MOBIL OPERATSION TIZIMLAR XAVFSIZLIGI VA FOYDALANUVCHI MA'LUMOTLARINI HIMOYALASH USULLARI

UMAROV BEKZOD AZIZOVICH
Farg'ona davlat unversiteti,
Amaliy matematika va informatika kafedrasi
katta o'qituvchisi p.f.d (PhD)
ubaumarov@mail.ru
RUSTAMOVA HUMORAXON SULTONBEK QIZI
Farg'ona davlat unversiteti talabasi
humoraxonrustamova05@gmail.com

ANNOTATSIYA. Bugungi kunda mobil qurilmalarning hayotimizdagi o'rni tobora ortib bormoqda. Ushbu qurilmalar orqali bank operatsiyalaridan tortib, shaxsiy yozishmalargacha bo'lgan turli nozik ma'lumotlar uzatiladi va saqlanadi. Shu sababli, mobil operatsion tizimlar (Android, iOS va boshqalar) xavfsizligi masalasi dolzarb mavzulardan biridir. Mazkur maqolada mobil OT xavfsizlik konsepsiyasi, asosiy tahdidlar, zaifliklar, ularni aniqlash va oldini olish bo'yicha zamonaviy usullar tahlil qilingan. Shuningdek, foydalanuvchi ma'lumotlarini himoyalashda autentifikatsiya, shifrlash algoritmlari, tarmoq xavfsizligi, ilovalarga ruxsatnoma siyosati, mobil ilovalarning xavfsiz rivojlanishi kabi elementlarga e'tibor qaratilgan. Android va iOS tizimlarining xavfsizlik yondashuvlari o'zaro solishtirilgan, ularning zaif va kuchli tomonlari taqqoslab tahlil qilingan. Jadval, grafik va real holatlar asosida berilgan tahlillar maqolani yanada boyitadi. Maqola so'ngida foydalanuvchilarga va ishlab chiquvchilarga xavfsizlikni oshirish uchun amaliy tavsiyalar keltirilgan. Tadqiqot mobil OT xavfsizligini oshirishga ilmiy asoslangan yondashuvni taklif etadi.

KALIT SO‘ZLAR. mobil xavfsizlik, operatsion tizimlar, Android xavfsizligi, iOS xavfsizligi, foydalanuvchi ma’lumotlari, himoyalash usullari, shifrlash algoritmlari, autentifikatsiya, kiberxavfsizlik, mobil ilovalar, ruxsat siyosati, tarmoq xavfsizligi

ANNOTATION. In the modern digital era, mobile devices have become an integral part of our lives, serving not only for communication but also for conducting financial transactions and storing sensitive personal information. As such, the security of mobile operating systems (such as Android and iOS) has emerged as a critical topic of concern. This paper provides an in-depth analysis of the security architecture of mobile operating systems, focusing on key vulnerabilities, potential threats, and the modern approaches to their mitigation. It discusses user data protection through methods such as biometric and multi-factor authentication, encryption algorithms, network security measures, application permission control, and secure mobile application development practices. The paper compares Android and iOS in terms of their security models, identifying strengths and weaknesses using tables and visual aids. Real-world examples and case studies add depth to the analysis. The article concludes with practical recommendations for both users and developers, offering a scientific and systematic perspective on strengthening mobile device security.

KEYWORD. mobile security, operating systems, Android security, iOS security, user data protection, encryption algorithms, authentication, cybersecurity, mobile applications, permission policies, network protection

АННОТАТСИЯ. Сегодня роль мобильных устройств в нашей жизни все больше возрастает. С помощью этих устройств передается и хранится различная конфиденциальная информация, от банковских транзакций до личной переписки. Поэтому вопрос безопасности мобильных операционных систем (Android, iOS и т. д.) является одним из актуальных. В данной статье анализируется понятие безопасности мобильных ОС, основные угрозы,

уязвимости, современные методы их обнаружения и предотвращения. Также уделяется внимание таким элементам, как аутентификация, алгоритмы шифрования, сетевая безопасность, политики разрешений приложений и безопасная разработка мобильных приложений в защите пользовательских данных. Сравниваются подходы к безопасности систем Android и iOS, анализируются их слабые и сильные стороны. Анализ, основанный на таблицах, графиках и реальных ситуациях, еще больше обогащает статью. В конце статьи даются практические рекомендации для пользователей и разработчиков по повышению безопасности. В исследовании предлагается научно обоснованный подход к повышению безопасности мобильных ОС.

