

Етичні виклики застосування мобільних технологій для збору доказів

Катерина Борисова

курсантка навчально-наукового інституту № 4, Харківський національний університет внутрішніх справ МВС України, м. Кам'янець-Подільський, Україна,
ORCID: <https://orcid.org/0009-0006-6015-1304>,
e-mail: kate.borisova0502@gmail.com

Михайло Нагорний

курсант навчально-наукового інституту № 4, Харківський національний університет внутрішніх справ МВС України, м. Кам'янець-Подільський, Україна, ORCID: <https://orcid.org/0009-0009-2622-2457>,
e-mail: misha.nagorny.2017@gmail.com

Віталій Світличний

кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, навчально-науковий інститут № 4, Харківський національний університет внутрішніх справ МВС України, м. Кам'янець-Подільський, Україна,
ORCID: <https://orcid.org/0000-0003-3381-3350>, e-mail: vit.svet@ukr.net

У сучасному світі мобільні технології відіграють ключову роль у зборі доказів, зокрема під час військових конфліктів, однак їхнє застосування пов'язане з низкою етичних викликів. Досліджено проблеми конфіденційності, маніпулювання даними й захисту прав людини в контексті користування мобільними застосунками для збору та збереження доказів. Розглянуто принципи згоди, прозорості процесу й убезпечення даних. Підкреслено важливість розроблення міжнародних етичних стандартів.

Ключові слова: мобільні технології; етика; збір доказів; конфіденційність; права людини; військові конфлікти; цифрові докази; міжнародні стандарти.

Ethical Challenges of Using Mobile Technologies for Evidence Collection

Kateryna Borysova, Mykhailo Nahornyi, Vitalii Svitlychnyi

In today's world, mobile technologies play a pivotal role in evidence collection, particularly during military conflicts. However, their use is linked to a number

of ethical challenges. The paper studies the issues of confidentiality, data manipulation, and human rights protection in the context of using mobile applications to collect and preserve pieces of evidence. The principles of consent, process transparency, and data security are taken into account. The significance of developing international ethical standards is emphasized.

Keywords: *mobile technologies; ethics; evidence collection; privacy; human rights; military conflicts; digital evidence; international standards.*

У сучасному світі мобільні технології стали важливим інструментом для збору доказів, особливо в умовах військових конфліктів, де традиційні методи документування можуть бути недоступними або небезпечними. Смартфони, планшети та спеціалізовані застосунки дають змогу швидко й ефективно фіксувати порушення прав людини, військові злочини й інші правопорушення, що стає ключовим елементом у забезпеченні справедливості та з'ясуванні істини. Проте поряд із новими можливостями виникає низка складних етичних питань, пов'язаних із конфіденційністю, цілісністю зібраних даних і захистом прав людини.

Виклики застосування мобільних технологій у зборі доказів

1. Конфіденційність. Збирання інформації через мобільні пристрої без явної згоди користувачів є одним із найбільш критичних етичних викликів. Оскільки мобільні пристрої можуть легко фіксувати особисті дані (місце знаходження, контактну інформацію, фото, відео тощо), виникає ризик порушення права на приватність осіб, чії дані збирають без їхньої інформованої згоди. Наприклад, під час військових конфліктів цивільних осіб

можуть піддати моніторингу або спостереженню, що порушує їхні базові права.

Розглянемо як приклад утиліту, що становить безпосередню небезпеку для забезпечення конфіденційності збирання інформації за допомогою застосування мобільних технологій. Аналізатор трафіку *Kismet* — це приклад програмного забезпечення з відкритим вихідним кодом, призначеного для виконання конкретних завдань. *Kismet* не просто аналізує мережевий трафік, він надає набагато більш розширені функційні можливості. Наприклад, він здатен проводити аналіз трафіку прихованих мереж і навіть бездротових мереж, які не транслюють свій ідентифікатор *SSID*. Використовуючи *Kismet*, можна моніторити активність пристроїв у бездротовій мережі, включно з їхніми *MAC*-адресами й типами пристроїв. Це можна застосувати для деанонімізації користувачів, визначення їхнього місця перебування або відстеження їхньої діяльності [1].

2. Цілісність даних і маніпуляція. Іншим важливим викликом є забезпечення цілісності зібраних доказів. Мобільні технології можуть бути вразливими до кібератак або маніпуляцій, що може призвести до підробки або фальсифікації доказів. Хакери

та зловмисники можуть утручатися в процес збору або обробки даних, змінюючи або видаляючи критично важливу інформацію.

Розглянемо як приклад програми, що можуть бути застосовані для потенційного порушення цілісності даних, а також із метою маніпуляції з протиправним умислом. Програму *DeepFaceLab* можна застосувати для створення *deepfake*-відео. Створені за допомогою *DeepFaceLab* відео можна застосувати як фальшиві докази в судових процесах або під час розв'язання конфліктів, підробляючи важливі моменти для обману суду або сторін конфлікту. Також не менш важливою складовою в підробці даних є зміна метаданих. Прикладом такої програми є *ExifTool* — програма для перегляду й редагування метаданих файлів [2, 3].

