https://doi.org/10.31891/2219-9365-2026-85-41
УДК 004.8

БЕРБЕЦ Денис
Хмельницький національний університет
https://orcid.org/0009-0000-6616-7952
e-mail: dberbets70@gmail.com
ПЕТЛЯК Наталія
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
МОСТОВИЙ Сергій
Хмельницький національний університет
https://orcid.org/0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua

КОМПЛЕКСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА СТІЙКОСТІ ANDROID-ПРИСТРОЇВ У СУЧАСНИХ УМОВАХ КІБЕРЗАГРОЗ

У статті досліджується сучасний стан екосистеми мобільної операційної системи Android з акцентом на проблеми кібербезпеки, основні загрози та методи протидії їм. Розглянуто фрагментацію версій Android, яка ускладнює розробку сумісних додатків і підвищує ризики безпеки через наявність невиправлених вразливостей у застарілих версіях. Проаналізовано загрози, пов'язані зі сторонніми додатками та бібліотеками збору даних, а також обмеження системи Google Play у запобіганні поширенню шкідливого програмного забезпечення. Окрему увагу приділено ризикам динамічного завантаження коду та атакам через сенсори мобільних пристроїв, що дають змогу отримувати конфіденційну інформацію або здійснювати несанкціоноване керування. Наведено класифікацію кіберзагроз Android-пристроїв, зокрема масових загроз (adware, ransomware, Mobile Unwanted Software) і цілеспрямованих атак класу APT, таких як Pegasus, SunBird, Gooligan і Dark Caracal. Виділено побічні атаки, що базуються на аналізі фізичних характеристик пристрою (енергоспоживання, електромагнітне випромінювання, акустичні сигнали, дані сенсорів) і здатні забезпечувати приховане вилучення чутливих даних. Також проаналізовано внутрішні кібератаки, спрямовані на експлуатацію вразливостей операційної системи, міжзастосункової взаємодії та апаратного забезпечення, зокрема обходу Android Keystore і зловживання дозволами. Підкреслено проблему поширення шкідливого ПЗ через Google Play із використанням обфускації, інкрементних оновлень і динамічного коду, а також роль соціальної інженерії та відкладеної активації шкідливих функцій, що ускладнює їх своєчасне виявлення.

Ключові слова: операційна система Android, кібербезпека, мобільні пристрої, шкідливе програмне забезпечення, кібератаки.

BERBETS Denys, PETLIAK Nataliia, MOSTOVYI Serhii
Khmelnytskyi National University

COMPREHENSIVE APPROACHES TO ENSURING THE CONFIDENTIALITY AND RESILIENCE OF ANDROID DEVICES IN CURRENT CYBERTHREAT CONDITIONS

The article examines the current state of the Android mobile operating system ecosystem, focusing on cybersecurity issues, threats, and mitigation methods. In particular, it considers the peculiarities of Android version fragmentation, which complicates the development of compatible applications and creates additional security risks, as older versions may contain unpatched vulnerabilities. Threats associated with the use of third-party applications and data collection libraries are analyzed, as well as the shortcomings of the Google Play system, which is not always able to effectively prevent the distribution of malicious software. Particular attention is paid to the risks arising from dynamic code loading, as well as attacks through mobile device sensors that allow for remote acquisition of sensitive information and unauthorized device control. The article reviews the classification of cyber threats for Android devices, including modern mass threats such as adware, ransomware, Mobile Unwanted Software, and complex targeted APT-class attacks, including Pegasus, SunBird, Gooligan, and Dark Caracal. A special category of side-channel attacks is highlighted, which are implemented through the analysis of physical device characteristics such as power consumption, electromagnetic radiation, acoustic signals, or inertial sensor data, and are capable of providing covert extraction of cryptographic keys, passwords, and personal identifiers. Internal cyberattacks aimed at exploiting vulnerabilities in the operating system, inter-process communication, and hardware are analyzed separately, including mechanisms for bypassing Android Keystore protection and the use of excessive permissions to implement malicious functionality. A significant security issue is the spread of malware through the official Google Play store. It has been established that malicious programs systematically enter the store due to the use of multi-level obfuscation techniques, incremental updates, recompilation, and dynamic code loading. Additionally, user security is affected by social engineering, which forces the installation of malicious applications under the guise of legitimate ones. It has been found that many malicious applications activate harmful code with a delay, making their timely detection by traditional antivirus tools impossible.

Keywords: Android operating system, mobile device cybersecurity, malicious software, side-channel attacks, Advanced Persistent Threats (APT).

Стаття надійшла до редакції / Received 04.01.2026
Прийнята до друку / Accepted 16.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Останніми роками відзначається інтенсивне зростання рівня поширення мобільних пристроїв, зокрема смартфонів та планшетів, які набули статусу невід'ємного елемента повсякденної і професійної діяльності користувачів. Розширений функціонал пристроїв, що охоплює засоби комунікації, навігаційні сервіси, мультимедійні ресурси та платформи соціальної взаємодії, забезпечує високий рівень мобільності та зручності у використанні. Окремої уваги заслуговує зростання їх застосування в корпоративному середовищі, що зумовлено поширенням гнучких моделей організації праці, зокрема дистанційного доступу до корпоративних мереж та реалізацією концепції Bring Your Own Device (BYOD).

