ISSN: 3060-4923 Impact Factor –7,212

MOBIL TELEFONLARNI XAKERLAR HUJUMIDAN HIMOYALASHNING AYRIM ZAMONAVIY YECHIMLARI

Ro‘ziboyeva Marjona Farhod qizi
Toshkent davlat iqtisodiyot universiteti To‘rtko‘l fakulteti
“Axborot tizimlari va texnologiyalari” yo‘nalishi 3-bosqich talabasi
E-mail: roziboyevamarjona006@gmail.com
https://doi.org/10.5281/zenodo.24397665

ANNOTATSIYA. Maqolada mobil telefonlarga qaratilgan zamonaviy xakerlik hujumlari va ularga qarshi eng so‘nggi himoya yechimlari tahlil qilingan. Tadqiqot 2020-2026 yillardagi xalqaro ilmiy nashrlar, NIST va OWASP standartlari, kiberxavfsizlik kompaniyalarining 2026-yilgi hisobotlari hamda O‘zbekiston Respublikasi Ichki ishlar vazirligining rasmiy ma’lumotlariga asoslanadi. Apparat darajasidagi xotira himoyasi, yuqori xavf rejimlari, sun’iy intellekt asosida zararli dasturlarni aniqlash, parolsiz (FIDO2/passkey) autentifikatsiya va “nol ishonch” arxitekturasi qiyosiy baholangan. Natijada olti qatlamli kompleks himoya modeli va zararli APK-fayllarga qarshi kurashish bo‘yicha amaliy tavsiyalar ishlab chiqilgan.
Kalit so‘zlar: mobil xavfsizlik, kiberhujum, zararli dastur, APK-fayl, smishing, sun’iy intellekt, FIDO2, passkey, nol ishonch arxitekturasi.

АННОТАЦИЯ. В статье анализируются современные хакерские атаки на мобильные телефоны и новейшие решения по защите от них. Исследование опирается на международные публикации 2020–2026 гг., стандарты NIST и OWASP, отчёты компаний в сфере кибербезопасности за 2026 г. и официальные данные МВД Республики Узбекистан. Проведена сравнительная оценка аппаратной защиты памяти, режимов повышенной защиты, обнаружения вредоносного ПО на основе искусственного интеллекта, беспарольной аутентификации (FIDO2/passkey) и архитектуры «нулевого доверия». Предложена шестиуровневая модель комплексной защиты и практические рекомендации по противодействию вредоносным APK-файлам.
Ключевые слова: мобильная безопасность, кибератака, вредоносное ПО, APK-файл, смишинг, искусственный интеллект, FIDO2, passkey, нулевое доверие.

ABSTRACT. The article analyses contemporary hacker attacks on mobile phones and the most recent solutions for protecting against them. The study draws on international publications from 2020–2026, NIST and OWASP standards, 2026 cybersecurity vendor reports, and official data from the Ministry of Internal Affairs of Uzbekistan. Hardware memory protection, high-risk protection modes, AI-based malware detection, passwordless (FIDO2/passkey) authentication and zero-trust architecture are comparatively assessed. A six-layer comprehensive protection model and practical recommendations for countering malicious APK files are proposed.
Keywords: mobile security, cyberattack, malware, APK file, smishing, artificial intelligence, FIDO2, passkey, zero trust.

KIRISH. Mobil telefon bugun bank kartalari, davlat xizmatlari, shaxsiy yozishmalar va biometrik ma’lumotlar jamlangan “raqamli seyf”ga aylangan, shu sababli kiberjinoyatchilarning asosiy nishoniga ham aylanmoqda. Kaspersky ma’lumotlariga ko‘ra, 2025-yilda Android

