УДК 004.056:004.056.5:004.056.2 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.9

Є. М. БРОВЧЕНКО
аспірант
Інститут комп'ютерних технологій
Відкритого міжнародного університету розвитку людини «Україна»
ORCID: 0000-0002-1416-0385

В. П. САМАРАЙ
кандидат технічних наук, старший науковий співробітник, доцент
Інститут комп'ютерних технологій
Відкритого міжнародного університету розвитку людини «Україна»
ORCID: 0000-0003-4419-1366

АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ НЕСТРУКТУРОВАНОЇ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ: СУЧАСНІ ВИКЛИКИ ТА ТЕНДЕНЦІЇ

У статті досліджено проблеми захисту неструктурованих даних на мобільних пристроях у контексті тривалих сесій, де одноразова автентифікація не забезпечує належного рівня безпеки. Запропоновано концептуальну рамку, що поєднує безперервну поведінкову автентифікацію, даноцентричні політики доступу та гібридну криптоконфігурацію: симетричне шифрування для контенту та асиметричне – для ключів. ***Мета.*** *Обґрунтувати модель, яка мінімізує ризики доступу до повідомлень, медіа, вкладень і кешованих даних у межах активної сесії. Основна увага приділяється поєднанню AES ↔ ECC, MFA ↔ поведінкової перевірки, а також безперервному моніторингу на основі динаміки дотиків, даних інерціальних сенсорів, злиття ознак, оцінок і рішень, ризик-адаптивних дій, локального та федеративного навчання, а також відтворюваних метрик.* ***Методи.*** *Здійснено огляд літератури з баз даних Web of Science та Scopus; систематизовано підходи до безперервної автентифікації та сенсорного злиття; проаналізовано гігієну дозволів і життєвий цикл тимчасових копій; розглянуто політики на основі підкріплення (RL) для step-up автентифікації та повторної перевірки; узгоджено модель із сучасними нормами керування сесіями та вимогами криптостійкості.* ***Результати.*** *Одноразова автентифікація не гарантує сталості ідентичності користувача. Безперервна перевірка, підсилена сенсорним злиттям, дозволяє зменшити «вікно ризику» без потреби у надмірних явних діях. Дотикові ознаки демонструють високу ефективність, а інерціальні сенсори забезпечують фоновий контроль. Політики RL активують втручання лише за умов підвищеного ризику (reauth, маскування прев'ю, призупинення експорту). Даноцентричні політики доступу зменшують площу атаки з урахуванням дозволів, побічних сенсорних каналів, форензичних артефактів, платформенних уразливостей. Нормативний блок закріплює гібридну модель «AES для контенту ↔ ECC для ключа/підписів» та доповнює її MFA і пост-логін моніторингом.* ***Висновки.*** *Запропонована конфігурація включає три основні компоненти: безперервна поведінкова перевірка; даноцентричні політики доступу (керування прев'ю, кешами, тимчасовими копіями, дозволами); гібридна криптографія, де симетричне шифрування захищає контент, а асиметричне – ключі та цифрові підписи. Інтеграція цих компонентів забезпечує баланс між точністю, затримками та енергоефективністю, що робить модель придатною для корпоративного використання та захищених месенджерів.*

Ключові слова: *безперервна автентифікація, мультибіометрія, даноцентричні політики доступу, гібридне шифрування AES/ECC, сесійний моніторинг.*

E. M. BROVCHENKO
Postgraduate Student
Institute of Computer Technologies
of Open International University of Human Development "Ukraine"
ORCID: 0000-0002-1416-0385

V. P. SAMARAY
Ph.D. in Technical Sciences, Senior Research Fellow, Associate Professor
Institute of Computer Technologies
of Open International University of Human Development "Ukraine"
ORCID: 0000-0003-4419-1366

ANALYSIS OF UNSTRUCTURED DATA PROTECTION ON MOBILE DEVICES: CURRENT CHALLENGES AND TRENDS

This article examines the challenges of protecting unstructured data on mobile devices in the context of prolonged sessions, where one-time authentication does not ensure an adequate level of security. A conceptual framework is proposed that combines continuous behavioral authentication, data-centric access policies, and a hybrid cryptographic configuration: symmetric encryption for content and asymmetric encryption for keys.

Purpose. *To substantiate a model that minimizes the risks of unauthorized access to messages, media, attachments, and cached data within an active session. The focus is on integrating AES with ECC, MFA with behavioral verification, as well as continuous monitoring based on touch dynamics, inertial sensor data, feature fusion, scoring and decision systems, risk-adaptive actions, local and federated learning, and reproducible metrics.*

Methods. *A literature review was conducted using Web of Science and Scopus databases; approaches to continuous authentication and sensor fusion were systematized; permission hygiene and the lifecycle of temporary copies were analyzed; reinforcement learning (RL)-based policies for step-up authentication and re-verification were examined; the proposed model was aligned with modern session management standards and cryptographic resilience requirements.*

Results. *One-time authentication does not guarantee the continuity of user identity. Continuous verification enhanced by sensor fusion reduces the "risk window" without requiring excessive explicit actions. Touch-based features demonstrate high effectiveness, while inertial sensors provide background monitoring. RL-driven policies trigger interventions only under elevated risk conditions (reauthentication, preview masking, export suspension). Data-centric access policies reduce the attack surface by accounting for permissions, side-channel sensor leaks, forensic artifacts, and platform vulnerabilities. The regulatory block consolidates the hybrid model "AES for content ↔ ECC for keys/signatures" and complements it with MFA and post-login monitoring.*

Conclusions. *The proposed configuration incorporates three key components: continuous behavioral verification; data-centric access policies (management of previews, caches, temporary copies, permissions); and hybrid cryptography, where symmetric encryption protects content while asymmetric encryption secures keys and digital signatures. The integration of these components ensures a balance between accuracy, latency, and energy efficiency, making the model suitable for corporate environments and secure messengers.*

Key words: *continuous authentication, multibiometrics, data-centric access policies, hybrid AES/ECC encryption, session monitoring.*

Постановка проблеми

Мобільні пристрої стали ключовим середовищем для створення, оброблення й обміну неструктурованою інформацією, зокрема текстовими повідомленнями, зображеннями, голосовими та відеофайлами, вкладеннями електронної пошти й месенджерів, кешами застосунків і файлами хмарних сервісів. На відміну від структурованих даних, характеризується високою мінливістю, фрагментарністю та схильністю до дублювання у різних контейнерах. Він постійно мігрує між корпоративним і персональним середовищами, особливо в умовах моделей BYOD та COPE. Різнорідність форматів, фрагментація мобільних екосистем, велика кількість дозволів, інтеграція сторонніх SDK, а також уразливості ланцюгів постачання створюють значні труднощі для класифікації чутливості даних, контролю доступу, журналювання активності та запобігання витокам інформації на рівні ендпоїнта (кінцевого пристрою).

