Taraqqiyot spektri
ILMIY JURNALI
Vol 2 № 6 2026

MOBIL ILOVALARDA MA’LUMOTLAR XAVFSIZLIGI VA FOYDALANUVCHI MA’LUMOTLARINI HIMOYALASH

Bazarboyev Nurbek Nuraddin o‘g‘li
Xorazm viloyati Urganch shahri Urganch raqamli texnoligiyalar texnikumi maxsus fan o‘qituvchisi
E-mail: bazarboyevnurbek011102@gmail.com

Annotatsiya. Ushbu maqolada mobil ilovalarda ma’lumotlar xavfsizligini ta’minlash masalalari, foydalanuvchi ma’lumotlarini saqlash usullari hamda zamonaviy mobil dasturlarda xavfsizlikni oshirish texnologiyalari yoritilgan. Mobil ilovalar kundalik hayotimizning muhim qismiga aylanganligi sababli foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilish dolzarb vazifalardan biri hisoblanadi. Maqolada ma’lumotlarni serverda saqlash, shifrlash usullari, autentifikatsiya jarayonlari va oddiy foydalanuvchilar bilishi zarur bo‘lgan xavfsizlik qoidalari tahlil qilingan.

Kalit so‘zlar: mobil ilova, data security, app security, ma’lumotlar xavfsizligi, autentifikatsiya, server, shifrlash, API, foydalanuvchi ma’lumotlari, kiberxavfsizlik.

1. Kirish. Bugungi kunda mobil qurilmalar va mobil ilovalar inson hayotining ajralmas qismiga aylanib ulgurgan. Bank ilovalari, messenjerlar, ijtimoiy tarmoqlar, elektron savdo platformalari hamda turli servis dasturlari millionlab foydalanuvchilar tomonidan kundalik ravishda ishlatilmoqda. Ushbu ilovalar foydalanuvchilardan turli xil ma’lumotlarni qabul qiladi: ism, telefon raqami, elektron pochta, joylashuv ma’lumotlari, bank kartalari, rasmlar va boshqa shaxsiy ma’lumotlar.

Mobil ilovalardan foydalanish ortib borayotgan sari ma’lumotlar xavfsizligi muammosi ham jiddiy masalaga aylanmoqda. Agar foydalanuvchi ma’lumotlari yetarlicha himoyalanmasa, bu ma’lumotlar uchinchi shaxslar qo‘liga tushishi, noqonuniy

Taraqqiyot spektri

foydalanilishi yoki moliyaviy zarar yetkazishi mumkin. Shu sababli mobil ilovalarni yaratishda xavfsizlik talablariga qat’iy amal qilish muhim hisoblanadi.

Mazkur maqolada mobil ilovalarda ma’lumotlarni xavfsiz saqlash usullari, foydalanuvchi ma’lumotlari qanday boshqarilishi hamda oddiy foydalanuvchilar xavfsizlik bo‘yicha nimalarni bilishi kerakligi haqida ma’lumot beriladi.

2. Mobil ilovalarda ma’lumotlar xavfsizligi

Mobil ilovalar foydalanuvchilarning ko‘plab shaxsiy ma’lumotlari bilan ishlaydi. Ushbu ma’lumotlar noto‘g‘ri boshqarilsa yoki himoya qilinmasa, xavfsizlik bilan bog‘liq jiddiy muammolar yuzaga keladi.

Mobil ilovalarda xavfsizlik deganda quyidagilar tushuniladi:

- foydalanuvchi ma’lumotlarini himoyalash;
- serverga yuborilayotgan ma’lumotlarni shifrlash;
- ilovaga ruxsatsiz kirishning oldini olish;
- akkauntlarni himoyalash;
- maxfiy ma’lumotlarning uchinchi shaxslarga sizib chiqishini oldini olish.

Masalan, bank ilovasida foydalanuvchining karta ma’lumotlari oddiy matn ko‘rinishida saqlansa, xakerlar ushbu ma’lumotlarni oson qo‘lga kiritishi mumkin.

