MA'LUMOTLARNI UZATISH TARMOG'IDA AXBOROTNI HIMOYALASH

Amriyeva Gulhayo G'aybulloyevna
Buxoro viloyati Gijduvon tuman
1-son texnikumi
Axborot xafvsizligi fani o'qituvchisi
Tel; 91 924 85 67
E pochta: amriyevagulhayo60@gmail.com

Anotatsiya

Ushbu maqolada ma’lumotlarni uzatish tarmoqlarida (kompyuter tarmoqlari, Internet, 5G, IoT va simsiz tarmoqlar) axborot xavfsizligining ilmiy va amaliy jihatlari chuqur tahlil qilinadi. Axborot uzatish jarayonidagi asosiy tahdidlar (eavesdropping, man-in-the-middle (MITM) hujumlari, DDoS, packet sniffing va fizik qatlam zaifliklari) misollar bilan ko‘rib chiqiladi. Himoya mexanizmlari — kriptografik shifrlash (AES-256, RSA, ECC), transport qatlam protokollari (TLS/SSL), tarmoq qatlam protokollari (IPsec), VPN tizimlari va zamonaviy yondashuvlar (fizik qatlam himoyasi — PLS, AI yordamida tahdid aniqlash) batafsil yoritiladi. Ilmiy jihatdan OSI modelining xavfsizlik qatlamlari, TLS handshake jarayoni va IPsec tunnel/transport rejimlari sxemalari bilan tahlil qilinadi. Natijalar shuni ko‘rsatadiki, **defense-in-depth** printsipi (ko‘p qatlamli himoya) va AI-integratsiyasi tarmoq xavfsizligini sezilarli darajada oshiradi. Maqola IT-mutaxassislar, tadqiqotchilar va tarmoq administratorlari uchun mo‘ljallangan bo‘lib, real hayot misollari (Heartbleed, LoRaWAN hujumlari, SD-WAN korporativ tarmoqlari) va diagrammalar bilan boyitilgan.

Kalit so‘zlar: axborot xavfsizligi, ma’lumotlarni uzatish tarmoqlari, kriptografiya, TLS protokoli, IPsec, VPN, man-in-the-middle hujumi, fizik qatlam himoyasi (PLS), DDoS, 5G/IoT xavfsizligi, OSI modeli.

Hozirgi davrda tashkilotlar samarali va produktiv muloqot qilish uchunasosankompyuter tarmoqlariga suyanadilar. Har bir xodimning maxsus ish stantsiyasibor deb taxmin qilsak, yirik kompaniyalarda ularning soni bir nechaminggayetishi mumkin, shuningdek, tarmoqda ko’plab serverlar hammavjudbo’lishimumkin. Ehtimol, ushbu ish stantsiyalarini markazdan boshqarish mumkinemasvaularning atrof-muhiti xavfsizligi ta’minlanmagan. Foydalanuvchilar orasidaturlixil sir tutilishi darajalariga ega bo’lgan xabarlarni, turli xil operatsiontizimlarga, qo’shimcha qurilmalarga, dasturlarga va protokollarga ega bo’lishi mumkinbo’lgan o’rtalikda almashish holatlari juda ko’p. Endi tasavvur qiling, kompaniyatarmog’idagi ushbu minglab ish stantsiyalari to’g’ridan - to’g’ri Internetgaulangan. Ko’plab zaifliklarga ega qimmatbaho ma’lumotlarni o’z ichiga olgan ushbuxavflitarmoq bir nechta xakerlar hujumi uchun oson

Bundatizim administratorining ishi va olib borayotgan nazorati katta ahamiyatta egadir. Masalan, foydalanuvchilarning tez-tez parollarni almashtirib turishlari va parollarning judauzunligiularni aniqlashni qiyinlashtiradi. Shuning uchun ham yangi foydalanuvchini qaydetishnicheklash (masalan, faqat ish vaqtida yoki faqat ishlayotgan korxonasida) muximdir. Foydalanuvchining xaqiqiyligini tekshirish uchun teskari aloqa qilib turish lozim(masalan, modem yordamida). Axborot zaxiralariga kirish huquqini chegaralash mexanizmini ishlatishva uning ta‘sirini LAN obyektlariga to’laligicha o’tkazish mumkin. Tarmoq, elementlariurtasida o’tkazilayotgan ma‘lumotlarni muxofaza etish uchun quyidagi choralarni ko’rishkerak: - ma‘lumotlarni aniqlab olishga yo’l qo’ymaslik; - axborot almashishni tahlil qilishgayo’l qo’ymaslik; - xabarlarni o’zgartirishga yo’l qo’ymaslik; - yashirincha ulanishgayo’lqo’ymaslik va bu xollarni tezda aniqlash.

