НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

8. Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова КМУ від 13 листопада 2025 року, № 1471. URL: https://zakon.rada.gov.ua/laws/show/1471-2025-п#n8
9. DataMining з використанням Python. Навчальний посібник // Юрченко І.В.– Чернівці: Чернівецький національний університет імені Юрія Федьковича, 2024.– 143 с. URL: https://surl.lu/szhxwy

Ключові слова: кібербезпека, управління кібербезпекою, кіберінцидент, кіберзлочин, ранжування кіберінциндентів, методи та засоби кібербезпеки.
Key words: cybersecurity, cybersecurity management, cyber incident, cyber crime, cyber incident ranking, cybersecurity methods and tools

БЕЗПЕКА ANDROID-ЗАСТОСУНКІВ НА KOTLIN ТА JETPACK COMPOSE

Манаков Сергій

кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Безпека мобільних застосунків у 2025 році стає актуальною компетенцією для розробників через швидку еволюцію загроз. Нативні Android-застосунки на Kotlin та Jetpack Compose вимагають особливого підходу до безпеки. Метадані компілятора Kotlin зберігають оригінальні імена навіть після обфускації, що спрощує зворотну розробку [1]. Дослідження показують, що жорстко закодовані API-ключі легко витягуються з APK, а багато застосунків використовують SharedPreferences без шифрування.

Основні загрози включають неправильне поводження з обліковими даними, слабку автентифікацію, недостатній захист бінарних файлів та небезпечне зберігання даних [2]. Особливої актуальності набула безпека ланцюга постачання для Compose-застосунків через інтенсивне використання залежностей та відсутність специфікації Software Bill of Materials. Важливою зміною 2025 року стала депрекація бібліотеки androidx.security:security-crypto, що вимагає міграції на пряме використання Android Keystore (база даних сертифікатів безпеки, яка створюється за допомогою програми keytool із пакету SDK для Java).

Практичні дослідження виявляють систематичні помилки безпеки в Kotlin-застосунках [3]. Серед найпоширеніших – жорстко закодовані облікові дані, зберігання секретів у налаштуваннях збирача проєктів gradle, ігнорування обфускації метаданих Kotlin та відсутність обробника винятків корутин CoroutineExceptionHandler. Специфічними для Compose помилками є зберігання чутливих даних у remember, витоки пам'яті через неправильне

використання DisposableEffect та захоплення у лямбда-виразах, що утримуються у ViewModel.

Для захисту даних Android Keystore System забезпечує апаратну ізоляцію ключів [4]. Рекомендованими алгоритмами є AES-256-GCM, ChaCha20-Poly1305 та ECC P-256+. Заборонено використовувати DES, 3DES, RC4, MD5, SHA-1 та RSA з ключами менше 2048 біт [5]. Для захисту локального сховища слід використовувати Encrypted Room з SQLCipher, а для DataStore реалізовувати власний шар шифрування. Ієрархія безпеки для зберігання ключів включає проксі на стороні сервера, Android Keystore, сховище NDK/C++ та BuildConfig.

Безпека API вимагає комплексного підходу [6]. У Retrofit та OkHttp захист забезпечується через interceptor'и та authenticatorи', які автоматично обробляють оновлення токенів. Ktor Client має вбудовану підтримку плагіну Auth з механізмом оновлення та захистом від атак DoS. Google не рекомендує закріплення сертифіката (certificate pinning), але якщо таке необхідне, слід використовувати резервні сертифікати (backup pins) та моніторинг терміну дії [7]. Network Security Configuration є рекомендованим методом 2025 року для налаштування безпеки мережі. Для автентифікації слід використовувати OAuth 2.0 та JWT, при цьому PKCE є обов'язковим для нативних застосунків. Найкращі практики для JWT включають короткий термін дії, валідацію при кожному використанні, зберігання в EncryptedSharedPreferences та використання м'ютекса для оновлення токена.

Специфіка безпеки Jetpack Compose включає проблему з наслідуванням FLAG_SECURE у спливаючих вікнах, що призводить до витоку даних через знімки екрана. Також, використання immutable String для полів паролів унеможливлює їх очищення з пам'яті, дозволяючи вилучення через дампи пам'яті. В свою чергу, поширеною проблемою є витоки даних через керування станом, коли remember зберігає чутливі дані довше, ніж потрібно, а також витоки пам'яті через захоплення у лямбда-виразах та неправильне використання DisposableEffect.

Інтеграція DevSecOps також стає необхідністю [8]. Підхід Shift-left security передбачає інтеграцію перевірок безпеки з першого дня розробки. Для статичного та динамічного аналізу використовуються інструменти MobSF, Detekt та SonarQube [9]. Безпековий конвеєр в GitHub Actions може включати валідацію Gradle Wrapper, Detekt, сканування через MobSF та OWASP Dependency-Check. Шлюзи безпеки (security gates) в CI/CD блокують збірки з критичними вразливостями. Для тестування на проникнення застосовують Frida, Objection, Drozer та Burp Suite [10].

Практичні рекомендації включають використання Android Keystore для ключів, EncryptedSharedPreferences для токенів, вимкнення логування чутливих даних та резервних копій (android:allowBackup=false), використання

FLAG_SECURE. Для криптографії слід застосовувати AES-256-GCM та SecureRandom. В автентифікації рекомендовані Credential Manager API, Passkeys, біометрія, валідація JWT та механізми захисту від перебору. Мережева безпека вимагає TLS 1.2+ та відмови від нешифрованого трафіку (cleartextTrafficPermitted=false). Безпека платформи передбачає мінімальні дозволи та валідацію вхідних даних. Якість коду забезпечується обфускацією ProGuard/R8, регулярним оновленням залежностей та використанням Play Integrity API.

