KONFERENSIYALAR UZ
ANJUMANLAR PLATFORMASI

O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

II RESPUBLIKA ILMIY-AMALIY KONFERENSIYA MATERIALLARI

IYUN, 2025-YIL

O‘ZBEKISTON 2030

KONFERENSIYALAR UZ
ANJUMANLAR PLATFORMASI

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

II RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, iyun

TOSHKENT-2025

ISBN 978-9910-09-204-6

O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI. II Respublika ilmiy-amaliy konferensiyasi materiallari. – Toshkent: Scienceproblems team, 2025. – 138 bet.

Elektron nashr: https://konferensiyalar.uz/uzbekistan-2030

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2025-yil, 23-iyun

Mas’ul muharrir:
Isanova Feruza Tulqinovna

Annotatsiya
Mazkur nashrda “O‘zbekiston — 2030: innovatsiya, fan va ta’lim istiqbollari” nomli II Respublika ilmiy-amaliy konferensiyasi doirasida taqdim etilgan ilmiy maqolalar to‘plami jamlangan. Unda O‘zbekistonning turli oliy ta’lim va ilmiy-tadqiqot muassasalari, tarmoq tashkilotlari, mustaqil tadqiqotchilar tomonidan taqdim etilgan ijtimoiy-gumanitar, iqtisodiyot, huquq, biologiya, tibbiyot va boshqa sohalarga oid maqolalar kiritilgan. Maqolalarda ilm-fanning zamonaviy yo‘nalishlari, innovatsion texnologiyalar, ta’lim islohotlari hamda barqaror taraqqiyotga oid masalalar muhokama qilingan. To‘plam akademik izlanishlar, amaliy tajribalar va ilmiy xulosalarni birlashtirgan holda, fanlararo integratsiyani chuqurlashtirish va ilmiy hamkorlikni kuchaytirishga xizmat qiladi.

Kalit so‘zlar: ilmiy-amaliy konferensiya, innovatsiya, fan va ta’lim, O‘zbekiston 2030, barqaror rivojlanish, ilmiy izlanishlar, fanlararo integratsiya, ilmiy hamkorlik, texnologik taraqqiyot, zamonaviy ta’lim.

ISBN 978-9910-09-204-6

MUNDARIJA

GEOGRAFIYA FANLARI

YURIDIK FANLAR

PEDAGOGIKA FANLARI

TEXNIKA FANLARI

5G TEXNOLOGIYASIDAGI XAVFSIZLIK MUAMMOLARINING TAHLILI

Mirabdullayev Fayzullo Zafarjon o‘g‘li
Muahammad al-Xorazmiy nomidagi TATU talabasi

Tursunov Otabek Odiljon o‘g‘li
Muahammad al-Xorazmiy nomidagi TATU,
Kriptologiya kafedrasi katta o‘qituvchisi

Annotatsiya. Ushbu ishda 5G arxitekturasi va uning asosiy komponentlari, 5G texnologiyasidagi mavjud xavfsizlik muammolari tahlil qilinib, xavfsizlikni ta’minlashdagi zamonaviy yondashuvlar o‘rganilgan va yangi strategiyalar taklif qilingan.

Kalit so‘zlar: Axborot himoyasi, 5G texnologiyasi, sizsiz tarmoq, xavfsizlik muammolari, 5G xavfsizlik yechimlari.

ANALYSIS OF SECURITY ISSUES IN 5G TECHNOLOGY

Mirabdullayev Fayzullo Zafarjon ogli
Student of Muhammad al-Khwarizmi Tashkent
University of Information Technologies

Tursunov Otabek Odiljon ogli
Senior Lecturer, Department of Cryptology, Muhammad
al-Khwarizmi Tashkent University of Information Technologies

Abstract. This work analyzes the 5G architecture and its main components, existing security problems in 5G technology, studies modern approaches to ensuring security, and proposes new strategies.

Key words: Information protection, 5G technology, wireless network, security problems, 5G security solutions.