3. Права людини та репресії. Збирання даних без чітко визначених етичних меж може призвести до застосування таких даних із метою репресій або незаконного стеження. Мобільні застосунки, призначені для збирання доказів, можна також застосовувати як інструменти масового нагляду.

Виклики застосування мобільних технологій у зборі доказів (конфіденційність, цілісність даних і дотримання прав людини) потребують застосування рішень, які враховують етичні норми й законодавчі межі. Для забезпечення конфіденційності користувачів необхідно визначити чіткі протоколи щодо отримання інформованої згоди й мінімізувати процес збирання даних

до необхідного рівня. Потрібно приділити більше уваги шляхам подолання зазначених перешкод на шляху застосування мобільних технологій.

Можливі рішення для етичного застосування мобільних технологій

1. Захист і безпека даних. Захист зібраних даних є ще одним важливим елементом етичного застосування мобільних технологій. Дані мають бути надійно захищеними від несанкціонованого доступу або маніпуляцій, щоб уникнути їхнього застосування для незаконних цілей або репресій. Захист та безпеку можна забезпечити за допомогою таких заходів:

- 1) застосування сучасних криптографічних алгоритмів (наприклад, AES або RSA) для шифрування даних під час їх передавання та зберігання;
- 2) підтримка мобільних пристроїв і програмного забезпечення в актуальному стані шляхом регулярних оновлень безпеки допоможе уникнути вразливостей, які здатні застосувати зловмисники.

Необхідно також переглянути перелік програм, що становлять пряму й непряму небезпеку на шляху збереження характеристик інформації, яку передають, їхніх категорій, зосередившись на можливості часткового обмеження або повної заборони загального доступу до них. Це може сприяти зменшенню активного застосування таких програм зловмисниками.

2. *Розроблення міжнародних етичних стандартів.* Міжнародна спільнота має розробити єдині етичні стандарти для застосування мобільних технологій у зборі доказів. Такі стандарти мають регулювати всі аспекти, пов'язані з конфіденційністю, цілісністю даних і правами людини. У цьому контексті важливу роль відіграють міжнародні регламенти (наприклад, Регламент ООН № 155 — Кібербезпека, який обумовлює вимоги до захисту інформації та безпеки систем, і Регламент ООН № 156 — Оновлення програмного забезпечення, що регулює безпечне та своєчасне оновлення ПЗ для забезпечення безперервного захисту даних). Ці регламенти можуть стати підґрунтям для глобальної гармонізації підходів до етичного застосування мобільних технологій. Хоча такі регламенти вже існують, але потрібно регулярно їх оновлювати через те, що комп'ютерні технології швидко розвиваються і щодня виникають нові виклики, які потрібно вирішувати та врегульовувати.

Підбиваючи підсумки, варто зауважити, що мобільні технології є надзвичайно перспективними інструментами у сфері документування правопорушень, особливо в умовах, де традиційні методи збору доказів недоступні або надто ризиковані. Завдяки мобільним пристроям і спеціалізованим застосункам стає можливим оперативно фіксувати свідчення про правопорушення, що є критично важливим для з'ясування істини та забезпечення справед-

ливості. Водночас застосування мобільних технологій у процесі збору доказів паралельно із численними перевагами породжує низку серйозних етичних викликів. Одним із основних питань є конфіденційність: мобільні пристрої можуть збирати особисті дані без згоди користувачів, що порушує їхні базові права на приватність. Це стає ще більш критичним під час конфліктів, коли необмежений збір інформації можуть застосувати для моніторингу цивільних осіб або зловживань з боку зацікавлених сторін. Іншою проблемою є забезпечення цілісності зібраних даних. Мобільні пристрої, як і будь-яка інша технологія, доволі вразливі до маніпуляцій, кібератак або фальсифікацій. Для гідної відповіді на ці етичні виклики необхідно розробити та запровадити чіткі міжнародні етичні стандарти, які регулюватимуть застосування мобільних технологій у процесі збору доказів. Такі стандарти мають забезпечити захист прав людини, а також гарантувати конфіденційність і цілісність зібраних даних. Окрім того, одним із потенційних рішень може бути часткове або повне обмеження доступу до програм, які становлять загрозу безпеці інформації та цілісності даних. Такі заходи можуть допомогти зменшити ризик зловживання мобільними технологіями з боку зловмисників.

Отже, мобільні технології мають значні можливості для збору доказів, проте для їх безпечного й етичного застосування потрібна надійна система захисту та стандартизації.

Перелік джерел посилання

1. Баштанник А. *Kismet* / Хабр. 29.07.2010. URL: <https://habr.com/ru/articles/100503/> (дата звернення: 04.10.2024).
2. *DeepFaceLab* 2.0 / DeepfakeVFX.com. URL: <https://www.deepfakevfx.com/downloads/deepfacelab/> (дата звернення: 04.10.2024).
3. ExifTool / Wikipedia. URL: <https://en.wikipedia.org/wiki/ExifTool> (дата звернення: 04.10.2024).