



TARMOQ KOMPYUTERLARI VIRTUAL SHAXSIY TARMOQ VPN

Jo'rayeva Sitora Ergash qizi

Buxoro viloyati G'ijduvon tuman 1-son Texnikumi

sitorasitora610@gmail.com

97 306 49 09

Annotatsiya

Ushbu maqolada kompyuter tarmoqlari infratuzilmasi va virtual shaxsiy tarmoq (VPN — Virtual Private Network) texnologiyasining ilmiy asoslari, tarixiy rivoji, kriptografik mexanizmlari, protokollari, xavfsizlik tahlili hamda kelajakdagi tendensiyalari chuqur ko'rib chiqiladi. Maqolada VPNning tunneling tamoyillari, shifrlash algoritmlari (AES-256, ChaCha20), asosiy protokollar (OpenVPN, WireGuard, IPSec)ning solishtirma tahlili, potentsial zaifliklar, quantum computing tahdidlari va Zero Trust Network Access (ZTNA), SASE kabi zamonaviy yondashuvlar bilan taqqoslanishi beriladi. VPN raqamli transformatsiya va kibertahdidlar sharoitida ma'lumotlar maxfiyligi va tarmoq xavfsizligining asosiy vositasi sifatida muhim o'rin tutadi.

Kalit so'zlar: Kompyuter tarmoqlari, Virtual shaxsiy tarmoq, VPN, Tunneling protokollari, OpenVPN, WireGuard, IPSec, Kriptografiya, Tarmoq xavfsizligi, Quantum-resistant shifrlash, ZTNA, SASE.

Kirish

Kompyuter tarmoqlari zamonaviy axborot jamiyatining asosiy infratuzilmasidir. Ular OSI yoki TCP/IP modeliga asoslanib, ma'lumotlar almashinuvi, resurslarni baham ko'rish va masofaviy boshqaruvni ta'minlaydi. Biroq, ochiq Internet muhiti eavesdropping, man-in-the-middle (MITM), IP-spoofing va boshqa kibertahdidlar xavfi yuqori.



Virtual shaxsiy tarmoq (VPN) jamoat tarmog'i (Internet) orqali shaxsiy tarmoqni virtual ravishda kengaytiradi va shifrlangan tunnel yaratadi. Bu foydalanuvchiga xuddi lokal tarmoq ichida ishlayotgandek xavfsiz aloqa o'rnatish imkonini beradi. VPN 1990-yillarda paydo bo'lib, bugungi kunda korporativ, shaxsiy va ilmiy tadqiqotlarda keng qo'llaniladi.

Zamonaviy dunyo internet muhitida axborot xavfsizligi va maxfiyligi tobora dolzarb masalaga aylanmoqda. Foydalanuvchilar shaxsiy ma'lumotlarini himoya qilish, internetga erkin kirish va cheklovlarni chetlab o'tish uchun turli texnologiyalardan foydalanishadi. Virtual Shaxsiy Tarmoq (VPN – Virtual Private Network) hisoblanadi. VPN texnologiyasi foydalanuvchining internetga ulanayotgan ma'lumotlarini shifrlab, uni maxfiy va xavfsiz holda uzatishga imkon beradi. Ushbu texnologiya orqali foydalanuvchi o'zining haqiqiy IP-manzilini yashirish va boshqa mamlakatlardagi serverlar orqali internetga ulanish imkoniyatiga ega bo'ladi. Bu esa nafaqat internetda shaxsiy hayotni himoya qilishga, balki ochiq Wi-Fi tarmoqlari orqali ulanishda ma'lumotlarning o'g'irlanishining oldini olishga ham yordam beradi. VPN texnologiyasining ishlash tamoyillari, uning asosiy turlari va foydalanuvchilarga taqdim etadigan afzalliklari haqida batafsil ma'lumot beriladi. VPN (Virtual Private Network) – bu internet orqali shifrlangan va xavfsiz aloqa kanalini ta'minlaydigan texnologiya bo'lib, u foydalanuvchilarga shaxsiy ma'lumotlarini himoya qilish, geo-cheklovlarni aylanib o'tish va anonimlikni ta'minlash imkonini beradi. VPN yordamida foydalanuvchining internetga kirish faoliyati shifrlanadi va maxsus serverlar orqali yo'naltiriladi, bu esa uning haqiqiy IP-manzilini yashirish imkonini beradi. Trafikni shifrlash – VPN foydalanuvchining qurilmasidan internetga yuborilayotgan ma'lumotlarni shifrlaydi, bu esa ma'lumotlarni uchinchi shaxslar tomonidan kuzatilishining oldini oladi. Trafikni yo'naltirish – Ma'lumotlar VPN serveri orqali



