УДК 004.056.5
DOI https://doi.org/10.32782/tnv-tech.2025.2.11

РОЗБІР ВИДІВ КІБЕРЗАХИСТУ В ОПЕРАЦІЙНИХ СИСТЕМАХ МОБІЛЬНИХ ТЕЛЕФОНІВ

Коновалов С. М. *– старший викладач кафедри технічної кібернетики й інформаційних технологій імені професора Р. В. Меркта Одеського національного морського університету*
ORCID ID: 0000-0002-2533-8660

Сучасні мобільні пристрої стали невід'ємною частиною повсякденного життя і активно використовуються як в особистих, так і корпоративних цілях. Це спричинило зростання кількості кіберзагроз, націлених на смартфони. У цій статті проведено аналіз видів кіберзахисту, що реалізуються в операційних системах мобільних телефонів, таких як Android та iOS. Розглядаються апаратні та програмні методи забезпечення безпеки, особливості архітектури та механізми захисту даних. Стаття містить порівняльну таблицю підходів двох провідних ОС, схеми рівнів захисту та опису функціонування основних технологій: шифрування, аутентифікація, пісочниця, контроль дозволів. Також обговорюються типові загрози та способи їхньої нейтралізації. Види кіберзахисту були описані та класифіковані, розглянуті їх механізми захисту та приклади реалізації. Апаратні механізми захисту розглянути на прикладі Secure Enclave (Apple) та Titan M (Google Pixel), представлена схема порівняння. Програмні захист представлений на прикладі пісочниця (sandboxing) та контролю дозволів. Перелічені методи аутентифікації та керування доступом, розглянута, наведена формула оцінки стійкості пароля з прикладом. Буди виділені такі мережеві та хмарні механізми захисту, як VPN та захищений DNS, Private Relay (iCloud+) та Google Play Protect. Наочно представлена схема роботи Private Relay та Google Play Protect. Також показані типові загрози для операційних систем мобільних телефонів та представлений порівняльний огляд систем безпеки Android та iOS за різними критеріями. Все це націлено проти шкідливого програмного забезпечення для безпеки даних мобільних пристроїв. Висновки ґрунтуються на узагальненні поточних реалізацій кіберзахисту, наукових публікацій та практичних досліджень. Представлений матеріал може бути корисним фахівцям у галузі інформаційної безпеки, розробникам мобільних додатків та користувачам, зацікавленим у захисті особистих даних.

Ключові слова: *мобільна безпека, операційні системи, кіберзахист, Android, iOS, шифрування, аутентифікація, пісочниця, шкідливе програмне забезпечення, безпека даних.*

Konovalov S. M. Analysis of types of cyber protection in mobile phone operating systems
Modern mobile devices have become an integral part of everyday life and are actively used for both personal and corporate purposes. This has led to an increase in the number of cyber threats targeting smartphones. This article analyzes the types of cyber protection implemented in mobile phone operating systems, such as Android and iOS. Hardware and software security methods, architectural features, and data protection mechanisms are considered. The article contains a comparative table of approaches of the two leading OSes, schemes of protection levels, and a description of the functioning of the main technologies: encryption, authentication, sandboxing, and permission control. Typical threats and methods for neutralizing them are also discussed. Types of cyber protection have been described and classified, their protection mechanisms and implementation examples have been considered. Hardware protection mechanisms are considered using the example of Secure Enclave (Apple) and Titan M (Google Pixel), and a comparison scheme is presented. Software protection is presented using the example of sandboxing and permission control. Authentication and access control methods are listed, a formula for assessing password strength with an example is considered. Network and cloud protection mechanisms such as VPN and secure DNS, Private Relay (iCloud+) and Google Play Protect will be highlighted. The scheme of operation of Private Relay and Google Play Protect is clearly presented. Typical threats to mobile phone operating systems are also shown and a comparative review of Android and iOS security systems is presented according to various criteria. All of this is aimed against malware for mobile device data security. The conclusions are based on a generalization of current implementations of cyber protection, scientific publications

and practical research. The presented material may be useful to information security specialists, mobile application developers and users interested in personal data protection.