Нормативні тенденції формують багатовимірний контекст проблеми захисту неструктурованих даних на мобільних пристроях. Поширення безпарольних методів автентифікації та вимога забезпечення «безшовного» користувацького досвіду зумовлюють потребу у безперервному підтвердженні особи на основі поведінкових ознак. Це, своєю чергою, висуває суворі вимоги до точності, стійкості до підробок і захисту приватності користувача. Впровадження наскрізного та клієнтського шифрування сприяє забезпеченню конфіденційності, але водночас ускладнює реалізацію механізмів контролю витоків даних (DLP) та аудиту. Розбудова архітектур Zero Trust на мобільних ендпоїнтах потребує контекстно- та контент-орієнтованого прийняття рішень в умовах обмежених обчислювальних і енергетичних ресурсів. Поява постквантової криптографії на горизонті розвитку безпеки ставить додаткові вимоги до криптоагільності, сумісності алгоритмів та адаптивності систем. Крім того, сучасні нормативні рамки, зокрема вимоги до безпеки оброблення даних та повідомлення про інциденти, зобов'язують забезпечити керованість усього життєвого циклу неструктурованої інформації.

Наукова складова дослідження полягає у формалізації моделей ризику для потоків неструктурованого контенту на мобільних пристроях, розробленні методів безперервної автентифікації з відтворюваними метриками та чіткими гарантіями приватності, синтезі контент- та контекст-орієнтованого контролю доступу в операційних системах, створенні алгоритмів автоматичного класифікування та лейблування даних для подальшого застосування політик DLP, а також у проєктуванні криптоагільних схем шифрування й відкритих бенчмарків для об'єктивної оцінки ефективності рішень.

Практична значущість дослідження проявляється у необхідності побудови мобільних Zero Trust-ландшафтів із керованими політиками доступу та телеметрією, впровадженні інтегрованих рішень, що поєднують класифікацію, лейблування, DLP і DRM/IRM для захисту контенту як на пристрої, так і в хмарному середовищі. Важливим

є також планування міграції до постквантових криптографічних профілів без деградації продуктивності, а також забезпечення відповідності регуляторним вимогам шляхом впровадження доказового журналювання, атестації та регулярних оцінок ризиків.

Таким чином, досліджувана проблема має міждисциплінарний характер і потребує узгоджених рішень на перетині безпеки даних, мобільної інженерії, криптографії та управління ризиками. Це дозволяє досягти стійкої рівноваги між конфіденційністю, спостережністю контрольних механізмів та зручністю для кінцевого користувача.

Аналіз останніх досліджень і публікацій

Проблема захисту неструктурованої інформації на мобільних пристроях послідовно висвітлюється у сучасних наукових працях, які охоплюють спектр від методів безперервної автентифікації до ширшого контексту загроз і уразливостей платформ. C. J. Jose і M. S. Rajasree запропонували модель імпліцитної безперервної автентифікації на основі підкріплювального навчання, яка адаптує рішення до змінних патернів взаємодії користувача. Водночас модель є чутливою до дрейфу даних і нестабільності сенсорних потоків [1].

D. Reichinger, E. Sonnleitner і M. Kurz продемонстрували переваги мультимодальної фузії поведінкових ознак над одномодальними підходами. Вони окреслили компроміс між точністю, затримкою та енергоспоживанням, що особливо важливо для реалізації таких рішень безпосередньо на мобільному пристрої [2].

P. M. A. B. Estrela, R. d. O. Albuquerque, D. M. Amaral, W. F. Giozza і R. T. de Sousa Júnior зосередили увагу на банківських сценаріях, досліджуючи динаміку дотиків як поведінкову ознаку. Вони продемонстрували життєздатність запропонованого рішення у продуктивному середовищі, водночас виявивши ризики імітаційних атак через відтворення жестів користувача [3]. S. Mekruksavanich і A. Jitpattanakul показали потенціал глибинних моделей, що навчаються на патернах активності, отриманих із мобільних сенсорів. Автори наголосили на критичній ролі коректного визначення вікон агрегації та вибору методів забезпечення приватності як у процесі навчання моделей, так і під час здійснення інференсу безпосередньо на кінцевому ендпоїнті [4].

P. Bansal і A. Ouda здійснили порівняльний аналіз поведінкових біометричних ознак і методів підкріплювального навчання для безперервної автентифікації. Вони акцентували увагу на проблемі узагальнюваності моделей між різними пристроями та відсутності уніфікованих бенчмарків, що ускладнює коректне порівняння результатів [5]. A. Ramaswamy та співавтори досліджували багатопристроєві сценарії, де здійснюється кореляція потоків даних з кількох смартпристроїв. Це дозволило виявити переваги фузії даних, але водночас підкреслило залежність загальної стійкості системи від надійності окремих вузлів екосистеми [6].

M. Abuhamad, A. Abusnaina, D. Nyang і D. Mohaisen здійснили систематизацію сенсорно орієнтованих підходів до безперервної автентифікації на смартфонах, а також типових векторів атак. Вони звернули увагу на дефіцит публічних, репрезентативних датасетів і різноспрямованість протоколів оцінювання, що ускладнює відтворюваність результатів і порівнянність моделей [7].

J. A. Delgado-Santos та співавтори показали, як мобільні сенсори можуть створювати побічні канали витоку неструктурованих даних. Дослідники обґрунтували необхідність запровадження обмежень на рівні операційної системи, а також розроблення продуманої моделі дозволів і прозорості для користувача [8]. P. Weichbroth і Ł. Łysik узагальнили сучасний ландшафт мобільних загроз і практик безпеки, підкреслили важливість поєднання гігієни дозволів, сегментації середовища і вбудованої криптографії з підходами, орієнтованими на дані та їхній рух між контейнерами [9]. A. Muñoz наголошує, що апаратні уразливості платформи Android здатні нівелювати прикладні політики безпеки, що свідчить про необхідність врахування взаємодії між апаратним і програмним рівнями в моделях ризику, а також про залежність рівня довіри від конкретної реалізації платформи [10].

S. Lee та колеги запропонували використання федеративного навчання для виявлення шкідливих застосунків із збереженням приватності і водночас окреслили виклики, пов'язані з різнорідністю пристроїв і загрозами отруєння під час розподіленого тренування моделей [11]. S. Ullah та співавтори дослідили поведінку користувачів щодо надання дозволів і виявили систематичні хиби в оцінці ризику, що пояснює витоки даних через формально дозволені доступи та вимагає вдосконалення інтерфейсів керування приватністю [12]. A. K. Sikder та співавтори здійснили огляд сенсорно орієнтованих атак і побічних каналів для смартпристроїв і підсумували необхідність багаторівневих механізмів захисту на етапах збирання і попередньої обробки даних [13]. S. Hutchinson та співавтори, на прикладі фітнес-застосунків, показали, як журнали активності і телеметрія формують вторинні носії неструктурованих даних із ризиковими налаштуваннями приватності, що має важливе значення для реалізації політик DLP безпосередньо на пристрої [14]. Z. Muhammad та колеги узагальнили загрози, що походять від цілеспрямованих атак і невідомих вразливостей у контексті смартфонів. Дослідники посилили аргументацію на користь поведінково-контекстних контролів доступу та безперервної автентифікації [15].

A. Alkinoon та співавтори простежили еволюцію шаблонів використання дозволів і характеристик мобільних застосунків і запропонували індикатори для профілювання ризику та пріоритизації політик на рівні ендпоїнта [16].