Ma‘lumotlarni tarmoqda uzatishpaytidakriptografik himoyalash usullaridan foydalaniladi, qayd etish jurnaliga ruxsat etilmagankirishlar amalga oshirilganligi xaqida ma‘lumotlar yozilib turilishi kerak. Bu jurnalgakirishnichegaralash ham himoya vositalari yordamida amalga oshirilishi lozim. Kompyuter tarmogidanazoratni olib borish murakkabligining asosiy sababi — dasturiy ta‘minot ustidannazoratolib borishning murakkabligidir. Bundan tashqari kompyuter viruslarining ko’pligi hamtarmoqda nazoratni olib borishni qiyinlashtiradi. Hozirgi vaqtgacha muxofazalashdasturiyta‘minoti xilma-xil bo’lsa ham, operatsion tizimlar zaruriy muxofazaning kerakli darajasinita‘minlamas edi. Himoyalanishni tahlillash vositalari zaifliklarni topib va o`z vaqtida yo`q qilib xujumni amalgaoshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishigabo`ladigan barcha sarf-harajatlar kamayadi. Himoyalanishni tahlillash vositalari tarmoqsathida, operattsion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlarsonini bora-bora ko`paytirish, axborot tizimiga "ichkarilab borish" va uning barchasathlarinitadqiqlash orqali zaifliklarni qidirishi mumkin. Tarmoq protokollari va servislarihimoyalanishini tahlillash vositalari. Har qanday tarmoqda abonentlarning o`zaroaloqasiikkita va undan ko`p uzellar orasida axborot almashinish muolajalarini belgilovchi tarmoqprotokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislariniishlab chiqishda ularga ishlanuvchi axborot xavfsizligini ta’minlash bo`yicha talablar qo`yilgan. SHu sababli, tarmoq protokollarida aniqlangan zaifliklar xususida axborotlar paydobo`lmoqda. Natijada, korporativ tarmoqda foydalanadigan barcha protokol va servislarnidoimo tekshirish zaruriyati tug’iladi. Himoyalanishni tahlillash tizimi zaifliklarni aniqlashbo`yicha testlar seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativtarmoqlarga xujumlarida qo`llaniladiganiga o`xshash. Zaifliklarni aniqlashmaqsadidaskanerlash tekshiruvchi tizim xususidagi dastlabki axborotni, xususan, ruxsat etilganprotokollar va ochiq portlar, operattsion tizimning ishlatiluvchi versiyalari va h. xususidagiaxborotni olish bilan boshlanadi. Skanerlash