КЛЮЧЕВЫЕ СЛОВА. мобильная безопасность, операционные системы, безопасность, Android, безопасность iOS, пользовательские данные, методы защиты, алгоритмы шифрования, аутентификация, кибербезопасность, мобильные приложения, политика разрешений, сетевая безопасность

KIRISH

So‘nggi yillarda mobil qurilmalar inson hayotining ajralmas qismiga aylandi. Statistik ma’lumotlarga ko‘ra, 2024-yil holatiga dunyo bo‘yicha 6,8 milliarddan ortiq mobil foydalanuvchi mavjud bo‘lib, bu raqam har yili ortib bormoqda. Ushbu qurilmalar orqali foydalanuvchilar shaxsiy yozishmalar, bank operatsiyalari, sog‘liq holati, geolokatsiya va boshqa ko‘plab nozik ma’lumotlarni almashadilar. Bunday keng ko‘lamdagi foydalanish mobil operatsion tizimlar (OT) xavfsizligini ta’minlashni nafaqat texnik, balki ijtimoiy masalaga aylantirmoqda. Mobil OTlar – bu qurilmalarda ishlaydigan va ularning barcha funksiyalarini boshqaruvchi dasturiy platformalardir. Eng keng tarqalganlari Android va iOS bo‘lib, ular foydalanuvchilar uchun keng qulayliklarni taqdim etadi. Biroq aynan shu qulayliklar – ochiq tizim, ko‘plab ilovalar va internetga ulanganlik – ular uchun xavfsizlik tahdidlarini ham kuchaytiradi. Kiberjinoyatchilar ma’lumot o‘g‘irlash,

qurilmalarni masofadan boshqarish, josuslik dasturlarini joylashtirish kabi ko‘plab usullarni qo‘llab, foydalanuvchilar xavfsizligiga tahdid solmoqdalar.

Bugungi kunda mobil qurilma xavfsizligini ta’minlash faqat operatsion tizim darajasida emas, balki foydalanuvchi darajasida ham hal qilinishi kerak bo‘lgan kompleks masaladir. Avvalgi yillarda faqat parol orqali himoyalash yetarli deb hisoblangan bo‘lsa, hozirda bu yondashuv o‘z samarasini yo‘qotgan. Endilikda autentifikatsiya, biometrik himoya, ma’lumotlarni shifrlash, ruxsatnoma siyosati, xavfsiz ilova ishlab chiqish, hamda foydalanuvchi xatti-harakatlarini nazorat qilish kabi bir qator zamonaviy mexanizmlar joriy qilinmoqda.

Mazkur maqola doirasida mobil operatsion tizimlar xavfsizligiga doir muammolar, ularning kelib chiqish sabablari, amalda qo‘llanilayotgan himoya usullari va foydalanuvchi ma’lumotlarini himoyalashning zamonaviy yondashuvlari atroflicha tahlil qilinadi. Android va iOS tizimlari misolida xavfsizlik arxitekturasi, ularning farqlari va o‘xshashliklari taqqoslanadi. Maqola amaliy ko‘rsatkichlar, jadval va real holatlar bilan boyitilgan bo‘lib, yakunida xavfsizlikni oshirish bo‘yicha ilmiy asoslangan tavsiyalar taklif etiladi.

