MOBIL OPERATSION SISTEMALARDA XAVFSIZLIKNI TA’MINLASHNING DASTURIY YONDASHUVLARI. IOS VA ANDROID TIZIMLARIDA XAVFSIZLIK

Farg‘ona davlat universiteti Amaliy matematika va informatika kafedrasi katta o‘qituvchisi

Umarov Bekzod Azizovich

ubaumarov@gmail.com

Farg‘ona davlat universiteti 2-kurs talabasi

Muhammaddiyorova Madina Bahodirjon qizi

mmuhammaddiyorova0110@gmail.com

Annotatsiya : Ushbu maqolada mobil operatsion sistemalarda xavfsizlikni ta’minlashning dasturiy yondashuvlari ko‘rib chiqilgan va Android hamda iOS tizimlarida qo‘llaniladigan dasturiy yondashuvlar taqqoslanganligi keltirilgan. Mobil qurilmalarning bugungi kundagi muhim rolidan tortib ularga qaratilgan xavfsizlikka qarshi tahdidlar, masalan, malware, fishing va ma’lumotlar o‘g‘irlanishlari kabi xavflarning tobora ortib va o‘zgarib borayotganigacha mavzu yoritildi. Bu kabi tahdidlarga qarshi kurashish uchun qo‘llaniladigan turli dasturiy usullar, jumladan, sandboxing, shifrlash, biometric tasdiqlash, ilova do‘konlarida (Play Store va AppStore kabi) qat’iy tekshiruv jarayonlarini va vaqtida yangilanishlar ham ushbu maqolada ko‘rib chiqildi.

Kalit so‘zlar: mobil xavfsizlik, operatsion tizimlar, fishing, malware, sandboxing, biometrik autentifikatsiya, shifrlash texnologiyalari.

Аннотация: В данной статье рассмотрены программные подходы к обеспечению безопасности в мобильных операционных системах, а также проведено сравнение программных решений, применяемых в системах Android и iOS.. Освещена важная роль мобильных устройств в современном мире, а также возрастающие и изменяющиеся угрозы безопасности, такие как вредоносное ПО, фишинг и кража данных. В статье представлены различные программные методы борьбы с такими угрозами, включая изоляцию приложений (sandboxing),

шифрование, биометрическую аутентификацию, строгие процедуры проверки в магазинах приложений (таких как Play Store и App Store), а также своевременное обновление программного обеспечения.

Ключевые слова: мобильная безопасность, операционные системы, фишинг, вредоносное программное обеспечение, песочница, биометрическая аутентификация, технологии шифрования.

Annotation: This article examines software-based approaches to ensuring security in mobile operating systems and compares the software solutions used in Android and iOS platforms. It highlights the crucial role of mobile devices in today's world and the growing and evolving security threats they face, such as malware, phishing, and data theft. The article examines various software methods used to counter these threats, including sandboxing, encryption, biometric authentication, strict app store review processes (such as those in the Play Store and App Store), and timely software updates.

Keywords: mobile security, operating systems, phishing, malware, sandboxing, biometric authentication, encryption technologies.

Kirish

Bugungi kunda mobil qurilmalar inson hayotining ajralmas bo‘lagiga aylangan. Smartfonlar yordamida foydalanuvchilar muloqot qiladi, moliyaviy operatsiyalarni amalga oshiradi, shaxsiy ma’lumotlarni saqlaydi va boshqa ko‘plab raqamli xizmatlardan foydalanadi. 2023-yil ma’lumotlariga ko‘ra, dunyoda 7,33 milliard mobil telefon foydalanuvchisi mavjud bo‘lib, bu aholining 90,97 foizini tashkil etadi. Shu bilan birga, 2021-yilda 9,6 milliondan ortiq malware, adware va riskware hujumlari qayd etilgan. Bu raqamlar mobil operatsion sistemalarda xavfsizlikni ta’minlashning dolzarbligini ko‘rsatadi va mobil qurilmalarda foydalanuvchi ma’lumotlarini himoya qilish bo‘yicha samarali yondashuvlar ishlab chiqilishini taqozo etmoqda. Shu munosabat bilan, ushbu maqolada mobil operatsion tizimlar uchun xavfsizlikni ta’minlashga qaratilgan dasturiy yondashuvlar — masalan, sandboxing texnologiyasi, shifrlash usullari, biometrik autentifikatsiya, ilovalarni ruxsat etish va tekshirish mexanizmlari hamda tizimli yangilanishlar tahlil qilinadi.