smartfonlariga bank troyanlari hujumlari 2024-yilga nisbatan 56 foizga oshgan, yangi bank troyanlari o‘rnatish paketlari soni esa 271 foizga ko‘payib, 255 090 taga yetgan [1]. 2026-yilning II choragida bank troyanlari aniqlangan zararli ilovalar orasida 30,77 foiz ulush bilan eng keng tarqalgan toifa bo‘lib qoldi [2], 2026-yilning yanvar-aprel oylarida esa bank kartasi ma’lumotlarini NFC orqali o‘g‘irlovchi hujumlar 188 foizga oshdi [3]. Zimperium kompaniyasining 2026-yilgi hisobotida xodimlarning mobil qurilmalaridagi fishing hodisalari 2025-yil yanvaridan buyon 380 foizga o‘sgani va fishing hujumlarining qariyb 86 foizida sun’iy intellekt yordamida yaratilgan elementlar mavjudligi qayd etilgan [4].

O‘zbekistonda ham vaziyat keskin. Ichki ishlar vazirligi ma’lumotlariga ko‘ra, 2026-yilning yanvar-sentabr oylarida axborot texnologiyalaridan foydalangan holda 69 962 ta jinoyat sodir etilgan, fuqarolarga qariyb 1 trillion so‘m zarar yetkazilgan. Bunday jinoyatlarning taxminan 50 foizi zararli APK-fayllar orqali, 90 foizi esa xorijdan turib amalga oshirilgan [5]. Shu davrda jinoyat bilan bog‘liq 43 001 ta bank kartasi bloklangan va 38 mingdan ortiq fishing dasturining faoliyati to‘xtatilgan [6]. Davlat darajasida “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonun [7] va Prezidentning 2026-yil 10-martdagi PF-38-son Farmoni bilan tasdiqlangan 2026-2030 yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi [8] anti-fishing platformasini yaratish, firibgar qo‘ng‘iroqlarni bloklash va onlayn xizmatlarda ko‘p faktorli autentifikatsiyani joriy etishni nazarda tutadi.

Maqolaning maqsadi – mobil telefonlarga qaratilgan zamonaviy hujumlar va ularga qarshi himoya yechimlarini tizimli tahlil qilib, O‘zbekiston sharoitiga moslashtirilgan kompleks himoya modelini ishlab chiqish. Vazifalar: 1) zamonaviy mobil tahdidlarni tasniflash; 2) apparat, operatsion tizim, ilova, autentifikatsiya va sun’iy intellekt darajasidagi yechimlarni qiyosiy tahlil qilish; 3) ko‘p qatlamli himoya modeli va amaliy tavsiyalarni ishlab chiqish.

MAVZUNING O‘RGANILGANLIK DARAJASI. Ilmiy adabiyotda eng ko‘p o‘rganilgan yo‘nalish – zararli dasturlarni mashinaviy o‘qitish yordamida aniqlash. Y. Liu va boshqalar [9] Android zararli dasturlariga qarshi chuqur o‘qitish usullarining tizimli sharhida statik va dinamik belgilarni birlashtirgan gibrid modellar yuqori aniqlikka erishishini, biroq modellarning o‘zi chetlab o‘tish (adversarial) hujumlariga zaif ekanini ko‘rsatgan. E. Taşkın va İ.A. Doğru [10] 12 000 ta APK-fayl asosida klassik mashinaviy o‘qitish, transformer va katta til modellarini (LLM) taqqoslab, maxsus sozlangan LLM 0,982, yengil transformer modeli esa 0,970 F1-ko‘rsatkichiga erishishini aniqlagan. C. Jiang va hammualliflar [11] shaxsiy ma’lumotlarni qurilmadan chiqarmasdan zararli ilovalarni tasniflovchi federativ o‘qitish modelini, M.L. Munoz va M.F. Islam [12] esa SMS-fishing xabarlarini 0,97 F1-ko‘rsatkich bilan aniqlovchi BERT asosidagi modelni taklif etgan.