ASOSIY QISM

Mobil operatsion tizimlar (OT) – bu mobil qurilmalar, xususan, smartfonlar, planshetlar va boshqa ko‘chma qurilmalarda ishlovchi platformalardir. Android, iOS, HarmonyOS kabi tizimlar bugungi kunda millionlab foydalanuvchilar tomonidan ishlatilmoqda. Har bir OT o‘zining xavfsizlik modeli va himoya qatlamlariga ega. Quyida Android va iOS tizimlaridagi asosiy xavfsizlik komponentlari ko‘rsatilgan:

Komponent	Android	iOS
Fayl tizimi xavfsizligi	SELinux, File-based Encryption	Data Protection API, NSFileProtection

Ilova izolyatsiyasi	Sandbox, UID-based access control	App Sandbox, entitlements
Kriptografiya	Keystore, Bouncy Castle	Secure Enclave, CryptoKit
Tizim yangilanishlari	Google Play Protect, OTA updates	iOS Updates, notarization
Avtorizatsiya va autentifikatsiya	Fingerprint, Face Unlock	Face ID, Touch ID, Passcode

Mobil operatsion tizimlar zamonaviy axborot-kommunikatsiya muhitida eng keng tarqalgan platformalardan biri bo‘lib, ularning xavfsizlik darajasi va foydalanuvchi ma’lumotlarini himoyalash salohiyati kundan-kunga yanada muhim ahamiyat kasb etmoqda. Mobil qurilmalar tobora ko‘proq shaxsiy, moliyaviy va ishbilarmonlik ma’lumotlarini o‘zida jamlab borayotganligi sababli, ular uchun ishlab chiqilgan operatsion tizimlarning himoya mexanizmlari ham shunga monand rivojlanmoqda. Android, iOS va boshqa mobil OT’lar turli arxitekturaga ega bo‘lishiga qaramay, ularning barchasi umumiy xavfsizlik tamoyillariga tayanadi: ma’lumotni maxfiy saqlash, ruxsatsiz kirishning oldini olish, foydalanuvchini autentifikatsiyalash va ilova xavfsizligini ta’minlash.

Bugungi kunda mobil OT’lar orasida eng keng tarqalgan ikki platforma – bu Android va iOS tizimlaridir. Android tizimi ochiq kodli bo‘lib, ishlab chiquvchilar uchun moslashuvchanlikni ta’minlaydi, biroq bu moslashuvchanlik xavfsizlik zaifliklariga ham sabab bo‘lishi mumkin. Boshqa tomondan, iOS yopiq arxitekturaga ega bo‘lib, xavfsizlikni qat’iy boshqaradi, biroq bu foydalanuvchining tizimga chuqur kirishini cheklaydi. Har ikkala tizim o‘ziga xos xavfsizlik infratuzilmasiga ega: Android’da SELinux, App Sandbox, ruxsatlar modeli va Google Play Protect tizimi mavjud bo‘lsa, iOS tizimida Secure Enclave, Data Protection API, Touch/Face ID kabi ilg‘or texnologiyalar mavjud.

Xavfsizlikka tahdid soluvchi omillar orasida zararli dasturlar (malware), phishing, root yoki jailbreak asosidagi hujumlar, ochiq Wi-Fi tarmoqlari orqali ma'lumot o'g'irlash holatlari, va foydalanuvchining o'zi tomonidan sodir etiladigan xavfsizlik xatolari alohida o'rin tutadi. Ayniqsa, ruxsatlar modeli noto'g'ri ishlatilganda yoki foydalanuvchi bexabar ravishda noma'lum dasturlarga ruxsat berganida, shaxsiy ma'lumotlar (kontaktlar, lokatsiya, mikrofon, kamera) sizib chiqadi. Bu holatda nafaqat foydalanuvchi xavf ostida qoladi, balki butun korporativ infratuzilma ham xavf ostida qolishi mumkin.