DOI: https://doi.org/10.47390/978-9910-09-204-6/uzb-02

Kirish

Yangi avlod tarmoq arxitekturasiga ega bo‘lgan 5G texnologiyasi ham iste’molchi, ham sanoat sohalarida minglab yangi ilovalarni qo‘llab-quvvatlash imkoniyatiga ega. 5G tezligi va o‘tkazuvchanlik qobiliyati hozirgi tarmoqlardan bir necha barobar yuqori bo‘lganligi sababli, uning imkoniyatlari deyarli cheksiz tuyuladi.

Telekommunikatsiya sohasida 5G to‘rtinchi avlod (4G) ning vorisi sifatida uyali tarmoq texnologiyasining “beshinchi avlodi” bo‘lib, 2019-yildan beri butun dunyo bo‘ylab uyali aloqa operatorlari tomonidan qo‘llanilmoqda. Ushbu maqolada 5G texnologiyasi yutuqlari, xavfsizlik muammolari va ularga yechimlar muhokama qilinadi.

Muhokama

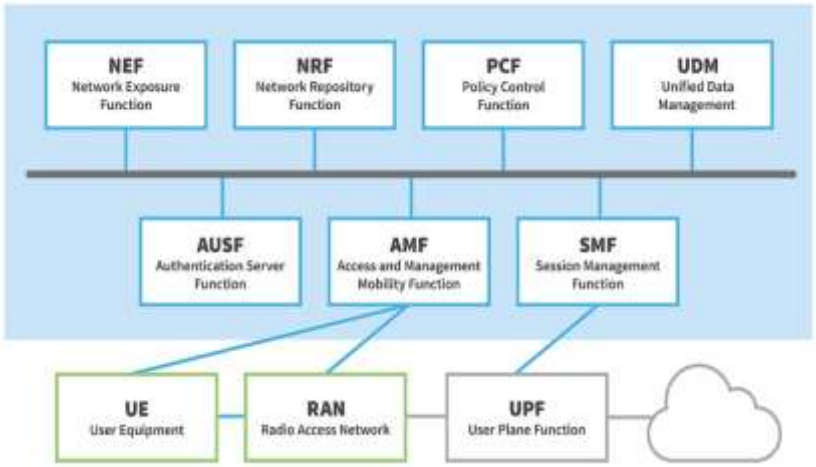
5G tarmoqlarining kengaytirilgan funksionalligini ta’minlaydigan 5G yadro tarmog‘i 5G tizimining uchta asosiy tarkibiy qismlaridan biri bo‘lib, 5GC(5G Core) nomi bilan ham tanilgan. Qolgan ikkita komponent - 5G Access tarmog‘i (5G-AN) va foydalanuvchi uskunalari (UE). 5G

yadrosi autentifikatsiya, xavfsizlik, seanslarni boshqarish va ulangan qurilmalardan trafikni jamlashni qo‘llab-quvvatlash uchun bulutga moslashtirilgan xizmatga asoslangan arxitekturadan (SBA) foydalanadi, bularning barchasi 5G yadrosi diagrammasida ko‘rsatilganidek, tarmoq funksiyalarining murakkab o‘zaro bog‘lanishini talab qiladi[1, 2-5b].

5G yadro arxitekturasining tarkibiy qismlariga quyidagilar kiradi:

- foydalanuvchi tekisligi funksiyasi (UPF);
- ma’lumotlar tarmog‘i (DN), masalan, operator xizmatlari, Internetga ulanish yoki tashqi xizmatlar;
- asosiy kirish va mobillikni boshqarish funksiyasi (AMF);
- authentication Server Function (AUSF);
- seans boshqaruvi funksiyasi (SMF);
- tarmoq bo‘laklarini tanlash funksiyasi (NSSF);
- tarmoq ta’sir funksiyasi (NEF);
- NF saqlash funksiyasi (NRF);
- siyosatni boshqarish funksiyasi (PCF);
- yagona ma’lumotlar boshqaruvi (UDM);
- amaliy funksiya (AF).