Autentifikatsiya borasida L. Lassak va boshqalar [13] FIDO2/passkey texnologiyasining fishingga chidamliligini e’tirof etib, uni joriy etishdagi to‘siqlar – hisobni tiklash, foydalanuvchi noqulayligi va tashkiliy omillarni aniqlagan. Korporativ darajada NIST SP 800-124 Rev.2 [14] mobil qurilmalarni boshqarish (MDM) va mobil tahdidlardan himoya (MTD) tizimlarini, SP 800-207 [15] esa “nol ishonch” arxitekturasini tavsiya etadi. OWASP Mobile Top 10 (2024) [16] mobil ilovalardagi eng xavfli o‘nta zaiflik toifasini belgilaydi. Foydalanuvchi ishtirokisiz ishga tushuvchi “nol klik” josuslik dasturlari Citizen Lab tomonidan hujjatlashtirilgan [17]. Mahalliy adabiyotda N.A. Shakirova va O.V. Obidov [18] O‘zbekistondagi onlayn firibgarlik turlarini tahlil qilgan. Muallifning hammualliflikdagi ishlarida mobil ilovalarda xavfsiz autentifikatsiya va maxfiylik [19] hamda federativ o‘qitish va blokcheyn asosida ma’lumotlarni himoyalash [20] masalalari yoritilgan.

Mavjud tadqiqotlar odatda bitta texnologik yo‘nalishga qaratilgan bo‘lib, apparat darajasidan davlat siyosatigacha bo‘lgan himoya qatlamlarini yagona tizimda ko‘rib chiquvchi va messenjerlar orqali tarqatiladigan APK-fayllar kabi mintaqaviy tahdidlarni hisobga oluvchi kompleks yondashuv yetarlicha yoritilmagan.

TADQIQOT METODOLOGIYASI. Tadqiqotda tizimli adabiyotlar sharhi, qiyosiy tahlil, tasniflash va sintez usullari qo‘llanildi. Manbalar sifatida 2020-2026 yillardagi xalqaro ilmiy nashrlar, NIST va OWASP standartlari, Apple va Google kompaniyalarining rasmiy texnik nashrlari, Kaspersky va Zimperium kompaniyalarining 2026-yilgi hisobotlari hamda O‘zbekiston Respublikasi me’yoriy-huquqiy hujjatlari va IIV ma’lumotlari olindi. Himoya yechimlari ta’sir darajasi bo‘yicha guruhlanib, har bir tahdid turiga qarshi samaradorligi baholandi va natijalar “tahdid – himoya qatlami” matritsasida umumlashtirildi. Sanoat hisobotlaridagi ko‘rsatkichlar kompaniyalarning o‘z telemetriyasiga asoslangani sababli tendensiyani ifodalovchi ko‘rsatkichlar sifatida talqin qilindi.

TAHLIL VA NATIJALAR. 1. Zamonaviy mobil tahdidlar. Tahlil asosida mobil tahdidlarni quyidagi guruhlarga ajratish mumkin: 1) zararli APK-fayllar va bank troyanlari (Mamont, Creduz oilalari) [1]; 2) SMS, messenjer va qo‘ng‘iroq orqali ijtimoiy muhandislik (smishing, vishing); 3) NFC orqali karta ma’lumotlarini o‘g‘irlash [3]; 4) qurilma ishlab chiqarilganda o‘rnatilgan zararli dasturlar (Triada, Keenadu) [1]; 5) eskirgan operatsion tizim zaifliklari; 6) “nol klik” josuslik dasturlari [17].

O‘zbekiston uchun eng xarakterli tahdid – Telegram orqali tarqatiladigan zararli APK-fayllar. IIV ma’lumotlariga ko‘ra, ular to‘y taklifnomasi, tanish odamning surati yoki ta’ziya xabari niqobida yuboriladi. Boshqa keng tarqalgan usul – “ovoz berish” havolasi orqali foydalanuvchidan Telegram tasdiqlash kodini olib, hisobni egallash va uning kontaktlaridan rahbar nomidan pul so‘rash [5]. O‘rnatilgan zararli ilova SMS-xabarlar va bildirishnomalarga kirish ruxsatini olib, bankning bir martalik kodlarini jinoyatchiga uzatadi. Shu sababli an’anaviy SMS orqali tasdiqlash qurilma zararlangan holatda himoya bera olmaydi. Global miqyosda bunga NFC hujumlari qo‘shilmoqda: jabrlanuvchi zararli ilova o‘rnatgach, bank kartasini telefonga tegizib PIN-kodni kiritishga ko‘ndiriladi va karta ma’lumotlari jinoyatchiga uzatiladi [3].

