Section: Information Technology, Cyber Security and Computer Engineering

ВПЛИВ ПОШИРЕННЯ ANDROID-ПРИСТРОЇВ НА ДЕАНОНІМІЗАЦІЮ КОРИСТУВАЧІВ ТА ПРОДАЖ ПЕРСОНАЛЬНИХ ДАНИХ РЕКЛАМНИМ КОРПОРАЦІЯМ

Шаповалова Олена
к.т.н., доцент
Вертебний Максим
здобувач вищої освіти магістерського рівня
Кафедра кібербезпеки та інформаційних технологій
Харківській національний економічний університет
імені Семена Кузнеця, Україна

Вступ

Мобільні пристрої стали невід'ємною частиною сучасного життя, забезпечуючи доступ до інформації, комунікацій та розваг. У світі, де понад 70% смартфонів працюють на базі операційної системи Android, масштаби збору даних набули безпрецедентного рівня. Android-платформа, що розробляється корпорацією Google, стала провідним інструментом не лише для зручного використання цифрових сервісів, але й для створення точних цифрових профілів користувачів. Це породжує серйозні виклики для конфіденційності, адже персональні дані стають ключовим активом для рекламних корпорацій.

Реклама в сучасному цифровому світі побудована на персоналізації, що неможлива без збору інформації про поведінку, геолокацію, уподобання та демографію користувачів. Унікальні особливості Android, такі як доступність і відкритість платформи для розробників, сприяють широкому збору даних. Однак це також збільшує ризики деанонімізації, коли користувачів можна ідентифікувати навіть без їхньої прямої згоди.

Екосистема Android та її вплив на приватність

Операційна система Android побудована на принципах відкритості, що дозволяє стороннім розробникам створювати додатки, які легко інтегруються в систему. Це робить Android привабливим як для виробників пристроїв, так і для розробників програмного забезпечення. Проте ця відкритість має зворотний бік: Android збирає і передає значні обсяги даних, які можуть використовуватися для таргетованої реклами.

Кожен Android-пристрій має унікальні ідентифікатори, такі як IMEI, MAC-адреса та Google Advertising ID (GAID). Ці ідентифікатори дозволяють корпораціям створювати профілі користувачів, навіть якщо вони обмежують

доступ до інших особистих даних. Наприклад, GAID, який спеціально призначений для рекламодавців, дозволяє ідентифікувати пристрій для таргетингу без використання персональної інформації, проте сам по собі є ключем до широкого збору поведінкових даних.

Додатки на Android, завдяки доступу до API, можуть отримувати інформацію про геолокацію, список контактів, SMS, історію дзвінків і багато іншого. Дослідження показують, що понад 70% популярних додатків запитують доступ до даних, які не завжди потрібні для їхньої роботи. Наприклад, програма ліхтарика може запитувати доступ до списку контактів, що створює ризик несанкціонованого витоку даних.

Роль додатків у деанонімізації користувачів

Додатки для Android виступають одним із основних каналів збору даних [3-5]. Багато розробників інтегрують у свої програми сторонні рекламні мережі, які відстежують поведінку користувачів, їхні геолокаційні дані та пристроєві характеристики. Ці дані обробляються алгоритмами машинного навчання, які створюють складні профілі користувачів. Наприклад, рекламні мережі можуть аналізувати патерни користування додатками, частоту використання певних функцій, відвідані вебсайти, а також вподобання у соціальних мережах.

Значну роль у цьому процесі відіграє крос-доменне відстеження, яке дозволяє поєднувати дані з різних додатків і вебсайтів. Наприклад, дані, зібрані одним додатком, можуть бути передані іншому, якщо вони використовують ту саму рекламну мережу. Це створює можливість відстеження дій користувача навіть у випадках, коли він використовує різні пристрої або облікові записи.

Проблему ускладнює відсутність прозорості в тому, як саме дані збираються та обробляються. Більшість користувачів не усвідомлюють обсяг інформації, яку вони надають додаткам, особливо якщо дозволи на доступ до даних запитуються непрозоро.