3. Ma’lumotlarni himoyalash usullari

Mobil ilovalar xavfsizligini oshirish uchun turli texnologiyalar qo‘llaniladi.

Shifrlash (Encryption): Ma’lumotlarni maxsus algoritmlar yordamida kodlash jarayoni shifrlash deyiladi. Hozirda AES va RSA kabi algoritmlar keng qo‘llaniladi.

Shifrlangan ma’lumotni faqat maxsus kalit yordamida ochish mumkin.

HTTPS protokoli: Mobil ilova va server o‘rtasida ma’lumot almashinuvi HTTPS orqali amalga oshirilishi kerak.cBu uchinchi shaxslarning ma’lumotni ushlab qolishini qiyinlashtiradi.

Taraqqiyot spektri

Token autentifikatsiyasi: Ko‘pgina ilovalar JWT (JSON Web Token) yoki OAuth texnologiyalaridan foydalanadi. Bu foydalanuvchining login-parolini qayta-qayta yubormasdan xavfsiz ishlash imkonini beradi.

Ikki bosqichli tasdiqlash: Ba’zi ilovalar SMS yoki email orqali qo‘shimcha tasdiqlash kodidan foydalanadi. Bu akkaunt himoyasini sezilarli oshiradi.

4. App security: oddiy foydalanuvchi nimalarni bilishi kerak?

Ko‘pchilik foydalanuvchilar ilovadan foydalanayotganda xavfsizlikka yetarlicha e’tibor bermaydi. Quyidagi qoidalarga amal qilish muhim:

- ilovalarni faqat rasmiy marketlardan yuklab olish;
- kuchli parollardan foydalanish;
- bir xil parolni barcha ilovalarda ishlatmaslik;
- noma’lum linklar orqali ilova o‘rnatmaslik;
- telefon operatsion tizimini yangilab borish;
- ilovaga berilgan ruxsatlarni tekshirish;
- ikki bosqichli himoyani yoqish.

Masalan, oddiy kalkulyator ilovasi kontaktlar yoki kamera uchun ruxsat so‘rasa, bunga e’tibor berish kerak.

Zamonaviy tahdidlar: Bugungi kunda mobil ilovalar quyidagi tahdidlarga duch kelmoqda:

- phishing hujumlari;
- zararli APK fayllar;
- ma’lumotlar sizib chiqishi;
- zararli reklama kodlari;

Taraqqiyot spektri

- Wi-Fi orqali ma’lumotlarni ushlash;
- foydalanuvchi sessiyasini o‘g‘irlash.

Shu sababli ishlab chiquvchilar ham, foydalanuvchilar ham xavfsizlikka jiddiy qarashi zarur.

Xulosa: Mobil ilovalar zamonaviy hayotning muhim qismiga aylangan bo‘lsa-da, ular bilan bog‘liq xavfsizlik masalalari ham dolzarb bo‘lib qolmoqda. Foydalanuvchi ma’lumotlarini himoya qilish dasturchilar uchun asosiy vazifalardan biri hisoblanadi. Shu bilan birga oddiy foydalanuvchilar ham ilovalardan foydalanishda xavfsizlik qoidalariga amal qilishi kerak. Kelajakda mobil ilovalar soni oshgani sari app security yanada muhim sohalardan biriga aylanadi.

Foydalanilgan adabiyotlar

1. Stallings W. Network Security Essentials. Pearson Education, 2020.
2. OWASP Mobile Application Security Testing Guide, 2024.
3. Android Developers Documentation – Security Best Practices.
4. Google Android Security Guide
5. OWASP Mobile Security Project
6. Apple Security Documentation
7. Axborot xavfsizligi asoslari. Toshkent, 2023.
8. Zamonaviy mobil ilovalar arxitekturasi va xavfsizlik texnologiyalari, 2024.

Taraqqiyot spektri