yo‘naltiriladi, bu esa foydalanuvchining haqiqiy IP-manzilini yashirish va boshqa mamlakatdagi server orqali ulanishni ta‘minlaydi. Internetga kirish – VPN orqali foydalanuvchi o‘z manzilini yashirib, internetga boshqa joylashuvdan kirayotgan kabi ko‘rinadi. Bu esa geo-cheklovlarni aylanib o‘tishga imkon beradi. Ulanish protokoliga ko‘ra VPN texnologiyasining bir nechta asosiy turlari: – PPTP (Point-to-Point Tunneling Protocol) – eski, ammo hali ham ishlatiladigan protokol. Tez ishlaydi, ammo xavfsizlik darajasi juda past. – L2TP/IPSec (Layer 2 Tunneling Protocol) – PPTP ga qaraganda xavfsizroq, lekin tezligi nisbatan pastroq bo‘lishi mumkin. – OpenVPN – eng mashhur va xavfsiz protokollardan biri bo‘lib, ochiq kodli va turli qurilmalarda ishlaydi.

WireGuard – yangi va tez ishlovchi protokol bo‘lib, sodda tuzilishga va yuqori xavfsizlik darajasiga ega. VPN texnologiyasining foydalanish turlariga ko‘ra turlari: – Shaxsiy (Personal) VPN – oddiy foydalanuvchilar tomonidan xavfsizlik va maxfiylikni ta‘minlash uchun ishlatiladi. – Korporativ (Business) VPN – kompaniyalar xodimlariga masofadan xavfsiz ulanishni ta‘minlash uchun qo‘llaniladi. – Bepul va pullik VPN xizmatlari – bepul VPN’lar cheklangan tezlik va xavfsizlikka ega bo‘lsa, pullik xizmatlar yaxshiroq himoya va tezlikni ta‘minlaydi. VPN’ning afzalliklari: 1. Maxfiylik va xavfsizlik – internet trafisini shifrlaydi, shaxsiy ma‘lumotlarni himoya qiladi. 2. Geo-cheklovlarni aylanib o‘tish – YouTube, Netflix, va boshqa geo-bloklangan xizmatlarga kirish imkonini beradi. 3. Jamoat Wi-Fi xavfsizligi – ochiq Wi-Fi tarmoqlarida ma‘lumotlarning o‘g‘irlanishidan himoya qiladi. 4. Internet provayder nazoratidan qochish – internet faoliyatining kuzatilishining oldini oladi. VPN texnologiyasining kamchiliklari haqida gapiradigan bo‘lsak Internet tezligining pasayishi – ma‘lumotlar shifrlangan va server orqali yo‘naltirilgani uchun tezlik pasayishi mumkin. Ishonchsiz VPN xizmatlari – ayrim bepul VPN’lar foydalanuvchilarning ma‘lumotlarini saqlab, uchinchi tomonlarga sotishi mumkin. Ba’zi xizmatlar tomonidan bloklanishi – ayrim



veb-saytlar va ilovalar (masalan, Netflix) VPN foydalanuvchilarini bloklashi mumkin. Shaxsiy VPN (Virtual Private Network) — bu foydalanuvchining internetga xavfsiz va anonim ulanishi uchun maxsus VPN ruxsatidir. Shaxsiy VPN foydalanuvchi foydalanuvchining o'z himoyasiga ko'ra so'z ya'ni o'zining shaxsiy moslashtirilgan ta'minoti hisoblanadi. Bu shaxsiy VPN foydalanuvchiga internetda anonimlikni saqlash, ma'lumotlarini shifrlash va onlayn almashtirishni qayd qiladi. Shaxsiy VPN Ishlash Tamoyillari foydalanuvchining internet foydalanish umumiy shifrlaydi va IP-manzilini yashiradi. Ammo shaxsiy VPN foydali afzalligi olinadi, u faqat bitta foydalanuvchi uchun so'z faqat o'sha foydalanuvchi sifatida saqlanadi. Shaxsiy VPN olingan shaxsiy vositalarni o'z ichiga oladi. Shaxsiy VPN Serverini Yaratish: VPN serveri yoki foydalanuvchining uyida maxsus serverda o'z nazorati ostida. Serverga kerakli VPN protokollari (masalan, OpenVPN, WireGuard yoki IKEv2) o'rnatilib, tarmoq ta'minlanadi.

2. VPNning tarixiy rivoji va ilmiy asoslari

VPNning dastlabki g'oyalari 1970-80-yillarda virtual circuit tushunchasidan kelib chiqqan. 1990-yillarda PPTP (Point-to-Point Tunneling Protocol) kabi protokollar paydo bo'ldi. Ilmiy jihatdan VPN OSI modelining 2- va 3-qatlamlarida (Data Link va Network) tunneling mexanizmlarini qo'llaydi.

Asosiy ilmiy tamoyillar:

- **Tunneling** — Paketlarni boshqa paket ichiga inkapsulyatsiya qilish.
- **Shifrlash** — Simmetrik (AES) va assimetrik (RSA, ECDH) kriptografiya.
- **Autentifikatsiya** — IKEv2, TLS va boshqalar orqali.