5G noldan boshlab ishlab chiqilgan va tarmoq funksiyalari xizmatlarga bo‘lingan. Shuning uchun bu arxitektura 5G core Service-Based Architecture (SBA) deb ham ataladi. Quyidagi (1.3-rasm) 5G tarmoq topologiyasi diagrammasida 5G asosiy tarmog‘ining asosiy tarkibiy qismlari ko‘rsatilgan:



1-rasm. 5G topologiyasi diagrammasi

Ushbu topologiya quyidagi prinsiplarda ishlaydi:

- 5G smartfonlari yoki 5G uyali qurilmalari kabi foydalanuvchi uskunalari (UE) 5G yangi radio kirish tarmog‘i orqali 5G yadrosiga va undan keyin Internet kabi ma’lumotlar tarmoqlariga (DN) ulanadi;
- foydalanish va harakatchanlikni boshqarish funksiyasi (AMF) UE ulanishi uchun bitta kirish nuqtasi vazifasini bajaradi;
- UE tomonidan so‘ralgan xizmat asosida AMF foydalanuvchi sessiyasini boshqarish uchun tegishli sessiyalarni boshqarish funksiyasini (SMF) tanlaydi;
- foydalanuvchi tekisligi funksiyasi (UPF) IP ma’lumotlar trafigini (foydalanuvchi tekisligi) foydalanuvchi uskunasi (UE) va tashqi tarmoqlar o‘rtasida uzatadi;

- autentifikatsiya serveri funksiyasi (AUSF) AMF ga 5G yadrosining UE va kirish xizmatlarini autentifikatsiya qilish imkonini beradi;
- Session Management Function (SMF), Policy Control Function (PCF), Application Function (AF) va Unified Data Management (UDM) kabi boshqa funksiyalar tarmoq xatti-harakatlarini boshqarish uchun siyosat qarorlarini qo‘llash va obuna ma’lumotlariga kirish orqali siyosatni boshqarish tizimini ta’minlaydi.

5G texnologiyasining xavfsizlikka ta’sir etuvchi xususiyatlari. 5G texnologiyasi o‘zining noyob xususiyatlari bilan oldingi avlod tarmoqlaridan tubdan farq qiladi. U foydalanuvchilarga yuqori tezlik, past kechikish va juda katta ulanish imkoniyatlarini taqdim etadi. Shu bilan birga, ushbu texnologiyaning xavfsizlik jihatlari ham o‘zgacha ko‘rinish oladi. Birinchidan, 5G’da juda ko‘p qurilmalar tarmoqqa ulangan bo‘ladi, bu esa hujumchilarga potensial hujum nuqtalarini ko‘paytiradi. Ikkinchidan, 5G arxitekturasi markazlashmagan (decentralized) shaklda ishlab chiqilgan, ya’ni ko‘plab xizmatlar markaziy serverlardan emas, balki edge computing (chekka hisoblash) orqali ishlaydi. Bu esa xavfsizlik monitoringi va nazoratini qiyinlashtiradi.

Shuningdek, 5G’da software-defined networking (SDN) va network function virtualization (NFV) kabi yangi texnologiyalar joriy etilgan. Ular tarmoqqa moslashuvchanlik va samaradorlik kiritadi, biroq shu bilan birga yangi xavfsizlik xatarlarini ham olib keladi. Masalan, SDN’da boshqaruv tekshiruvi markaziy bo‘lgani uchun, ushbu markaziy nuqta hujumga uchrasa, butun tarmoq izdan chiqishi mumkin. Bundan tashqari, 5G’da virtual tarmoq bo‘laklari (slicing) joriy etilganligi sababli, har bir slice o‘z xavfsizlik siyosatiga ega bo‘lishi zarur. Agar bir slice’da muammo yuzaga kelsa, bu boshqa slice’larni ham xavf ostiga qo‘yishi mumkin.

Yana bir muhim jihat — 5G’da foydalanuvchi identifikatsiyasi va autentifikatsiyasi jarayonlari murakkablashgan. Masalan, 5G tarmog‘ida IMSI (International Mobile Subscriber Identity) maxfiyligi yaxshilangan, ammo hali ham signalizatsiya kanalida qoldirilgan ayrim zaifliklar mavjud. Shu sababli, 5G texnologiyasi xavfsizlikni oshirishda oldingi avlod tarmoqlaridan farqli yondashuvlarni talab qiladi.