keng tarqalgan xujumlar, masalan, to`liqsaralashusuli bo`yicha parollarni tanlashdan foydalanib, suqilib kirishni imitatsiyalashga urinishbilantugaydi. Himoyalanishni tahlillash vositalari yordamida tarmoq sathida nafaqat Internetningkorporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichkitarmog'ida tekshirishni amalga oshirish mumkin. Tarmoq sathida himoyalanishni tahlillashtizimi tashkilot xavfsizlik darajasini baholashga hamda tarmoq dasturiy va apparat ta'minotinisozlash samaradorligini nazoratlashga xizmat qiladi. Tarmoq axborotini tahlillash usullari. Mohiyati bo`yicha, xujumlarni aniqlashjarayonikorporativ tarmoqda bo`layotgan shubhali harakatlarni baholash jarayonidir. Boshqachaaytganda xujumlarni aniqlash - hisoblash yoki tarmoq resurslariga yo`naltirilganshubhaliharakatlarni identifikattsiyalash va ularga reaktsiya ko`rsatish jarayoni. Hozirda xujumlarnianiqlash tizimida quyidagi usullar ishlatiladi: - statistik usul; - ekspert tizimlari; - neyrontarmoqlari. Statistik usul. Statistik yondashishning asosiy afzalligi allaqachon ishlabchiqilganva o`zini tanitgan matematik statistika apparatini ishlatish va sub'ekt xarakterigamoslash. Avval tahlillanuvchi tizimning barcha sub'ektlari uchun profillar aniqlanadi. nishonga aylanadi. Tarmoq, muxofazasini tashkil etishda quyidagilarni e'tiborga olish lozim: - muxofazatizimining nazorati; - fayllarga kirishning nazorati; - tarmoqda ma'lumot uzatishningnazorati;- axborot zaxiralariga kirishning nazorati; - tarmoq bilan ulangan boshqa tarmoqlargama'lumot tarqalishining nazorati. Tarmoq himoyasini tashkil qilish asoslari. Maxfiyaxborotniqayta ishlash uchun kerakli tekshiruvdan o'tgan kompyuterlarni ishlatish lozimbo'ladi. Muxofaza vositalarining funksional to'lik bo'lishi muxim hisoblanadi. Zamonaviy globallashgan jamiyatda axborot uzatish tarmoqlari (TCP/IP asosidagi Internet, 5G, IoT va simsiz tarmoqlar) iqtisodiyot, tibbiyot, ta'lim va davlat boshqaruvining asosini tashkil etadi. Biroq, ochiq kanallar orqali uzatiladigan ma'lumotlar eavesdropping, o'zgartirish yoki buzilish xavfiga duch keladi. Axborot xavfsizligining uch asosiy tamoyili —

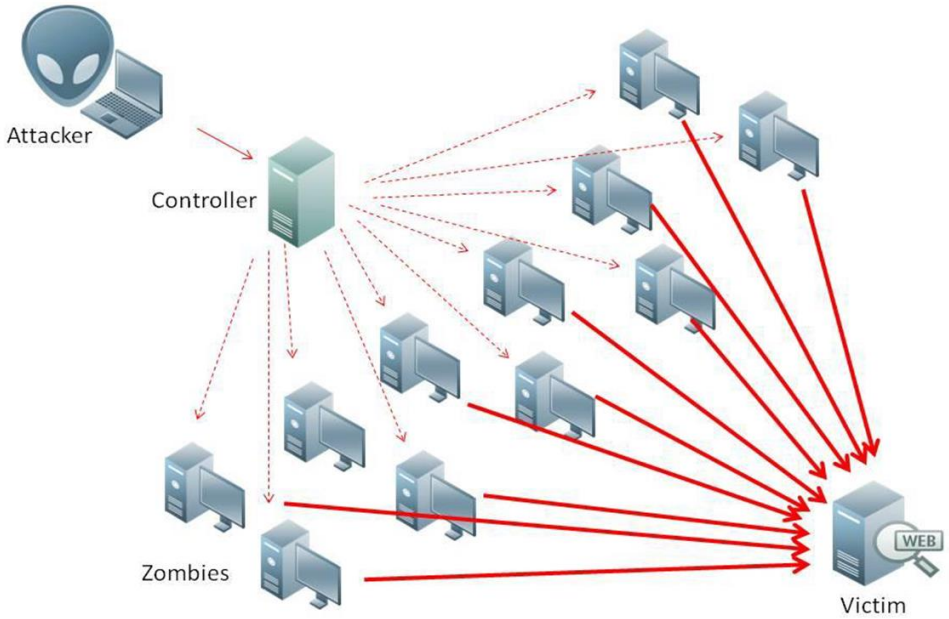
maxfiylik (confidentiality), **butunlik (integrity)** va **mavjudlik (availability)** — tarmoq muhitida eng muhim ahamiyatga ega.

Ilmiy tadqiqotlar shuni ko‘rsatadiki, har yili millionlab kiberhujumlar sodir bo‘lmoqda, ularning 70% dan ortig‘i ma’lumot uzatish jarayonida amalga oshiriladi. 2024–2025 yillarda 5G va IoT tarmoqlarining kengayishi bilan tahdid yuzasi yanada oshgan. Ushbu maqolada OSI modeli asosida xavflar tahlil qilinadi, himoya protokollari sxemalari bilan ko‘rsatiladi va real misollar keltiriladi.

