SCIENCE HUB REVIEW
2026
Volume 1
Issue 5
www.sciencehubreview.uz
ILMIY ELEKTRON JURNAL

MOBIL ILOVALARDA SHAHSIY MA'LUMOTLARGA BERILADIGAN RUSXSATLARNING FOYDALANUVCHI TOMONIDAN TUSHUNILISHI

Yusupov Samandar Anvarovich

OXUS Universiteti katta o'qituvchisi, Toshkent 100208, O'zbekiston

Samandar75781111@gmail.com

Jabborov Javohir Nodir o'g'li

OXUS University kompyuter ilimlari 501-26 guruh talabasi, 100105, O'zbekiston

javohirjabbarov60@gmail.com

Tursunboyev Xaydarali To'lqin o'g'li

OXUS University kompyuter ilimlari 501-26 guruh talabasi, 111500, O'zbekiston

xaydaralitursunboyev1@gmail.com

Qodirov Bahromjon Botirovich

OXUS University kompyuter ilimlari 501-26 guruh talabasi, Toshkent 100208, O'zbekiston

qodirovbahrom128@gmail.com

Annotatsiya

Mazkur maqolada mobil ilovalar so'raydigan ruxsatlar (kamera, mikrofon, joylashuv, kontaktlar, xotira va boshqalar) foydalanuvchilar tomonidan qanday tushunilishi tahlil qilinadi. Android va iOS operatsion tizimlaridagi ruxsat modellari qiyoslanadi, foydalanuvchilarning ruxsatlarni noto'g'ri talqin qilishining asosiy sabablari ko'rsatiladi hamda ularni bartaraf etish bo'yicha takliflar beriladi. Tadqiqot natijalari shuni ko'rsatadiki, aksariyat foydalanuvchilar ruxsat so'rovlariga mazmunini to'liq anglamasdan rozilik bildiradi, bu esa shaxsiy ma'lumotlar xavfsizligiga jiddiy tahdid tug'diradi.

Kalit so'zlar

mobil ilovalar, ruxsatlar, shaxsiy ma’lumotlar, maxfiylik, foydalanuvchi xulq-atvori, Android, iOS, axborot xavfsizligi.

Kirish.

Bugungi kunda smartfonlar insonning kundalik hayotining ajralmas qismiga aylangan. Ular orqali muloqot qilamiz, to‘lovlarni amalga oshiramiz, sog‘lig‘imizni kuzatamiz va ijtimoiy tarmoqlarda faol qatnashamiz. Natijada qurilmada juda katta hajmdagi shaxsiy ma’lumotlar to‘planadi: kontaktlar, fotosuratlar, geolokatsiya, xabarlar, biometrik ma’lumotlar va boshqalar.

Mobil qurilmalardan foydalanish kengaygani sari ularda qayta ishlanadigan ma’lumotlarning turi ham ko‘paymoqda. Masalan, xarita ilovalari foydalanuvchining qayerda ekanini aniqlashi, messenjerlar kontaktlar va kamera bilan ishlashi, bank ilovalari esa to‘lovga oid ma’lumotlarni qayta ishlashi mumkin. Shu sababli har bir ruxsatning mazmunini tushunish raqamli xavfsizlikning muhim qismiga aylangan. Shaxsiy ma’lumot deganda faqat ism, familiya yoki telefon raqami tushunilmaydi. Qurilma identifikatori, IP-manzil, joylashuv tarixi, suratlar, ovoz yozuvlari va foydalanuvchining ilovadagi xatti-harakatlari ham shaxsga aloqador ma’lumotlar bo‘lishi mumkin. Ayrim ma’lumotlar alohida olinganda oddiy ko‘rinsa-da, birlashtirilganda insonning kundalik odatlari va qiziqishlari haqida keng tasavvur hosil qiladi. Ruxsat oynasidagi tanlov foydalanuvchining ma’lumotlari qanday ishlatilishiga ta’sir qiladi. Shuning uchun rozilik berishdan oldin ilovaning vazifasi, so‘ralayotgan ruxsat va uning zarurati o‘rtasidagi bog‘liqlikni baholash lozim. Masalan, videoqo‘ng‘iroq ilovasi uchun kamera va mikrofon zarur bo‘lishi mumkin, biroq oddiy kalkulyator ilovasi uchun bu ruxsatlar odatda asosiy vazifaga aloqador emas.