5G texnologiyasining xavfsizlikka ta’sir etuvchi xususiyatlari haqida so‘z borar ekan, tarmoqni maqsadli ravishda optimallashtirish va kengaytirish uchun amalga oshirilgan o‘zgarishlar alohida e’tiborga loyiqdir. 5G arxitekturasi o‘zining markazlashtirilgan va virtualizatsiyalangan yondashuvlari orqali yuqori moslashuvchanlik va samaradorlikni taqdim etadi, biroq bu, o‘z navbatida, yangi xavfsizlik xatarlariga olib keladi.

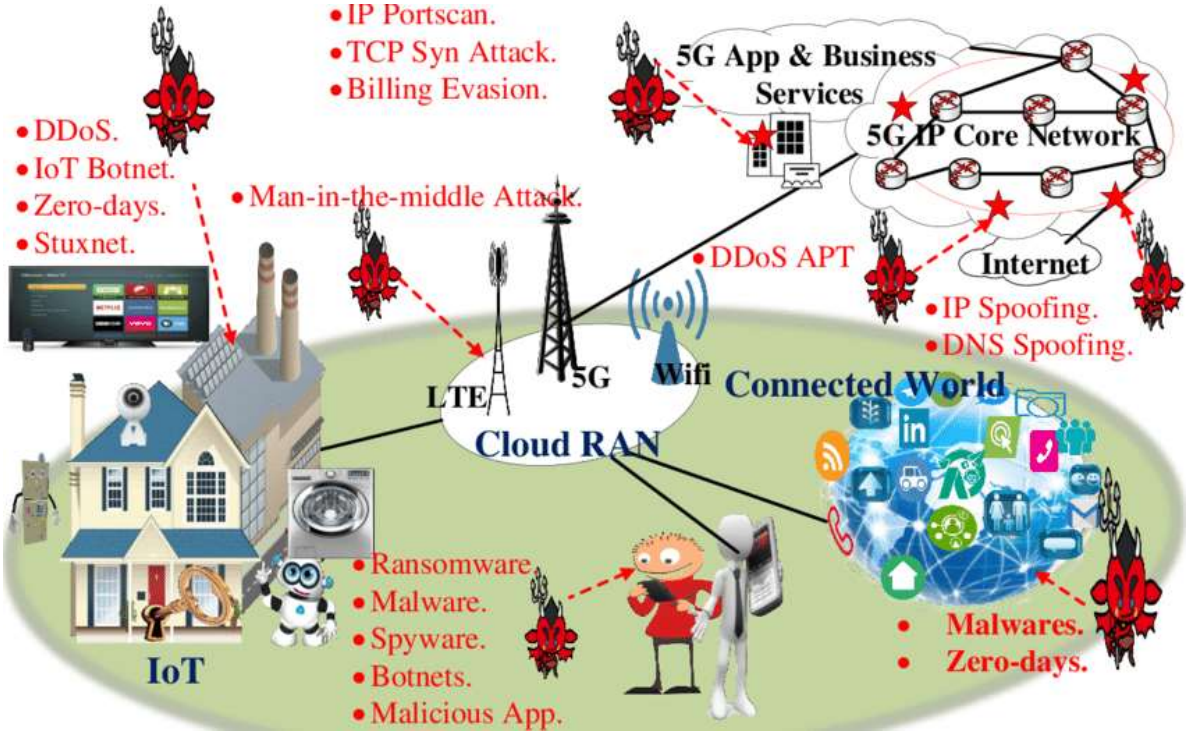
Virtualizatsiya va bulut texnologiyalari joriy etilishi tarmoq boshqaruvini markazlashtirishga imkon beradi, lekin bu markazlashgan tizimlarga hujum qilish imkoniyatini oshiradi. Agar markaziy server yoki boshqaruv platformasi xavf ostida bo‘lsa, butun tarmoqni boshqarish va xizmat ko‘rsatishni ta’minlashga salbiy ta’sir ko‘rsatishi mumkin. Virtualizatsiya orqali tarmoqning bo‘laklarga bo‘linishi esa boshqa bir muammolarni keltirib chiqaradi. Har bir bo‘lakning izolyatsiyasi, ya’ni ularning bir-biridan ajratilishi, zaif bo‘lishi mumkin. Tarmoqning yirikligi va murakkabligi tufayli, har bir bo‘lakning o‘z xavfsizlik siyosati va resurslari mavjud bo‘lishi kerak. Boshqacha aytganda, tarmoqni to‘liq xavfsiz qilish uchun nafaqat markaziy, balki har bir segmentga alohida e’tibor qaratish zarur.