Key words: *mobile security, operating systems, cyber protection, Android, iOS, encryption, authentication, sandboxing, malware, data security.*

Вступ. Зростання цифровізації всіх сфер життя супроводжується активним поширенням смартфонів, які зберігають та обробляють чутливі персональні дані. Зі збільшенням обчислювальних можливостей мобільних пристроїв зростає та їхня привабливість для зловмисників. Кіберзагрози еволюціонують, стають дедалі витонченішими, що потребує постійного вдосконалення механізмів захисту [1, 2]. Мобільні операційні системи (ОС), в першу чергу Android та iOS, включають цілий спектр вбудованих рішень з кібербезпеки. Проте підходи, які у цих системах, значно різняться [3, 4]. Мета цієї статті – провести системний розбір видів кіберзахисту, що застосовуються в мобільних ОС, виділити їх сильні та слабкі сторони, а також визначити перспективи розвитку.

Класифікація видів кіберзахисту в мобільних ОС. В таблиці 1 показані різні рівні кіберзахисту з наведенням механізмів та прикладів реалізації цих рівнів захисту [3].

Таблиця 1

Класифікація видів кіберзахисту в мобільних ОС

Рівень захисту	Механізми захисту	Приклади реалізації
Апаратний	Шифрування чіпів, довірене середовище	Apple Secure Enclave, Titan M
Програмний	Пісочниця, контроль дозволів	SELinux (Android), App Sandbox (iOS)
Мережевий	VPN, фільтрація трафіку, firewall	Private Relay (iOS), захисні проксі
Поведінковий	Аналіз активності, евристика	Google Play Protect
Користувальницький	Біометрія, PIN, 2FA	Face ID, Touch ID, Smart Lock

Апаратні механізми захисту. Сучасні мобільні ОС використовують вбудовані апаратні модулі безпеки:

– Secure Enclave (Apple) – співпроцесор, який зберігає ключі шифрування та обробляє біометрію;

– Titan M (Google Pixel) – чіп, який перевіряє цілісність завантаження та керування ключами.

Схема порівняння Secure Enclave (Apple) та Titan M представлена на рисунку 1.

Програмний захист. На рівні програмного захисту використовується:

– пісочниця (sandboxing) – кожна програма працює у своєму ізольованому середовищі. Це обмежує доступ до даних та запобігає розповсюдженню шкідливого коду;

– контроль дозволів – система запитує у користувача доступ до чутливих функцій (камера, мікрофон, розташування). У iOS дозволи видані суворо, в Android – гнучкіше, але це спричиняє ризик. В таблиці 2 порівняно контролю дозволів в Android та iOS.

Аутентифікація та керування доступом. Використовуються такі методи:

– паролі та PIN-коди;

– біометрія (Face ID, Touch ID, відбиток);

– двофакторна аутентифікація (2FA).

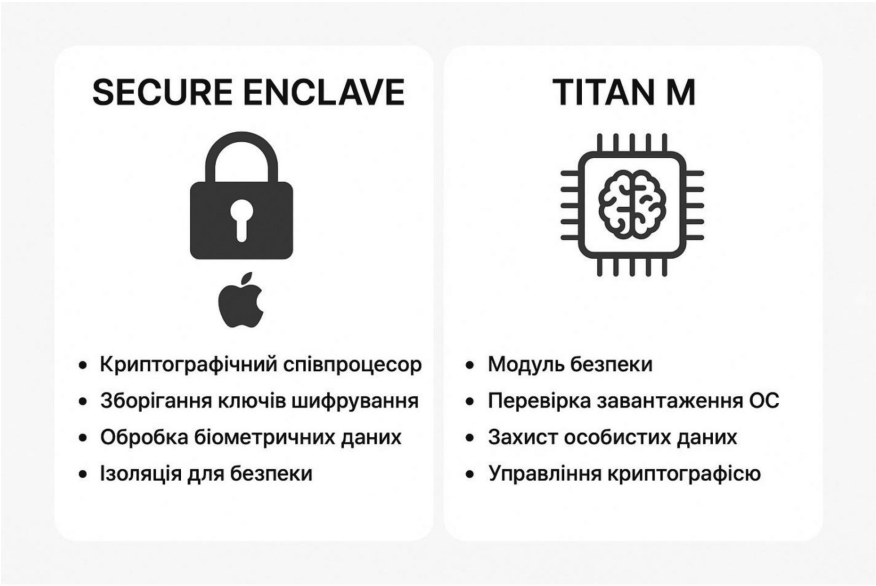

Рис. 1. Архітектура апаратного захисту в iOS та Android

Таблиця 2

Порівняння контролю дозволів в Android та iOS

Функція	Android	iOS
Запит дозволів	Під час встановлення або використання	Тільки при використанні або завжди
Зміна прав	Дозволено користувачем	Через налаштування
Обґрунтування доступу	Необов'язково	Обов'язково