3. VPNning ishlash tamoyillari va arxitekturas

VPN quyidagi bosqichlarda ishlaydi:

1. Autentifikatsiya va sessiya o'rnatish.
2. Kuchli shifrlash (masalan, AES-256-GCM).



3. Tunneling (GRE, IP-in-IP va boshqalar).

4. Routing va IP-manzil yashirish.

Ilmiy tahlilda VPN trafikining o'ziga xos xususiyatlari (packet size, timing, entropy) machine learning orqali aniqlanishi mumkin, bu esa traffic analysis hujumlarini o'rganishga yordam beradi.

4. Asosiy VPN protokollari: Solishtirma ilmiy tahlil

- **PPTP** — Eski, RC4 shifrlashi zaif, tavsiya etilmaydi.
- **L2TP/IPSec** — Yaxshi, lekin sekinroq.
- **OpenVPN** — Ochiq kodli, SSL/TLS ga asoslangan, juda moslashuvchan. AES-256 bilan yuqori xavfsizlik, ammo kod bazasi katta (taxminan 70 000 satr) bo'lgani uchun audit qilish murakkab.
- **IPSec** — Korxona darajasida, kuchli autentifikatsiya (IKEv2). Apparat tezlashtirishni qo'llab-quvvatlaydi.
- **WireGuard** — Zamonaviy (2015-yildan), juda sodda (4000 satr kod), ChaCha20-Poly1305 va Curve25519 kriptografiyasidan foydalanadi. Eng tezkor protokollardan biri: OpenVPNGa nisbatan 2-3 baravar tezroq, kamroq CPU va latency.

Solishtirma jadval (2026-yil holatiga ko'ra):

Protokol	Tezlik	Xavfsizlik darajasi	Kod hajmi	Moslashuvchanlik	Quantum qarshiligi
OpenVPN	O'rtacha	Yuqori	Katta	Yuqori	O'rtacha
WireGuard	Eng yuqori	Yuqori	Juda kichik	Yuqori	Yaxshi (ChaCha20)
IPSec	Yuqori	Yuqori	O'rtacha	O'rtacha	O'rtacha

WireGuardning kichik kod bazasi xatoliklar sonini kamaytiradi va auditni osonlashtiradi.



5. Kriptografik jihatlar va xavfsizlik tahlili

VPNlarda AES-256, ChaCha20 kabi algoritmlar qo'llaniladi. AES-256 quantum brute-force hujumlariga nisbatan nisbatan chidamli (Grover algoritmi uni 2^{128} darajaga tushiradi, ammo hali ham xavfsiz).

Potentsial zaifliklar:

- Port shadow zaifliklari (OpenVPN, WireGuardda ba'zi holatlarda).
- No-log siyosati va provayder ishonchliligi.
- Traffic analysis va correlation attacks.

Zamonaviy tadqiqotlarda machine learning VPN trafikini aniqlash va tasniflash uchun qo'llanilmoqda.

6. Quantum tahdidlari va post-quantum yechimlar

Quantum kompyuterlar Shor algoritmi orqali RSA/ECC ni buzishi mumkin. AES-256 va ChaCha20 simmetrik shifrlash uchun nisbatan xavfsizroq. WireGuard va boshqa protokollar hybrid (klassik + post-quantum, masalan Kyber/ML-KEM) yondashuvlar bilan yangilanmoqda.

7. Zamonaviy tendensiyalar va kelajak istiqbollari

An'anaviy VPNlar asta-sekin **Zero Trust Network Access (ZTNA)** va **SASE (Secure Access Service Edge)** bilan almashtirilmoqda. ZTNA "hech kimga ishonma, har safar tekshir" tamoyiliga asoslanadi. SASE esa SD-WAN va xavfsizlik xizmatlarini (FWaaS, SWG, CASB) birlashtiradi.

Bu yondashuvlar bulutli muhit, IoT va hybrid ish uchun samaraliroq.

Xulosa

Kompyuter tarmoqlari va VPN texnologiyasi ma'lumotlar xavfsizligining ilmiy va amaliy asoslarini tashkil etadi. WireGuard kabi yangi protokollar tezlik va



xavfsizlikni oshirsa-da, quantum tahdidlari va murakkab tahdid landshafti post-quantum kriptografiya va ZTNA/SASE ga o'tishni talab qiladi. Kelgusidagi tadqiqotlar VPN trafik analizini, AI-integratsiyasini va quantum-safe yechimlarni rivojlantirishga qaratilishi lozim. Mutaxassislar va tashkilotlar uchun zamonaviy VPN va uning evolyutsiyasi kibertahdidlarga qarshi strategiyaning muhim qismidir.

Foydalanilgan adabiyotlar

1. Liu, Z. et al. (2023). Application and Security Analysis of Virtual Private Network.
2. Akinsanya, M. O. & Ekechi, C. C. Virtual Private Networks (VPN): A Conceptual Review.
3. Ellafy, A. (2025). A Systematic Review of VPN Technologies.
4. IVPN. PPTP vs IPSec IKEv2 vs OpenVPN vs WireGuard.
5. Palo Alto Networks & boshqa manbalar (2025-2026).