Mobil operatsion tizimlar foydalanuvchi uchun qulay interfeyslar va keng imkoniyatlarni taklif qilgani bilan birga turli xil xavfsizlik tahdidlariga ham duch kelmoqda. Ular orasida eng keng tarqalganlari quyidagilardan iborat:

Zararli dasturlar (malware): Mobil qurilmalar uchun ishlab chiqilgan zararli dasturlar, foydalanuvchi ruxsatisiz qurilma resurslaridan foydalanish, ma’lumotlarni to‘plash, va hatto qurilmani nazoratga olishga qodir. Android operatsion tizimi ochiq manbali bo‘lgani sababli, ushbu platformada malware tarqalish xavfi yuqoriroq hisoblanadi. Ilovalarni rasmiy do‘konlar o‘rniga noma’lum manbalardan yuklab olish — ayniqsa xavflidir. Masalan, 2017-yilda “CopyCat” malware 14 million Android qurilmasiga ta’sir qilib, foydalanuvchilarning shaxsiy ma’lumotlarini o‘g‘irlash va reklama firibgarligi orqali millionlab dollar zarar keltirgan. Shu kabi hujumlar Androidning ochiq manbali tuzilishi tufayli yuqori xavfni ko’rsatadi.

Fishing (phishing): Bu usul orqali xakerlar foydalanuvchilarga soxta sahifalar yoki xabarlar yuborib, ularning login ma’lumotlarini, bank kartasi raqamlarini yoki boshqa shaxsiy ma’lumotlarini qo‘lga kiritadi. Fishing mobil platformalarda SMS, e-mail va hatto ilova bildirishnomalari orqali amalga oshirilmoqda. Statistikaga ko‘ra, 2021-yilda mobil platformalardagi phishing hujumlarining 85 foizi SMS va ilova bildirishnomalari orqali amalga oshirilgan. Masalan, foydalanuvchilarni soxta bank ilovalari orqali aldagan “FluBot” malware 2021-yilda Yevropada keng tarqalgan edi.

Ma’lumotlar o‘g‘irlanishi: Mobil qurilmalarda saqlanadigan kontaktlar, fotosuratlar, geolokatsiya ma’lumotlari, shaxsiy fayllar va parollar — kiber jinoyatchilar uchun ayniqsa qimmatli maqsaddir. Zararli ilovalar yoki xakerlar ushbu ma’lumotlarni turli yo‘llar bilan o‘g‘irlashi mumkin, masalan, zaif ilova ruxsatnomalari yoki tarmoq orqali yuborilayotgan ma’lumotlarning shifrlanmaganligi. 2015-yilda iOS platformasida “XCodeGhost” malware App Store orqali tarqalib, minglab ilovalarga zarar yetkazdi va foydalanuvchilarning shaxsiy ma’lumotlarini o‘g‘irladi. Bu holat hatto qat’iy tekshiruvlardan o‘tgan ilova do‘konlarida ham zaifliklar mavjudligini ko’rsatadi.

Ushbu tahdidlar soni va murakkabligi ortib borayotganligi tufayli, mobil qurilmalarni himoya qilish uchun samarali dasturiy yondashuvlar joriy etilishi zarur.

Ushbu xavfsizlik tahdidlariga qarshi kurashishda bir nechta samarali dasturiy yondashuvlar mavjud. Ular orasida sandboxing texnologiyasi muhim o‘rin tutadi va mobil ilovalarning izolyatsiyalangan muhitda ishlashini ta’minlash orqali tizimni ichki hujumlardan himoya qiladi.