2. Apparat va operatsion tizim darajasidagi yechimlar. Murakkab josuslik dasturlari xotira bilan ishlashdagi xatoliklardan foydalanadi. Apple 2025-yil sentabrida iPhone 17 qurilmalarida Arm arxitekturasining kengaytirilgan xotirani teglash (EMTE) texnologiyasiga asoslangan Memory Integrity Enforcement himoyasini joriy etdi: xotiraning har bir bo‘lagiga maxfiy teg biriktiriladi va noto‘g‘ri murojaat apparat darajasida bloklanadi, bu esa “nol klik” ekspluatlarini ishlab chiqishni keskin qiyinlashtiradi [21]. Yuqori xavf ostidagi foydalanuvchilar uchun iOS tizimida Lockdown Mode, Android 16 tizimida esa Advanced Protection rejimi mavjud. Ikkinchisi eng qat’iy sozlamalarni bir tugma bilan yoqadi va qurilmaga hujum izlarini keyingi tahlil uchun saqlaydi [22]. O‘zbekiston uchun ayniqsa muhim yechim – Android tizimidagi qo‘ng‘iroq paytidagi himoya: telefon suhbati davomida Play Protect himoyasini o‘chirish, rasmiy do‘kondan tashqari ilova o‘rnatish va maxsus imkoniyatlar (Accessibility) ruxsatini berish taqiqlanadi, qulflangan ekranda esa bir martalik kodlar yashiriladi [22]. Bu “bank xodimi” niqobidagi firibgarning jabrlanuvchini APK o‘rnatishga ko‘ndirish sxemasini texnik jihatdan uzib qo‘yadi.

3. Sun’iy intellekt asosidagi aniqlash. Imzo asosidagi antivirus usullari doimiy o‘zgartiriladigan zararli dasturlarga qarshi samarasiz bo‘lib qolmoqda, shu sababli aniqlash tizimlari mashinaviy o‘qitish va til modellariga o‘tmoqda [9; 10]. Google kompaniyasi Gemini Nano modeli yordamida firibgarlik xabarlari va sahifalarini bevosita qurilmaning o‘zida aniqlash funksiyasini joriy etdi [22]. Bu yondashuvda foydalanuvchi ma’lumotlari serverga yuborilmaydi. Federativ o‘qitish [11; 20] millionlab qurilmalarga umumiy modelni shaxsiy ma’lumotlarni oshkor qilmasdan o‘qitish imkonini beradi. Shu bilan birga, hujumchilar ham sun’iy intellektdan faol foydalanmoqda [4] va aniqlash modellarini chalg‘itish uchun maxsus namunalar tayyorlamoqda [9], shuning uchun bunday tizimlar boshqa himoya qatlamlari bilan birga qo‘llanilishi lozim.

4. Fishingga chidamli autentifikatsiya va korporativ himoya. SMS orqali yuboriladigan bir martalik kodlar SIM-kartani almashtirish, zararli dastur yoki ijtimoiy muhandislik yo‘li bilan qo‘lga kiritilishi mumkin. FIDO2/passkey texnologiyasida maxfiy kalit qurilmaning himoyalangan apparat modulida saqlanadi va faqat haqiqiy sayt yoki ilova domeni bilan ishlaydi, shuning uchun foydalanuvchi soxta saytga kirganda ham hisob ma’lumotlari jinoyatchiga o‘tmaydi [13]. PF-38-son Farmonda ko‘zda tutilgan ko‘p faktorli autentifikatsiyani [8] aynan shunday fishingga chidamli usullar asosida joriy etish maqsadga muvofiq. Tashkilotlarda esa MDM/MTD tizimlari [14], har bir so‘rovni foydalanuvchi va qurilma holati bo‘yicha tekshiruvchi “nol ishonch” tamoyili [15] va ilovalarni OWASP talablari [16] bo‘yicha ishlab chiqish zarur.

