

AQLLI KIBERHIMOYA: MOBIL EKOTIZIMLARDA OFLAYN AI MODELLARINING SAMARADORLIGI

¹Primbetov Abbaz, ²Xamidov Xusniddin, ³Mamedov Kamron, ⁴Xakimov Muhammadillo

¹*Toshkent amaliy fanlar universiteti Komputar injeneringi katta o'qituvchisi*

^{2,3,4}*Toshkent Amaliy fanlar universiteti Axborot xavfsizligi talabalari*

abbaz0203@mail.ru, husniddinhamidov@hotmail.com, mamedovkamron2002@gmail.com,
dilloxabib@gmail.com

Annotatsiya

Ushbu ilmiy maqolada zamonaviy kiber-tahdidlarga qarshi kurashishda sun'iy intellekt (AI) texnologiyalarini integratsiya qilishning dolzarb masalalari tadqiq etiladi. Tadqiqot obyekti sifatida "Cyber Brother" mobil xavfsizlik majmuasi tanlab olingan bo'lib, unda oflayn rejimda ishlovchi mashinali o'rganish modellarining samaradorligi tahlil qilingan. Maqolada mobil qurilmalarni zararli dasturlardan (malware) himoya qilishning yangi metodologiyasi, real vaqt rejimidagi monitoring tizimlari va fishing hujumlariga qarshi "Red Alert" protokoli tavsiflangan. Olingan natijalar AI asosidagi avtonom tizimlarning an'anaviy metodlarga qaraganda yangi turdagi (zero-day) hujumlarni aniqlashda yuqori samaradorlikka ega ekanligini ko'rsatadi.

Kalit so'zlar: Sun'iy intellekt, kiberxavfsizlik, Android, Cyber Brother, Malware tahlili, oflayn AI raqamli transformatsiya, kiber-hujum, Red Alert, Intent-Interception.

Kirish

Raqamli transformatsiya davrida mobil qurilmalar global axborot almashinuvining asosiy tuguniga aylandi. Bugungi kunda smartfonlar nafaqat aloqa vositasi, balki bank xizmatlari, shaxsiy ma'lumotlar, biznes operatsiyalari va hatto davlat xizmatlariga kirish uchun asosiy platforma sifatida foydalanilmoqda. Ushbu jarayon mobil qurilmalarni kiberjinoyatchilar uchun eng jozibador nishonga aylantirmoqda. So'nggi yillarda kiber-tahdidlarning murakkabligi sezilarli darajada oshdi. Ayniqsa, generativ sun'iy intellekt texnologiyalarining rivojlanishi bilan zararli dasturlar yaratish jarayoni sezilarli darajada tezlashdi va avtomatlashtirildi. Natijada, har kuni minglab yangi zararli dasturlar (malware) paydo bo'lmoqda. Ushbu zararli dasturlarning aksariyati polimorfik va metamorfik xususiyatlarga ega bo'lib, ular o'z kodini doimiy ravishda o'zgartiradi va an'anaviy imzo asosidagi antivirus tizimlarini chetlab o'tishga muvaffaq bo'ladi. Bundan tashqari, zamonaviy hujumlar faqat zararli dasturlar bilan cheklanib qolmayapti. Phishing hujumlari, ijtimoiy muhandislik (social engineering), nol kunlik zaifliklar (zero-day vulnerabilities), zararli tarmoq trafiklari va AI yordamida yaratilgan firibgarlik sxemalari ham tez sur'atlarda ko'paymoqda. Bu esa an'anaviy xavfsizlik tizimlarining samaradorligini pasaytirmoqda va yangi, aqlli himoya mexanizmlarini talab qilmoqda.

Shu sababli, kiberxavfsizlik tizimlariga sun'iy intellektni integratsiya qilish muhim strategik yo'nalishga aylandi. Ayniqsa, qurilmaning o'zida ishlovchi (On-device AI) modellar xavfsizlikni yangi bosqichga olib chiqmoqda. Bunday modellar real vaqt rejimida tahdidlarni aniqlash, foydalanuvchi xatti-harakatlarini tahlil qilish va potensial hujumlarni oldindan bashorat qilish imkonini beradi. Bundan tashqari, on-device AI texnologiyasi foydalanuvchi ma'lumotlarini tashqi serverlarga yubormasdan, mahalliy darajada qayta ishlash imkonini beradi, bu esa maxfiylik va ma'lumotlar xavfsizligini yanada oshiradi.

