VPN TEXNOLOGIYASINING XAVFSIZLIKDAGI O‘RNI
РОЛЬ VPN-ТЕХНОЛОГИИ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ
THE ROLE OF VPN TECHNOLOGY IN SECURITY

Ibragimov Sh.M.[1], Akramjonova G.O.[2]

[1]*FarDU dotsenti, shavkat19702008@gmail.com*

[2]*FarDU talabasi, lunnesa18o2@gmail.com*

Annotatsiya: *Ushbu maqolada VPN (Virtual Private Network) texnologiyasining axborot xavfsizligini ta’minlashdagi o‘rni tahlil qilindi. VPN texnologiyasining ishlash prinsiplari, uning asosiy protokollari va tarmoq xavfsizligini oshirishdagi ahamiyati yoritildi. Shuningdek, ushbu texnologiyani qo‘llashdagi afzalliklar va mavjud muammolar ko‘rib chiqildi. VPN texnologiyasi zamonaviy tarmoqlarda ma’lumotlarni himoyalashning samarali vositalaridan biri hisoblanadi.*

Kalit so‘zlar: *VPN, virtual xususiy tarmoq, axborot xavfsizligi, shifrlash, tunnellash, IPsec, SSL, kiberxavfsizlik, ma’lumot uzatish, tarmoq himoyasi.*

Аннотация: *В статье рассматривается роль технологии VPN (Virtual Private Network) в обеспечении информационной безопасности. Проанализированы принципы работы VPN, основные протоколы и их значение для защиты сетей. Также освещены преимущества и проблемы применения данной технологии. VPN является эффективным средством защиты данных в современных сетях.*

Ключевые слова: *VPN, виртуальная частная сеть, информационная безопасность, шифрование, туннелирование, IPsec, SSL, кибербезопасность, передача данных, защита сети.*

Abstract: *This article examines the role of VPN (Virtual Private Network) technology in ensuring information security. The working principles of*

VPN, its main protocols, and its importance in network protection are analyzed. The advantages and challenges of implementing this technology are also discussed. VPN is considered an effective tool for protecting data in modern networks.

Keywords: *VPN, virtual private network, information security, encryption, tunneling, IPsec, SSL, cybersecurity, data transmission, network security.*

KIRISH

Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi natijasida internet global kommunikatsiya vositasiga aylanib, turli sohalarda keng qo‘llanilmoqda. Elektron tijorat, onlayn bank xizmatlari, masofaviy ta’lim, bulutli texnologiyalar va ijtimoiy tarmoqlarning ommalashuvi natijasida uzatilayotgan ma’lumotlar hajmi keskin ortib bormoqda. Bunday sharoitda axborotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash masalasi dolzarb ahamiyat kasb etmoqda. Shu bilan birga, kiberhujumlar, ma’lumotlarni noqonuniy qo‘lga kiritish, tarmoq trafigini kuzatish va zararli dasturlar orqali hujum qilish holatlari ham tobora ko‘payib bormoqda.

Ochiq tarmoqlarda, xususan internet orqali uzatilayotgan ma’lumotlar ko‘pincha uchinchi shaxslar tomonidan kuzatilishi yoki o‘zgartirilishi mumkin. Bu esa foydalanuvchilar uchun jiddiy xavf tug‘diradi. Ayniqsa, maxfiy ma’lumotlar — login va parollar, bank kartasi rekvizitlari, shaxsiy yozishmalar kabi axborotlarning himoyasiz uzatilishi katta muammolarga olib kelishi mumkin. Shu sababli, zamonaviy axborot tizimlarida ma’lumotlarni ishonchli himoyalashga qaratilgan texnologiyalarni qo‘llash zarurati ortib bormoqda.

VPN (Virtual Private Network) texnologiyasi aynan shu ehtiyojlardan kelib chiqqan holda ishlab chiqilgan bo‘lib, u ochiq tarmoqlar orqali xavfsiz va shifrlangan aloqa kanalini yaratish imkonini beradi. VPN texnologiyasi yordamida foydalanuvchi qurilmasi va server o‘rtasida maxsus “tunnel” hosil qilinadi va ushbu tunnel orqali uzatilayotgan barcha ma’lumotlar kuchli kriptografik algoritmlar yordamida shifrlanadi. Natijada, uzatilayotgan axborotni uchinchi shaxslar tomonidan o‘qish yoki o‘zgartirish deyarli imkonsiz bo‘ladi.