Ma’lumotlarni uzatish tarmoqlaridagi asosiy xavf-xatarlar

Tarmoq orqali uzatiladigan axborotga quyidagi ilmiy tasniflangan tahdidlar xos:

1. **Eavesdropping (tinglash)** — ochiq kanallarda (masalan, Wi-Fi yoki LoRaWAN) ma’lumotlar to‘liq o‘qilishi mumkin. Misol: 2023-yilda LoRaWAN protokolida zaif kriptografiya tufayli millionlab IoT qurilmalari tinglangan.

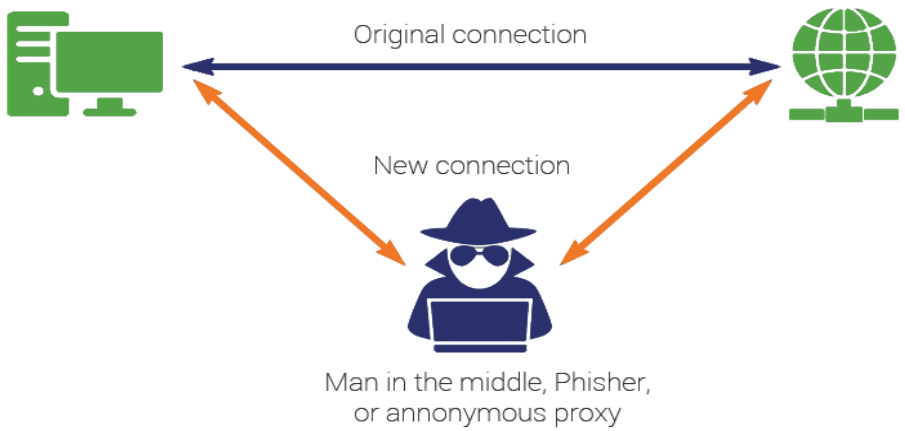


pcmag.com

Server Error: Distributed Denial-of-Service (DDoS) Attacks Explained | PCMag

DDoS hujumi sxemasi: Hujumchi botnet orqali serverga ko‘p sonli so‘rovlar yuborib, tarmoqni to‘sib qo‘yadi (rasmda ko‘rsatilganidek).

2. **Man-in-the-Middle (MITM) hujumi** — hujumchi ikki tomon o‘rtasidagi aloqani buzib, ma’lumotlarni o‘zgartiradi yoki o‘g‘irlaydi. Real misol: Heartbleed zaifligi (2014) TLS protokolida millionlab sertifikatlar o‘g‘irlangan.



thesslstore.com

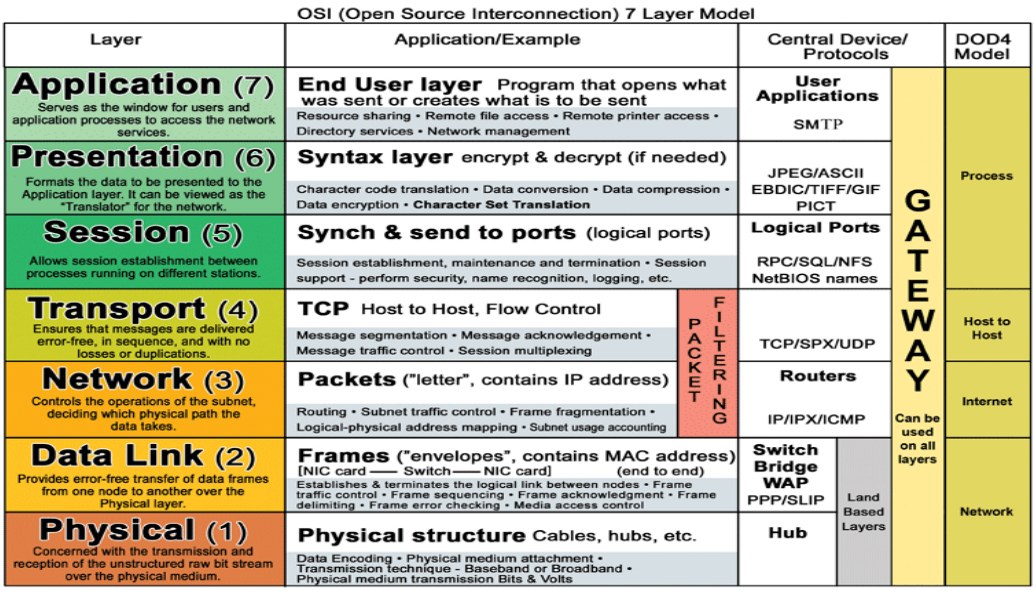
Executing a Man-in-the-Middle Attack in just 15 Minutes - Hashed Out

MITM hujumi sxemasi: Hujumchi “o‘rtada” joylashib, original aloqani buzadi.