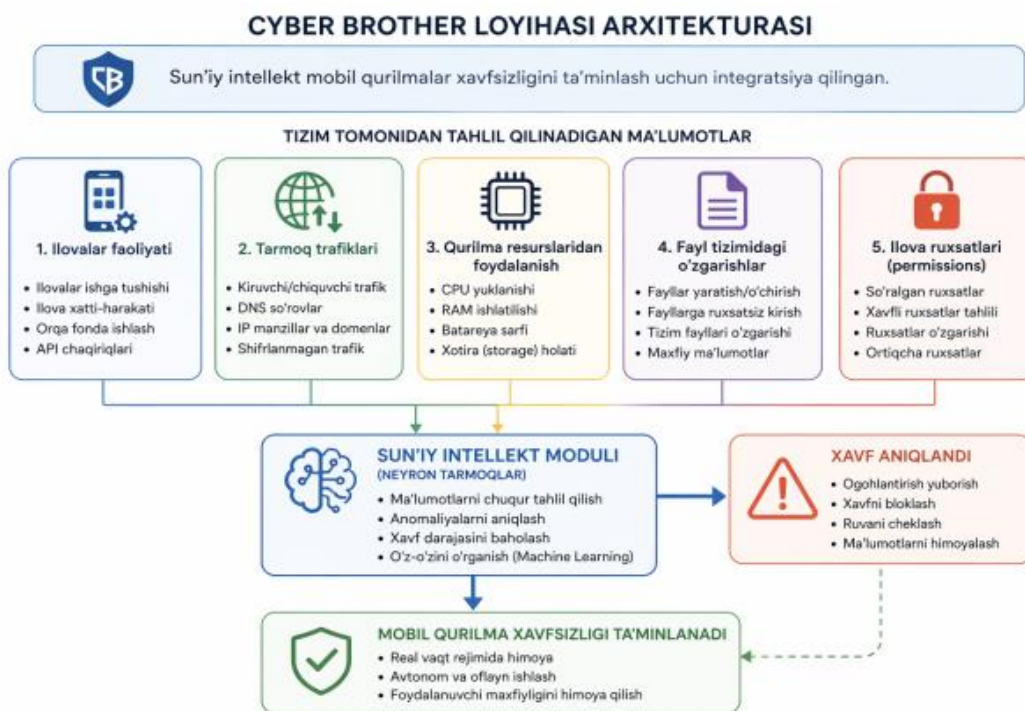
"Cyber Brother" loyihasi aynan shu konsepsiyaga asoslangan bo'lib, sun'iy intellekt yordamida mobil qurilmalarni kompleks himoya qilishni maqsad qiladi. Ushbu loyiha zamonaviy tahdidlarga

moslashuvchan, real vaqt rejimida ishlovchi va foydalanuvchining maxfiyligini saqlovchi innovatsion kiberxavfsizlik platformasini yaratishga qaratilgan.

Mazkur maqola "Cyber Brother" loyihasining texnik arxitekturasini, sun'iy intellekt modellarining ishlash tamoyillari hamda ularning kiberxavfsizlik tizimlarida qo'llanilish imkoniyatlarini ilmiy va amaliy jihatdan tahlil qilishga bag'ishlanadi. Shuningdek, maqolada ushbu integratsiyaning afzalliklari, cheklavlari va kelajakdagi rivojlanish istiqbollari ham ko'rib chiqiladi.

Kiberxavfsizlikda Sun'iy Intellektning O'rni

Sun'iy intellekt (AI) kiberxavfsizlik sohasida tahdidlarni aniqlash, tahlil qilish va ularga tezkor javob berishda muhim rol o'ynamoqda. An'anaviy xavfsizlik tizimlari asosan imzo (signature-based) va qoidalarga (rule-based) asoslanadi. Biroq, zamonaviy kiberhujumlar tez o'zgaruvchan bo'lgani sababli bunday yondashuvlar har doim ham samarali emas. Ayniqsa, polimorfik zararli dasturlar, zero-day zaifliklar va ijtimoiy muhandislik hujumlari an'anaviy himoya mexanizmlarini chetlab o'tishi mumkin. Sun'iy intellekt esa katta hajmdagi ma'lumotlarni real vaqt rejimida tahlil qilib, g'ayritabiiy faoliyatni aniqlash imkonini beradi. Machine Learning va Deep Learning modellar foydalanuvchi xatti-harakatlarini, ilovalar faoliyatini va tarmoq trafiklarini o'rganadi. Natijada, tizim ilgari noma'lum bo'lgan tahdidlarni ham aniqlash imkoniyatiga ega bo'ladi.