Bundan tashqari, 5G tarmoqlarida xizmat ko‘rsatuvchi provayderlar o‘rtasidagi hamkorlik va ma’lumot almashinuvi ko‘payishi mumkin, bu esa tarmoqda boshqa provayderlar

tomonidan kirish huquqini nazorat qilishni murakkablashtiradi. Agar bu hamkorlikda bir provayder tarmoq xavfsizligini to‘liq ta’minlamasa, boshqa provayderlar ham xavf ostida bo‘lishi mumkin. Shu sababli, interoperability (boshqa tarmoqlar bilan ishlash) va access control (kirish nazorati) muhim ahamiyatga ega bo‘ladi.

5G’da xavfsizlikning muhim jihatlaridan biri bu raqamli identifikatsiya va autentifikatsiyadir. Yuqori tezlikda ishlaydigan tarmoqda tarmoqga ulangan har bir qurilma va foydalanuvchining identifikatsiyasi va autentifikatsiyasi alohida e’tibor talab qiladi. Agar autentifikatsiya mexanizmlari noto‘g‘ri sozlansa yoki hujumchilarning kirish imkoniyatlari oshsa, foydalanuvchi ma’lumotlarini o‘g‘irlash va xizmatlar ustidan nazoratni qo‘lga kiritish mumkin bo‘ladi.

Bundan tashqari, 5G tarmog‘ining xavfsizlikka ta’sir etuvchi xususiyatlaridan yana biri – bu ma’lumotlarni real vaqt rejimida qayta ishlash zarurati. Agar tarmoqda ma’lumotlar to‘g‘ri qayta ishlanmasa yoki monitoring tizimi ishlamasligi tufayli tahdidlar aniqlanmasa, hujumchilar tomonidan uzatilayotgan zararli ma’lumotlar tarmoqni butunlay ishdan chiqarishi mumkin.



2-rasm. 5G tarmog‘ida sodir bo‘lishi mumkin bo‘lgan hujumlari grafikasi[6]

1-jadval

5G texnologiyasidagi xavfsizlik muammolarining batafsil tahlili

№	Xavfsizlik muammosi	Ta’rifi	Asosiy sabablar	Potensial oqibatlar	Kamaytirish/ uskunalar yoki chora-tadbirlar
1	Yangi arxitekturaga xos zaifliklar	5G tarmog‘i virtualizatsiya va “software-defined networking” (SDN) asosida ishlaydi, bu esa yangi zaifliklarni keltirib chiqaradi	Virtualizat-siya, SDN, ochiq interfeyslar	Tarmoqni to‘liq egallash, xakerlik hujumlari	Segmentatsiya, monitoring vositalari, xavfsiz API dizayni

