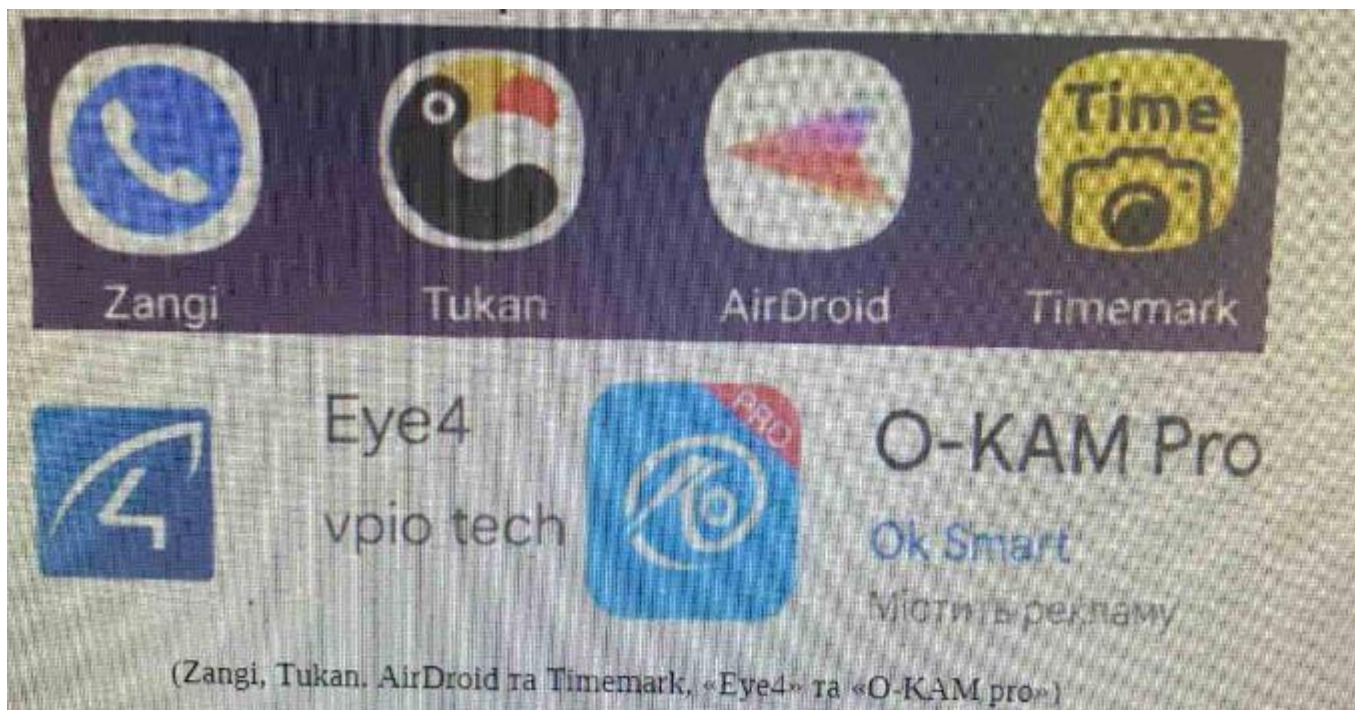




## ⚠ Увага! Небезпечні мобільні застосунки

Шановні учні та батьки!

Звертаємо вашу увагу на потенційно небезпечні мобільні застосунки, які не рекомендовано встановлювати на пристрої дітей:

- Zangi
- Tukan
- AirDroid
- Timemark
- Eye4 (vpio tech)
- O-KAM Pro

Чому це небезпечно?

### 1. Порушення приватності

Ці застосунки можуть запитувати надмірні дозволи: доступ до камери, мікрофона, геолокації, контактів, повідомлень, файлів на телефоні, що створює ризик витоку особистої інформації.

### 2. Сумнівне походження

Деякі з цих застосунків розроблені компаніями з країн, де контроль за кібербезпекою є низьким. Існує ймовірність, що дані можуть передаватися на сторонні сервери.

### 3. Можливість стеження

Наприклад, O-KAM Pro та Eye4 призначені для підключення до камер відеоспостереження. У разі неправильного налаштування або злому, третя особа може отримати доступ до камери без відома власника.

#### 4. Функції прихованого керування

Такі застосунки, як **AirDroid**, дозволяють віддалено керувати пристроєм, що в разі потрапляння до рук зловмисників може використовуватися для контролю, шантажу або кібербулінгу.

#### 5. Використання в шахрайських схемах

Деякі з цих застосунків можуть бути використані шахраями для збору особистих даних або фінансової інформації користувачів.

#### **! Рекомендації:**

- ✓ Перевіряйте встановлені застосунки на пристроях дітей
- ✓ Обмежуйте доступ до дозволів для підозрілих застосунків
- ✓ Встановлюйте антивірус та функцію батьківського контролю
- ✓ Проводьте розмови з дітьми про цифрову безпеку
- ✓ У разі підозри – звертайтеся до вчителя інформатики або спеціаліста з кібербезпеки

💡 **Безпека в Інтернеті починається з уважності. Дбаймо про цифрове здоров'я разом!**