D. Progonov та співавтори узагальнили методи поведінкової автентифікації на мобільних пристроях у різних умовах використання та звернули увагу на точність, частоту хибних спрацювань і стійкість до відтворення поведінки користувача [17].

З урахуванням наведеного аналізу, залишаються відкритими низка критичних питань, що стримують прогрес у сфері захисту неструктурованих даних на мобільних пристроях. Насамперед, відсутність узгоджених публічних бенчмарків для реалістичних сценаріїв ускладнює відтворюваність результатів і коректне порівняння підходів. Якість моделей значною мірою залежить від складу датасетів та протоколів оцінювання, що створює ризики обмеженої узагальнюваності. Особливо слабкою є міжплатформна переносимість: навіть високоточні моделі демонструють деградацію продуктивності при перенесенні між версіями ОС і класами пристроїв. Ця проблема загострюється компромісами між точністю, швидкодією та енергоспоживанням, а також труднощами кореляції потоків у багатопристроєвих конфігураціях. Недостатньо вирішеною залишається стійкість до відтворення поведінки користувача (spoofing), маніпуляцій із сенсорами та атак отруєння даних у процесі розподіленого навчання. Незважаючи на значний прогрес у дослідженнях, зберігаються апаратно-програмні ризики, здатні нівелювати прикладні політики безпеки, а також поведінкові хиби користувачів процесі надання дозволів. Це сприяє формуванню вторинних носіїв чутливої інформації у телеметрії та журналах активності.

Водночас бракує інтегрованих рішень, що поєднують безперервну автентифікацію з даноцентричними політиками доступу для неструктурованого контенту безпосередньо на пристрої, з урахуванням руху даних між контейнерами та загроз цілеспрямованих атак. Потребують подальшого розвитку прозорість і пояснюваність моделей, а також баланс між точністю, приватністю та зручністю для користувача. Ці аспекти підтверджують узагальнення та емпіричні спостереження останніх дослідженнях.

Формулювання мети дослідження

Метою статті є обґрунтування та пропозиція цілісної рамки захисту неструктурованої інформації на мобільних пристроях, яка поєднує безперервну поведінкову автентифікацію, даноцентричні політики доступу та сучасні криптографічні засоби. Запропонована модель враховує обмеження продуктивності, енергоспоживання та вимоги до приватності, що є критично важливими для мобільного середовища. Актуальність дослідження зумовлена тим, що саме неструктурований контент становить більшість корпоративних даних, активно мігрує між контейнерами та каналами передачі, і є основною мішенню витоків інформації. Наявні підходи до його захисту залишаються фрагментованими, не забезпечують узгоджених критеріїв вибору рішень і не гарантують відтворюваності результатів у реалістичних сценаріях.

Для досягнення поставленої мети спочатку сформовано формальну модель загроз і контекстів використання неструктурованого контенту на мобільному ендпоїнті; уточнено, де й чому виникають витоки даних, а також проаналізовано вплив платформи, системи дозволів і поведінки користувача.

Наступним етапом здійснено порівняльний аналіз методів шифрування та автентифікації, у межах якого розглянуто практичні ролі й обмеження алгоритмів AES та ECC у забезпеченні захисту контенту та керуванні ключами, а також досліджено взаємодоповнюваність класичної багатофакторної автентифікації та поведінкової аналітики у формуванні довіри на етапі входу й упродовж сесії.

На основі отриманих результатів запропоновано архітектурний підхід, який поєднує безперервну автентифікацію з класифікацією та маркуванням неструктурованих даних на пристрої, а також він включає політику запобігання витокам, орієнтовану на контент та його рух між контейнерами. Наступним кроком визначено відтворювану методику оцінювання, що охоплює чітко визначені метрики точності, затримки, енерговитрат, стійкості до відтворення поведінки, сенсорного спуфінгу та здатності до узагальнення між платформами.

Завершальним етапом є узагальнення практичних рекомендацій щодо впровадження запропонованих рішень у сценаріях корпоративного і змішаного володіння пристроями. Окрему увагу приділено вимогам до прозорості та пояснюваності процесу прийняття рішень, що забезпечує можливість їх аудиту з позицій безпеки і приватності.

Такий план забезпечує логічну послідовність викладу – від постановки ризиків до інструментальних рішень і критеріїв перевірки. Він робить внесок у науку через систематизований порівняльний аналіз і відтворюваний протокол оцінювання. Для практичного застосування план пропонує цільову архітектуру та набір перевірених кроків, що сприяють зниженню ймовірність витоків даних і підвищенню керованості неструктурованої інформації на мобільних платформах.

Викладення основного матеріалу дослідження

Мобільні пристрої стали основним середовищем, у якому виникає й циркулює неструктурована інформація, зокрема повідомлення, фото, голосові нотатки, кешовані дані та вкладення. Після розблокування пристрою цей тип контенту є найбільш уразливим, оскільки зберігається у різних контейнерах і швидко мігрує між застосунками та хмарними сервісами. Традиційні разові перевірки під час входу й периметрові бар'єри не забезпечують належного рівня безпеки в умовах динамічного середовища мобільних платформ. У зв'язку з цим виникає потреба у рішеннях, що діють упродовж усього сеансу та враховують поведінку, контекст і властивості даних. У подальшому викладі послідовно демонструється, як поєднання безперервної автентифікації, даноцентричних політик доступу та сучасних криптографічних методів сприяє зменшенню вікна ризику для неструктурованого контенту на смартфоні й забезпечують керованість без суттєвого впливу на зручність користування.

Одноразова автентифікація під час входу не усуває ключову вразливість мобільних сценаріїв. Після розблокування пристрою зловмисник може використати короткий проміжок часу, коли увага власника розсіяна, щоб отримати доступ до листування, фото, кешів застосунків та робочих документів, що не мають жорстко визначеної структури. Безперервна та неявна автентифікація зменшує це вікно ризику, оскільки система постійно звіряє поточну взаємодію з очікуваним профілем користувача й оновлює оцінку довіри протягом усього сеансу [1, с. 1358]. Важливим є врахування дрейфу поведінки. Зміни у хваті, темпі введення тексту та жестах під час руху містом або перебування у транспорті призводять до зниження точності, якщо модель автентифікації є статичною. Адаптивний підхід, який дозволяє системі змінювати рішення у часі та динамічно налаштовувати пороги прийняття, забезпечує вищу стійкість до природних коливань і повсякденних відхилень [1, с. 1360]. Доцільно також оцінювати не лише факт помилки автентифікації, а й швидкість її виявлення. Чим раніше система фіксує нетипову взаємодію, тим менше повідомлень, файлів і тимчасових артефактів встигає потрапити до сторонньої особи. У виробничих умовах це безпосередньо пов'язано з політикою доступу до неструктурованого контенту, який підтягується на екрані за запитом і може бути вибірково прихований у разі зниження рівня довіри [1, с. 1361]. Таким чином, перехід від одноразової перевірки до безперервної оцінки ідентичності формує базову лінію для подальшої логіки контролю даних на пристрої [1, с. 1359].