2	Tarmoq bo‘ylab “Man-in-the-middle” hujumlari	Foydalanuvchi va tarmoq orasidagi ma’lumotlar o‘g‘irlanishi yoki o‘zgartirilishi	Shifrlashning yo‘qligi yoki zaifligi, noto‘g‘ri autentifikat-siya	Maxfiy ma’lumotlar o‘g‘irlanadi, aloqalarning buzilishi	Shifrlash (end-to-end), kuchli autentifikatsiya
3	IoT qurilmalari orqali kirish hujumlari	5G IoT qurilmalar bilan chambarchas bog‘langan, ularning zaif xavfsizligi xakerlar uchun oson nishon	IoT qurilmalari-ning arzonligi va xavfsiz dizayn yetishmasligi	Tarmoqda botnet hujumlari, ma’lumotlar o‘g‘irlanadi	IoT xavfsizlik standartlari, tarmoq monitoringi
4	Denial of Service (DoS) va Distributed DoS (DDoS)	Tarmoq xizmatlarini ishdan chiqarish uchun ko‘p miqdordagi so‘rovlar yuboriladi	Tarmoqqa ochiq kirish, IoT qurilmalar orqali	Tarmoq ishlashining to‘xtashi, foydalanuv-chilarga zarar	Traffic filtering, AI asosidagi anomaliya aniqlovchi tizimlar
5	Qurilma autentifikatsi-yasining zaifligi	Qurilma yoki foydalanuvchining haqiqiyligini aniqlash tizimlari yetarli emas	Noto‘liq identifikatsi-ya jarayoni	Soxta qurilmalar tarmoqqa ulanadi, ma’lumotlar o‘g‘irlanadi	SIM/USIM xavfsizligi, multifaktor autentifikatsiya
6	Raqamli maxfiylik muammolari	5G orqali uzatilayotgan ma’lumotlar, geolokatsiya va shaxsiy ma’lumotlar himoyasi	Trafik tahlili orqali foydalanuv-chi aniqlanishi	Shaxsiy hayotga tajovuz, ma’lumotlar noqonuniy ishlatiladi	Shifrlash, metadata kamaytirish, maxfiylik siyosatlari
7	Tarmoqlararo xavfsizlik muammolari (Roaming, slicing)	Tarmoq slicing texnologiyasi va boshqa operatorlar bilan aloqa (roaming) orqali xavf	Segmentlar-aro zaif izolyatsiya, noto‘g‘ri konfiguratsi-ya	Segmentlar o‘rtasida hujumlar, resurslar o‘g‘irlanishi	Slicing xavfsizlik siyosatlari, segmentlararo izolyatsiya
8	Sun’iy intellektning noto‘g‘ri ishlatilishi	AI yordamida 5G tarmog‘ida xavfsizlikni boshqarish avtomatlashtiril-gan, ammo AI ham hujum obyekti bo‘lishi mumkin	Model zaifliklari, noto‘g‘ri o‘rgatilgan AI tizimlar	Noto‘g‘ri xavfsizlik qarorlari, hujumlarning ko‘zdan qochishi	AI xavfsizlik auditi, xatoliklarni aniqlash algoritmlari
9	Ochiq standartlar va uchinchi tomon ta’minotchilari ishtiroki	5G global standartlarga asoslangan, bu esa bir nechta ishlab chiqaruvchilarni jalb etadi	Tashqi provayderlar-ning ishonchliligi yo‘qligi	Orqa eshiklar, tahdidlarning ichki kirishi	Sertifikatlash, ishonchli ishlab chiqaruvchilar-dan foydalanish
10	5G bazaviy stansiyalarning fizik xavfsizligi	Bazaviy stansiyalar ko‘plab joylarda o‘rnatiladi, ularni himoya qilish qiyin	Ochiq joylashuv, muhofaza yo‘qligi	Fizik buzishlar, zarar yetkazish orqali tarmoq ishdan chiqadi	Kamera, qulf, signalizatsiya, stansiyalar joylashuvini optimallashtirish

Natijalar

Ushbu jadvalda 5G texnologiyasi bilan bog‘liq asosiy xavfsizlik muammolari tizimli tarzda tahlil qilinib, har bir muammo tavsifi, yuzaga kelish sabablari, mumkin bo‘lgan tahdidlar va ularni kamaytirish bo‘yicha takliflar keltirilgan.

An’anaviy xavfsizlik mexanizmlari ushbu murakkab va dinamik tarmoq arxitekturasi uchun yetarli emas. Shu bois, 5G xavfsizligini ta’minlash uchun zamonaviy yondashuvlar va global miqyosda qabul qilingan standartlarga asoslangan strategiyalar muhim ahamiyat kasb etadi.

Ushbu maqolada 3GPP[2, 2-6b] va ITU tomonidan ishlab chiqilgan xavfsizlik standartlari, foydalanuvchini identifikatsiya va autentifikatsiya qilish mexanizmlari, ma’lumotlarni shifrlash texnologiyalari hamda Zero-Trust arxitekturasi kabi zamonaviy yondashuvlar atroflicha tahlil qilinadi.

Xalqaro standartlashtirish tashkilotlari – 3GPP (3rd Generation Partnership Project) va ITU (International Telecommunication Union) tomonidan zamonaviy xavfsizlik me’yorlari ishlab chiqilgan. Bu standartlar foydalanuvchi ma’lumotlarini himoya qilish, tarmoqni tahdidlardan saqlash va ishonchli muhitni yaratish uchun asosiy mezon hisoblanadi[3, 3-5b].