Mobil ilova bu ma’lumotlarga kirishi uchun foydalanuvchidan ruxsat (permission) so‘raydi. Nazariy jihatdan ruxsat mexanizmi foydalanuvchiga o‘z ma’lumotlari ustidan nazorat berishi kerak. Biroq amalda foydalanuvchilar ko‘pincha so‘rovni o‘qimasdan, “Ruxsat berish” tugmasini bosadi. Bu holat maxfiylik bo‘yicha tadqiqotlarda “rozilik muammosi” (consent dilemma) deb ataladi.

Tadqiqotning maqsadi —foydalanuvchilarning mobil ilova ruxsatlarini qanchalik tushunishini o‘rganish va bu tushunishga ta’sir qiluvchi omillarni aniqlashdir.

Vazifalar:

1. Android va iOS ruxsat modellarini tahlil qilish;

2. Foydalanuvchilar tomonidan ruxsatlarning noto‘g‘ri tushunilish sabablarini aniqlash;

3. Muammoni kamaytirish bo‘yicha amaliy takliflar ishlab chiqish.

1. Mobil ilovalarda ruxsat mexanizmlari

1.1. Android tizimida ruxsatlar

Android operatsion tizimida ruxsatlar an’anaviy ravishda ikki asosiy toifaga bo‘linadi: *oddiy (normal)* ruxsatlar, ular tizim tomonidan avtomatik beriladi (masalan, internetga ulanish), va *xavfli (dangerous)* ruxsatlar, ular foydalanuvchining aniq roziligini talab qiladi (kamera, mikrofon, joylashuv, kontaktlar, SMS va h.k.).Android qurilmasida foydalanuvchi ilova ruxsatlarini o‘rnatishdan keyin ham boshqarishi mumkin. Sozlamalarning ilovalar yoki maxfiylik bo‘limida qaysi dastur kamera, mikrofon, joylashuv yoki kontaktlardan foydalanishi ko‘rsatiladi. Menyu nomlari Android versiyasi va telefon ishlab chiqaruvchisiga qarab biroz farq qilishi mumkin.

Ayrim ruxsatlar bir-biridan farqli darajada ma’lumot beradi. Masalan, taxminiy joylashuv hududni aniqlashga yordam bersa, aniq joylashuv qurilmaning joyini ancha batafsil ko‘rsatadi. Ilovaning vazifasi uchun aniq koordinatalar talab qilinmasa, taxminiy joylashuvni tanlash ma’lumotni kamroq ulashish imkonini beradi.

Android tizimida ruxsatning berilgani ilova undan doimiy ravishda foydalanayotganini anglatmaydi. Biroq ruxsat mavjud bo‘lsa, ilova tegishli funksiyaga murojaat qilishi mumkin. Shu bois foydalanuvchi ruxsatlarni vaqti-vaqti bilan tekshirishi, foydalanmaydigan ilovalarga berilgan huquqlarni cheklashi maqsadga muvofiq.

Android 6.0 (API 23) versiyasidan boshlab *runtime permissions* modeli joriy etildi: ilova xavfli ruxsatni o‘rnatish vaqtida emas, balki kerak bo‘lgan paytda so‘raydi. Keyingi versiyalarda “faqat ilova ishlatilayotganda ruxsat berish”, “taxminiy joylashuv” va bir martalik ruxsatlar kabi imkoniyatlar qo‘shildi.