Надійність безперервної перевірки зростає за умови використання кількох незалежних ознак. Окремі модальності є чутливими до контексту і шумів, тоді як інтеграція кількох каналів дозволяє вирівнювати випадкові сплески та знижує ефективність спроб обману. Концептуально злиття можливе на різних рівнях – від об'єднання сирих ознак до поєднання часткових рішень, що наєдає проєктувальнику гнучкість у відповідності до обмежень часу і енергоспоживання [2, с. 2]. Поєднання фізіологічних і поведінкових характеристик підвищує стабільність у повсякденних діях, як-от прокручування стрічки або швидкий перегляд вкладень. При цьому не вимагається додаткових дій з боку користувача, якщо пороги й розміри ковзних вікон налаштовані відповідно до сценарію використання [2, с. 3]. Для мобільних систем, що працюють з неструктурованим контентом, доцільно застосовувати рішення з адаптивними вікнами накопичення сигналів. У випадках короткої взаємодії вікно стискається, що забезпечує швидке реагування моделі. Коли користувач читає довгий ланцюжок повідомлень або виконує повторювані жести, система накопичує більше контексту і знижує ймовірність хибного спрацьовування без втрати чутливості [2, с. 4].

У фінансових застосунках, де ціна помилки є особливо високою, практичним виявився підхід до безперервної перевірки на основі дотикової динаміки. Формуються профілі взаємодії з сенсорною панеллю, які відображають темп, траєкторії, силу натиску та мікропаузи. У таких системах доцільно розділяти фази логіна і постлогіна що дозволяє підтримувати низький рівень помилок і водночас уникати надмірного навантаження на користувача під час перегляду історій і вкладень [3, с. 2].

Багатоскоупне представлення дає змогу виявляти як короткі, так і довші патерни, що покращує стабільність рішення у змішаних сесіях банкінгу, коли користувач часто перемикається між екранами. Для захисту неструктурованого вмісту зручно застосовувати м'які обмеження. У разі зниження рівня впевненості система може приховувати попередні перегляди у списках або запитувати швидке підтвердження перед відкриттям вкладення, замість повного завершення сесії [3, с. 1].

Окрему увагу слід приділяти ризику імітаційних атак. У випадках, коли зловмисник намагається відтворити схожі жести за відеозаписом або тренується на викраденому пристрої, система з багатоскоупним відбором ознак ефективніше виявляє нетипові мікропатерни, знижуючи ймовірність непомітного доступу до чутливих артефактів сеансу [3, с. 4]. Цей підхід природно переноситься з банкінгу на менеджери файлів, електронну пошту та месенджери, оскільки характер взаємодії з екраном у кожного користувача є досить стабільним у межах одного дня [3, с. 5].

Інший напрямок пов'язаний із використанням інерціальних сенсорів для непомітного відтворення поведінкового підпису. Дані акселерометра, гіроскопа і магнітометра формують часові послідовності, на основі яких модель навчається відрізняти власника від сторонньої особи – навіть тоді, коли на екрані відбувається пасивне читання або швидке гортання списків. Це особливо актуально для контенту, який не має фіксованих структур і відкривається пакетно, як-от галереї або довгі чати [4, с. 1]. Результативність у таких сценаріях забезпечують глибокі архітектури, що поєднують згорткові і рекурентні компоненти. Згорткові шари ефективно виявляють локальні ритми руху, а рекурентна частина – відслідковує довготривалі залежності, що разом сприяє зниженню кількості помилкових рішень у реальних умовах, де змінюється темп взаємодії та спосіб носіння пристрою [4, с. 3]. Практична реалізація таких систем потребує ретельної нормалізації розташування й орієнтації телефона, а також вибору частоти дискретизації, яка не призводить до надмірного споживання енергії. За таких умов система залишається прозорою для користувача та не потребує додаткових дій під час роботи з повідомленнями або перегляду документів, що зберігаються у кеші застосунків [4, с. 2]. Підхід на основі інерціальних сенсорів добре узгоджується з ідеєю фонової перевірки. Модель працює у тлі і підвищує рівень контролю лише у випадках зростання сукупного ризику для поточної сесії – наприклад, коли характер рухів раптово відрізняється від звичного профілю [4, с. 4].

У розгорнутих сесіях доцільно додавати адаптивність політик через підкріплювальне навчання. Агент спостерігає за стисненим вектором показників якості перевірки та контекстних ознак, поступово навчаючись активувати або посилювати контроль у разі зростання ризику, а також зменшувати його за умов стабільної поведінки користувача. Це дозволяє досягти балансу між безпекою та зручністю для користувача, який працює з файлами та повідомленнями без додаткових бар'єрів [5, с. 2]. Важливо правильно формувати функцію винагороди, щоб система не перетворювалася на агресивний фільтр, який постійно перериває взаємодію в умовах підвищеної складності. Натомість, за правильної постановки задачі агент підтримує низький рівень інтегральної помилки та зберігає прийнятну точність на тестуванні з реальними даними, що підтверджує життєздатність такого способу керування ризиком до неструктурованих артефактів сеансу [5, с. 3]. Додатковою перевагою є енергоефективність. Агент навчається звертатися до більш витратних сенсорів або ініціювати явне підтвердження лише тоді, коли сукупна невизначеність перевищує безпечний поріг, а отже зменшує кількість зайвих звернень до користувача і подовжує час автономної роботи пристрою [5, с. 1].

У багатопристроєвих сценаріях контроль ідентичності має спиратися не на один канал спостереження, а на узгоджене трактування кількох потоків сигналів, що надходять від смартфона, носимих сенсорів і допоміжних периферійних пристроїв. Такий підхід дає змогу виявляти розбіжності між очікуваним профілем взаємодії та фактичною поведінкою, знижуючи ризик непомітного доступу до неструктурованого вмісту, коли один з вузлів екосистеми виявляється скомпрометованим або тимчасово недоступним [6, с. 2]. Ефективність підходу забезпечується застосуванням правил кореляції і часових вікон, у яких рішення кожного вузла важить пропорційно його надійності для конкретного контексту, що підвищує стабільність розпізнавання особи під час швидких перемикань між застосунками та режимами взаємодії з файлами й повідомленнями [6, с. 5]. У виробничих умовах це дозволяє реалізовувати м'які дії замість повного блокування – наприклад, система може приховати попередні перегляди вкладень у чатах або відкладене розкриття зображень до моменту, коли агрегований показник довіри не повернеться у безпечний діапазон [6, с. 7].

Систематизація методів сенсорно орієнтованої перевірки дозволяє виявити критичні обмеження, які безпосередньо впливають на захист неструктурованого контенту. Найбільш критичні серед них – нестача публічних репрезентативних датасетів, розбіжності у протоколах валідації та відсутність уніфікованих метрик, що ускладнює порівнянність і відтворюваність результатів у реальних мобільних сценаріях [7, с. 9130]. Для практики це означає, що навіть високі значення точності, отримані на контрольних вибірках, можуть не переноситися на ситуації, де користувач одночасно працює з галереєю, електронною поштою, нотатками і кешованими даними, а пристрій піддається впливу шумів руху та змін хвату [7, с. 9136]. Акцент на прозорих метриках і відкритих процедурах порівняння створює основу для впровадження політик доступу, які базуються не на декларативних порогах, а на перевірених показниках часу виявлення ймовірної підміни в активному сеансі [7, с. 9139].