Bundan tashqari, VPN texnologiyasi foydalanuvchi IP manzilini yashirish, geografik cheklovlarni chetlab o‘tish va anonimlikni ta’minlash imkonini ham beradi. Ayniqsa, masofaviy ishlash keng rivojlanayotgan hozirgi davrda VPN korporativ tarmoqlarga xavfsiz ulanishni ta’minlovchi muhim vosita sifatida qo‘llanilmoqda. Korxonalar va tashkilotlar o‘z xodimlariga internet orqali ichki resurslarga xavfsiz kirish imkonini yaratishda aynan VPN texnologiyasidan keng foydalanmoqda.

Yuqoridagi mavzuning dolzarbligi shundaki, zamonaviy axborot jamiyatida xavfsizlik va maxfiylik masalalari ustuvor ahamiyat kasb etmoqda. VPN texnologiyasi esa ushbu muammolarni hal etishda samarali yechimlardan biri sifatida namoyon bo‘lmoqda. Shu bois, uning ishlash prinsiplari, afzalliklari va qo‘llanish imkoniyatlarini chuqur o‘rganish muhim ilmiy-amaliy ahamiyatga ega.

Ushbu maqolada VPN texnologiyasining nazariy asoslari, ishlash mexanizmlari, xavfsizlikni ta’minlashdagi o‘rni hamda zamonaviy tarmoqlarda qo‘llanish istiqbollari batafsil tahlil qilinadi.

ADABIYOTLAR TAHLILI VA USULLARI

VPN texnologiyasi bo‘yicha ilmiy tadqiqotlar asosan tarmoq xavfsizligi, kriptografiya va ma’lumotlarni uzatish sohalariga oid fundamental hamda amaliy ishlarga tayanadi. Mazkur yo‘nalishda olib borilgan tadqiqotlar VPN texnologiyasining nazariy asoslarini, ishlash mexanizmlarini hamda amaliy qo‘llanilish imkoniyatlarini chuqur o‘rganishga qaratilgan. Xususan, tarmoq xavfsizligi bo‘yicha yaratilgan klassik ilmiy manbalarda ochiq tarmoqlarda ma’lumotlarni himoyalash muammolari, shifrlash algoritmlarining samaradorligi va xavfsizlik protokollarining o‘rni batafsil yoritilgan.

VPN texnologiyasining rivojlanishida IPsec (Internet Protocol Security) protokoli muhim o‘rin egallaydi. Ilmiy adabiyotlarda IPsec asosida qurilgan VPN tizimlari tarmoq darajasida xavfsizlikni ta’minlashning eng ishonchli vositalaridan biri sifatida e’tirof etiladi. Ushbu protokol autentifikatsiya, yaxlitlikni tekshirish va ma’lumotlarni shifrlash funksiyalarini birlashtirgan holda ishlaydi. Tadqiqotlarda

IPsecning AH (Authentication Header) va ESP (Encapsulating Security Payload) komponentlari orqali ma’lumotlarni himoyalash mexanizmlari keng tahlil qilingan.

Bundan tashqari, SSL/TLS (Secure Sockets Layer / Transport Layer Security) protokollariga asoslangan VPN texnologiyalari ham ilmiy izlanishlarda muhim o‘rin tutadi. Ushbu protokollar transport darajasida ishlaydi va asosan veb-ilovalar hamda brauzer orqali amalga oshiriladigan xavfsiz ulanishlarni ta’minlaydi. Ilmiy manbalarda SSL VPN’larning foydalanuvchilar uchun qulayligi, oson sozlanishi va keng qo‘llanish imkoniyatlari alohida ta’kidlangan. Ayniqsa, masofaviy ishlash va mobil qurilmalardan foydalanish sharoitida SSL/TLS asosidagi VPN texnologiyalari samarali yechim sifatida qaraladi.

Zamonaviy tadqiqotlarda OpenVPN va WireGuard kabi yangi avlod VPN texnologiyalarining samaradorligi ham keng o‘rganilmoqda. OpenVPN ochiq kodli dasturiy ta’minot sifatida moslashuvchanligi va kuchli kriptografik himoyasi bilan ajralib turadi. WireGuard esa soddalashtirilgan arxitekturasi, yuqori tezligi va kam resurs talab qilishi bilan e’tiborga molikdir. Ilmiy tahlillar ushbu texnologiyalarning an’anaviy VPN yechimlariga nisbatan samaradorligini oshirganini ko‘rsatadi.