1.2. iOS tizimida ruxsatlar

iOS tizimida ham ruxsatlar kontekstga bog‘liq tarzda, ilova ma’lumotga birinchi marta murojaat qilganda so‘raladi. Ilova ishlab chiquvchisi so‘rov oynasida ruxsat nima uchun kerakligini tushuntiruvchi matn (purpose string) berishi shart. Bundan tashqari, iOS “App

Tracking Transparency” mexanizmi orqali foydalanuvchini kuzatish uchun alohida rozilik talab qiladi.

iOS foydalanuvchiga ayrim ma’lumotlarga kirishni cheklangan shaklda taqdim etish imkoniyatlarini ham beradi. Masalan, fotosuratlar uchun butun kutubxonaga kirish o‘rniga faqat tanlangan suratlarni ulashish mumkin bo‘lgan holatlar mavjud. Bu yondashuv ilovaning vazifasini bajarish bilan birga ortiqcha ma’lumot berilishining oldini olishga xizmat qiladi.iOS sozlamalaridagi maxfiylik bo‘limi orqali kamera, mikrofon, joylashuv va boshqa ma’lumotlarga kirish huquqlarini ko‘rib chiqish mumkin. Foydalanuvchi avval bergan roziligini keyinchalik o‘zgartirishi yoki bekor qilishi mumkin. Demak, ruxsat berish doimiy va qaytarib bo‘lmaydigan qaror emas.

App Tracking Transparency mexanizmi ilovalar va boshqa kompaniyalarning foydalanuvchini turli ilova hamda saytlar bo‘ylab kuzatishiga doir alohida tanlovni taqdim etadi. Bu mexanizm kamera yoki mikrofon ruxsatidan farq qiladi: uning asosiy maqsadi reklama va tahlil uchun kuzatuvga rozilikni boshqarishdir.

Ikki tizimning qiyosiy tahlili

Mezon	Android	iOS
Ruxsat so‘rash vaqti	Runtime (Android 6.0 dan)	Birinchi murojaatda
Tushuntirish matni	Ixtiyoriy (ilova o‘zi ko‘rsatishi mumkin)	Majburiy (purpose string)
Joylashuv ruxsati	Aniq / taxminiy, ilova ishlatilganda / doimo	Aniq / taxminiy, ilova ishlatilganda / doimo
Ruxsatni keyin o‘zgartirish	Sozlamalar orqali	Sozlamalar orqali
Kuzatuvga alohida rozilik	Reklama identifikatori sozlamalari	App Tracking Transparency

Foydalanuvchilar ruxsatlarni qanday tushunadi

Maxfiylik sohasidagi xalqaro tadqiqotlar (masalan, Felt va hammualliflarning Android ruxsatlari bo‘yicha ishi) shuni ko‘rsatadiki, foydalanuvchilarning katta qismi ruxsat so‘rovlariga e’tibor bermaydi yoki ularning ma’nosini to‘g‘ri tushunmaydi. Asosiy kuzatuvlar quyidagilar:

Foydalanuvchining ruxsatni tushunishi faqat texnik atamalarni bilishiga bog‘liq emas. U ilovaning nima maqsadda yaratilgani, ishlab chiquvchiga qanchalik ishonishi, so‘rov qachon paydo bo‘lgani va ekranda qanday izoh berilganiga ham bog‘liq. Ruxsat ilovaning asosiy funksiyasi bajarilayotgan vaqtda so‘ralsa, uning zarurati foydalanuvchiga aniqroq

koʻrinishi mumkin. Masalan, foydalanuvchi xarita ilovasini ochib, yoʻnalish qidirayotganida joylashuv soʻralishi mantiqan tushunarli. Aksincha, ilova hali hech qanday tegishli xizmatni koʻrsatmasdan turib kontaktlar yoki mikrofon ruxsatini talab qilsa, foydalanuvchida savol tugʻilishi tabiiy. Kontekstning mavjudligi qarorni ongliroq qabul qilishga yordam beradi. Ruxsatlarni tushunishda foydalanuvchining tajribasi ham muhim. Ilovalarni tez-tez oʻrnatadigan, sozlamalarni tekshiradigan va maxfiylik haqida ma'lumotga ega insonlar soʻrovlarni sinchiklab koʻrib chiqishi mumkin. Biroq tajribali foydalanuvchilar ham koʻp sonli bildirishnomalar va shoshilinch vaziyatlarda avtomatik qaror qabul qilishi ehtimoldan xoli emas.