Приватність сенсорів перетворюється на центральний чинник, оскільки з сирих потоків формується поведінковий підпис, що керує доступом до чутливого контенту. Аналіз уразливостей показує, що низка сенсорів здатна відновлювати фрагменти взаємодії користувача або витягувати індикатори контексту навіть без явних дозволів, що створює побічні канали витоку інформації, особливо у фонових процесах, що супроводжують роботу з неструктурованими даними [8, с. 4]. особливо у фонових процесах, що супроводжують роботу з неструктурованими даними Практичне вирішення цієї проблеми полягає у мінімізації збору даних, локальному навчанні моделей безпосередньо на пристрої та впровадженні політик, які не зберігають і не передають сирі траєкторії або графи взаємодії, залишаючи за межами пристрою лише агреговані ознаки або короткочасні оцінки ризику для прийняття рішень у реальному часі [8, с. 12]. Така організація усуває потребу у централізованому накопиченні даних про користувача, водночас зберігаючи здатність системи оперативно реагувати на ознаки захоплення сесії під час переходів між застосунками та контейнерами [8, с. 18].

З урахуванням загрозливого ландшафту архітектура захисту має виходити за межі моделі одноразового логіна і повинна включати сегментацію доступу до даних, жорстке керування дозволами та контроль міжпроцесних взаємодій. Огляд тенденцій свідчить, що поєднання гігієни дозволів із наскрізним шифруванням і контекстними перевірками під час роботи із вкладеннями, кешами та журналами знижує площу атаки, зменшує вразливість до соціальної інженерії та перенесення зловмисних активностей між застосунками [9, с. 5]. Для неструктурованих даних доцільним є запровадження режимів попереднього приховання приватного вмісту, зокрема, показ чутливих прев'ю відкладається до моменту отримання додаткового сигналу довіри від локальної поведінкової моделі, що мінімізує експозицію у випадках короткочасного відволікання користувача [9, с. 9]. Крім того, рекомендовано пов'язувати життєвий цикл тимчасових копій та індексів пошуку з поточним рівнем ризику, що дозволяє уникнути неконтрольованого накопичення відбитків неструктурованого контенту у фонових сховищах, що підвищує загальний рівень безпеки [9, с. 12].

Надійність рішень на рівні застосунків залежить від глибинної стійкості платформи. Дослідження уразливостей апаратних компонентів показує, що недоліки у мікропрограмному забезпеченні, контролерах пам'яті та каналах міжпроцесної взаємодії здатні обходити механізми розмежування. Це створює ризик несанкціонованого

читання або копіювання чутливого вмісту поза межами прикладних політик [10, с. 6]. З огляду на це, постає потреба у багаторівневому підході до захисту, де поведінкова перевірка доповнюється регулярним оновленнями мікропрограм, вимкненням відомо небезпечних інтерфейсів і прив'язкою дій доступу до даних до перевіреного стану пристрою, що дозволяє, навіть у разі часткового компромісу апаратного шару, припинити виконання чутливих операцій із неструктурованим контентом або перевести їх у деградований режим перегляду без можливості експорту чи копіювання [10, с. 9]. Це поєднання знижує ймовірність успішного обходу контролів, особливо у випадках, коли зловмисник намагається використати відомі апаратні недоліки під час активного сеансу роботи з файлами, галереями чи месенджерами [10, с. 12].

У випадках, коли моделі виявлення шкідливих застосунків навчаються централізовано, процес збору сирих даних створює додаткові канали витоку неструктурованого контенту, тому доцільно переносити навчання ближче до еджу і агрегувати лише параметри моделей, зберігаючи телеметрію на пристроях [11, с. 1]. Практичні експерименти з федеративним навчанням показують, що за умови раціонального підбору гіперпараметрів, навіть при неідеальному розподілі даних між клієнтами, можливо досягти прийнятної точності детекції без передачі сирих артефактів взаємодії користувача зі застосунками, що скорочує експозицію неструктурованих даних під час активних сесій [11, с. 3]. Водночас слід враховувати обмеження ефективності у випадках патологічно нерівномірного розподілу даних, коли локальні вибірки є надто вузькими за класами, а глобальна модель повільно збігається, що слід враховувати при проєктуванні політик доступу, які залежать від швидкості виявлення ризику [11, с. 5].

На рівні поведінки користувача джерелом ризику стає неправильна оцінка сенсу дозволів, коли доступ до місцеположення, контактів або сховищ надається автоматично, без усвідомлення наслідків. У таких випадках навіть легальні запити можуть створювати обхідні шляхи для захисту неструктурованого вмісту [12, с. 1]. Емпіричні спостереження підтверджують, що значна частка інсталяцій супроводжується погодженням на надлишкові дозволи, що зумовлено браком прозорих підказок і недостатнім розумінням моделей доступу, що вимагає поєднувати технічні контролі з інтерфейсними втручаннями під час роботи з файлами, вкладеннями і кешами [12, с. 6].

Сенсори мобільних пристроїв формують окрему площину атак, де побічні канали зчитують або відновлюють чутливі атрибути взаємодії навіть за відсутності явного доступу до вмісту. Це явище безпосередньо стосується неструктурованих даних, що виникають у процесі звичайних жестів та контекстних змін [13, с. 1323]. Систематизація таких загроз засвідчує необхідність у багаторівневому захисті на етапі збору сигналів, зокрема через нормалізацію частоти вибірки, застосування методів шумопригнічення і впровадження політик мінімізації збереження, щоб зменшити сліди поведінки, які можуть бути використані для вторинної реконструкції вмісту [13].

Форензичні дослідження мобільних застосунків для носимих фітнес-пристроїв демонструють, що значні обсяги артефактів зберігаються локально у вигляді журналів кешів і проміжних файлів. Ці об'єкти часто містять непрямі посилання на повідомлення, зображення або історії взаємодій, які користувач вважає приватними [14]. Аналіз карти збережених артефактів у таких клієнтських застосунках свідчить, що навіть без доступу до основної бази даних можливо відновити часові ланцюжки активності та опосередковані індикатори стану здоров'я, що підсилює аргументацію на користь даноцентричних політик приховання та контролю життєвого циклу тимчасових копій неструктурованого контенту [14].

На тлі цілеспрямованих атак і швидкої еволюції платформ класичні підходи, базуються на статичних сигнатурах, демонструють обмежену ефективність. Сучасні обхідні техніки активно експлуатують як незакриті уразливості, так і помилки конфігурацій дозволів у застосунках, що працюють з файлами і повідомленнями [15]. Огляд сучасних технік підкреслює важливість безперервних поведінково-контекстних контролів і багатошарових криптографічних практик для зниження ризику витоків у динамічних сценаріях, коли неструктуровані дані швидко мігрують між контейнерами і сервісами [15].