5. Olti qatlamli kompleks himoya modeli. Tahlil natijalari asosida birorta yechim barcha tahdidlarga qarshi yetarli emasligini hisobga olib, har bir tahdid kamida ikki-uch mustaqil qatlam bilan to‘siladigan olti qatlamli model taklif etildi (1-jadval).

1-jadval. Mobil telefonlarni himoyalashning olti qatlamli modeli

Himoya qatlami	Asosiy zamonaviy yechimlar	To‘sadigan tahdidlar
1. Apparat va OT	Xotirani teglash (MIE/EMTE), xavfsizlik yangilanishlari, Lockdown Mode / Advanced Protection [21; 22]	“Nol klik” ekspluatlar, eskirgan OT
2. Ilova	OWASP talablari, Play Protect, ruxsatlarni cheklash, qo‘ng‘iroq paytida o‘rnatishni taqiqlash [16; 22]	Zararli APK, bank troyanlari
3. Autentifikatsiya	FIDO2/passkey, biometrik va ilova ichidagi kriptografik tasdiqlash [13]	Fishing, SMS-kodni ushlash, SIM-swap
4. Sun’iy intellekt	Qurilmadagi ML/LLM-modellar, federativ o‘qitish, smishing filtrlari [10-12]	Smishing, yangi zararli dasturlar
5. Tarmoq va operator	Anti-fishing platformasi, firibgar qo‘ng‘iroqlarni bloklash, kartalarni bloklash mexanizmi [6; 8]	Fishing havolalari, vishing
6. Tashkiliy-huquqiy va ta’lim	O‘RQ-764, PF-38, “nol ishonch”, MDM/MTD, kibergigiyena [7; 8; 14; 15]	Inson omili, ijtimoiy muhandislik

Model bo‘yicha zararli APK orqali mablag‘ o‘g‘irlash sxemasi beshta qatlamda to‘siladi: messenjer va tarmoq darajasida zararli fayl aniqlanadi, operatsion tizim qo‘ng‘iroq paytida o‘rnatishni taqiqlaydi, sun’iy intellekt shubhali xatti-harakatni aniqlaydi, passkey ishlatilganda ushlangan SMS-kod foyda bermaydi va kibergigiyena esa foydalanuvchining noma’lum faylni ochmasligini ta’minlaydi. Bunday yondashuvning amaliy samarasini firibgarlikka qarshi bank tizimlari 2026-yilning birinchi yarmida 462 mlrd so‘mlik noqonuniy o‘tkazmalarni to‘xtatgani [23] hamda APK-fayllardan himoyalovchi “Qo‘riqchi” ilovasidan qariyb 3 million fuqaro foydalanayotgani [5] ham tasdiqlaydi.

Tahlil asosida quyidagi tavsiyalar ishlab chiqildi: 1) banklar va to‘lov tizimlarida SMS-tasdiqlashdan FIDO2/passkey va ilova ichidagi kriptografik tasdiqlashga bosqichma-bosqich o‘tish; 2) mobil banking ilovalarida qo‘ng‘iroq yoki ekran namoyishi paytida ogohlantirish berish va SMS hamda Accessibility ruxsatiga ega shubhali ilovalarni tekshirish; 3) mahalliy APK namunalari asosida o‘qitilgan, maxfiylikni saqlovchi federativ aniqlash modellarini yaratish; 4) oliy ta’lim muassasalarida “mobil kibergigiyena” bo‘yicha amaliy mashg‘ulotlarni joriy etish; 5) aholiga

ilovalarni faqat rasmiy do‘konlardan o‘rnatish, tizimni o‘z vaqtida yangilash va bir martalik kodlarni hech kimga bermaslik qoidalarini keng targ‘ib qilish.