Sandboxing — bu dasturlarni alohida, izolyatsiyalangan muhitda ishga tushirish orqali tizim xavfsizligini ta’minlaydigan dasturiy yondashuvdir. Mobil operatsion tizimlarda, ayniqsa Android va iOS platformalarida, har bir ilova o‘zining "sandbox"ida faoliyat yuritadi. Bu degani, biror ilova boshqa ilovaning ma’lumotlariga yoki tizim resurslariga bevosita kira olmaydi.

Bu yondashuv quyidagi afzalliklarni beradi:

- Zararli faoliyatlarning cheklanishi: Agar ilova zararli kodga ega bo‘lsa ham, u boshqa ilovalarga yoki tizim fayllariga zarar yetkaza olmaydi.
- Ma’lumotlar maxfiyligini himoyalash: Ilovalar orasida ma’lumotlar oqimi faqat operatsion tizim ruxsat bersagina amalga oshadi.
- Foydalanuvchi nazorati: Har bir ilova uchun ruxsatlar (kamera, joylashuv, kontaktlar) foydalanuvchi tomonidan alohida boshqariladi.

Android tizimi har bir ilovani alohida foydalanuvchi identifikatori (UID) bilan ajratib, tizimdagi boshqa ilovalardan mustaqil ishlashini ta’minlaydi. iOS esa ilovalarni yanada qat’iy chegaralovchi sandbox mexanizmlari orqali nazorat qiladi.

Shunday qilib, sandboxing mobil xavfsizlik arxitekturasining asosiy bo‘g‘inlaridan biri bo‘lib, ilovalararo xavfli o‘zaro ta’sirlarning oldini olishda muhim rol o‘ynaydi.

Keyingi himoya usuli shifrlash texnologiyalaridan foydalanishdir. Shifrlash — bu ma’lumotlarni maxfiy va yetkazib bo‘lmaydigan holatga keltirish orqali ularni uchinchi tomonlar aralashuvidan himoya qilishning asosiy usullaridan biridir. Mobil operatsion tizimlarda shifrlash texnologiyalari foydalanuvchi ma’lumotlari, ilova fayllari va tarmoq orqali uzatiladigan axborotlarni himoya qilishda keng qo‘llaniladi.

Asosiy shifrlash usullari quyidagilarni o‘z ichiga oladi:

- Disk darajasida shifrlash: Bu usulda butun fayl tizimi shifrlanadi. Android va iOS operatsion tizimlari hozirgi kunda foydalanuvchi qurilmasining xotirasini to‘liq shifrlaydi.

- Tarmoq orqali uzatilayotgan ma’lumotni shifrlash: HTTPS, VPN va boshqa tarmoq protokollari orqali foydalanuvchi ma’lumotlari uzatilish jarayonida shifrlanadi. Bu internet orqali yuborilgan ma’lumotlarning o‘g‘irlanishini oldini oladi.
- Ilova ichidagi shifrlash: Ba’zi mobil ilovalar foydalanuvchi ma’lumotlarini o‘z bazalarida shifrlangan holda saqlaydi, bu esa ilovaga ruxsatsiz kirish holatlarida ma’lumotlarni himoya qiladi.

Shifrlashda ishlatiladigan algoritmlar (AES, RSA, ECC va boshqalar) mobil qurilmalarda resurslardan samarali foydalanishni ham hisobga olgan holda tanlanadi. Masalan, mobil qurilmalarda AES (Advanced Encryption Standard) algoritmi juda keng qo‘llaniladi, chunki u tez ishlashi va kam resurs talab qilishi bilan ajralib turadi. Masalan, Android 7.0 dan boshlab fayl sari shifrlash (file-based encryption) joriy qilingan bo‘lib, har bir fayl alohida kalit bilan shifrlanadi. RSA va ECC (Elliptic Curve Cryptography) algoritmlari esa kalit almashish va raqamli imzolarda ishlatiladi, lekin resurs talab qilishi tufayli faqat muayyan vazifalarda qo‘llaniladi. iOSda Advanced Data Protection end-to-end shifrlashni ta’minlaydi, bu esa iCloud ma’lumotlarini ham himoya qiladi (Apple, 2023).