Shuningdek, ilmiy adabiyotlarda VPN texnologiyasining qo‘llanilish sohalari ham keng yoritilgan. Xususan, korporativ tarmoqlarda filiallar o‘rtasida xavfsiz aloqa o‘rnatish, masofaviy foydalanuvchilarni ichki tarmoqqa ulash, davlat tashkilotlarida maxfiy ma’lumotlarni uzatish va bulutli xizmatlardan xavfsiz foydalanish kabi yo‘nalishlarda VPN texnologiyasining ahamiyati yuqori baholanadi. Ayrim tadqiqotlarda esa VPN texnologiyasining kiberhujumlarga qarshi kurashdagi roli, jumladan, trafikni himoyalash va foydalanuvchi anonimligini ta’minlashdagi imkoniyatlari tahlil qilingan.

Mazkur tadqiqotda yuqorida keltirilgan ilmiy manbalar asosida bir qator usullar qo‘llanildi. Tahliliy usul yordamida VPN texnologiyasining nazariy asoslari, ishlash prinsiplari va asosiy protokollari chuqur o‘rganildi. Solishtirma tahlil usuli orqali IPsec, SSL/TLS, OpenVPN va WireGuard kabi turli VPN texnologiyalarining xavfsizlik darajasi, tezligi va qo‘llanish imkoniyatlari taqqoslandi. Tizimli

yondashuv asosida VPN texnologiyasi yagona xavfsizlik tizimi sifatida ko‘rib chiqilib, uning tarkibiy qismlari va o‘zaro bog‘liqligi tahlil qilindi.

Bundan tashqari, umumlashtirish usuli yordamida turli ilmiy tadqiqotlar natijalari birlashtirilib, VPN texnologiyasining zamonaviy holati va rivojlanish tendensiyalari bo‘yicha xulosalar chiqarildi. Shu bilan birga, amaliy kuzatishlar asosida VPN texnologiyasining real tarmoqlardagi samaradorligi va qo‘llashdagi muammolari ham baholandi.

Natijada, qo‘llanilgan usullar VPN texnologiyasining nafaqat nazariy, balki amaliy jihatdan ham muhim va samarali xavfsizlik vositasi ekanligini asoslash imkonini berdi.

MUHOKAMA

VPN texnologiyasi zamonaviy tarmoqlarda xavfsizlikni ta’minlashning muhim vositalaridan biri hisoblanadi. Uning asosiy vazifasi — ochiq tarmoq orqali uzatilayotgan ma’lumotlarni shifrlash va himoyalangan kanal yaratishdir.

VPN ishlash prinsipi tunnellash va shifrlash jarayonlariga asoslanadi. Tunnellash orqali ma’lumotlar maxsus “tunel” ichida uzatiladi, shifrlash esa ularni begona shaxslar o‘qiy olmasligini ta’minlaydi.

VPN texnologiyasining asosiy afzalliklari quyidagilardan iborat:

- ✓ ma’lumotlarni yuqori darajada himoyalash;
- ✓ foydalanuvchi maxfiyligini ta’minlash;
- ✓ geografik cheklovlarni chetlab o‘tish imkoniyati;
- ✓ masofaviy ishlashda xavfsiz ulanish.

Quyidagi jadvalda VPN va oddiy ochiq tarmoq orqali uzatish taqqoslangan:

1-jadval. VPN va oddiy tarmoqning taqqoslanishi

Mezoni	Oddiy tarmoq	VPN texnologiyasi
Xavfsizlik	Past	Yuqori
Shifrlash	Yo‘q yoki cheklangan	Kuchli shifrlash mavjud
Maxfiylik	Ta’minlanmaydi	To‘liq ta’minlanadi

Mezoni	Oddiy tarmoq	VPN texnologiyasi
Hujumga chidamlilik	Past	Yuqori
Qo‘llanish sohasi	Ochiq tarmoqlar	Korporativ va shaxsiy tarmoqlar

Shu bilan birga, VPN texnologiyasining ayrim kamchiliklari ham mavjud. Masalan, ulanish tezligining pasayishi, konfiguratsiya murakkabligi va ayrim hollarda yuqori xarajat talab qilinishi mumkin.

Bugungi kunda VPN texnologiyasi korporativ tarmoqlar, bank tizimlari, davlat muassasalari va masofaviy ishlash tizimlarida keng qo‘llanilmoqda. Bu esa uning amaliy ahamiyatini yanada oshiradi.