Zamonaviy mobil OT'lar bu kabi xavflarga qarshi kurashishda bir qator samarali texnologiyalardan foydalanmoqda. Ulardan biri – kriptografiya. Android tizimi File-based Encryption va Keystore xizmatlari orqali ma'lumotlarni disk darajasida himoya qiladi. iOS esa Secure Enclave yordamida shifrlash kalitlarini maxfiy muhitda saqlaydi. Bunda AES algoritmi asosiy simmetrik shifrlash vositasi sifatida qo'llaniladi. Asimmetrik shifrlash esa foydalanuvchi autentifikatsiyasi va kalitlar almashinuviga xizmat qiladi, bu orqali end-to-end (E2E) xavfsizlik ta'minlanadi.

Shuningdek, biometrik autentifikatsiya ham muhim o'rin tutadi. Mobil qurilmalarda barmoq izi (fingerprint), yuzni aniqlash (Face ID) yoki ko'z qorachig'ini skanerlash kabi mexanizmlar keng joriy etilgan. Ular parollarni eslab qolish zaruratini kamaytiradi va shu orqali parolga asoslangan tahdidlarni kamaytiradi. Biroq, biometrik ma'lumotlar qayta tiklab bo'lmaydigan ma'lumotlar hisoblanadi, shuning uchun ularning saqlanishi yuqori darajada ishonchli tizimlarda amalga oshirilishi lozim.

Ilovalarning xavfsiz ishlashi uchun sandboxing texnologiyasi qo'llaniladi. Bu har bir ilovaning alohida muhitda ishlashini ta'minlab, uning boshqa tizim komponentlariga ruxsatsiz kirishini cheklaydi. Shuningdek, Android va iOS tizimlari permission model orqali foydalanuvchidan aniq ruxsatlarni so'raydi. Bu model orqali ilovaning qanday resurslardan foydalanishi to'liq nazorat qilinadi.

Shu bilan birga, foydalanuvchilar tomonidan bu ruxsatlarni ongli ravishda berish masalasi ham dolzarbdir, chunki ko‘pchilik foydalanuvchilar ilovani o‘rnatishda barcha ruxsatlarni avtomatik tarzda taqdim etadi.

Mobil xavfsizlikni oshirish uchun ikki bosqichli autentifikatsiya (2FA) tizimlari ham keng joriy qilinmoqda. Bu foydalanuvchini faqat parol bilan emas, balki ikkinchi xavfsizlik elementi – maxfiy SMS kod, elektron pochta orqali yuborilgan tasdiq, yoki autentifikator ilovasi orqali ham aniqlash imkonini beradi. Bu orqali tahdidlar sezilarli darajada kamayadi. Ayniqsa, korporativ darajadagi mobil xavfsizlikda bu tizimlar alohida o‘rin egallaydi. Korporatsiyalar uchun maxsus mobil boshqaruv tizimlari (Mobile Device Management – MDM) mavjud bo‘lib, ular orqali barcha qurilmalarning xavfsizlik siyosati markazlashtirilgan holda boshqariladi.

Interaktiv xavfsizlik monitoring tizimlari esa mobil OT’larning yangi bosqichi sifatida e’tirof etilmoqda. Bu tizimlar foydalanuvchining xatti-harakatlarini real vaqt rejimida kuzatib boradi va g‘ayrioddiy holatlarda avtomatik ogohlantirish yuboradi yoki qurilmani bloklaydi. Masalan, foydalanuvchi odatda Toshkentdan kiradigan bo‘lsa, lekin kutilmaganda boshqa davlatdan kirish holati aniqlansa, tizim bu kirishni shubhali deb hisoblab, tasdiq so‘raydi. Shu tarzda sun’iy intellekt asosida ishlovchi tizimlar mobil xavfsizlikni yanada mustahkamlaydi.