Сучасний ринок мобільних операційних систем представлений такими платформами, як Android, iOS, Windows, BlackBerry, Symbian, Tizen та Harmony. Серед них операційна система Android посідає провідне місце за показниками розповсюдженості та частки ринку. Водночас її популярність зумовила підвищений інтерес з боку кіберзлочинців, що сприяло зростанню кількості та складності кібератак [1-2]. Зокрема, зафіксовано появу високорозвинених зразків шкідливого програмного забезпечення, таких як Pegasus, які належать до класу Advanced Persistent Threat (APT) та орієнтовані на тривале приховане проникнення в мобільні системи [3]. Основною метою подібних атак є здійснення цілеспрямованого шпигування щодо окремих категорій користувачів, зокрема посадових осіб, представників державних та приватних інституцій, наглядових органів, а також широкого кола пересічних користувачів, з метою несанкціонованого доступу до конфіденційної інформації – журналів викликів, контактних даних, мультимедійних файлів, фінансових застосунків та документів [4].

Попри систематичні зусилля, спрямовані на вдосконалення механізмів безпеки, автентифікації та захисту мобільних платформ, операційна система Android і надалі залишається вразливою до широкого спектра кіберзагроз [5]. У процесі еволюції платформи регулярно виявляються нові вразливості, усунення яких потребує значних часових і ресурсних витрат. Частина таких вразливостей характеризується високим рівнем складності та потребує глибокого науково-технічного аналізу, що зумовлює тривале перебування користувачів у зоні підвищеного ризику.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

В умовах трансформації сучасного середовища кіберзагроз особливої актуальності набувають атаки з використанням побічних каналів (side-channel attacks), а також поширення шкідливого програмного забезпечення через офіційні канали розповсюдження, зокрема магазин Google Play [6-7]. Хоча низка попередніх досліджень присвячена проблемам безпеки мобільних платформ, значна їх частина не враховує актуальні загрози, пов'язані з APT-кампаніями, атаками через побічні канали та інфікуванням пристроїв через легітимні джерела. З огляду на зазначене, у статті здійснено комплексний аналіз сучасного стану екосистеми Android з акцентом на ключові безпекові виклики та можливі напрями їх подолання.

Теоретичні та прикладні аспекти кібербезпеки мобільних пристроїв є предметом активних наукових досліджень як у вітчизняному, так і в зарубіжному науковому просторі. Зокрема, технічні аспекти захисту інформаційних систем, а також специфіка реалізації механізмів інформаційної безпеки представлені у працях О. Неретіна, О. Новікова, В. Савченка, В. Харченка, О. Шаповаленка та інших. Серед зарубіжних дослідників слід зазначити Р. Муді, Л. Стрельцова, Л. Керулуса, Е. Грінберга й інших.

На сьогодні в наукових і прикладних джерелах представлено значну кількість публікацій, що висвітлюють різні підходи та технологічні рішення у сфері мобільної безпеки. Водночас більшість досліджень не забезпечує цілісного аналізу практичних можливостей існуючих систем та меж їх ефективного застосування у реальних умовах експлуатації. У зв'язку з цим у межах даного дослідження проведено комплексний аналіз функціональних можливостей систем захисту мобільних пристроїв, орієнтованих на протидію кіберзагрозам та кібератакам під час підключення користувацьких пристроїв до корпоративних інформаційно-комунікаційних систем. Отримані результати дозволяють визначити ефективні стратегії запобігання витоку, компрометації та втраті важливої інформації, що сприяє підвищенню загального рівня кіберстійкості в умовах сучасного середовища.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті полягає у комплексному аналізі сучасного стану безпеки мобільної операційної системи Android, ідентифікації основних вразливостей і кіберзагроз, включаючи масове шкідливе програмне забезпечення, цілеспрямовані атаки класу APT та побічні атаки, а також оцінці ефективності сучасних методів захисту, таких як статичний і динамічний аналіз додатків, апаратні засоби безпеки та впровадження постквантової криптографії для підвищення стійкості та конфіденційності користувацьких даних у мобільних пристроях.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Вразливості операційної системи Android являють собою сукупність програмно-технічних недоліків і слабких місць, експлуатація яких може призводити до несанкціонованого доступу, порушення керованості або повного контролю над мобільним пристроєм. Такі вразливості виникають внаслідок помилок програмного коду, використання застарілих версій системного та прикладного програмного забезпечення, а також неналежного або некоректного конфігурування компонентів операційної системи. У контексті платформи Android наявність вразливостей створює передумови для компрометації конфіденційної інформації, зокрема персональних і фінансових даних, а також для інсталяції та виконання шкідливого програмного забезпечення, що негативно впливає на рівень безпеки та конфіденційності пристрою. В окремих випадках такі вразливості можуть бути використані як елемент багатоступеневих атак, спрямованих на інші пристрої або інформаційні системи, зокрема шляхом поширення шкідливого коду чи реалізації атак типу відмови в роботі програмного забезпечення чи обслуговуванні.