Biometrik autentifikatsiya ham mobil operatsion tizimlarda maxfiylikni saqlash va himoyalanish uchun qo‘llaniladigan vositalardan biri bo‘lib, foydalanuvchini uning jismoniy yoki xulq-atvorga oid noyob belgilariga asoslangan holda aniqlaydi. Ushbu usul mobil qurilmalarda xavfsizlik darajasini oshirishda tobora keng qo‘llanilmoqda, chunki u parollar yoki PIN-kodlarga nisbatan qulayroq va firibgarlikdan himoyalanish darajasi yuqoriroq. Androidda Biometric API ilovalarga barmoq izi va yuz tanishuvini xavfsiz integratsiya qilish imkonini beradi, ma’lumotlar esa Trusted Execution Environmentda saqlanadi. iOSning Secure Enclave protsessori Face ID va Touch ID ma’lumotlarini shifrlangan holda saqlaydi va ularni tashqi serverlarga uzatmaydi. Biometrik autentifikatsiyaning zaif tomoni sifatida soxta yuz niqoblari yoki barmoq izi replikalari kabi hujumlar mavjud, lekin ko‘p faktorli autentifikatsiya bu xavfni kamaytiradi.

Mobil operatsion tizimlarda keng tarqalgan biometrik autentifikatsiya turlari quyidagilardan iborat:

- Barmoq izi skaneri: Android va iOS qurilmalarida eng keng qo‘llaniladigan usul bo‘lib, foydalanuvchining barmoq izlari qurilma xotirasidagi maxsus xavfsiz sohada (Trusted Execution Environment yoki Secure Enclave) saqlanadi.
- Yuzni aniqlash: Bu texnologiya foydalanuvchining yuz tuzilishini skanerlaydi va uni qurilmada saqlangan ma’lumotlar bilan solishtiradi. Face ID (Apple) va Face Unlock (Android) kabi tizimlar bu texnologiyaga asoslanadi.
- Ko‘z to‘r pardasini skanerlash: Nisbatan kam tarqalgan, biroq yuqori darajadagi aniqlikni ta’minlaydigan usul hisoblanadi. Ayrim Android qurilmalarda bu texnologiya qo‘llanilgan.

Biometrik ma’lumotlar qurilmadan tashqariga uzatilmaydi va foydalanuvchi maxfiyligini saqlash uchun faqat lokal tarzda shifrlangan holda saqlanadi. Shu bilan birga, ishlab chiquvchilar biometrik autentifikatsiyani ilovalarga qo‘shish uchun Android Biometric API yoki Apple Face ID/Touch ID API laridan foydalanadilar.

Biometrik autentifikatsiyaning afzalliklari qulaylik, tezkorlik va yuqori xavfsizlik bo‘lsa-da, uning kamchiliklari ham mavjud. Masalan, ayrim holatlarda yuz niqobi yoki barmoqdagi jarohatlar autentifikatsiyani buzishi mumkin.

Shu sababli, biometrik autentifikatsiya ko‘pincha boshqa xavfsizlik mexanizmlari bilan birgalikda qo‘llaniladi va ko‘p faktorli autentifikatsiya tizimlarining ajralmas qismiga aylanmoqda.

Mobil operatsion tizimlar uchun mo‘ljallangan ilovalar ko‘pincha rasmiy ilova do‘konlari — Google Play Store va Apple App Store orqali tarqatiladi. Ushbu do‘konlar foydalanuvchi qurilmalarini zararli dasturlardan himoya qilishda muhim rol o‘ynaydi. Shu sababli, ilovalarni joylashtirishdan oldin qat’iy xavfsizlik tekshiruvlari o‘tkaziladi.