– **Ruxsat nomlarini tushunmaslik.** "Qurilma holati va identifikatorini oʻqish" kabi texnik iboralar oddiy foydalanuvchi uchun noaniq.

– **Ruxsat va funksiya oʻrtasidagi bogʻliqlikni koʻra olmaslik.** Foydalanuvchi, masalan, fonar ilovasi nima uchun kontaktlarga kirishni soʻrayotganini baholay olmaydi.

– **Oqibatlarni past baholash.** Joylashuv yoki mikrofon ma'lumotlari qanday toʻplanishi, saqlanishi va uchinchi tomonlarga uzatilishi mumkinligi haqida tasavvur yetarli emas.

– **Berilgan ruxsatlarni unutish.** Foydalanuvchilar bir marta berilgan ruxsatlarni keyinchalik qayta koʻrib chiqmaydi.

Tushunishga ta'sir qiluvchi omillar

Rozilik charchogʻi (consent fatigue)

Bitta ilovaning oʻzi bir necha ruxsat soʻraydi, qurilmada esa oʻnlab ilovalar bor. Takroriy soʻrovlar foydalanuvchini avtomatik ravishda "Ruxsat berish"ni bosishga oʻrgatadi. Rozilik charchogʻi ayniqsa birinchi marta oʻrnatilayotgan ilovalarda seziladi. Foydalanuvchi ketma-ket bir nechta oynani koʻrganda, har birining mazmunini alohida tahlil qilishga vaqt ajratmasligi mumkin. Natijada ruxsat soʻrovi muhim xavfsizlik qarori emas, balki ilovani tezroq ishga tushirish uchun bosib oʻtiladigan oddiy bosqich sifatida qabul qilinadi. Bu muammoni kamaytirish uchun ilovalar barcha ruxsatlarni birdaniga soʻramasligi, balki tegishli funksiya ishlatilgandagina murojaat qilishi kerak. Foydalanuvchiga qisqa va aniq izoh berilishi, rad etish imkoniyati ham rozilik berish kabi tushunarli koʻrinishda boʻlishi lozim.

Qulaylikni xavfsizlikdan ustun qo‘yish

Foydalanuvchi ilovadan tezroq foydalanishni istaydi. Ruxsatni rad etish ilova ishlashiga to‘sqinlik qiladi deb hisoblanib, rozilik beriladi. Bu holat xulq-atvor iqtisodiyotida “maxfiylik paradoksi” sifatida ma’lum: odamlar maxfiylikni muhim deb hisoblasa-da, amalda uni ilova qulayligiga almashtiradi.

Qulaylik va xavfsizlik o‘rtasidagi tanlov ko‘pincha kundalik vaziyatlarda yuz beradi. Masalan, foydalanuvchi ro‘yxatdan o‘tishni tez yakunlash yoki kerakli xizmatdan darhol foydalanish uchun ruxsat matnini o‘qimasligi mumkin. Bunday holatda qisqa muddatli qulaylik uzoq muddatli maxfiylik xavflaridan ustun qo‘yiladi.

Maxfiylik paradoksini kamaytirish uchun foydalanuvchiga murakkab hujjatlarni o‘qitishning o‘zi yetarli emas. Muhim ma’lumotlar sodda tilda, aynan qaror qabul qilinayotgan paytda ko‘rsatilishi kerak. Masalan, joylashuv nima uchun kerakligi, qachon ishlatilishi va ruxsat berilmasa qaysi funksiya cheklanishi aniq tushuntirilsa, tanlov mazmunliroq bo‘ladi.