2-jadval

5G texnologiyasi himoya usullari yondashuvlar tahlili

№	Texnologiya / Yondashuv	Ta’rif / Ishlash prinsipi	Xavfsizlikka ta’siri	O‘zbekiston-da qo‘llanilishi	Izoh
1	3GPP xavfsizlik standartlari	3GPP (3rd Generation Partnership Project) tomonidan ishlab chiqilgan tarmoq xavfsizligi standartlari; TS 33.501 5G tizimlar xavfsizligi uchun asosiy hujjat hisoblanadi	Tizimli, qatlamli xavfsizlikni ta’minlaydi – autentifikatsi-ya, identifikatsiya, shifrlash kabi jarayonlarni boshqaradi	Qisman qo‘llanmoqda (asosan mobil operatorlar tomonidan)	UzMobile, Beeline va Ucell kabi kompaniyalar asosiy 3GPP talablari asosida 5G sinovlarini olib bormoqda
2	ITU-T X.805 xavfsizlik me’yorlari	ITU (Xalqaro Telekommunikatsi-ya Ittifoqi) tomonidan ishlab chiqilgan xavfsizlik ramkasi – tarmoq xavfsizligi uchun 8 qatlamli model	Tarmoq dizayni va boshqaruvida xavfsizlikni har bir qatlamda nazorat qiladi	To‘liq joriy etilmagan	ITU standartlari konseptual jihatdan e’tirof etilgan, lekin amaliy joriy qilish hali to‘liq emas
3	Identifikatsi-ya: SUPI / SUCI	SUPI (Subscription Permanent Identifier) – foydalanuvchi identifikatori, SUCI esa shifrlangan identifikator	Foydalanuvchi-ning maxfiyligini saqlaydi va IMSI-catching (stingray) hujumlaridan himoya qiladi	Sinov bosqichida	Hozircha to‘liq integratsiya qilingan emas, faqat nazariy qo‘llanilmoq-da
4	Autentifikat-siya: SEAF va AUSF	SEAF (Serving Network Authentication	Yangi 5G autentifikatsiya modeli,	Joriy etilmagan	Hozirda 4G LTE asosidagi autentifikatsi-ya tizimi

		Function) va AUSF (Authentication Server Function) – foydalanuvchini tasdiqlashni boshqaradi	foydalanuvchi-ni xavfsiz va kuchli tasdiqlaydi		ishlatilmoqda5G autentifikatsiyasi hali qo‘llanilma-gan
5	End-to-End Encryption (E2EE)	Ma’lumotlar jo‘natuvchidan qabul qiluvchigacha to‘liq shifrlanadi; oraliq tarmoqlar ma’lumotni o‘qiy olmaydi	Maxfiylik va xavfsizlikni sezilarli darajada oshiradi	To‘liq joriy qilinmagan	Foydalanuv-chi darajasida (messenjer-lar), lekin 5G tarmog‘i darajasida emas
6	Integrity Protection	Ma’lumotlar o‘zgartirilmaganli-gini tekshiradi; noto‘g‘ri ma’lumot uzatish xavfini kamaytiradi	Tarmoqqa soxta yoki buzilgan ma’lumot kirishini oldini oladi	Amalda mavjud emas	Bu himoya 5G yadro tarmog‘ida faollashtirili-shi lozim, lekin O‘zbekiston-da amalda mavjud emas
7	Zero-Trust arxitekturasi (ZTA)	“Hech kimga ishonilmaydi” prinsipiga asoslangan model – har bir kirish alohida tekshiriladi	Har bir tarmoq elementining xavfsizligini mustahkamlay-di, ichki tahdidlarga qarshi himoya	Joriy etilmagan	ZTA hozirda ilg‘or kompaniyalar tomonidan o‘rganilmoq-da, biroq 5G tarmoq arxitekturasi hali bu bosqichda emas
8	Network Slicing xavfsizligi	Tarmoq bo‘linmalari (slice) alohida xizmatlar uchun ajratiladi; har bir slice uchun alohida xavfsizlik siyosati qo‘llaniladi	Har xil xavf darajasidagi xizmatlar izolyatsiya qilinadi	Eksperimental holatda	Operatorlar tarmoq slicing texnologiya-sini joriy qilishni rejalashtir-moqda, lekin xavfsizlik moduli hali to‘liq ishlab chiqilmagan
9	AI asosida xavfsizlik monitoringi	AI algoritmlari orqali tarmoqda anomal xatti-harakatlar aniqlanadi	DDoS va murakkab hujumlarni oldindan aniqlash imkonini beradi	Amalga oshirilmagan	AI asosidagi monitoring hali tarmoq xavfsizligi uchun ishlatilmaydi, lekin tadqiqotlar olib borilmoqda
10	Mutlaq kriptografik xavfsizlik (Post-Quantum Crypto)	Kvant kompyuterlar qarshisida ham mustahkam turgan shifrlash algoritmlari	Kelajakda kvant hujumlaridan himoya qiladi	Yo‘q	Bu texnologiya hali global darajada ham eksperimen-tal bosqichda