Отже, безпека Android-застосунків на Kotlin та Jetpack Compose у 2025 році вимагає комплексного підходу. Обфускація є недостатньою через розкриття метаданих Kotlin. Депрекація бібліотеки Jetpack Security crypto вимагає глибокого розуміння Android Keystore API. Jetpack Compose створює виклики, пов'язані з FLAG_SECURE, обробкою паролів та витоками пам'яті. Інтеграція інструментів DevSecOps (MobSF, Detekt) в CI/CD стала необхідністю. Підхід Shift-left security забезпечує раннє виявлення вразливостей, що суттєво знижує вартість виправлення. Основні рекомендації розробникам являють: використання Android Keystore, імплементація OAuth 2.0 з PKCE, обережне застосування закріплення сертифіката, регулярне оновлення залежностей та проведення тестування безпеки.

Список використаних джерел

1. Mazuera-Rozo A., Escobar-Velásquez C., Espitia-Acero J., Vega-Guzmán D., Trubiani C., Linares-Vásquez M., Bavota G. Taxonomy of security weaknesses in Java and Kotlin Android apps. *Journal of Systems and Software*. 2022. Vol. 187. P. 111233. DOI: https://doi.org/10.1016/j.jss.2022.111233
2. Garg S., Baliyan N. Android security assessment: A review, taxonomy and research gap study. *Computers & Security*. 2021. Vol. 100. P. 102087. DOI: https://doi.org/10.1016/j.cose.2020.102087
3. Egele M., Brumley D., Fratantonio Y., Kruegel C. An empirical study of cryptographic misuse in android applications. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. P. 73-84. DOI: https://doi.org/10.1145/2508859.2516693
4. Enck W., Nadkarni A. Android's Security Framework: Understanding the Security of Mobile Phone Platforms. Encyclopedia of Cryptography, Security and Privacy. Springer, 2021. DOI: https://doi.org/10.1007/978-3-642-27739-9_121-2
5. Kalanj M., Popović T., Krčo S. Analysis of Cryptography Algorithms Implemented in Android Mobile Application. *Information Technology and Control*. 2021. Vol. 50, No. 4. P. 786-803. DOI: https://doi.org/10.5755/j01.itc.50.4.29464
6. Sun Y., Wang Y., Zhang Q., Chen K. CryptoEval: Evaluating the risk of cryptographic misuses in Android apps with data-flow analysis. *IET Information Security*. 2023. Vol. 17, No. 4. P. 564-580. DOI: https://doi.org/10.1049/ise2.12117
7. Ardito L., Coppola R., Malnati G., Torchiano M. Effectiveness of Kotlin vs. Java in android app development tasks. *Information and Software Technology*. 2020. Vol. 127. 106374. DOI: https://doi.org/10.1016/j.infsof.2020.106374

8. Abiona O. O., Oladapo O. J., Modupe O. T., Oyeniran O. C., Adewusi A. O., Komolafe A. M. The emergence and importance of DevSecOps: Integrating and reviewing security practices within the DevOps pipeline. *World Journal of Advanced Engineering Technology and Sciences*. 2024. Vol. 11, No. 2. P. 127-133. DOI: https://doi.org/10.30574/wjaets.2024.11.2.0093
9. Zhao X., Hoda R., Clear T., MacDonell S. G. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *Journal of Systems and Software*. 2024. Vol. 214. 112059. DOI: https://doi.org/10.1016/j.jss.2024.112059
10. Akbar M. A., Smolander K., Mahmood S., Alsanad A. Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology*. 2022. Vol. 147. 106894. DOI: https://doi.org/10.1016/j.infsof.2022.106894

Ключові слова: безпека Android, Kotlin, Jetpack Compose, криптографія мобільних застосунків, DevSecOps, вразливості застосунків, захист даних.
Keywords: Android security, Kotlin, Jetpack Compose, mobile application cryptography, DevSecOps, application vulnerabilities, data protection.

КОНЦЕПЦІЯ ТА РОЗГОРТАННЯ ВИСОКОІНТЕРАКТИВНОГО ХАНІПОТУ НА НА ОСНОВІ ЕМУЛЯЦІЇ ЛЕГІТИМНОГО ВЕБСЕРВЕРА (NGINX)

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Ханіпотом (медовим горщиком) називають спеціальний пасивний засіб захисту — по суті, пастку, що є приманкою для шкідливого програмного забезпечення. По суті, це — спеціалізований пасивний засіб збору розвідувальних даних, що є приманкою для зловмисників та шкідливого ПЗ, основне завдання якого виявляти нові й цільові атаки Zero-day, які погано піддаються розпізнаванню традиційними методами [1].

Існуючі рішення для ханіпотів традиційно поділяються на дві основні категорії: низькоінтерактивні та високоінтерактивні. Низькоінтерактивні ханіпоти, як-от Cowrie (для емуляції SSH) або Dionaea (для мережевих сервісів), швидко емулюють лише необхідні аспекти реального сервісу, що робить їх економічними, але водночас вкрай вразливими до автоматизованого розпізнавання досвідченими ботами та зловмисниками. Натомість, високоінтерактивні ханіпоти використовують повну віртуалізацію операційної системи або сервісу, що вимагає значно більших ресурсів, але надає максимально детальні та цінні розвідувальні дані про поведінку атакуючого. Більшість готових комерційних та open-source рішень часто є гібридами, які намагаються знайти баланс між ресурсоємністю та глибиною взаємодії, проте їхня широка відомість і типові мережеві відбитки є головною вразливістю [2].

ЗМІСТ