Аналіз сучасного стану безпеки Android-платформи свідчить про тенденцію до поступового зростання кількості виявлених вразливостей, що вказує на сталі виклики у сфері забезпечення її кіберзахисту, незважаючи на систематичні зусилля розробників і дослідників. За характером впливу такі вразливості зазвичай пов’язані з можливістю виконання довільного коду, переповненням буфера, несанкціонованим розкриттям інформації та ескалацією підозрілого трафіку. Їх експлуатація створює умови для реалізації широкого спектра атак – від порушення конфіденційності даних до повного захоплення контролю над мобільним пристроєм. Проблематика вразливостей тісно корелює з кіберзагрозами, спрямованими як на технічну експлуатацію слабких місць операційної системи, так і на використання методів соціальної інженерії, що спонукають користувачів до розкриття персональних даних або встановлення шкідливого програмного забезпечення. У загальному вигляді такі загрози охоплюють сучасні масові кібератаки, малопоширені або спеціалізовані загрози, а також атаки класу APT, які відзначаються високим рівнем складності та цілеспрямованості.

Сучасні кіберзагрози для Android-пристроїв характеризуються різноманіттям видів шкідливого програмного забезпечення, спрямованого на порушення конфіденційності, цілісності та доступності інформації. До найбільш поширених форм належить рекламне шкідливе ПЗ, яке ініціює нав’язливе відображення реклами та часто поширюється разом із легітимними застосунками або через компрометовані вебресурси. Значну небезпеку становлять backdoor-механізми, що забезпечують прихований несанкціонований доступ до системи та виконання зловмисного коду. File infector-загрози приєднуються до файлів, зокрема APK-пакетів, з метою отримання доступу до даних застосунків, їх викрадення або шифрування. Окрему групу становить Mobile Unwanted Software, яка включає програмні продукти з неетичними або прихованими функціями, зокрема імітацією легітимних застосунків чи незаконним збором користувацьких даних. Особливо небезпечними є ransomware-атаки, що передбачають шифрування даних із подальшим вимаганням викупу. До інших поширених типів належать riskware, scareware, spyware та троянські програми, які маскуються під корисні застосунки, але реалізують приховані зловмисні функції.

Окрему категорію становлять стійкі цілеспрямовані загрози, що реалізуються у вигляді тривалих, високоточних і складних до виявлення атак, орієнтованих на конкретні об’єкти або групи користувачів. Такі атаки зазвичай здійснюються організованими кіберзлочинними угрупованнями або структурами, пов’язаними з державними інтересами. Прикладами є використання шпигунського програмного забезпечення Pegasus, здатного експлуатувати як взаємодію з користувачем, так і механізми типу zero-click, що забезпечують доступ до повідомлень, дзвінків і даних геолокації. Іншим прикладом є шкідливе ПЗ Gooligan, яке поширюється через заражені застосунки та надає зловмисникам доступ до облікових записів Google. Загроза Dark Caracal реалізується через маскування під легітимний застосунок і спрямована на збір конфіденційної інформації, зокрема записів дзвінків і текстових повідомлень. Як правило, подібні атаки поширюються за допомогою фішингових кампаній або підроблених вебресурсів і забезпечують прихований віддалений доступ до пристрою та його інформаційних ресурсів.

В умовах стрімкого зростання поширення мобільних пристроїв, зокрема на базі операційної системи Android, сервіс Google Play Store продовжує виконувати роль основного каналу розповсюдження прикладного програмного забезпечення. Незважаючи на впровадження компанією Google комплексу захисних механізмів, зокрема системи Play Protect, що передбачає застосування методів статичного та динамічного аналізу для виявлення шкідливих програм, практичний досвід засвідчує обмежену ефективність таких заходів. Шкідливе програмне забезпечення систематично проникає до офіційного магазину застосунків, обходячи наявні механізми перевірки шляхом використання складних багаторівневих технік маскування та модифікації програмного коду [8-9].

Однією з найбільш поширених технік є динамічне завантаження коду, за якого шкідливі компоненти дозавантажуються вже після інсталяції застосунку, зокрема із використанням механізмів Java Reflection або аналогічних інструментів [10]. За таких умов шкідливий функціонал не проявляється на етапі попередньої перевірки та, відповідно, не ідентифікується системами автоматизованого аналізу. Інший підхід полягає у застосуванні інкрементних оновлень, коли до спочатку легітимного програмного продукту поступово

інтегрується шкідливий код, часто у поєднанні з методами обфускації, що включають шифрування, перейменування ідентифікаторів та введення надлишкових конструкцій. Це істотно ускладнює аналіз і знижує ефективність антивірусних засобів. Крім того, поширеною є практика повторного компілювання легітимних застосунків після їх декомпіляції та інтеграції шкідливих модулів, що дозволяє маскувати небезпечний код під виглядом популярних і перевірених програм. Значну роль у цьому процесі відіграють методи соціальної інженерії, спрямовані на психологічний вплив на користувачів із метою спонукання до інсталяції замаскованого шкідливого програмного забезпечення.