1-rasm Loyiha arxitekturasini

Cyber Brother loyihasining asosini tashkil etuvchi sun'iy intellekt modeli foydalanuvchi va ilovalarning odatiy xatti-harakatlarini muntazam o'rganish orqali g'ayritabiiy faoliyatlarni real vaqt rejimida aniqlashga ixtisoslashgan. Tizimning o'ziga xosligi shundaki, u nafaqat ma'lum viruslar bazasiga tayanadi, balki xulq-atvoriga asoslangan tahlil (Behavioral Analysis) metodologiyasidan foydalanadi. Masalan, oddiy ilova kutilmaganda fon rejimida shubhali ma'lumotlarni uzatishni boshlasa yoki o'z vazifasiga zid bo'lgan maxfiy ruxsatlarni talab qilsa, sun'iy intellekt buni potensial xavf sifatida baholaydi. Ushbu yondashuv hali dunyo miqyosida ro'yxatga olinmagan yangi turdagi "zero-day" hujumlarini samarali aniqlash imkonini beradi.

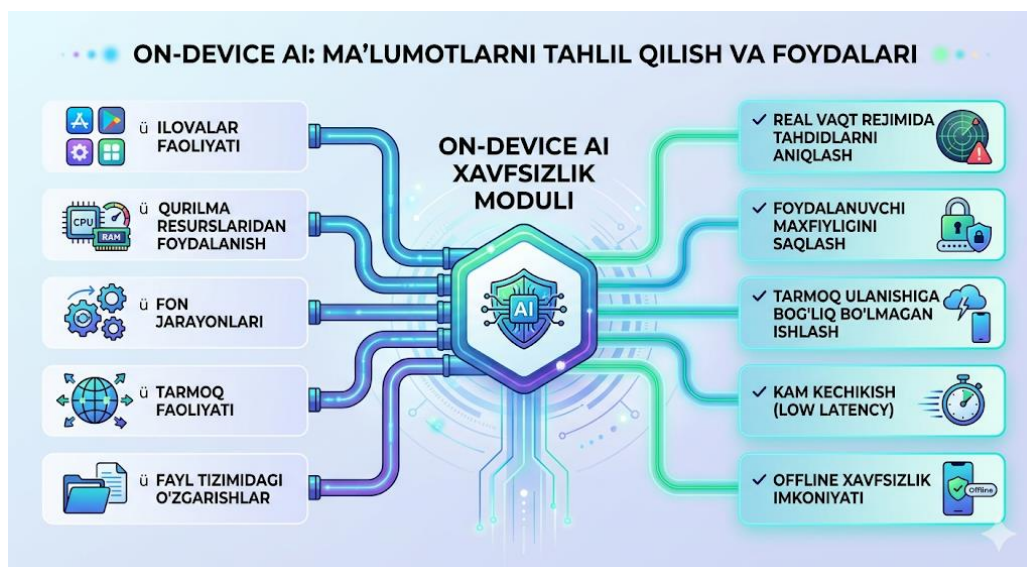
Loyihaning eng muhim texnologik afzalligi — sun'iy intellekt modelining bevosita qurilmaning o'zida (On-device AI) ishlashidir. Bu usul foydalanuvchi ma'lumotlarini qurilma ichida saqlash orqali maksimal maxfiylikni ta'minlaydi va tashqi serverlarga bog'liqlikni bartaraf etadi. Natijada, tizim internetga ulanmagan holatda ham avtonom himoyani davom ettiradi va tahdidlarga soniyaning son ulushlarida, ya'ni tezkor javob qaytaradi.

Xavf aniqlangan lahzada Cyber Brother avtomatik himoya choralari ishga tushiradi. Bu jarayonda shubhali ilova faoliyati cheklanadi, zararli trafik oqimi bloklanadi va tizim xavfsizligiga rahna solayotgan jarayonlar darhol to'xtatiladi. Shu bilan bir qatorda, amalga oshirilgan barcha himoya choralari va aniqlangan xavf darajasi haqida foydalanuvchiga batafsil ogohlantirish yuboriladi, bu esa qurilma egasiga o'z raqamli xavfsizligini to'liq nazorat qilish imkonini beradi. Bundan tashqari, Cyber Brother tizimi kelajakda federated learning texnologiyasini qo'llash orqali global tahdidlarni aniqlash imkoniyatini ham kengaytiradi. Bu esa turli qurilmalardan olingan anonim ma'lumotlar asosida AI modelni yanada takomillashtirish imkonini beradi. Natijada, sun'iy intellekt kiberxavfsizlik tizimlarini yanada aqlli, moslashuvchan va samarali qiladi. Cyber Brother loyihasida AI integratsiyasi mobil qurilmalar uchun real vaqt rejimidagi, maxfiylikni ta'minlovchi va zamonaviy tahdidlarga qarshi samarali himoya tizimini yaratishga xizmat qiladi. Sun'iy intellekt kiberxavfsizlikda uchta asosiy yo'nalishda inqilobiy o'zgarishlar yasamoqda:

1. **Prediktiv tahlil:** Ma'lum bir naqshlar asosida hujum sodir bo'lishidan oldin uni bashorat qilish.
2. **Anomaliyalarni aniqlash:** Foydalanuvchi yoki tizim xatti-harakatidagi shubhali chetlanishlarni real vaqtda qayd etish.
3. **Avtonom qaror qabul qilish:** Inson omilisiz kiber-hujumni bloklash va tizimni tiklash.

“Cyber Brother” Tizimining Arxitekturasi va Innovatsiyalari

"Cyber Brother" — bu Android ekotizimi uchun mo'ljallangan kompleks xavfsizlik yechimidir. Uning o'ziga xosligi bulutli hisoblashlarga tayanmasdan, qurilma resurslari doirasida yuqori aniqlikdagi tahlilni amalga oshirishidadir. "Cyber Brother" tizimi zamonaviy kiberxavfsizlik talablariga mos ravishda modulli va kengaytiriladigan arxitektura asosida ishlab chiqilgan. Tizim sun'iy intellekt texnologiyalarini mobil qurilma darajasida integratsiya qilish orqali real vaqt rejimida tahdidlarni aniqlash va ularni oldini olishga qaratilgan. Ushbu arxitektura bir nechta mustaqil, ammo o'zaro integratsiyalashgan modullardan tashkil topgan bo'lib, ular birgalikda kompleks va ko'p qatlamli himoya mexanizmini ta'minlaydi.

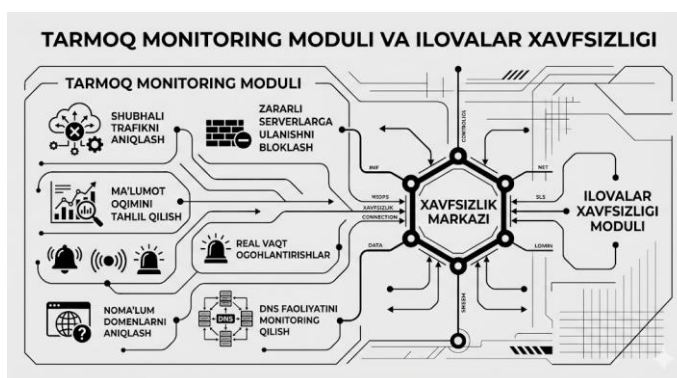


2-rasm. On device moduli tahlili

On-device AI moduli Cyber Brother arxitekturasining asosiy komponentlaridan biri On-device AI modulidir. Ushbu modul sun'iy intellekt modellarini bevosita foydalanuvchi qurilmasida ishga tushirish imkonini beradi. On-device AI yondashuvi ma'lumotlarni tashqi serverlarga uzatmasdan, mahalliy darajada tahlil qilishni ta'minlaydi. Bu esa tizimning samaradorligini oshirish bilan birga foydalanuvchi maxfiylikni ham ta'minlaydi. On-device AI modeli foydalanuvchining odatiy xatti-harakatlarini o'rganadi va g'ayritabiiy faoliyatni aniqlaydi. Bu yondashuv noma'lum tahdidlarni aniqlash hamda zero-day hujumlarni aniqlashda samarali hisoblanadi.

Tarmoq monitoring moduli. Cyber Brother tizimi tarmoq trafiklarini real vaqt rejimida tahlil qiladi. Ushbu modul shubhali ulanishlar, noma'lum domenlar, zararli IP manzillar hamda ma'lumot uzatishdagi g'ayritabiiy faoliyatni aniqlashga qaratilgan. Sun'iy intellekt modeli tarmoq trafiklaridagi anomal xatti-harakatlarni aniqlaydi va zarur hollarda ulanishlarni avtomatik ravishda cheklaydi.