Google Play Protect — Android qurilmalarda o‘rnatilgan xavfsizlik tizimi bo‘lib, u Play Store’dan yuklab olingan ilovalarni avtomatik ravishda skanerlab, zararli faoliyatlarni aniqlaydi. Bundan tashqari, u fonda doimiy ishlab turib, allaqachon o‘rnatilgan ilovalarni ham muntazam tekshiradi.

Apple App Store esa ilovalarni joylashtirishdan oldin har bir dasturni qo‘lda ko‘rib chiqadi. Bunda ilovaning funksionalligi, foydalanuvchi ma’lumotlarini qanday yig‘ishi va xavfsizlik standartlariga muvofiqligi baholanadi. App Store ilovalari uchun App Review

Guidelines mavjud bo‘lib, ular orqali ishlab chiquvchilardan aniq xavfsizlik va maxfiylik talablariga rioya qilish talab etiladi.

Shuningdek, har ikkala do‘kon ham zararli yoki siyosatga zid ilovalarni aniqlagan holda ularni do‘kondan olib tashlash vakolatiga ega. Bu foydalanuvchilar uchun xavfsizlik kafolatini sezilarli darajada oshiradi.

Ayrim hollarda, zararli ilovalar rasmiy tekshiruvlardan ham o‘tib ketishi mumkin. Shu sababli, foydalanuvchilar ham do‘konlardagi reyting va izohlarni tekshirish, ilovaning ishlab chiquvchisini aniqlash va kerakli ruxsatlar so‘ralayotganini diqqat bilan ko‘rib chiqishlari tavsiya etiladi.

Ilova do‘konlaridagi xavfsizlik nazorati doimiy yangilanib boradi va yangi tahdidlar yuzaga chiqqan sari bu jarayonlar ham rivojlanib boradi. Bu esa mobil ekotizimning xavfsiz va ishonchli bo‘lishini ta’minlaydi.

Mobil operatsion tizimlar va ulardagi ilovalar muntazam ravishda yangilanib boradi. Bu yangilanishlar nafaqat yangi funksiyalarni qo‘shish, balki mavjud zaifliklarni bartaraf etish, xavfsizlik darajasini oshirish maqsadida ham amalga oshiriladi. Zero, kiberxavfsizlik sohasidagi tahdidlar tez o‘zgarib borar ekan, tizimlarni doimiy ravishda himoya qilishning eng samarali usullaridan biri bu — vaqtida dasturiy yangilanishlarni amalga oshirishdir.

Zamonaviy mobil operatsion tizimlar, xususan Android va iOS, har chorakda yoki xavfsizlik bo‘yicha zarurat tug‘ilganda maxsus security patchlar chiqaradi. Ushbu xavfsizlik yangilanishlari orqali aniqlangan zaifliklar bartaraf qilinadi, bu esa zararli dasturlarning tizimga kirib olish ehtimolini kamaytiradi.

Bundan tashqari, ilovalar ishlab chiquvchilari ham o‘z dasturlarini xavfsizligini oshirish maqsadida yangilab borishlari zarur. Eskirgan ilovalar zamonaviy xavfsizlik standartlariga javob bermasligi va foydalanuvchi ma’lumotlariga tahdid tug‘dirishi mumkin.

Avtomatik yangilanish funksiyasi orqali foydalanuvchilarning ko‘pchiligi yangilanishlardan bexabar qolmaydi. Shu bilan birga, foydalanuvchilarning o‘zlari ham yangilanishlar haqida xabardor bo‘lishi va ularni iloji boricha tezroq o‘rnatishga e’tibor berishlari kerak.