Аналіз динаміки дозволів в екосистемі Android свідчить про поступове зростання як кількості, так і різноманіття запитів доступу. При цьому виявляються стійкі патерни надмірних запитів у певних категоріях застосунків, що має бути враховано при формуванні моделей ризику для неструктурованого вмісту [16]. Дослідження тенденцій на великій вибірці дозволяє сформувати пріоритети для політик доступу, зокрема ідентифікувати групи дозволів, які потребують більш жорстких перевірок у реальному часі під час відкриття вкладень або перегляду кешованих документів [16].

Для підтримання стійкого рівня довіри протягом усієї сесії доцільно поєднувати непомітні поведінкові перевірки з контекстним керуванням доступом. Такий підхід дозволяє приймати рішення на основі даних сенсорів і патернів взаємодії без необхідності частих явних автентифікацій під час роботи з повідомленнями файлами і медіа [17]. Експериментальні оцінки у різних сценаріях використання підтверджують, що мультисенсорні та контекстно залежні моделі здатні знижувати рівень помилок прийняття та відхилення, водночас зберігаючи прийнятний рівень зручності. Це створює передумови для практичної інтеграції таких моделей із політиками захисту неструктурованого контенту на рівні ОС і застосунків [17].

З метою узгодження технічних рішень із криптографічними та автентифікаційними засадами, необхідно спершу конкретизувати ролі та порівнювану стійкість симетричних і асиметричних алгоритмів задля захисту

неструктурованого контенту на мобільному пристрої, а вже потім – правила підтримання довіри під час тривалих сесій доступу до такого контенту [18, с. 66–67]. Симетричні алгоритми, як правило, застосовуються для шифрування самих даних, тоді як асиметричні – для встановлення або захисту сеансового ключа, а також для цифрових підписів [18, с. 40–43]. У практичній конфігурації це зводиться до гібридної зв'язки «контент шифрується симетрично, а симетричний ключ передається та засвідчується асиметрично», що водночас забезпечує керованість, продуктивність і узгодженість криптографічних гарантій [18, с. 66–67]. Для узгодження вибору криптографічних механізмів із вимогами до порівнюваної стійкості та ролей алгоритмів систематизовано переваги й обмеження симетричного AES і асиметричного ECC у мобільному контексті захисту неструктурованого контенту (див. табл. 1).

Таблиця 1

Переваги й обмеження AES та ECC

Алгоритм	Переваги	Обмеження
AES (симетричний)	1) Придатний для масового шифрування даних «у спокої» та під час передавання завдяки особливостям симетричних шифрів. 2) Дає чітко визначені рівні стійкості 128/192/256 біт та прогнозовані криптографічні властивості. 3) Легко інтегрується в гібридні криптографічні схеми, де відповідає за шифрування контенту. 4) Знижує витрати на протокол, оскільки один ключ може використовуватися для шифрування великих обсягів. 5) Узгоджується з вимогою щодо порівнюваної стійкості при поєднанні з асиметричними механізмами	1) Потребує безпечного способу встановлення/розповсюдження симетричного ключа за допомогою додаткових механізмів. 2) Компрометація сеансового ключа призводить до розкриття всього зашифрованого в межах сеансу контенту. 3) Не забезпечує неоспорюваності дій без використання додаткових засобів підпису. 4) Не вирішує завдання автентифікації сторін без додаткових механізмів. 5) Вимагає узгодження стійкості з асиметричними компонентами
ECC (асиметричний)	1) Дозволяє встановлювати або приховувати симетричний ключ із використанням коротших ключів за умови за зіставної стійкості. 2) Дає можливість створювати цифрові підписи для атестації дій. 3) Ефективно інтегрується в протоколи доступу та керування ключами. 4) У гібридних схемах відокремлює функції «ключі ↔ дані», підвищуючи керованість. 5) Дозволяє досягати рівня криптостійкості, порівнюваного з AES, при менших розміріах ключів	1) Не призначений для масового шифрування контенту, застосовується переважно для встановлення ключів та цифрових підписів. 2) Потребує наявності інфраструктури керування ключами/ сертифікатами. 3) За призначенням вимагає погодження параметрів із симетричними алгоритмами для забезпечення зіставної стійкості. 4) Криптографічні безпека контенту залежить від коректної від правильної інтеграції в гібридну схему. 5) Вибір кривих і параметрів визначається політикою безпеки та має бути узгоджений із вимогами до рівня стійкості

Джерело: власна розробка авторів на основі [18]

Підсумовуючи, доцільно використовувати симетричне шифрування для захисту контенту, а асиметричні алгоритми – для встановлення ключів і створення цифрових підписів, дотримуючись порівнюваних рівнів стійкості між класами алгоритмів, як це передбачено рекомендаціями.

На рівні контролю доступу під час реальної взаємодії з неструктурованим вмістом процес автентифікації не завершується на етапі входу, оскільки сесія має власний життєвий цикл і потребує підтримання довіри згідно з політиками керування сесією. Рекомендації передбачають періодичну повторну автентифікацію та допускають пасивний моніторинг ознак підміни, що дає змогу зменшувати «вікно ризику» між явними підтвердженнями без створення надмірного навантаження на користувача під час роботи з файлами, вкладеннями та кешами. Така організація процесу дозволяє підвищувати рівень контролю лише за умов зростання ризику, зберігаючи звичний характер взаємодії у стандартних сценаріях доступу до неструктурованих даних. [19, с. 56–58]. З метою визначення ролі MFA у контексті безперервного сесійного контролю та обґрунтування їхню взаємодоповнюваність під час роботи з неструктурованими даними, узагальнимо їхні переваги та обмеження у порівняльній таблиці 2.

Початкова MFA надійно ініціалізує процес входу, тоді як поведінкова аналітика підтримує довіру протягом сесії та запускає додаткові перевірки за наявності ризику; у поєднанні з гібридною зв'язкою «асиметрія для ключів ↔ симетрія для даних» це забезпечує як криптографічну, так і процесну цілісність захисту неструктурованого контенту на мобільних платформах [19, с. 57–58].

У підсумку, застосована конфігурація шифрування ґрунтується на гібридному підході: симетричний алгоритм використовується для захисту вмісту даних, а асиметричний – для встановлення й охорони сеансового ключа та підтвердження автентичності цифрових підписів, із забезпеченням порівнюваних рівнів стійкості між класами алгоритмів. Такий розподіл функцій гарантує необхідну продуктивність на мобільному ендпоїнті та криптографічну узгодженість у роботі з неструктурованими даними як у стані збереження, так і під час передавання.