3.3. Raqamli savodxonlik darajasi

Yoshi, ta’lim darajasi va texnik bilimi ruxsatlarni tushunishga bevosita ta’sir qiladi. Kompyuter yo‘nalishida o‘qimaydigan foydalanuvchilar uchun ruxsatning texnik ma’nosi ko‘pincha tushunarsiz bo‘lib qoladi.

Raqamli savodxonlik faqat kompyuterdan foydalanishni bilish bilan cheklanmaydi. U shaxsiy ma’lumotlarni tanish, ilovaning so‘rovini baholash, xavfsiz sozlamalarni tanlash va shubhali holatlarni aniqlash ko‘nikmalarini ham qamrab oladi. Shu sababli bu bilimlarni turli yoshdagi foydalanuvchilar uchun muntazam rivojlantirish zarur.

Ruxsat oynalarida ishlatiladigan texnik iboralar oddiy misollar bilan izohlansa, tushunish osonlashadi. Masalan, “geolokatsiyaga kirish” iborasiga “ilova joylashuvingizni aniqlashi mumkin” degan sodda izoh qo‘shilishi foydalanuvchiga qarorning mohiyatini anglashga yordam beradi.

3.4. Interfeys dizayni

Tushuntirishsiz, qisqa va standart shakldagi so‘rov oynalari foydalanuvchini fikrlashga undamaydi. Ba’zi ilovalarda esa “qorong‘i naqshlar” (dark patterns) qo‘llanadi: rozilik tugmasi yirik va rangli, rad etish tugmasi esa kichik va ko‘rinmas qilib beriladi.

Interfeysdagi rang, tugma hajmi va joylashuvi ham qarorga ta’sir ko‘rsatadi. Agar “Ruxsat berish” tugmasi ko‘zga yaqqol tashlanib, “Rad etish” varianti yashirilsa, foydalanuvchi o‘z xohishiga to‘liq mos bo‘lmagan qarorni qabul qilishi mumkin. Bunday dizayn foydalanuvchi manfaatini emas, ilova egasining maqsadini ustun qo‘yadi.

Yaxshi interfeysda ikkala tanlov ham aniq ko‘rinishi, ruxsatning sababi oldindan tushuntirilishi va foydalanuvchi qarorini bosimsiz qabul qilishi kerak. Shuningdek, ruxsat rad etilganda ilova xatolik haqida tushunarli xabar berishi va mavjud muqobil imkoniyatlarni ko‘rsatishi maqsadga muvofiq.

3.5. Maxfiylik siyosatining murakkabligi

Maxfiylik siyosati odatda uzun va yuridik tilda yoziladi, shuning uchun foydalanuvchilarning aksariyati uni o‘qimaydi. Solove ta’kidlaganidek, foydalanuvchidan har bir ma’lumot to‘plashga mustaqil ravishda “ongli rozilik” berishni kutish real emas.

Maxfiylik siyosatida qanday ma’lumot yig‘ilishi, nima maqsadda ishlatilishi, qancha muddat saqlanishi va kimlar bilan ulashilishi kabi savollarga javob bo‘lishi kerak. Foydalanuvchi uchun aynan shu ma’lumotlar muhim hisoblanadi. Hujjatning mavjudligi uning mazmuni hamma uchun tushunarli degani emas.

Shu sababli maxfiylik siyosatining qisqa xulosasi yoki asosiy bandlar bo‘yicha sodda izohlar foydali bo‘lishi mumkin. To‘liq hujjat ham ochiq va oson topiladigan joyda saqlanishi kerak. Qisqa izoh to‘liq siyosatning o‘rnini bosmaydi, balki uni tushunishga yordam beruvchi vosita bo‘lib xizmat qiladi.