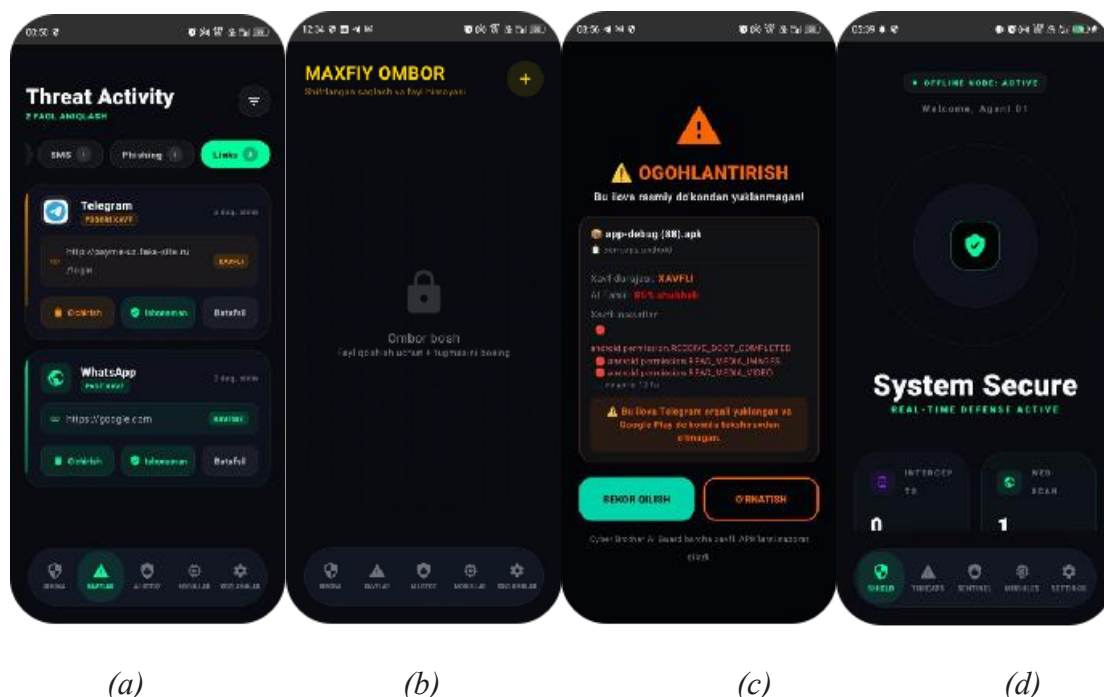
3-rasm. Tarmoq monitoring modullari xavfsizligi



Cyber Brother tizimining tarkibiy qismi bo'lgan ilovalar xavfsizligi moduli mobil qurilmaga o'rnatilgan barcha dasturlarning faoliyatini uzluksiz nazorat qilishga xizmat qiladi. Ushbu modul ilovalarning ruxsatnomalari, ularning fon rejimidagi harakatlari va tashqi tarmoqlar bilan ma'lumot almashish jarayonlarini chuqur tahlil qiladi.

Tahlil jarayonida tizim bir nechta muhim parametrlarni, jumladan, ilovaga berilgan ruxsatlar mosligini, fon jarayonlarining faolligini, ma'lumot uzatish hajmi va chastotasini, shuningdek, qurilma resurslaridan foydalanish darajasini doimiy ravishda kuzatib boradi. Bunday

kompleks yondashuv nafaqat ma'lum bo'lgan zararli dasturlarni, balki yashirin faoliyat yurituvchi josuslik dasturlarini va foydalanuvchi ruxsatisiz amalga oshiriladigan ma'lumotlar uzatilishini o'z vaqtida aniqlash hamda ularni bartaraf etish imkonini beradi.



4-rasm. Ilova bilan tanishuv

a-rasmda Cyber Brother tizimining asosiy boshqaruv interfeysi va real vaqt rejimidagi himoya holati tasvirlangan.

b-rasmda sun'iy intellekt asosida aniqlangan tahdidlar va ilovalar faoliyatining monitoringi ko'rsatilgan.

c-rasmda foydalanuvchi ma'lumotlarini himoyalash uchun mo'ljallangan xavfsiz ombor (Secure Storage) moduli aks ettirilgan.

d-rasmda esa shubhali ilovalar aniqlanganda foydalanuvchini ogohlantirish tizimi namoyish etilgan. Ushbu interfeyslar Cyber Brother tizimining real vaqt rejimidagi monitoring va avtomatlashtirilgan himoya imkoniyatlarini ko'rsatadi.