Нижче наведена формула оцінки стійкості пароля:

$$S = N^L, \tag{1}$$

де S – загальна кількість можливих комбінацій;

N – кількість допустимих символів;

L – довжина пароля.

Наприклад: за $N = 62$, $L = 8 \rightarrow S = 2{,}18 \cdot 10^{14}$.

Мережеві та хмарні механізми захисту. Виділяють такі мережеві та хмарні механізми захисту [5]:

– VPN та захищений DNS. Використовуються для захисту мережевого трафіку та запобігання MITM-атакам;

– Private Relay (iCloud+) – маскує IP-адресу користувача та шифрує DNS-запити;

– Google Play Protect – перевіряє програми до та після встановлення, виявляє шкідливу поведінку.

На рисунку 2 наочно представлена схема роботи Private Relay та Google Play Protect.

Типові загрози та методи захисту. В таблиці 3 показані типові загрози для операційних систем мобільних телефонів [6].

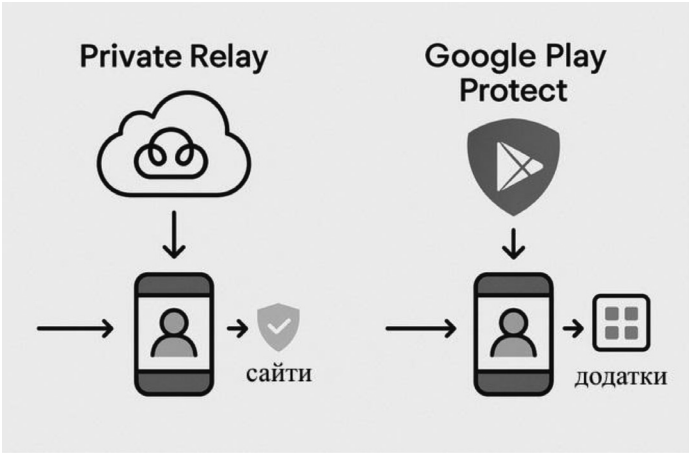

Рис. 2. Схема роботи Private Relay та Google Play Protect

Таблиця 3

Типові загрози та методи захисту

Загроза	Методи захисту
Шкідливі програми	Перевірка підписів, магазини програм, sandbox
Фішинг та соціальна інженерія	Антифішинг-фільтри, навчання користувача
Уразливості ОС	Регулярні оновлення, контроль цілісності
Перехоплення трафіку	VPN, HTTPS, firewall

Порівняльний аналіз Android та iOS за рівнями захисту. В таблиці 4 представлений порівняльний огляд систем безпеки Android та iOS за різними критеріями.

Таблиця 4

Порівняльний огляд систем безпеки

Критерій	Android	iOS
Частота оновлень	Залежать від виробника	Централізовано, часто
Встановлення сторонніх програм	Дозволено	Заборонено
Контроль доступу додатків	Менш суворий	Жорсткий
Захищеність від фішингу	Середня	Висока
Рівень ізоляції програм	Високий (але варіюється)	Дуже високий

Висновки. Операційні системи мобільних телефонів розвивають дедалі складніші механізми захисту, поєднуючи апаратні, програмні та поведінкові методи. Незважаючи на відмінності в архітектурі та ступені відкритості Android та iOS, обидві системи демонструють високий рівень кіберзахисту. Однак уразливості залишаються, особливо при застарілих версіях ОС та низької цифрової грамотності користувача. Майбутнє мобільної безпеки пов'язане з розвитком штучного інтелекту для аналізу загроз у реальному часі, більш прозорою політикою конфіденційності та навчанням користувачів. Комплексний підхід, що включає як технічні заходи, так і свідому поведінку власника пристрою, залишається ключем до ефективного захисту від кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Безпека і кібербезпека смартфонів. *Datami Newsroom*. 2025. URL: https://datami.ee/ua/blog/bezpeka-i-kiberbezpeka-smartfoniv/ (дата звернення: 22.04.2025).