Взаємодія з рекламними корпораціями

Android як платформа має тісну інтеграцію з сервісами Google, що дає змогу рекламним корпораціям використовувати дані для таргетованої реклами. Алгоритми, які обробляють ці дані, забезпечують високу точність у визначенні інтересів користувачів, їхніх уподобань і навіть фінансового стану.

Дослідження показують [1-2], що рекламні мережі на базі Android збирають дані не лише про дії користувачів у додатках, але й про їхню активність у реальному світі. Наприклад, геолокаційні дані дозволяють відстежувати маршрути користувачів, їхні звички та навіть час перебування в певних місцях. Ця інформація може використовуватися для створення детальних профілів, які продаються рекламним агентствам.

Однак інтеграція Google з Android викликає значну критику з боку експертів із конфіденційності. Попри впровадження таких функцій, як контроль за дозволами додатків або обмеження доступу до геолокації, користувачі залишаються вразливими через складність налаштування системи.

Проблеми регулювання та роль користувачів

Хоча Android постійно впроваджує нові функції для захисту конфіденційності, такі як контроль дозволів та шифрування даних, цього недостатньо для ефективного запобігання деанонімізації. Основною проблемою є незнання користувачами ризиків, пов'язаних зі збором даних. Багато з них автоматично надають дозволи на доступ до даних, навіть без читання запитів додатків.

Законодавчі ініціативи, такі як GDPR [1] у Європейському Союзі, спрямовані на обмеження збору даних без згоди користувачів. Проте реальні механізми їхнього виконання поки що залишаються слабкими. Рекламні корпорації знаходять обхідні шляхи, наприклад, через використання псевдонімізації даних, яка не повністю захищає конфіденційність.

Крім того, проблема регулювання ускладнюється різними підходами до захисту даних у різних країнах. Наприклад, у США вимоги до конфіденційності значно менш суворі, ніж у ЄС, що дає рекламним корпораціям більше свободи для збору даних.

Рекомендації для покращення ситуації

Для зменшення впливу Android-пристроїв на конфіденційність користувачів необхідно впровадити комплексний підхід, який включає технологічні, правові та освітні заходи:

1. Технологічні заходи:

a. Впровадження анонімізації даних на рівні операційної системи.

b. Використання алгоритмів, які дозволяють генерувати псевдовипадкові ідентифікатори для кожного сеансу роботи.

c. Забезпечення прозорості у зборі даних через інтерактивні інструменти, які дозволяють користувачам бачити, які дані збираються і як вони використовуються.

2. Правові заходи:

a. Посилення контролю за дотриманням законодавства щодо конфіденційності.

b. Розробка єдиних міжнародних стандартів для збору і обробки даних.

3. Освітні заходи:

a. Підвищення обізнаності користувачів про ризики, пов’язані зі збором даних.

b. Навчання правильному налаштуванню дозволів і використанню альтернативних додатків, орієнтованих на конфіденційність.

Висновок

Android-пристрої стали одним із ключових інструментів для збору персональних даних і деанонімізації користувачів. Рекламні корпорації активно використовують унікальні ідентифікатори, поведінкові дані та геолокаційну інформацію для створення таргетованих рекламних кампаній. Відсутність достатньої обізнаності користувачів та недоліки в регулюванні сприяють масовому витоку даних, створюючи загрозу конфіденційності.

Удосконалення технічних засобів захисту, введення жорсткіших правових норм

і освітні ініціативи є критично важливими для обмеження впливу рекламних корпорацій на приватність. Це дозволить не лише підвищити рівень захисту особистих даних, а й створить передумови для більш відповідального підходу до обробки інформації в епоху цифровізації.

Список використаних джерел

1. Європейський Союз. Загальний регламент про захист даних (GDPR) [Електронний ресурс]. – Режим доступу: https://gdpr-info.eu/
2. Google. Android Platform Overview [Електронний ресурс]. – Режим доступу: https://developer.android.com
3. Роль додатків у зборі даних // TechCrunch. – 2024. – Режим доступу: https://techcrunch.com
4. Публікації про конфіденційність користувачів у Google Advertising ID (GAID) // The Verge [Електронний ресурс]. – Режим доступу: https://theverge.com
5. Аналітика ринку Android // Statista [Електронний ресурс]. – Режим доступу: https://www.statista.com/markets