XULOSA. Mobil telefonlarga qaratilgan hujumlar va ulardan ko‘rilayotgan zarar ham global miqyosda, ham O‘zbekistonda o‘sishda davom etmoqda. 2026-yilda mamlakatdagi kiberjinoyatlarning yarmi zararli APK-fayllar orqali sodir etilmoqda. Tadqiqot shuni ko‘rsatdiki, xotirani teglash texnologiyalari murakkab ekspluatlarni qiyinlashtirmoqda, qo‘ng‘iroq paytidagi himoya mexanizmlari ijtimoiy muhandislik sxemalarini uzmoqda, sun’iy intellekt yangi tahdidlarni aniqlash imkonini bermoqda, FIDO2/passkey esa fishing va SMS-kodni ushlashga asoslangan hujumlarni samarasiz qilmoqda. Biroq birorta texnologiya mutlaq himoya bermaydi, shuning uchun taklif etilgan olti qatlamli model eng ishonchli yondashuv hisoblanadi. Ishlab chiqilgan tavsiyalar 2026-2030 yillarga mo‘ljallangan Kiberxavfsizlik strategiyasini amalga oshirishda foydalanilishi mumkin. Kelgusi tadqiqotlarda mahalliy zararli dastur namunalari asosida aniqlash modellarini eksperimental baholash maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI.

1. Kaspersky. The number of Trojan banker attacks on smartphones increased by 56% in 2025 [Elektron resurs]. – 2026-yil 4-mart. – URL: https://www.kaspersky.com/about/press-releases/the-number-of-trojan-banker-attacks-on-smartphones-increased-by-56-in-2025
2. Kivva A. IT threat evolution in Q2 2026. Mobile statistics [Elektron resurs] // Securelist (Kaspersky). – 2026-yil 10-avgust. – URL: https://securelist.com/malware-report-q2-2026-mobile-statistics/120948/
3. Kaspersky. NFC relay attacks on smartphones surged by 188% in 2026, Kaspersky reveals [Elektron resurs]. – 2026-yil 1-iyun. – URL: https://me-en.kaspersky.com/about/press-releases/nfc-relay-attacks-on-smartphones-surged-by-188-in-2026-kaspersky-reveals
4. Zimperium. New Zimperium Research Reveals that AI-based Attacks are Targeting and Succeeding on Mobile (2026 Global Mobile Threat Report) [Elektron resurs]. – 2026-yil 29-iyul. – URL: https://zimperium.com/resources/new-zimperium-research-reveals-that-ai-based-attacks-are-targeting-and-succeeding-on-mobile
5. Kiberjinoyatchilar pullarni qanday o‘zlashtiradi? IIV — firibgarlik usullari haqida [Elektron resurs] // Gazeta.uz. – 2026-yil 10-oktabr. – URL: https://www.gazeta.uz/oz/2026/10/10/kiberjinoyat/
6. IIV kiberjinoyatlar bo‘yicha fuqarolarga 209 mlrd so‘mdan ortiq zarar qoplanganini bildirdi [Elektron resurs] // Vzglyad.uz. – 2026-yil 13-oktabr. – URL: https://vzglyad.uz/uz/2026/10/13/iiv-kiberjinoyatlar-boyicha-fuqarolarga-209-mlrd-somdan-ortiq-zarar-qoplanganini-bildirdi
7. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni. – URL: https://lex.uz/docs/5960604
8. O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi “O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida”gi PF-38-son Farmoni. – URL: https://lex.uz/docs/8079286
9. Liu Y., Tantithamthavorn C., Li L., Liu Y. Deep Learning for Android Malware Defenses: A Systematic Literature Review // ACM Computing Surveys. – 2022. – Vol. 55, № 8. – Art. 153. https://doi.org/10.1145/3544968
10. Taşkın E., Doğru İ.A. From Hand-Crafted Features to Large Language Models: A Comparative Evaluation of Android Malware Detection Paradigms // Applied Sciences. – 2026. – Vol. 16, № 11. – Art. 5600. https://doi.org/10.3390/app16115600