Xulosa qilib aytganda, mobil operatsion tizimlar xavfsizligi va foydalanuvchi ma’lumotlarini himoya qilish masalasi ko‘plab texnik, tashkiliy va xulqiy yondashuvlarni talab etadi. Texnik jihatdan – kriptografik vositalar, autentifikatsiya va sandbox mexanizmlari; tashkiliy jihatdan – yangilanish siyosati, xavfsizlik siyosatini boshqarish; xulqiy jihatdan esa foydalanuvchining ongli xatti-harakati bu tizimning samarali ishlashini ta’minlaydi. Hozirgi texnologik sharoitda mobil qurilmalarning faqatgina apparat darajasidagi himoyasi yetarli emas – foydalanuvchining xabardorligi va xatti-harakatlari ham shunchalik muhimdir.

Mobil xavfsizlikni oshirish strategiyalari

Himoya darajasi	Amalga oshiriladigan choralar	Qamrab oladigan foydalanuvchilar soni
Asosiy	PIN, biometrik tekshiruvlar	95%+
O‘rta	2FA, shifrlash, xavfsiz Wi-Fi	60–70%
Yuksak	App hardening, Secure Enclave, VPN	10–15% (korporativ foydalanuvchilar)

NATIJA

Yuqorida olib borilgan tahlillar mobil operatsion tizimlar xavfsizligini ta’minlashda kompleks yondashuv zarurligini ko‘rsatadi. Android va iOS kabi mashhur platformalarning xavfsizlik arxitekturasi o‘zaro farq qilsa-da, ular foydalanuvchini himoya qilishda qator o‘xshash tamoyillarga asoslanadi: ma’lumotlarni shifrlash, ilovalarni izolyatsiyalash, ruxsatlar tizimi orqali nazorat, biometrik autentifikatsiya va yangilanishlarni muntazam joriy qilish. Tahdidlarning xilma-xilligi, xususan, zararli dasturlar, phishing hujumlari, root/jailbreak harakatlari yoki foydalanuvchining noto‘g‘ri xatti-harakati – xavfsizlikni ta’minlashda nafaqat texnik, balki xulqiy choralarni ham dolzarb qiladi.

Tadqiqotlar shuni ko‘rsatadiki, mobil OT xavfsizligida foydalanuvchi bilim darajasi va xabardorligi ham texnologik himoya vositalari qatori hal qiluvchi omil hisoblanadi. Masalan, kuchli parollarni yaratish, biometrik autentifikatsiyadan foydalanish, faqat ishonchli manbalardan ilovalarni yuklab olish va ruxsatlarni nazorat qilish orqali foydalanuvchi o‘z qurilmasining xavfsizlik darajasini sezilarli darajada oshirishi mumkin. Bundan tashqari, ikki bosqichli tekshirish va avtomatik yangilanishlar xavf xavfini kamaytiradi.

Shuningdek, korporativ muhitda mobil qurilmalar xavfsizligi yanada murakkab bo‘lib, MDM (Mobile Device Management) tizimlarining joriy qilinishi, foydalanuvchi siyosatini qat’iylashtirish va xavfsizlik monitoringi mexanizmlarining faol ishlatilishi zarur bo‘ladi. Natijalar shuni ko‘rsatadiki, mobil

OT xavfsizligining eng samarali modeli — bu foydalanuvchi, ishlab chiquvchi va tizim yetkazib beruvchilar o‘rtasida mas’uliyatni taqsimlagan, integratsiyalashgan yondashuv hisoblanadi.

XULOSA

Mobil operatsion tizimlar xavfsizligini ta'minlash bugungi kunda nafaqat texnologik, balki ijtimoiy va iqtisodiy jihatdan ham dolzarb masalaga aylangan. Foydalanuvchilarning shaxsiy hayoti, moliyaviy axborotlari hamda korporativ ma’lumotlarning himoyasi – mobil qurilmalar va ularga xizmat qiluvchi dasturiy platformalarning ishonchliligiga bevosita bog‘liq. Android va iOS tizimlari har biri o‘ziga xos arxitekturaviy yondashuvlar orqali foydalanuvchi xavfsizligini ta'minlashga intiladi. Ularning xavfsizlik strategiyalari orasida ma’lumotlarni shifrlash, ilovalarni izolyatsiyalash, foydalanuvchi autentifikatsiyasini kuchaytirish va ruxsatlarni aniq boshqarish asosiy o‘rin tutadi.