Hozirgi kunda iOS va Android mobil qurilmalar uchun eng keng qo‘llanilayotgan tizimlar bo‘lganligi uchun ular o‘rtasidagi ba’zi farqlarni bilish kelajakda sodir bo‘lish ehtimoli bor tahdidlarga tayyor turish va bu ikki tizimlardagi xavfsizlikni ta’minlash funksiyalarini bilib olish zarur. Shu sababdan ham quyida bu ikki tizimlar xafvsizligini taqqoslaydigan jadval keltirilgan:

Himoyalash usuli	Android	iOS
Sandboxing	Linuxga asoslangan UID orqali ilovalarni izolyatsiya qiladi. Har bir ilovaga alohida foydalanuvchi identifikatori beriladi.	Secure Encslave va App Sandbox orqali qat’iy izolyatsiya qiladi. Ilovalar tizim fayllariga kira olmaydi.
Shifrlash	Fayl sari shifrlash (Android 7.0 dan boshlab) va to‘liq disk shifrlashni amalga oshiradi. Bunda AES algoritmidan foydalaniladi.	End-to-end shifrlash, Advanced Data Protection (iCloud ma’lumotlari uchun), AES va Secure Enclave ishlatiladi.
Biometrik autentiifikatsiya	Barmoq izi, yuzni aniqlash, Biometric APIdan foydalaniladi hamda ma’lumotlar Trusted Execution Environmentda saqlanadi.	Face ID, Touch ID va Secure Enclaveda shifrlangan ma’lumotlar bo‘ladi va ular tashqi serverlarga uzatilmaydi.
Ilova do‘koni tekshiruvi	Google Play Protect avtomatik skanerlash va real	App Storeda qo‘lda tekshiruv mavjud hamda App Review Guidelinesga

	vaqtda zararli ilovalarni aniqlash imkoni mavjud.	qat'iy rioya qilish talab etiladi.
Yangilanishlar	Avtomatik yangilanishlarni qo‘llab-quvvatlaydi lekin ko‘p holatlarda bu ishlab chiqaruvchiga bog‘liq bo‘ladi. Fragmentatsiya kechikishlariga olib keladi.	Rapid Security Responses, o‘z vaqtida va markazlashgan yangilanishlarni qo‘llab-quvatlaydi.

Jadvaldan ko‘rinib turibdiki, Android ochiq manbali tuzilishi tufayli moslashuvchanlikni ta’minlasa, iOS qat’iy nazorat va markazlashgan yangilanishlar orqali yuqori xavfsizlikni ta’minlaydi.

Xulosa: Mobil operatsion tizimlarning keng tarqalishi va ulardan foydalanuvchilarning ko‘pligi zamonaviy raqamli dunyoda ularning xavfsizligini ta’minlash masalasini dolzarb qilib qo‘ymoqda. Ushbu maqolada mobil tizimlarga tahdid soluvchi asosiy xavf-xatarlar – zararli dasturlar (malware), fishing hujumlari, ma’lumotlar o‘g‘irlanishi va boshqa turdagi xakerlik harakatlari tahlil qilindi.

Shuningdek, bunday tahdidlarga qarshi samarali kurashishda dasturiy yondashuvlarning ahamiyati yoritildi. Xususan, sandboxing texnologiyasi, shifrlash usullari, biometrik autentifikatsiya vositalari, ilovalarni tekshirish jarayonlari hamda tizim yangilanishlarini vaqtida amalga oshirish kabi usullar muhim ekani ko‘rsatib berildi.

Android va iOS tizimlarining xavfsizlik mexanizmlari o‘zaro taqqoslab chiqilib, har ikkala platformaning o‘ziga xos afzallik va cheklovlari mavjudligi aniqlandi. Tadqiqotlar shuni ko‘rsatmoqdaki, har ikki tizimda xavfsizlikni ta’minlashda yondashuvlar farqli bo‘lsada, asosiy maqsad – foydalanuvchi ma’lumotlarini himoya qilish – umumiy bo‘lib qolmoqda.