Результати аналізу свідчать, що через Google Play Store у різні періоди поширювалися десятки типів шкідливого програмного забезпечення, елементи коду яких було ідентифіковано у сотнях застосунків. Незважаючи на активні дії компанії Google щодо виявлення, видалення та блокування таких програм, наявність системних вразливостей у процесі перевірки залишається актуальною проблемою, що зумовлює потребу в подальшому вдосконаленні механізмів верифікації та контролю. Застосунки, інстальовані з офіційного магазину, можуть приховано здійснювати збір персональних даних, ініціювати нав'язливу рекламну активність або отримувати розширені привілеї управління пристроєм [11]. Ускладнює виявлення таких загроз те, що значна частина шкідливих програм активує свої функції із затримкою, що знижує ефективність традиційних методів детектування.

Важливим аспектом забезпечення безпеки мобільних пристроїв є аналіз дозволів, які запитує застосунок під час інсталяції або в процесі роботи. Статистика свідчить про те, що шкідливі програми часто ініціюють запит на доступ до чутливих ресурсів, зокрема геолокації, контактів, журналів викликів, камери та мікрофона, що не відповідає задекларованій функціональності. Таким чином, аналіз набору дозволів може слугувати ефективним індикатором потенційної небезпеки ще на етапі прийняття рішення про встановлення застосунку. Водночас наявність певних дозволів не може розглядатися як однозначний критерій шкідливості, а потребує комплексної оцінки у поєднанні з іншими ознаками поведінки програмного забезпечення [12].

Сучасні наукові дослідження також фіксують зростання кількості атак, спрямованих на експлуатацію сенсорів мобільних пристроїв. Зокрема, вразливості GPS-модулів можуть використовуватися для прихованого відстеження місцезнаходження користувачів або маніпулювання координатами, що створює загрози конфіденційності та може застосовуватися з метою шахрайства чи фізичного переслідування [13]. Аналогічно, недоліки в реалізації технології NFC відкривають можливості для перехоплення, модифікації або підміни даних, що передаються між пристроями, зокрема в межах атак типу скімінгу, ретрансляції та клонування. Окремий клас загроз становлять атаки, спрямовані на виснаження енергетичних ресурсів мобільних пристроїв. Шляхом ініціювання фонових процесів із підвищеним споживанням ресурсів, зокрема під час прихованого криптомайнінгу або багаторазового циклічного підключення до бездротових мереж, зловмисники можуть суттєво скоротити час автономної роботи або повністю вивести пристрій з експлуатації. Додаткову небезпеку становлять атаки через бездротові мережі Wi-Fi, включно зі створенням фальшивих точок доступу, реалізацією сценаріїв «людина посередині» та використанням так званих «злих двійників», що дозволяє перехоплювати трафік, викрадати облікові дані або перенаправляти користувачів на фішингові ресурси.

Суттєвим викликом залишаються також атаки на біометричні механізми автентифікації. До них належать презентаційні атаки, використання технологій deepfake, підробка відбитків пальців, голосові підміни та маніпуляції з алгоритмами розпізнавання обличчя або сітківки ока. Дослідження демонструють, що значна частина наявних біометричних систем характеризується недостатньою стійкістю до таких методів впливу.

Таким чином, сукупність вразливостей Android-пристроїв, пов'язаних із механізмами розповсюдження застосунків через Google Play Store, використанням сенсорів та бездротових інтерфейсів, формує комплексні виклики для забезпечення цифрової безпеки. Подальший розвиток ефективних систем виявлення загроз, удосконалення процедур перевірки програмного забезпечення, а також підвищення рівня обізнаності користувачів щодо ризиків, пов'язаних із поведінкою застосунків і запитуваними дозволами, залишаються пріоритетними напрямами наукових досліджень і практичних рішень у сфері кібербезпеки.

Побічні атаки формують окремий клас кіберзагроз, спрямованих на несанкціоноване отримання конфіденційної інформації з мобільних пристроїв шляхом аналізу непрямих характеристик їх функціонування. На відміну від традиційних методів доступу до даних через програмні інтерфейси введення та виведення, такі атаки експлуатують фізичні властивості апаратного забезпечення, зокрема параметри енергоспоживання, електромагнітні випромінювання, акустичні сигнали або вібраційні ефекти, що виникають під час виконання обчислювальних операцій [14]. У середовищі Android подібні підходи можуть бути реалізовані з метою вилучення криптографічних ключів, автентифікаційних даних або іншої чутливої інформації без прямого порушення програмних механізмів захисту.

Показовим прикладом є атаки на основі аналізу слідів дотику, за яких зловмисник, отримавши фізичний доступ до пристрою, досліджує залишкові відбитки на сенсорному екрані з метою відновлення графічного ключа або PIN-коду. Подібні методи є універсальними та застосовуються не лише до смартфонів, а й до банкоматів, IoT-пристроїв та інших систем із сенсорними інтерфейсами. Іншу категорію становлять

атаки, що базуються на аналізі даних інерційних сенсорів, зокрема акселерометра та гіроскопа. Обробка сигналів, зафіксованих під час введення інформації, дозволяє корелювати мікрорухи пристрою з конкретними натисканнями клавіш, відновлюючи введені символи.