Tahlillar shuni ko‘rsatadiki, mobil operatsion tizim xavfsizligi yakkayu yagona texnologik yechim bilan emas, balki kompleks, ko‘p bosqichli yondashuvlar orqali samarali amalga oshiriladi. Bunda foydalanuvchining o‘zi, ishlab chiquvchilar va operatsion tizim ishlab chiqaruvchilarning o‘zaro hamkorligi muhim rol o‘ynaydi. Foydalanuvchilar uchun esa raqamli gigiyena qoidalariga amal qilish, ilova ruxsatlarini ongli boshqarish, ikki bosqichli autentifikatsiyani yoqish, qurilmani muntazam yangilab borish hamda noma'lum manbalardan ilova yuklamaslik kabi ehtiyot choralar zarurdir.

Kelajakda mobil xavfsizlik sohasida sun’iy intellekt, mashinali o‘qitish va real vaqtli monitoring tizimlarining rivojlanishi mobil OT himoyasini yanada yuqori bosqichga olib chiqadi. Shu boisdan, ushbu yo‘nalishda ilmiy-tadqiqot ishlarini davom ettirish, yangi xavfsizlik protokollarini ishlab chiqish va foydalanuvchilarning raqamli savodxonligini oshirish dolzarb ahamiyat kasb etadi. Faqatgina kuchli texnologik infratuzilma emas, balki ongli va mas’uliyatli foydalanuvchi madaniyati mobil xavfsizlikning poydevori bo‘lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. (2019). *Operating Systems: Internals and Design Principles* (9th ed.). Pearson Education.

2. Enck, W., Octeau, D., McDaniel, P., & Chaudhuri, S. (2011). *A Study of Android Application Security*. Proceedings of the USENIX Security Symposium.

3. Umarov B. RAQAMLI TEXNOLOGIYALAR VOSITASIDA PEDAGOGLARNING PROFESSIONAL KOMPETENTLIGINI RIVOJLANTIRISH MAZMUNI //Евразийский журнал математической теории и компьютерных наук. – 2023. – Т. 3. – №. 5. – С. 87-93.

4. Azizovich U. B. PRINCIPLES OF FORMING TEACHER COMPETENCE THROUGH INNOVATIVE TECHNOLOGIES. Finland International Scientific Journal of Education //Social Science & Humanities. – 2023. – Т. 11. – №. 5. – С. 823-828.

5. Azizovich U. B. PEDAGOGICAL-PSYCHOLOGICAL PRINCIPLES OF THE FORMATION OF PROFESSIONAL COMPETENCE //Confrencea. – 2023. – Т. 6. – №. 6. – С. 204-212.

6. Azizovich U. B., Zarifjon o'g'li X. N. BULUT TEXNOLOGIYALARINING AFZALLIKLARI VA KAMCHILIKLARI //TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 46-54.

7. Azizovich U. B., Rustamjon o'g'li R. Z. MA'LUMOTLARNI SHIRFLASH TENALOGIYALARI VA XAVFSIZLIK STANDARTLARI //TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 105-108.

8. Azizovich U. B. et al. OLAP TIZIMLARINING ASOSIY PRINSIPLARI //TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – Т. 1. – №. 1. – С. 81-86.

9. Azizovich U. B. THE DEVELOPMENT OF PROFESSIONAL COMPETENCY OF TEACHERS IN EDUCATIONAL TECHNOLOGY BASED ON DIGITAL TECHNOLOGIES //Eurasian Journal of Mathematical Theory and Computer Sciences. – 2024. – Т. 4. – №. 7. – С. 11-14.

10. Azizovich U. B. et al. MASHINALI O ‘QITISHDA REGRESSIYA ENG KICHIK KVADRATLAR USULINI QO ‘LLASH //INNOVATION IN THE MODERN EDUCATION SYSTEM. – 2024. – Т. 5. – №. 46. – С. 266-270.