4. Xavflar

Ruxsatlarning noto‘g‘ri tushunilishi quyidagi xavflarni keltirib chiqaradi:

Bundan tashqari, ortiqcha ma’lumot yig‘ilishi foydalanuvchining raqamli izini kengaytiradi. Turli ilovalardan olingan joylashuv, qidiruv va foydalanish ma’lumotlari birlashtirilsa, insonning qaysi joylarga borishi, qaysi xizmatlardan foydalanishi yoki qaysi mavzularga qiziqishi haqida xulosa chiqarilishi mumkin.

Ma’lumotlar saqlanadigan tizimlarda xavfsizlik kamchiligi yuzaga kelsa, avval yig‘ilgan ma’lumotlar begona shaxslar qo‘liga tushishi ehtimoli mavjud. Bunday

vaziyatda foydalanuvchi nafaqat maxfiylik, balki firibgarlik va soxta xabarlar bilan bog‘liq muammolarga ham duch kelishi mumkin.

Ruxsatlarning noto‘g‘ri boshqarilishi bolalar va tajribasi kam foydalanuvchilar uchun ham alohida xavf tug‘diradi. Ular ilova so‘rovining oqibatlarini to‘liq anglamasdan ma’lumot ulashishi mumkin. Shu bois tushuntirishlar sodda, aniq va yoshga mos bo‘lishi muhim.

1. Ortiqcha ruxsatlar orqali ma’lumotlarning ruxsatsiz yig‘ilishi va reklama maqsadlarida ishlatilishi;

2. Joylashuv va odatlar asosida foydalanuvchi profilining shakllantirilishi;

3. Zararli yoki soxta ilovalar tomonidan ma’lumotlarning o‘g‘irlanishi (fishing, spyware);

4. Ma’lumotlarning uchinchi tomonlarga uzatilishi va nazoratdan chiqishi.

5. Takliflar va yechimlar

Foydalanuvchilar uchun:

– Ilovaga faqat uning asosiy vazifasi uchun zarur bo‘lgan ruxsatlarni berish (minimal huquq tamoyili);

– Imkon bo‘lsa, “faqat ilova ishlatilganda” yoki “bir martalik” variantni tanlash;

– Sozlamalardagi maxfiylik bo‘limini davriy tekshirib, keraksiz ruxsatlarni qaytarib olish;

– Ilovalarni faqat rasmiy do‘konlardan (Google Play, App Store) yuklab olish.

Ishlab chiquvchilar uchun:

– Ruxsatni so‘rashdan oldin oddiy tilda nima uchun kerakligini tushuntirish;

– Faqat zarur ruxsatlarni so‘rash va ularni kerak bo‘lgan paytda (just-in-time) so‘rash;

– Ruxsat berilmagan taqdirda ham ilovaning asosiy funksiyalari ishlashini ta’minlash;

– Dark patterns’dan voz kechish.

Ta’lim va tashkilotlar uchun:

– Maktab va oliy o‘quv yurtlarida raqamli maxfiylik savodxonligini oshirish bo‘yicha kurslar o‘tkazish;

– O‘zbekistonda “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonun talablariga ilova ishlab chiquvchilari tomonidan amal qilinishini kuchaytirish.

Xulosa

Ruxsatlarni baholash bo‘yicha amaliy yondashuv

Foydalanuvchi ruxsat so‘rovini ko‘rganda uchta asosiy savolni berishi mumkin: birinchidan, bu ruxsat ilovaning asosiy vazifasini bajarish uchun haqiqatan zarurmi; ikkinchidan, ilova ushbu ma’lumotdan qachon va qanday foydalanadi; uchinchidan, ruxsat berilmasa qanday imkoniyatlar cheklanadi? Ushbu savollar qarorni shoshilmasdan qabul qilishga yordam beradi. Masalan, suratga olish ilovasi kamera ruxsatiga ehtiyoj sezishi tabiiy. Biroq suratlarni tahrirlash uchun mo‘ljallangan dastur kontaktlar ro‘yxatiga ham kirishni so‘rasa, foydalanuvchi bu talabning sababini tekshirishi kerak. Xuddi shuningdek, ob-havo ilovasi hudud bo‘yicha prognoz berish uchun joylashuvdan foydalanishi mumkin, lekin ayrim hollarda shaharni qo‘lda tanlash ham yetarli bo‘ladi. Ruxsat berilgandan keyin ham nazorat davom etishi kerak. Ilova uzoq vaqt ishlatilmasa, uning ruxsatlarini qayta ko‘rib chiqish, keraksizlarini bekor qilish va ilova yangilanishlaridan keyin maxfiylik sozlamalarini tekshirish foydali odat hisoblanadi. Bu yondashuv foydalanuvchining ma’lumotlar ustidan nazoratini kuchaytiradi.