Окремий напрям становлять фізичні атаки на апаратну складову мобільних пристроїв, які ґрунтуються на індукції збоїв шляхом навмисного порушення параметрів електроживлення або електромагнітного середовища. Метою таких атак є обхід механізмів апаратного захисту, витяг конфіденційних даних або виконання несанкціонованого коду. Прикладом є атака VoltJockey, що використовує маніпуляції з напругою живлення для компрометації ізольованого середовища ARM TrustZone. Для протидії подібним загрозам застосовуються як апаратні засоби, зокрема захищені чипи безпеки типу Titan M, так і програмні механізми, серед яких перевірка цілісності процесу завантаження за допомогою Android Verified Boot.

Значну небезпеку становлять також атаки, засновані на аналізі споживаної потужності. Прості та диференціальні методи аналізу енергоспоживання, у поєднанні зі статистичною обробкою сигналів, дозволяють відновлювати криптографічні ключі або реконструювати дії користувача. Для зменшення ефективності таких атак застосовуються методи додавання шуму, фільтрації сигналів енергоспоживання, а також використання ізольованих криптографічних модулів, зокрема Android Keystore. Паралельно спостерігається зростання кількості атак, спрямованих безпосередньо на компрометацію криптографічних алгоритмів, що реалізується шляхом навмисного внесення збоїв у виконання операцій блочного шифрування, хеш-функцій або легких потокових шифрів, унаслідок чого з’являється можливість відновлення ключів або обходу механізмів контролю цілісності.

Окрему категорію становлять внутрішні кібератаки, реалізовані через експлуатацію вразливостей операційної системи Android, мобільних застосунків або апаратного забезпечення. Зокрема, атаки на міжзастосункову взаємодію використовують недоліки в механізмах обробки інтенцій, підміни активностей або ескалації прав доступу. Значну загрозу становлять атаки, пов’язані з підміною інтерфейсу легітимного застосунку, що дає змогу перехоплювати облікові дані користувачів. У випадку атак на Android Keystore метою є модифікація або фальсифікація контейнерів із криптографічними ключами, що потенційно дозволяє підписувати шкідливі застосунки сертифікатами, ідентичними до сертифікатів легітимного програмного забезпечення. Незважаючи на використання механізмів ізоляції на основі пісочниць, шкідливі застосунки можуть обходити обмеження через надмірні дозволи, вразливості операційної системи або застосування рефлексії для динамічного завантаження коду. Особливу складність становлять атаки на прикладному рівні, де відкриті мережеві порти створюють передумови для реалізації SQL-ін’єкцій або міжсайтового скриптингу.

Суттєвим джерелом ризиків залишаються вразливості мобільних мереж. Атаки в мережах 3G, 4G та 5G включають викрадення ідентифікаторів абонентів, несанкціоноване відстеження місцезнаходження, перехоплення голосового трафіку та реалізацію атак типу відмови в обслуговуванні. У наукових дослідженнях описано практичні сценарії атак на IMSI, протокол автентифікації AKA та інші елементи стільникової інфраструктури. Попри технологічні переваги мереж п’ятого покоління, зокрема підвищену пропускну здатність і знижену затримку, вони залишаються вразливими до зловмисного використання трансляційних і сигнальних протоколів.

Отже, після проведеного аналізу сучасних кіберзагроз та особливостей їх реалізації на мобільних пристроях, стає очевидним, що ефективна протидія шкідливому програмному забезпеченню на платформі Android потребує системного підходу до його виявлення та класифікації. Зокрема, різноманітність загроз – від масових adware та ransomware до цілеспрямованих атак класу APT і побічних атак через сенсори та енергоспоживання – зумовлює необхідність використання комплексних методів аналізу [15]. У цьому контексті актуальним стає застосування статичного та динамічного аналізу, а також інтеграція апаратних і програмних засобів захисту для своєчасного виявлення шкідливих компонентів і мінімізації ризиків для користувачів.

Статичний аналіз шкідливого програмного забезпечення в середовищі Android ґрунтується на дослідженні коду та структурних елементів застосунків без його фактичного виконання з метою виявлення потенційно небезпечних або зловмисних компонентів. Даний підхід передбачає отримання та опрацювання різнорідної інформації, здобутої в процесі реверс-інжинірингу, зокрема сигнатур шкідливого ПЗ, переліку запитуваних дозволів, закодованих рядків, мережевих протоколів, характеристик функцій, послідовностей байткоду та графів керування потоком виконання. Аналіз цих даних дає змогу ідентифікувати характерні для шкідливих застосунків шаблони та здійснювати їх класифікацію за рівнем потенційної небезпеки. У низці випадків застосовується ручний аналіз, за якого фахівець безпосередньо досліджує програмний код, виявляючи підозрілі конструкції, нетипові дозволи або відомі шаблони зловмисної поведінки. До основних методів статичного аналізу належать сигнатурне виявлення, аналіз дозволів, детальний розбір байткоду та операційних послідовностей, а також дослідження жорстко закодованих рядків, що можуть містити URL- або IP-адреси командно-контрольних серверів. Важливим елементом є аналіз файлу AndroidManifest.xml, який містить ключові атрибути конфігурації та функціональні характеристики застосунку.

