведено запропонований спосіб виявлення зловмисного програмного забезпечення на базі статичного аналізу, описано його логіку та алгоритм роботи, а також детально розібрано кожен з його етапів.

*У п’ятому розділі* наведено результати тестування програмного забезпечення, котре реалізовує запропонований в даній роботі спосіб. Результати було наведено на прикладі повного аналізу тестового застосунку, а також на прикладі окремо розібраних тестових випадків.

*У висновках* представлено підсумок проведеної роботи.

Робота представлена на 83 аркушах та містить посилання на список використаних літературних джерел.

**Ключові слова**: статичний аналіз, зловмисне програмне забезпечення, вразливості, операційна система Android.

**ABSTRACT**

**Actuality of theme.** Mobile devices are an integral part of the everyday life of mankind. From social media to banking transactions, mobile devices are trusted by millions of people around the world. At the same time, there is an increasing trend in the number of malicious software that is relevant for all popular mobile platforms.

At the moment, the Android operating system is the most common mobile platform in the world. Due to this fact, countless malicious applications are deployed on it every year, with the aim of harming the device and gaining access to the user's confidential data. Based on the above information, the problem of detecting such applications is extremely relevant today and therefore requires new ideas and approaches.

**The object of the study** is a detection of malicious software in the Android operating system based on the method of static analysis of software.

**The subject of the study** is the software that implements the proposed method of detecting malicious software in the application of the Android operating system.

**Purpose:** to investigate the methodology for detecting malicious software and the method of static analysis in particular; analyze the architecture and security of the Android operating system, develop and implement an algorithm to detect malicious software by static analysis of the application in the Android operating system.

**The scientific novelty is the following:** a flexible method of detecting malicious software based on static analysis of an application in the Android operating system is proposed, and a program using the above-mentioned method is implemented.

**The practical value of the results obtained in this work** is that the proposed method makes it possible to analyze applications for the presence of signs of malicious software within the Android operating system more efficiently in terms of flexibility and details of the information that is obtained during analysis. The developed software makes it possible to analyze applications and prevent malicious programs from entering a personal mobile device.

**Approbation of work.** The main provisions and results of the work were presented and discussed at the XIV scientific conference of undergraduates and graduate students "Applied Mathematics and Computing" PMK-2021 (Kyiv, November 17-19, 2021), at the LXVII International Scientific and Practical Conference "Information Society: technological, economic and technical aspects of formation "(Ternopil, May 12, 2022) and at the at the international multidisciplinary scientific Internet conference "The World of Scientific Research. Issue 18" (Ternopil (Ukraine) - Perevorsk (Poland), April 20-21, 2023).

**Structure and scope of work.** The master's dissertation consists of an introduction, five chapters and conclusions.

*In the introduction,* a general overview of the work is presented, an assessment of the current state of the problem is made, the relevance of the research direction is substantiated, the aim and objectives of the research are formulated, the scientific novelty and practical value of the work are demonstrated.

*In the first section* the statement of the problem is considered in more detailed way, an analysis of existing solutions and tools for analyzing the security of mobile applications is carried out, the main requirements for the software are defined, and certain regularities in the development of programs based on static analysis for the detection of malicious software in the Android operating system are identified. An own approach to solving the specified problem is proposed.

*The second section* examines the architecture and security model of the Android operating system in order to get better understanding of existing mechanisms and how they are used to detect malware.

*In the third section* methods and strategies of static software analysis are considered, their advantages and disadvantages are discussed, and it is indicated to what extent these methods can contribute to the detection of potential security issues in mobile applications for the Android OS. In addition, the algorithm for analyzing applications in this system is dissected, and the sequence of stages of this process is presented.

*In the fourth chapter,* the proposed method of detecting malicious software based on static analysis is introduced, its logic and working algorithm are described, and each of its stages is thoroughly analyzed.

*In the fifth chapter,* the results of testing the software that implements the method proposed in this work are presented. The results were demonstrated using the example of a full analysis of a test application, as well as separately analyzed test cases.

*The conclusion* presents the results of the work.

The work is presented on 83 sheets and contains references to the list of used literature sources.

**Keywords:** static analysis, malware, vulnerabilities, Android operating system.