2. Кібербезпека. Аспект 2: мобільні телефони. *Міністерство оборони України*. URL: https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-2-mobilni-telefoni.html (дата звернення: 22.04.2025).

3. Практичні підходи до кіберзахисту мобільних пристроїв за допомогою рішення Endpoint Detection and Response / Р. Штонда та ін. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. Том 1, № 21. С. 17–31. ISSN 2663-4023. DOI: https://doi.org/10.28925/2663-4023.2023.21.1731

4. Безпека мобільних пристроїв. *Кібер Брама*. URL: https://stopfraud.gov.ua/cybersecurity-in-life/bezpeka-mobilnyh-prystroyiv-i734 (дата звернення: 23.04.2025).

5. Безпека у хмарі: поради та кращі практики. *Smart*. 2023. URL: https://cloud.smart-it.com/news-post/cloud-security-tips-and-best-practices/ (дата звернення: 24.04.2025).

6. Інтернет-безпека телефона: як запобігти інфікуванню пристроїв. ESET. 2019. URL: https://www.eset.com/ua/about/newsroom/blog/smartphone-security/internet-bezopasnost-telefona-kolichestvo-vredonosnykh-programm-dlya-mobilnykh-devaysov-vozroslo/?srsltid=AfmBOoouo2vzh7CtIfYsO8OuzYxKOiHWraRxnEz-GWOZA6uslkFRLmB43 (дата звернення: 24.04.2025).

REFERENCES:

1. (2025) Bezpeka i kiberbezpeka smartfoniv [Smartphone safety and cybersecurity]. *Datami Newsroom*. Retrieved from https://datami.ee/ua/blog/bezpeka-i-kiberbezpeka-smartfoniv/ (date of access: 22.04.2025) [in Ukrainian].

2. Kiberbezpeka. Aspekt 2: mobilni telephony [Cybersecurity. Aspect 2: Mobile Phones]. *Ministerstvo oborony Ukrainy – Ministry of Defense of Ukraine*. Retrieved from https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-2-mobilni-telefoni.html (date of access: 22.04.2025) [in Ukrainian].

3. R. Shtonda and others (2023). Praktychni pidkhody do kiberzakhystu mobilnykh prystroiv za dopomohoiu rishennia Endpoint Detection and Response [Practical approaches to mobile cyber security using Endpoint Detection and Response solutions]. Elektronne fakhove naukove vydannia “Kiberbezpeka: osvita, nauka, tekhnika” – Electronic scientific publications “Cybersecurity: education, science, technology”. Volume 1, № 21, 17–31. ISSN 2663-4023. DOI: https://doi.org/10.28925/2663-4023.2023.21.1731 [in Ukrainian].

4. Bezpeka mobilnykh prystroiv [Mobile device security]. *Kiber Brama – Cyber Gate*. Retrieved from https://stopfraud.gov.ua/cybersecurity-in-life/bezpeka-mobilnyh-prystroyiv-i734 (date of access: 23.04.2025) [in Ukrainian].

5. (2023) Internet-bezpeka telefona: yak zapobihty infikuvanniu prystroiv [Phone Internet Security: How to Prevent Devices from Being Infected]. *Smart*. Retrieved from https://cloud.smart-it.com/news-post/cloud-security-tips-and-best-practices/ (date of access: 24.04.2025) [in Ukrainian].

6. (2019) Internet-bezpeka telefona: yak zapobihty infikuvanniu prystroiv [Phone Internet Security: How to Prevent Devices from Being Infected]. *ESET*. Retrieved from https://www.eset.com/ua/about/newsroom/blog/smartphone-security/internet-bezopasnost-telefona-kolichestvo-vredonosnykh-programm-dlya-mobilnykh-devaysov-vozroslo/?srsltid=AfmBOoouo2vzh7CtIfYsO8OuzYxKOiHWraRxnEz-GWOZA6uslkFRLmB43 (date of access: 24.04.2025) [in Ukrainian].