Динамічний аналіз шкідливого програмного забезпечення орієнтований на дослідження поведінки

застосунку під час його виконання в ізольованому та контрольованому середовищі, зокрема у пісочниці, на емуляторі або у віртуальній машині. Цей підхід дозволяє в режимі реального часу відстежувати дії програми, включаючи системні виклики, звернення до ресурсів пристрою, виклики прикладних програмних інтерфейсів, зміни у пам'яті та файловій системі, а також мережеву активність. Застосування методів інструментування коду забезпечує вставлення контрольних точок, що дає змогу здійснювати детальний моніторинг процесів виконання та виявляти приховані або відкладені зловмисні дії, які не можуть бути ідентифіковані засобами статичного аналізу.

Постквантова криптографія (Post-Quantum Cryptography, PQC) набуває особливої актуальності для сучасних смарт-пристроїв, у яких забезпечення довготривалої криптографічної стійкості є пріоритетним завданням. Критично важливі операції, зокрема підписання застосунків, формування та захист сховищ ключів, обмін ключовими матеріалами та реалізація цифрових підписів, потребують інтеграції надійних постквантових рішень. Важливою складовою таких систем є механізми виявлення збоїв, які забезпечують коректність виконання криптографічних алгоритмів шляхом фіксації аномалій та перевірки правильності кожного етапу обчислень. Для підвищення стійкості реалізацій застосовуються методи корекції помилок, контролю цілісності та цілеспрямовані ін'єкції збоїв, що використовуються для тестування надійності апаратно-програмних реалізацій.

Сучасні постквантові алгоритми демонструють можливість ефективної адаптації до ресурсних обмежень мобільних платформ. Зокрема, версія SIKE Round 3 оптимізована для мікроконтролерів з низьким енергоспоживанням, що дозволяє зменшити розмір ключів і зашифрованих повідомлень при одночасному підвищенні продуктивності. Імплементація алгоритму Kyber на 64-бітній архітектурі ARM Cortex-A використовує апаратні можливості процесора для прискорення операцій інкапсуляції та декодування ключів з мінімальними затримками, що робить її придатною для мобільних пристроїв, вбудованих систем і високопродуктивних серверних середовищ. Додатково, апаратні прискорювачі для цифрового підпису Ed25519 забезпечують значне зростання швидкодії порівняно з програмними реалізаціями та інтегрують механізми захисту від атак через побічні канали, підвищуючи загальний рівень безпеки. Увага також приділяється захисту легковагових криптографічних алгоритмів від атак, що ґрунтуються на ін'єкції збоїв. Для цього застосовуються методи виявлення помилок, спрямовані на запобігання навмисному порушенню коректності обчислень з метою вилучення конфіденційної інформації. Так, у шифрі Pomaranch, орієнтованому на пристрої з обмеженими ресурсами, реалізуються механізми дублювання критичних компонентів і використання кодів виявлення помилок для оперативної ідентифікації атак. Аналогічні підходи застосовуються і для криптографічної хеш-функції Grostl, де методи модульного резервування дозволяють виявляти збої шляхом порівняння результатів незалежних обчислювальних модулів. У блокових шифрах Midori та RECTANGLE реалізовано спеціалізовані схеми контролю помилок на різних рівнях шифрування, від S-блоків до раундових структур, із використанням перевірок парності, циклічних кодів та лічильників збоїв, що забезпечує своєчасне виявлення потенційних загроз і підвищує загальну надійність криптографічних реалізацій.

Таким чином, проведений аналіз методів захисту мобільних пристроїв на платформі Android демонструє, що комплексне забезпечення безпеки вимагає поєднання різних підходів. Статичний аналіз дозволяє ідентифікувати потенційно шкідливі компоненти застосунків без їх виконання, використовуючи сигнатури, дозволи, байткод та структурні характеристики додатків. Динамічний аналіз, у свою чергу, забезпечує моніторинг поведінки програм під час виконання, фіксуючи системні виклики, доступ до ресурсів пристрою та мережеву активність, що дозволяє виявляти приховані або відкладені шкідливі дії. Для забезпечення довготривалої стійкості криптографічних операцій на мобільних пристроях актуальним є впровадження постквантової криптографії, інтеграція механізмів виявлення збоїв та контролю цілісності обчислень.

Спеціалізовані методи резервування та дублювання критичних компонентів у легковагових шифрах і блокових алгоритмах, а також контроль парності і циклічні коди, підвищують надійність криптографічних операцій і дозволяють своєчасно виявляти потенційні загрози. Загалом, ефективний захист Android-пристроїв потребує синтезу статичних і динамічних методів аналізу, інтеграції апаратно-програмних механізмів безпеки та застосування сучасних постквантових рішень, що забезпечує комплексну протидію кіберзагрозам і захист конфіденційної інформації користувачів.

Узагальнену класифікацію загроз та відповідних методів захисту наведено в таблиці 1.

Оціночна імовірність прояву є безрозмірною нормованою величиною, що визначається в інтервалі від 0 до 1 та використовується для відображення відносної частоти фіксації окремих класів кібератак у практиці кіберінцидентів. На відміну від абсолютної статистичної ймовірності конкретної події, цей показник має порівняльний характер і формується на основі узагальнення відкритих аналітичних звітів і наукових публікацій. Значення, близькі до 0, відповідають загрозам, прояв яких у реальних інцидентах спостерігається вкрай рідко або практично не фіксується, тоді як значення, наближені до 1, відображають сценарії майже постійного або домінуючого прояву відповідного типу атак. Проміжні значення характеризують відносну частоту появи загроз порівняно з іншими класами кібератак у межах єдиної нормованої шкали.