3. **DDoS va packet sniffing** — tarmoqni to‘sish yoki trafigini tahlil qilish. 5G HetNets da beamforming zaifligi tufayli hujumlar kuchaygan.
4. **IoT va simsiz tarmoq zaifliklari** — ZigBee yoki MQTT protokollarida kalit almashinuvi muammosi. O‘zbekistonda simsiz tarmoqlar xavfsizligi tadqiqotlari ham shu muammoni ta’kidlaydi.

Axborotni himoyalash usullari va protokollari (ilmiy tahlil)

Axborot himoyasi OSI modelining turli qatlamlarida amalga oshiriladi.



blog.smartbuildingsacademy.com

What is the OSI Model

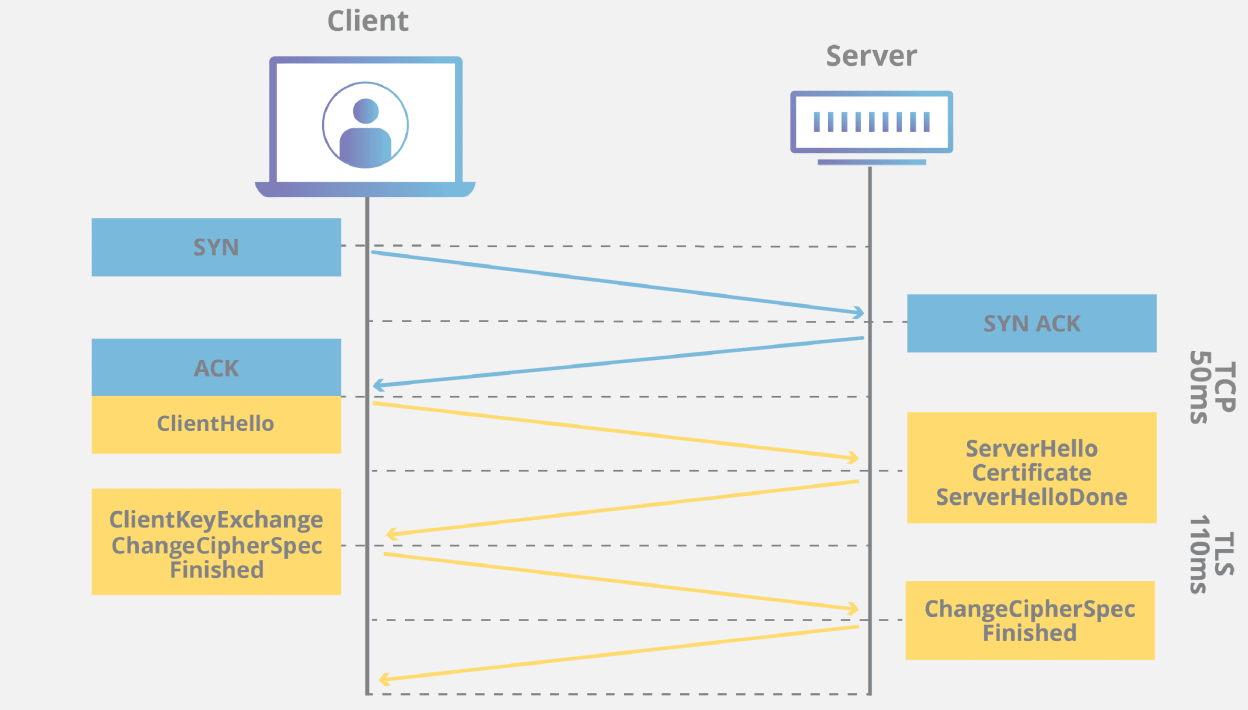
OSI modeli va xavfsizlik qatlamlari sxemasi: Har bir qatlamda alohida himoya (Transport — TLS, Network — IPsec).