Kelgusida mobil xavfsizlik sohasida sun’iy intellekt (AI), mashinani o‘qitish, blockchain va kvant shifrlash kabi ilg‘or texnologiyalar muhim rol o‘ynaydi. Sun’iy

intellekt real vaqtda tahdidlarni aniqlashda keng qo‘llanilmoqda. Masalan, Google Play Protect AI asosidagi algoritmlar yordamida ilovalarni doimiy skanerlaydi va 2023-yilda 2,5 million zararli ilovani bloklagan. Mashinani o‘qitish yordamida yangi malware turlari imzo asosidagi usullarga qaraganda 97,82% aniqlik bilan aniqlanmoqda.

Blockchain texnologiyasi xavfsiz tranzaksiyalar va decentralized identity tizimlari uchun potensial yechim sifatida ko‘rilmoqda. Masalan, blockchain asosidagi autentifikatsiya tizimlari foydalanuvchi ma’lumotlarini markazlashgan serverlarsiz himoya qilishi mumkin, bu esa man-in-the-middle hujumlarini kamaytiradi.

Kvant shifrlash kelajakdagi kvant kompyuterlarning AES va RSA kabi algoritmlarni zaiflashtirish xavfini bartaraf etish uchun ishlab chiqilmoqda. Post-quantum cryptography algoritmlari, masalan, lattice-based shifrlash, mobil qurilmalarda xavfsizlikni ta’minlashda muhim bo‘lad.

Yangi biometrik usullar, masalan, retina skanerlash yoki venalar tanishuvi, an’anaviy barmoq izi va yuz tanishuvidan yuqori aniqlik beradi. Masalan, Samsung ba’zi qurilmalarida iris skanerlashni joriy qilgan. Ushbu texnologiyalar mobil operatsion sistemalarning himoya darajasini yanada oshiradi.

Foydalanilgan adabiyotlar:

1. J.J. Atamuradov, S.S. Salimov. *Mobil ilovalar yaratish.* O‘quv qo‘llanma. Buxoro – 2024

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

3. 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.

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

5. Azizovich U. B., Zarifjon o'g'li X. N. BULUT TEXNOLOGIYALARINING AFZALLIKLARI VA KAMCHILIKLARI //TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – T. 1. – №. 1. – C. 46-54.

6. Azizovich U. B., Rustamjon o'g'li R. Z. MA'LUMOTLARNI SHIRFLASH TENALOGIYALARI VA XAVFSIZLIK STANDARTLARI //TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – T. 1. – №. 1. – C. 105-108.

7. Azizovich U. B. et al. OLAP TIZIMLARINING ASOSIY PRINSIPLARI //TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI. – 2024. – T. 1. – №. 1. – C. 81-86.

8. 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. – T. 4. – №. 7. – C. 11-14.

9. Azizovich U. B. et al. MASHINALI O 'QITISHDA REGRESSIYA ENG KICHIK KVADRATLAR USULINI QO 'LLASH //INNOVATION IN THE MODERN EDUCATION SYSTEM. – 2024. – T. 5. – №. 46. – C. 266-270.

10. Drake, J. J., Lanier, Z., Mulliner, C., Fora, P. O., & Ridley, S. A. (2014). Android Hacker's Handbook. Wiley.

11. Miller, C., Blazakis, D., Dai Zovi, D., Esser, S., Iozzo, D., & Weinmann, R.-P. (2012). iOS Hacker's Handbook. Wiley.

12. Clark, C., Dwivedi, H., & Thiel, D. (2010). Mobile Application Security. McGraw-Hill.

13. https:\\uz.wikipedia.org

14. Boudriga, N. (2010). Security of Mobile Communications. Auerbach Publications.

15. Talukder, M., & Ghosh, R. (2020). Mobile Security: Threats and Best Practices. Security and Communication Networks, 2020, 8828078.

16. Varghese, J., & Jevitha, K. P. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. Frontiers in Computer Science.

17. Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2013). A Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials, 15(1), 446-471.

18. GetAstra. (2023). iOS vs Android Security: A Comprehensive Comparison.

19. Kaspersky. (2023). Android vs. iPhone Mobile Security.