Xulosa

Tahlil jarayonida 5G tarmog‘ining murakkab arxitekturasi, yangi protokollar, edge computing va massaviy qurilma ulanishi kabi omillar xavfsizlik nuqtai nazaridan qanday xavf tug‘dirishi aniqlangan. Shuningdek, ushbu xavflar 4G va oldingi avlod texnologiyalaridan farqli ravishda ko‘proq qatlamli va ko‘p manbali tahdidlar ekanligi ta’kidlangan. Jadval orqali xavfsizlik muammolarining texnik va amaliy jihatlari yoritilib, ularni bartaraf etish uchun tavsiya etilayotgan zamonaviy yondashuvlarga e’tibor qaratilgan.

Jadvaldan ko‘rinadiki, ushbu xavfsizlik yondashuvlarining ko‘pchiligi hali O‘zbekiston sharoitida to‘liq joriy etilmagan. Ayni paytda ayrim operatorlar tomonidan 3GPP asosidagi asosiy xavfsizlik talablari sinov tariqasida qo‘llanmoqda, biroq SEAF/AUSF, Zero-Trust, E2EE kabi ilg‘or yondashuvlar amaliyotda mavjud emas. Bu esa mamlakatda 5G xavfsizligi bo‘yicha kompleks yondashuvlar ishlab chiqish va milliy strategiyani shakllantirish zaruratini ko‘rsatadi. 5G tarmoqlari xavfsizligini ta’minlash bo‘yicha zamonaviy yondashuvlarning O‘zbekistonda to‘liq va kompleks joriy qilinishi mamlakat raqamli infratuzilmasining barqaror rivojlanishi uchun muhim ahamiyatga ega.

Adabiyotlar/Литература/References:

1. Olimov I.S., Ortiqboyev A.M., “Buyumlar internetining (Internet of things, IOT) Arxitekturasi va xavfsizlik muammolari”. Axborot kommunikatsiyalari: Tarmoqlar, Texnologiyalar, Yechimlar. №2 (54). Toshkent-2020. -B. 32-41.
2. 3GPP TS 33.501: Security architecture and procedures for 5G system (Release 15). 3rd Generation Partnership Project (3GPP), 2020.
3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.
4. ITU-T Y.3101. Requirements of the IMT-2020 network. International Telecommunication Union, 2018.
5. Tang, F., McCann, J. A., & Jiang, L. (2019). Enabling end-to-end secure slicing in 5G networks. IEEE Communications Standards Magazine, 3(1), 34–40.
6. NGMN Alliance. 5G White Paper. Next Generation Mobile Networks (NGMN), 2015.
7. ETSI (European Telecommunications Standards Institute). Mobile Edge Computing (MEC); Framework and Reference Architecture. ETSI GS MEC 003 V1.1.1, 2016.

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

I RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, 23-iyun

Mas’ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI. *II Respublika ilmiy-amaliy konferensiyasi materiallari.* – Toshkent: Scienceproblems team, 2025. – 138 bet.

Elektron nashr: https://konferensiyalar.uz/uzbekistan-2030

Konferensiya tashkilotchisi: Scienceproblems Team

Konferensiya o‘tkazilgan sana: 2025-yil, 23-iyun

ISBN 978-9910-09-204-6