Qo’shimchasiga, VPN texnologiyasining imkoniyatlari faqatgina ma’lumotlarni shifrlash bilan cheklanib qolmaydi. U tarmoq darajasida autentifikatsiya va foydalanuvchini tekshirish mexanizmlarini ham o‘z ichiga oladi. Bu esa tarmoqqa faqat ruxsat etilgan foydalanuvchilarning kirishini ta’minlab, noqonuniy kirishlarning oldini olishga xizmat qiladi. Ayniqsa, IPsec va SSL/TLS protokollari asosida ishlovchi VPN tizimlarida autentifikatsiya, kalit almashinuvi va ma’lumot yaxlitligini tekshirish jarayonlari yuqori darajada tashkil etilgan.

VPN texnologiyasi zamonaviy kiberxavfsizlik tizimlarining muhim komponenti sifatida boshqa himoya vositalari bilan birgalikda qo‘llanilganda yanada samarali natija beradi. Masalan, xavfsizlik devorlari (firewall), antivirus dasturlari va tarmoq monitoring tizimlari bilan integratsiya qilingan VPN infratuzilmasi ko‘p bosqichli himoya tizimini yaratadi. Bunday yondashuv esa turli xil kiberhujumlar, jumladan, “man-in-the-middle”, sniffing va DDoS hujumlariga qarshi kurashishda yuqori samaradorlikni ta’minlaydi.

Shuningdek, VPN texnologiyasi bulutli hisoblash (cloud computing) muhitida ham keng qo‘llanilmoqda. Korxonalar o‘z ma’lumotlarini bulutli serverlarda saqlagan holda, VPN orqali ushbu resurslarga xavfsiz kirish imkoniyatiga ega bo‘ladi. Bu esa masofaviy ishlashni rivojlantirish, filiallar o‘rtasida xavfsiz aloqa o‘rnatish va global miqyosda faoliyat yuritish imkoniyatlarini kengaytiradi.

Yana bir muhim jihat shundaki, VPN texnologiyasi foydalanuvchi faoliyatini kuzatish va nazorat qilish imkonini ham beradi. Tarmoq administratorlari VPN orqali ulangan foydalanuvchilarning faoliyatini monitoring qilish, xavfsizlik siyosatlarini joriy etish va muammolarni tezkor aniqlash imkoniyatiga ega bo‘ladi. Bu esa tizimning umumiy xavfsizlik darajasini oshirishga xizmat qiladi.

So‘nggi yillarda mobil qurilmalar sonining ortishi bilan mobil VPN texnologiyalariga bo‘lgan talab ham keskin oshdi. Mobil VPN’lar foydalanuvchilarga harakat davomida ham uzluksiz va xavfsiz ulanishni ta’minlaydi. Bu ayniqsa, xizmat safaridagi xodimlar yoki masofadan ishlovchi mutaxassislar uchun muhim hisoblanadi.

Kelajak istiqbollari nuqtai nazaridan qaraganda, VPN texnologiyasi sun’iy intellekt va avtomatlashtirilgan xavfsizlik tizimlari bilan integratsiyalashgan holda yanada takomillashib borishi kutilmoqda. Bu esa tahdidlarni oldindan aniqlash, ularga tezkor javob berish va xavfsizlikni yangi bosqichga olib chiqish imkonini beradi.

Umuman olganda, VPN texnologiyasi nafaqat hozirgi davrda, balki kelajakda ham tarmoq xavfsizligini ta’minlashning ajralmas qismi sifatida o‘z ahamiyatini saqlab qoladi va uning qo‘llanish doirasi yanada kengayib boradi.

NATIJALAR

Tadqiqot natijalari shuni ko‘rsatdiki, VPN texnologiyasi axborot xavfsizligini ta’minlashda muhim vosita hisoblanadi. Xususan, shifrlangan kanal orqali uzatilgan ma’lumotlarning himoyalanganlik darajasi ancha yuqori ekani aniqlandi.

VPN yordamida foydalanuvchi ma’lumotlarini uchinchi tomonlardan himoyalash, IP manzilni yashirish va tarmoq xavfsizligini oshirish mumkinligi asoslandi.