Mobil ilovalardagi ruxsat mexanizmi texnik jihatdan foydalanuvchiga nazorat beradi, biroq amalda bu nazorat ko‘pincha samarasiz bo‘lib qoladi. Buning sababi — ruxsat matnlarining murakkabligi, rozilik charchog‘i, raqamli savodxonlikning yetarli emasligi hamda interfeys dizaynidagi kamchiliklardir. Muammoni hal qilish uchun faqat texnik choralar yetarli emas: ishlab chiquvchilar shaffof va tushunarli so‘rovlar yaratishi, foydalanuvchilar esa ongli qaror qabul qilishga o‘rganishi kerak. Kelajakdagi tadqiqotlar O‘zbekiston foydalanuvchilari o‘rtasida so‘rovnoma o‘tkazish orqali mahalliy holatni aniqlashga qaratilishi mumkin.

Amaliy jihatdan foydalanuvchi har bir yangi ilovani o‘rnatganda uning ishlab chiquvchisi, baholari, izohlari va talab qilinadigan ruxsatlarini tekshirishi lozim. Ilovaning asosiy vazifasiga aloqasi bo‘lmagan ruxsatlar so‘ralishi ehtiyotkorlik bilan yondashish uchun sabab bo‘la oladi. Biroq faqat ruxsatlar soniga qarab ilovani xavfsiz yoki xavfli deb qat’iy baholab bo‘lmaydi; uning vazifasi va ma’lumotlardan foydalanish tartibi ham hisobga olinishi kerak.

Tashkilotlar va ta’lim muassasalari foydalanuvchilarga real misollar asosida tushuntirish berishi mumkin. Masalan, kamera, mikrofon va joylashuv ruxsatlari qaysi vaziyatlarda zarur bo‘lishi, qachon esa rad etilishi mumkinligi muhokama qilinadi. Bunday mashg‘ulotlar nazariy bilimni kundalik amaliyot bilan bog‘laydi.

Kelgusidagi tadqiqotlarda O‘zbekiston foydalanuvchilari o‘rtasida anonim so‘rovnoma va suhbatlar o‘tkazish foydali bo‘ladi. Unda respondentlarning ruxsat oynalarini o‘qish odati, qaysi atamalarni tushunishi, qaysi ruxsatlarni ko‘proq berishi va sozlamalarni qay darajada tekshirishi o‘rganilishi mumkin. Olingan natijalar mahalliy foydalanuvchilar uchun mos tavsiyalar ishlab chiqishga yordam beradi.

Foydalanilgan adabiyotlar

1. Felt A. P., Ha E., Egelman S., Haney A., Chin E., Wagner D. Android Permissions: User Attention, Comprehension, and Behavior. SOUPS, 2012.

2. Kelley P. G., Consolvo S., Cranor L. F., Jung J., Sadeh N., Wetherall D. A Conundrum of Permissions: Installing Applications on an Android Smartphone. 2012.

3. Acquisti A., Brandimarte L., Loewenstein G. Privacy and Human Behavior in the Age of Information. Science, 2015.

4. Solove D. J. Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 2013.

5. Android Developers: Permissions on Android (developer.android.com).

6. Apple Developer: Requesting Authorization to Access Private Data (developer.apple.com).

7. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni (2019).