1. Kriptografik shifrlash

- **Simmetrik**: AES-256 (tezlik yuqori, kalit bitta).
- **Nosimmetrik**: RSA/ECC (kalit almashinuvi xavfsiz).
- Ilmiy misol: AES algoritmi matematik jihatdan blok shifrlash asosida ishlaydi (128/192/256 bit kalit).

2. Transport qatlam himoyasi — TLS/SSL

TLS handshake jarayoni quyidagicha:



keyfactor.com

Demystifying the TLS Handshake: What it is and how it works | Keyfactor

TLS handshake diagrammasi: ClientHello → ServerHello → Sertifikat almashinuvi → KeyExchange → Finished. Bu jarayon maxfiylik va autentifikatsiyani ta’minlaydi. Real misol: HTTPS veb-saytlarida qo‘llaniladi; korporativ SD-WAN da TLS/DTLS control channel sifatida ishlatiladi.

3. Tarmoq qatlam himoyasi — IPsec

IPsec ikki rejimda ishlaydi:

twingate.com

IPsec Tunnel Mode vs. Transport Mode | Twingate

IPsec Tunnel vs Transport rejimi sxemasi: Tunnel rejimi butun paketni kapsulalaydi (VPN uchun ideal), Transport rejimi faqat payloadni himoyalaydi.

- **AH (Authentication Header)** — butunlik va autentifikatsiya.

- **ESP (Encapsulating Security Payload)** — shifrlash + autentifikatsiya. Real misol: Site-to-site VPN da ikki ofis o‘rtasida IPsec tunnel yaratiladi (AWS VPC yoki Cisco SD-WAN).

4. Zamonaviy yondashuvlar

- **VPN**: IPsec yoki WireGuard asosida xavfsiz tunnel.
- **Fizik qatlam himoyasi (PLS)** — 5G da cooperative jamming va beamforming orqali shifrlashsiz himoya.

Physical layer security with its applications in 5G networks: A review | Semantic Scholar

5G da fizik qatlam himoyasi sxemasi: Kriptografiyadan mustaqil signal ishlov berish.

- **AI yordamida himoya**: Big Data asosidagi tahdid aniqlash (security situation awareness).

Natijalar va muhokama

Ilmiy tadqiqotlar (2024–2025) shuni ko‘rsatadiki, bitta protokol yetarli emas. **Defense-in-Depth** (TLS + IPsec + AI) eng samarali. Masalan, Cisco SD-WAN da IPsec + TLS kombinatsiyasi korporativ tarmoqlarda qo‘llanilmoqda. O‘zbekistonda simsiz tarmoq xavfsizligi bo‘yicha tadqiqotlar ham shu yondashuvni tavsiya etadi. Kelajakda kvant kriptografiyasi va zero-trust arxitekturasi ustunlik qiladi.

Xulosa

Ma’lumotlarni uzatish tarmoqlarida axborotni himoyalash — strategik zarurat. Kriptografik protokollar (TLS, IPsec), VPN va AI-integratsiyasi birgalikda qo‘llanilganda xavf-xatarlar sezilarli kamayadi. Ilmiy diagrammalar va real misollar shuni tasdiqlaydiki, ko‘p qatlamli himoya zamonaviy tarmoqlarning asosiy talabidir. Har bir tashkilot axborot xavfsizligini doimiy yangilab borishi lozim.

Foydalanilgan adabiyotlar

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2017.

2. Chen F. Data Transmission Security in Computer Network Communication // IOP Conference Series, 2021.
3. Onyebuchi E.C. et al. Security Issues in Digital Data Communication – A Review // IRE Journals, 2025.
4. Saidov J. Axborotlarni tarmoqda uzatishda himoyalash usullari // CyberLeninka, 2025.
5. Kompyuter tarmoqlarida uzatilayotgan axborotni kriptografik himoyalash usuli // ResearchGate, 2025.
6. Sharma H. et al. AI-assisted secure data transmission techniques for next-generation HetNets // Computer Networks, 2024.
7. Czeczot G. Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol // Electronics, 2023.
8. Simsiz tarmoq xavfsizligiga tahdidlar va ular echimlari // ResearchGate, 2026.
9. Zhydka O. et al. Research on data transmission technologies and information security in IoT networks // CEUR-WS, 2024.
10. Wang X. Security situation awareness algorithm of network information transmission based on big data // Scientific Reports, 2025.