Після первинного входу підтримання довіри реалізується через політики керування сесією, які передбачають періодичну повторну автентифікацію та пасивний моніторинг, що дозволяє скоротити «вікно ризику» для доступу до повідомлень, вкладень і кешів у процесі активної взаємодії. Сесійний контроль активує ризик-адаптивні дії лише за наявності ознак відхилення – від вимоги повторного підтвердження до тимчасового маскування

Таблиця 2

Переваги й обмеження MFA та поведінкової аналітики

Метод	Переваги	Обмеження
MFA (login-phase)	1) Підвищує поріг автентифікації та знижує ризик компрометації на етапі входу. 2) Узгоджується з рівнями запевнення автентифікаторів і політикою доступу. 3) Дозволяє вимагати повторну автентифікацію за подіями або після завершення визначеного часу. 4) Формує чіткий момент ініціалізації довіри в системі. 5) Підтримує сценарії підвищеного ризику через механізм step-up згідно з політикою	1) Не забезпечує контроль сталість ідентичності протягом сесії між явними перевірками. 2) Додає крок автентифікації на вході, що може впливати на зручність. 3) Уразлива до перехоплення сесії після успішного входу без додаткових захисних механізмів. 4) Потребує чітко визначеної політики потворної автентифікації для тривалих сесій. 5) Не забезпечує контекстної оцінки ризику під час щоденної взаємодії без допоміжних засобів
Поведінкова аналітика (post-login)	1) Підтримує довіру упродовж сесії завдяки пасивному моніторингу відповідно до політики. 2) Зменшує «вікно ризику» між явними підтвердженнями. 3) Дозволяє адаптивно реагувати на ризики шляхом ініціювання повторної автентифікації або обмеження доступу. 4) Мінімізує кількість явних запитів у стандартних сценаріях роботи з контентом. 5) Узгоджується з політикою керування сесіями без порушення звичних сценаріїв взаємодії	1) Залежить від якості та релевантності обраних сигналів моніторингу. 2) Не замінює початкову автентифікацію, а функціонує як доповнення. 3) Вимагає точного налаштування порогів і тригерів для уникнення надмірних втручань. 4) Потребує узгодження з політиками повторної автентифікації та журналювання. 5) Має функціонувати в межах політики конфіденційності та мінімізації збору даних

Джерело: власна розробка авторів на основі [19]

прев'ю або паузи експорту – без створення надмірного навантаження у стандартних сценаріях. У сукупності ці механізми поєднують гарантії на вході з безперервною перевіркою ідентичності протягом сесії, формуючи нормативно обґрунтовану рамку захисту неструктурованого контенту на мобільних платформах.

Висновки

У роботі обґрунтовано цілісну модель захисту неструктурованих даних на мобільних пристроях, яка поєднує безперервну поведінкову автентифікацію, даноцентричні політики доступу та гібридну криптографічну конфігурацію. Показано, що така композиція знижує експозицію повідомлень, медіафайлів, вкладень і кешованих даних протягом тривалих сесій без створення надмірного навантаження на користувача і без істотного впливу на енергоспоживання. Гібридне поєднання симетричних і асиметричних механізмів забезпечує продуктивне шифрування контенту та надійне встановлення і захист сеансових ключів, а початкова багатофакторна перевірка узгоджується з пост-логін моніторингом поведінки, що дозволяє підтримувати довіру між явними підтвердженнями.

Практичні рекомендації охоплюють два рівні. На рівні автентифікації доцільним є поєднання дотикової динаміки та інерціальних сенсорів зі злиттям ознак і оцінок, а також використання ризик-адаптивних політик, які запускають повторне підтвердження або м'які обмеження лише за умов зростання загроз. На рівні доступу до даних ефективними є політики, що керують попередній перегляд, кешування та тимчасові копії, а також гігієна дозволів із урахуванням форензичних артефактів і платформних уразливостей. У сукупності це забезпечує керованість та відтворюваність рішень, узгоджених з вимогами реальних корпоративних сценаріїв.

Обмеження пов'язані з дефіцитом відкритих репрезентативних датасетів, розбіжностями в протоколах оцінювання, а також із необхідністю балансування між точністю і приватністю сенсорних потоків. Перспективи подальших досліджень охоплюють стандартизацію метрик і протоколів, розробку енергоефективних моделей для тривалих сесій, запровадження приватних і федеративних схем навчання, перевірку узгодженості політик на різних платформах та інтеграцію з корпоративними засобами керування пристроями. Запропонована модель створює надійну основу для поетапного впровадження та подальшого вдосконалення захисту неструктурованого контенту на мобільних платформах.

Список використаної літератури

1. James Jose C., S. Rajasree M. Implicit Continuous User Authentication for Mobile Devices based on Deep Reinforcement Learning. *Computer Systems Science and Engineering*. 2023. Vol. 44, no. 2. P. 1357–1372. URL: https://doi.org/10.32604/csse.2023.025672 (date of access: 10.09.2025).

2. Reichinger D., Sonnleitner E., Kurz M. Continuous Mobile User Authentication Using Combined Biometric Traits. *Applied Sciences*. 2021. Vol. 11, no. 24. P. 11756. URL: https://doi.org/10.3390/app112411756 (date of access: 10.09.2025).

3. A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Banking Applications / P. M. A. B. Estrela et al. *Sensors*. 2021. Vol. 21, no. 12. P. 4212. URL: https://doi.org/10.3390/s21124212 (date of access: 10.09.2025).

4. Mekruksavanich S., Jitpattanakul A. Deep Learning Approaches for Continuous Authentication Based on Activity Patterns Using Mobile Sensing. *Sensors*. 2021. Vol. 21, no. 22. P. 7519. URL: https://doi.org/10.3390/s21227519 (date of access: 10.09.2025).

5. Bansal P., Ouda A. Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics. *Computers*. 2024. Vol. 13, no. 4. P. 103. URL: https://doi.org/10.3390/computers13040103 (date of access: 10.09.2025).

6. Lee H.-H., Sung H.-C. Unveiling the Confirmation Factors of Information System Quality on Continuance Intention towards Online Cryptocurrency Exchanges: The Extension of the Expectation Confirmation Model. *Information*. 2023. Vol. 14, no. 9. P. 482. URL: https://doi.org/10.3390/info14090482 (date of access: 10.09.2025).

7. Abuhamad M., Abusnaina A., Nyang D., Mohaisen D. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: a contemporary survey. *IEEE Internet of Things Journal*. 2020. Vol. 7, no. 10. P. 9128–9143. URL: https://davidmohaisen.github.io/files/iotj20.pdf (date of access: 09.09.2025).

8. A Survey of Privacy Vulnerabilities of Mobile Device Sensors / P. Delgado-Santos et al. *ACM Computing Surveys*. 2022. 2022. Vol. 54, Iss. 11s. Art. 224. P. 1–30. URL: https://doi.org/10.1145/3510579 (date of access: 10.09.2025).

9. Weichbroth P., Łysik Ł. Mobile Security: Threats and Best Practices. *Mobile Information Systems*. 2020. Vol. 2020. P. 1–15. URL: https://doi.org/10.1155/2020/8828078 (date of access: 10.09.2025).

10. Muñoz A. Cracking the Core: Hardware Vulnerabilities in Android Devices Unveiled. *Electronics*. 2024. Vol. 13, no. 21. P. 4269. URL: https://doi.org/10.3390/electronics13214269 (date of access: 10.09.2025).

11. Lee S. Distributed Detection of Malicious Android Apps While Preserving Privacy Using Federated Learning. *Sensors*. 2023. Vol. 23, no. 4. P. 2198. URL: https://doi.org/10.3390/s23042198 (date of access: 10.09.2025).