Таблиця 1

Класифікація кіберзагроз Android-пристроїв та методи протидії

Тип загрози	Характеристика загрози	Основні приклади	Оціночна імовірність прояву	Методи виявлення та захисту
Масове шкідливе ПЗ	Орієнтоване на широкий круг користувачів, часто маскується під легітимні застосунки	Adware, ransomware, spyware, Mobile Unwanted Software	0.6–0.9	Статичний аналіз (сигнатури, дозволи), Play Protect, поведінковий аналіз, контроль дозволів
Цілеспрямовані атаки (APT)	Складні, довготривалі атаки, спрямовані на конкретних користувачів або організації	Pegasus, Gooligan, Dark Caracal, SunBird	0.01–0.05	Динамічний аналіз, моніторинг мережевої активності, апаратні модулі безпеки (TrustZone, Titan M)
Атаки на мережеві інтерфейси	Компрометація бездротових і мобільних мереж	MITM, fake Wi-Fi AP, IMSI-catcher	0.3–0.5	Шифрування трафіку, VPN, перевірка автентичності мереж
Атаки на біометрію	Обхід механізмів біометричної автентифікації	Deepfake, підробка відбитків, голосові атаки	0.02–0.08	Мультифакторна автентифікація, liveness-detection
Побічні (side-channel) атаки	Отримання даних через фізичні характеристики пристрою	Аналіз енергоспоживання, інерційних сенсорів, акустичних сигналів	0.05–0.15	Додавання шуму, ізольовані криптомодулі, контроль цілісності, резервування обчислень
Атаки через сенсори	Зловживання доступом до сенсорів без явної взаємодії з користувачем	GPS-tracking, акселерометрні атаки, NFC-скімінг	0.2–0.35	Обмеження дозволів, політики доступу, поведінковий моніторинг
Внутрішні атаки ОС	Експлуатація вразливостей Android або міжзастосункової взаємодії	Intent spoofing, privilege escalation, Android Keystore bypass	0.15–0.3	Sandbox-ізоляція, перевірка інтенцій, Verified Boot
Криптографічні атаки	Компрометація криптографічних алгоритмів або ключів	Fault-injection, differential power analysis	0.01–0.05	Постквантова криптографія, контроль помилок, дублювання модулів

Наведена узагальнювальна таблиця засвідчує, що ефективне забезпечення безпеки Android-пристроїв можливе лише за умови комплексного поєднання програмних, апаратних і криптографічних механізмів захисту, адаптованих до різних класів кіберзагроз та сценаріїв їх реалізації. Запропонована систематизація типів загроз і відповідних методів протидії може слугувати основою для розроблення та вдосконалення політик безпеки мобільних пристроїв у корпоративних і критично важливих інформаційних середовищах, а також підтверджує доцільність подальших наукових досліджень у напрямі інтеграції статичного й динамічного аналізу з апаратно орієнтованими та постквантовими криптографічними підходами.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже, на підставі комплексного аналізу екосистеми Android встановлено, що широке використання цієї операційної системи на глобальному ринку мобільних пристроїв обумовлює її пріоритетний статус як об’єкта кібератак. Незважаючи на постійне вдосконалення вбудованих механізмів безпеки, платформа залишається вразливою до широкого спектра. Сучасна архітектура безпеки Android стикається з істотними викликами, зумовленими обмеженою ефективністю традиційних методів контролю та фільтрації контенту в офіційних каналах розповсюдження програмного забезпечення. Зокрема, магазин Google Play неодноразово використовується зловмисниками як вектор поширення шкідливого ПЗ шляхом застосування технік динамічного завантаження коду, інкрементних оновлень та обфускації, що дозволяє приховувати зловмисний функціонал і обходити механізми захисту Play Protect. Додаткову критичну загрозу становлять атаки через побічні канали, засновані на аналізі фізичних характеристик функціонування пристрою, таких як енергоспоживання або дані інерційних сенсорів, що створює передумови для прихованого вилучення криптографічних ключів і персональних ідентифікаторів користувачів. Ефективна протидія зазначеним загрозам потребує інтеграції комплексних підходів, які поєднують методи статичного та динамічного аналізу програмного забезпечення з використанням апаратно орієнтованих засобів захисту, зокрема спеціалізованих безпекових модулів типу Titan M. Водночас системні обмеження платформи, зокрема висока фрагментація версій операційної системи та тривалий цикл поширення оновлень виробниками пристроїв, призводять до збереження значної кількості мобільних систем із незакритими вразливостями протягом тривалого часу. Окремим стратегічним викликом для безпеки Android є розвиток квантових обчислень, який потенційно підриває криптостійкість класичних алгоритмів шифрування, таких як RSA та ECC. Це зумовлює необхідність завчасної інтеграції механізмів постквантової криптографії в ресурсно обмежену архітектуру мобільних

пристроїв. У цьому контексті забезпечення належного рівня безпеки Android потребує переходу від переважно реактивних моделей захисту до проактивних стратегій, що передбачають використання федеративного навчання для збереження приватності користувачів, а також підвищення стійкості криптографічних модулів до атак ін'єкції збоїв і побічних каналів.