11. Jiang C., Yin K., Xia C., Huang W. FedHGCDroid: An Adaptive Multi-Dimensional Federated Learning for Privacy-Preserving Android Malware Classification // Entropy. – 2022. – Vol. 24, № 7. – Art. 919. https://doi.org/10.3390/e24070919
12. Munoz M.L., Islam M.F. Deep Learning Approaches for Multi-Class Classification of Phishing Text Messages // Journal of Cybersecurity and Privacy. – 2025. – Vol. 5, № 4. – Art. 102. https://doi.org/10.3390/jcp5040102
13. Lassak L., Pan E., Ur B., Golla M. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication // Proceedings of the 33rd USENIX Security Symposium. – USENIX Association, 2024.
14. Howell G., Franklin J.M., Sritapan V., Souppaya M., Scarfone K. Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST SP 800-124 Rev. 2). – NIST, 2023. https://doi.org/10.6028/NIST.SP.800-124r2
15. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture (NIST SP 800-207). – NIST, 2020. https://doi.org/10.6028/NIST.SP.800-207
16. OWASP Foundation. OWASP Mobile Top 10 (2024) [Elektron resurs]. – URL: https://owasp.org/www-project-mobile-top-10/
17. Marczak B., Scott-Railton J., Abdul Razzak B., Aljizawi N., Anstis S., Berdan K., Deibert R. FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild [Elektron resurs] // The Citizen Lab. – 2021-yil 13-sentabr. – URL: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
18. Shakirova N.A., Obidov O.V. Kiberxavfsizlik 2025-yilda: O‘zbekistonda onlayn firibgarliklardan qanday himoyalanish mumkin // Global Science Review. – 2025. – Vol. 9, № 1. – B. 205-214.
19. Gupta D., Abdullaeva I., Abdullayev A.F.U. va boshq. AI-Based Mobile Devices/Smart Gadgets in Library and Information Sciences // AI Applications, Tools, and Algorithms for Advancing Library Sciences / Eds. S. Umair, K. Butt. – Hershey: IGI Global Scientific Publishing, 2027. – P. 283-320. https://doi.org/10.4018/979-8-3373-7262-4.ch010
20. Khayrullayev I., Swetha G., Shruthishree S.H., Raghu N., Abdullayev A.F.U. va boshq. Revolutionizing Vehicle Safety Through AI-Driven V2X and Digital Twin Technologies // Revolutionizing Transportation Safety With AI / Eds. Q. Ali, M.A. Mahmood, M.T.I. Khan. – Hershey: IGI Global Scientific Publishing, 2027. – P. 197-228. https://doi.org/10.4018/979-8-3373-3231-4.ch007
21. Apple Security Engineering and Architecture. Memory Integrity Enforcement: A complete vision for memory safety in Apple devices [Elektron resurs] // Apple Security Research. – 2025-yil 9-sentabr. – URL: https://security.apple.com/blog/memory-integrity-enforcement/
22. Lakshmanan R. Google Rolls Out On-Device AI Protections to Detect Scams in Chrome and Android [Elektron resurs] // The Hacker News. – 2025-yil 9-may. – URL: https://thehackernews.com/2025/05/google-rolls-out-on-device-ai.html
23. Mansabdorlar uchun javobgarlik, maktablarda kibergigiyena darslari, milliy SOC markazlari. O‘zbekiston kiberxavfsizlik sohasida o‘z oldiga qanday vazifalar qo‘ymoqda? [Elektron resurs] // Gazeta.uz. – 2026-yil 30-sentabr. – URL: https://www.gazeta.uz/oz/2026/09/30/cybersecurity/