12. Understanding Users' Behavior towards Applications Privacy Policies / S. Ullah et al. *Electronics*. 2022. Vol. 11, no. 2. P. 246. URL: https://doi.org/10.3390/electronics11020246 (date of access: 10.09.2025).

13. A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications / A. K. Sikder et al. *IEEE Communications Surveys & Tutorials*. 2021. Vol. 23, no. 2. P. 1125–1159. URL: https://doi.org/10.1109/comst.2021.3064507 (date of access: 10.09.2025).

14. Investigating Wearable Fitness Applications: Data Privacy and Digital Forensics Analysis on Android / S. Hutchinson et al. *Applied Sciences*. 2022. Vol. 12, no. 19. P. 9747. URL: https://doi.org/10.3390/app12199747 (date of access: 10.09.2025).

15. Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses / Z. Muhammad et al. *Technologies*. 2023. Vol. 11, no. 3. P. 76. URL: https://doi.org/10.3390/technologies11030076 (date of access: 10.09.2025).

16. Alkinoon A., Dang T. C., Alghuried A., Alghamdi A., Choi S., Mohaisen M., Wang A., Salem S., Mohaisen D. A Comprehensive Analysis of Evolving Permission Usage in Android Apps: Trends, Threats, and Ecosystem Insights. *Journal of Cybersecurity and Privacy*. 2025. Vol. 5, № 3. P. 58. URL: https://doi.org/10.3390/jcp5030058 (date of access: 11.09.2025).

17. Behavior-based user authentication on mobile devices in various usage contexts / D. Progonov et al. *EURASIP Journal on Information Security*. 2022. Vol. 2022, no. 1. URL: https://doi.org/10.1186/s13635-022-00132-x (date of access: 10.09.2025).

18. Temoshok D., Fenton J. L., Choong Y.-Y., Lefkovitz N., Regenscheid A., Galluzzo R., Richer J. P. Digital Identity Guidelines: Authentication and Authenticator Management. NIST Special Publication 800-63B-4. Gaithersburg: National Institute of Standards and Technology, 2025. 142 p. URL: https://doi.org/10.6028/NIST.SP.800-63B-4 (date of access: 11.09.2025).

19. Barker E., Chen L., Roginsky A., Vassilev A., Davis R., Simon S. Recommendation for key management. Part 1 – General. NIST Special Publication 800-57, Part 1, Rev. 5. Gaithersburg: National Institute of Standards and Technology, 2020. 171 p. URL: https://doi.org/10.6028/NIST.SP.800-57pt1r5 (date of access: 10.09.2025).

References

1. James Jose, C., & S. Rajasree, M. (2023). Implicit Continuous User Authentication for Mobile Devices based on Deep Reinforcement Learning. *Computer Systems Science and Engineering*, *44*(2), 1357–1372. https://doi.org/10.32604/csse.2023.025672

2. Reichinger, D., Sonnleitner, E., & Kurz, M. (2021). Continuous Mobile User Authentication Using Combined Biometric Traits. *Applied Sciences*, *11*(24), 11756. https://doi.org/10.3390/app112411756

3. Estrela, P. M. A. B., Albuquerque, R. d. O., Amaral, D. M., Giozza, W. F., & Júnior, R. T. d. S. (2021). A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Banking Applications. *Sensors*, *21*(12), 4212. https://doi.org/10.3390/s21124212

4. Mekruksavanich, S., & Jitpattanakul, A. (2021). Deep learning approaches for continuous authentication based on activity patterns using mobile sensing. *Sensors, 21*(22), 7519. https://doi.org/10.3390/s21227519

5. Bansal, P., & Ouda, A. (2024). Continuous authentication in the digital age: An analysis of reinforcement learning and behavioral biometrics. *Computers, 13*(4), 103. https://doi.org/10.3390/computers13040103

6. Lee, H.-H., & Sung, H.-C. (2023). Unveiling the confirmation factors of information system quality on continuance intention towards online cryptocurrency exchanges: The extension of the expectation confirmation model. *Information, 14*(9), 482. https://doi.org/10.3390/info14090482

7. Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2020). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal, 7*(10), 9128–9143. https://davidmohaisen.github.io/files/iotj20.pdf

8. Delgado-Santos, P., Stragapede, G., Tolosana, R., Guest, R., Deravi, F., & Vera-Rodriguez, R. (2022). A Survey of Privacy Vulnerabilities of Mobile Device Sensors. *ACM Computing Surveys*. https://doi.org/10.1145/3510579

9. Weichbroth, P., & Łysik, Ł. (2020). Mobile security: Threats and best practices. *Mobile Information Systems, 2020*, 1–15. https://doi.org/10.1155/2020/8828078

10. Muñoz, A. (2024). Cracking the core: Hardware vulnerabilities in Android devices unveiled. *Electronics, 13*(21), 4269. https://doi.org/10.3390/electronics13214269

11. Lee, S. (2023). Distributed detection of malicious Android apps while preserving privacy using federated learning. *Sensors, 23*(4), 2198. https://doi.org/10.3390/s23042198

12. Ullah, S., Khan, M. S., Lee, C., & Hanif, M. (2022). Understanding Users' Behavior towards Applications Privacy Policies. *Electronics*, *11*(2), 246. https://doi.org/10.3390/electronics11020246

13. Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2021). A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications. *IEEE Communications Surveys & Tutorials*, *23*(2), 1125–1159. https://doi.org/10.1109/comst.2021.3064507

14. Hutchinson, S., Mirza, M. M., West, N., Karabiyik, U., Rogers, M. K., Mukherjee, T., Aggarwal, S., Chung, H., & Pettus-Davis, C. (2022). Investigating Wearable Fitness Applications: Data Privacy and Digital Forensics Analysis on Android. *Applied Sciences*, *12*(19), 9747. https://doi.org/10.3390/app12199747

15. Muhammad, Z., Anwar, Z., Javed, A. R., Saleem, B., Abbas, S., & Gadekallu, T. R. (2023). Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. *Technologies*, *11*(3), 76. https://doi.org/10.3390/technologies11030076

16. Alkinoon, A., Dang, T. C., Alghuried, A., Alghamdi, A., Choi, S., Mohaisen, M., Wang, A., Salem, S., & Mohaisen, D. (2025). A comprehensive analysis of evolving permission usage in Android apps: Trends, threats, and ecosystem insights. *Journal of Cybersecurity and Privacy, 5*(3), 58. https://doi.org/10.3390/jcp5030058

17. Progonov, D., Cherniakova, V., Kolesnichenko, P., & Oliynyk, A. (2022). Behavior-based user authentication on mobile devices in various usage contexts. *EURASIP Journal on Information Security*, *2022*(1). https://doi.org/10.1186/s13635-022-00132-x

18. Temoshok, D., Fenton, J. L., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. P. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4

19. Barker, E., Chen, L., Roginsky, A., Vassilev, A., Davis, R., & Simon, S. (2020). *Recommendation for key management. Part 1 – General* (NIST Special Publication 800-57, Part 1, Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Дата першого надходження рукопису до видання: 18.09.2025
Дата прийнятого до друку рукопису після рецензування: 13.10.2025
Дата публікації: 28.11.2025