References

1. Naeem M. R., Khan M., Abdullah A. M., et al. A Malware Detection Scheme via Smart Memory Forensics for Windows Devices. Mobile Information Systems. 2022. Art. 9156514. 16 p. https://doi.org/10.1155/2022/9156514
2. Kwon H.-Y., Kim T., Lee M.-K. Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods. Electronics. 2022. Vol. 11, no. 6. P. 867. https://doi.org/10.3390/electronics11060867
3. Hossain M. A., Islam M. S. Enhanced detection of obfuscated malware in memory dumps: a machine learning approach for advanced cybersecurity. Cybersecurity. 2024. Vol. 7, no. 16. https://doi.org/10.1186/s42400-024-00205-z
4. Zgheib A., Potin O., Rigaud J.-B., Dutertre J.-M. A CFI Verification System based on the RISC-V Instruction Trace Encoder. 2022 25th Euromicro Conference on Digital System Design (DSD), Maspalomas, Spain, 2022. P. 456–463. https://doi.org/10.1109/DSD57027.2022.00067
5. Mailewa A., Rozendaal K. A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study. Advances in Technology. 2022. Vol. 2, no. 3. P. 291–321. https://doi.org/10.31357/ait.v2i3.5584
6. Koyirar W., Harris B., Williams J., et al. Efficient Ransomware Detection through Process Memory Analysis in Operating Systems. Authorea. 2024. https://doi.org/10.22541/au.172806160.00635511/v1
7. Zhang W., Li X., Zhu T. Entropy and Memory Forensics in Ransomware Analysis: Utilizing LLaMA-7B for Advanced Pattern Recognition. TechRxiv. 2023. https://doi.org/10.36227/techrxiv.24742389.v1
8. Bakar A., Kijsirikul B. Enhancing Network Visibility and Security with Advanced Port Scanning Techniques. Sensors. 2023. Vol. 23, no. 17. P. 7541. https://doi.org/10.3390/s23177541
9. Woralert C., Liu C., Blasingame Z. HARD-Lite: A Lightweight Hardware Anomaly Realtime Detection Framework Targeting Ransomware. IEEE Transactions on Circuits and Systems I: Regular Papers. 2023. Vol. 70, no. 12. P. 5036–5047. https://doi.org/10.1109/TCSI.2023.3299532
10. Hassin T. M., Al-rimy B. A. S., Muchtar F. B., Singh P. K. Early Detection of Crypto-Ransomware Pre-encryption Phases: A Review. Proceedings of International Conference on Recent Innovations in Computing. ICRIC 2023. Springer, Singapore, 2024. Vol. 1194. https://doi.org/10.1007/978-981-97-2839-8_17
11. Taylor T., Hill N., Harrington E., et al. Dynamic Anomaly-Driven Detection for Ransomware Identification: An Innovative Approach Based on Heuristic Analysis. TechRxiv. 2024. https://doi.org/10.36227/techrxiv.173203089.97125949/v1
12. Limer A., Abramovich R., Devereux G., et al. Automated Ransomware Detection Using Dynamic Behavior Trace Profiling. TechRxiv. 2024. https://doi.org/10.36227/techrxiv.173030558.85237080/v1
13. Matae T., Fentiman K., Kingsleigh S., et al. Introducing Adaptive Sequence Embedding for Effective Ransomware Detection. Authorea. 2024. https://doi.org/10.22541/au.173161592.25153018/v1
14. Rezvani M., Jahanshahi A., Wong D. Characterizing In-Kernel Observability of Latency-Sensitive Request-Level Metrics with eBPF. 2024 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), Indianapolis, IN, USA, 2024. P. 24–35. https://doi.org/10.1109/ISPASS61541.2024.00013
15. Bashir R., Janicke H., Zeng W. Evaluating the impact of sandbox applications on live digital forensics investigation. EAI Endorsed Transactions on Security and Safety. 2021. Vol. 7, no. 25. Art. e2. https://doi.org/10.4108/eai.8-4-2021.169179
16. Tarness S., Bennett M., Halloway F., et al. Introducing Dynamic Entropy Layer Profiling: A Novel Approach for Ransomware Detection through Behavioral Feature Analysis. Research Square. 2024. PREPRINT (Version 1). DOI: https://doi.org/10.21203/rs.3.rs-5358022/v1
17. Anikolova E., Martins S., Rozental D., et al. Ransomware Detection Through Behavioral Attack Signatures Evaluation: A Novel Machine Learning Framework for Improved Accuracy and Robustness. TechRxiv. 2024. https:///doi.org/10.36227/techrxiv.173092022.26611647/v1
18. Yu R., Li P., Hu J., et al. Ransomware Detection Using Dynamic Behavioral Profiling: A Novel Approach for Real-Time Threat Mitigation. TechRxiv. 2024. https://doi.org/10.36227/techrxiv.173047864.44215173/v1