Cyber Brother ilovasini hozirda ommaga ishlatish uchun chiqarganmiz hamda bizda bir nechta fikr mulohazalar kelib tushgan ulardan asosiysi "Ilovani o'rnatish jarayoni biroz qiyin ekan shuni ossonroq qilsa bolmaydimi?" Bizning jamoa bu savolga yechim topish uchun juda uzoq ishladi va qo'ldan kelgancha harakat qildi, ammo yangilanayotgan Android qurilmalarida bunday antivirus ilovalar uchun cheklovlar yetarlicha. Shuning uchun biz yo'riqnoma tayyorladik hamda uni taqdim etdik, va hozircha barchasi yaxshi ketmoqda kelasi update (Yangilanish)larda biz ko'proq UI va UX o'zgarishlarini amalga oshiramiz.

Xulosa

O'tkazilgan tadqiqot natijalari shuni ko'rsatadiki, zamonaviy kiberxavfsizlik muhitida sun'iy intellekt texnologiyalarining integratsiyasi nafaqat yordamchi vosita, balki strategik ahamiyatga ega asosiy komponent hisoblanadi. Raqamli tizimlarda tahdidlar soni va murakkabligi ortib borayotgan sharoitda an'anaviy himoya mexanizmlari yetarli darajada samarali bo'lmay qolmoqda. Shu nuqtayi nazardan, "Cyber Brother" loyihasi doirasida ishlab chiqilgan AI asosidagi yondashuvlar yangi avlod kiberhimoya tizimlarining amaliy modelini namoyon etadi. Tadqiqot

davomida aniqlanishicha, oflayn rejimda ishlovchi neyron tarmoqlar mobil ekotizimlarda mustaqil qaror qabul qilish imkonini berib, internetga bog‘liqlikni kamaytiradi hamda “zero-day” kabi noma’lum tahdidlarga qarshi tezkor javob berish samaradorligini oshiradi. Bu esa real vaqt rejimida ishlovchi adaptiv xavfsizlik tizimlarining dolzarbligini yanada kuchaytiradi.

Bundan tashqari, tizimning keng foydalanuvchi auditoriyasi uchun moslashtirilishi uning ijtimoiy ahamiyatini oshiradi, ya’ni raqamli savodxonlik darajasidan qat’i nazar, har bir foydalanuvchi uchun minimal xavfsizlik standartlarini ta’minlash imkonini beradi. Bu holat kiberxavfsizlikni faqat texnik emas, balki ijtimoiy infratuzilma elementi sifatida ham ko‘rib chiqish zarurligini ko‘rsatadi. Kelajak istiqbollari sifatida generativ sun’iy intellekt va o‘z-o‘zini o‘rganuvchi (self-learning) algoritmlarni rivojlantirish orqali kiberhujumlarni oldindan modellashtirish va ularni prognoz qilish imkoniyati paydo bo‘ladi. Natijada, kiberxavfsizlik tizimlari reaktiv yondashuvdan proaktiv va prediktiv himoya modeliga o‘tadi.

Umuman olganda, “Cyber Brother” kabi AI asosidagi tizimlar raqamli muhitda xavfsizlikni ta’minlashning yangi paradigmasini shakllantiradi hamda kelajakda milliy va global kiberxavfsizlik infratuzilmasining muhim tarkibiy qismiga aylanishi mumkin.

Foydalanilgan adabiyotlar ro‘yxati

1. Generativ sun’iy intellekt sharoitida ta’lim tizimlari va kiberxavfsizlikni transformatsiya qilish: Xalqaro konferensiya materiallari, Toshkent, 2026.
2. OWASP Foundation. *OWASP Top 10 Mobile Risks*, 2023 Update.
3. Android Developers. *Security Best Practices & App Manifest Protection*, Google Documentation, 2025. <https://developer.android.com>
4. IEEE Access. *Artificial Intelligence Techniques in Cybersecurity: A Comprehensive Survey*, 2023–2024 (survey articles collection).
5. Zhang, Y., et al. “Machine Learning-Based Intrusion Detection Systems: A Survey.” *ACM Computing Surveys*, 2023.
6. Brown, T. et al. “Language Models are Few-Shot Learners.” *NeurIPS Proceedings*, 2020.
7. Cyber Brother loyihasi texnik spesifikasiyalari va dasturiy kod tahlili hisoboti (2025–2026), ichki ilmiy-texnik hujjat.
8. Stallings, W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2022.