Shuningdek, turli VPN protokollarini taqqoslash natijasida IPsec va SSL asosidagi VPN tizimlari eng keng qo‘llaniladigan va ishonchli usullar ekanligi aniqlandi. Zamonaviy WireGuard texnologiyasi esa tezlik va xavfsizlik jihatidan yuqori natijalarni ko‘rsatdi.

Amaliy jihatdan VPN texnologiyasi masofaviy ishlash, onlayn xizmatlardan foydalanish va korporativ tarmoqlarga ulanishda katta qulaylik yaratadi.

Biroq, texnologiyaning ayrim cheklovlari ham mavjud bo‘lib, ular orasida tezlikning pasayishi va texnik sozlash murakkabligi muhim o‘rin tutadi.

XULOSA

Olib borilgan tadqiqotlar shuni ko‘rsatdiki, VPN texnologiyasi zamonaviy axborot xavfsizligini ta’minlashda muhim va samarali vositalardan biri hisoblanadi. Uning asosiy ustunligi shundaki, ochiq va himoyasiz tarmoqlarda ham yuqori darajadagi xavfsiz, shifrlangan aloqa kanalini yaratish imkonini beradi. Natijada, foydalanuvchilar va tashkilotlar o‘z ma’lumotlarini tashqi tahdidlardan himoyalangan holda uzatish imkoniga ega bo‘ladi.

VPN texnologiyasi yordamida uzatilayotgan ma’lumotlar kuchli kriptografik algoritmlar asosida shifrlanadi, bu esa ularni uchinchi shaxslar tomonidan o‘qish yoki o‘zgartirishni deyarli imkonsiz qiladi. Bundan tashqari, VPN foydalanuvchi IP manzilini yashirish orqali anonimlikni ta’minlaydi, bu esa shaxsiy ma’lumotlarni himoyalashda muhim ahamiyatga ega. Ayniqsa, ochiq Wi-Fi tarmoqlaridan foydalanishda VPN texnologiyasi kiberhujumlardan himoyalanishning eng samarali vositalaridan biri sifatida namoyon bo‘ladi.

Tadqiqot natijalari shuni ham ko‘rsatdiki, VPN texnologiyasi nafaqat shaxsiy foydalanuvchilar uchun, balki korporativ tizimlar uchun ham muhim ahamiyatga ega. U masofaviy ishlash jarayonida xodimlarga ichki tarmoqlarga xavfsiz ulanish imkonini beradi, bu esa tashkilotlar faoliyatining uzluksizligini ta’minlashga xizmat qiladi. Shu bilan birga, bank tizimlari, davlat muassasalari va strategik infratuzilmalarda maxfiy ma’lumotlarni himoyalashda VPN texnologiyasining o‘rni beqiyosdir.

Biroq, VPN texnologiyasining ayrim cheklovlari ham mavjud. Jumladan, tarmoq tezligining pasayishi, ayrim xizmatlar bilan moslashuv muammolari va konfiguratsiya jarayonining murakkabligi uning keng qo‘llanilishiga

ma’lum darajada to‘sqinlik qilishi mumkin. Shuningdek, barcha VPN xizmatlari ham bir xil darajada ishonchli emasligi sababli, ularni tanlashda ehtiyotkorlik zarur.

Shunga qaramay, zamonaviy texnologiyalarning rivojlanishi ushbu kamchiliklarni bosqichma-bosqich bartaraf etishga xizmat qilmoqda. Yangi avlod VPN protokollari (masalan, WireGuard) yuqori tezlik, soddalik va kuchli xavfsizlikni ta’minlash orqali ushbu sohaning yanada takomillashayotganini ko‘rsatmoqda.

Umumiy xulosa sifatida aytish mumkinki, VPN texnologiyasi hozirgi va kelajakdagi axborot xavfsizligini ta’minlashning muhim tarkibiy qismi bo‘lib qoladi. Uning rivojlanishi nafaqat mavjud kiberxavflarga qarshi kurashishda, balki yangi avlod xavfsizlik tizimlarini shakllantirishda ham muhim rol o‘ynaydi. Shu sababli, VPN texnologiyalarini chuqur o‘rganish, ularni amaliyotga keng joriy etish va takomillashtirish zamonaviy axborot jamiyatining ustuvor vazifalaridan biri hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1. *Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. Pearson, 2021.*
2. *Tanenbaum A.S., Wetherall D.J. Computer Networks. Pearson, 2011.*
3. *Stallings W. Network Security Essentials. Pearson, 2017.*
4. *Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. Prentice Hall, 2002.*
5. *Rescorla E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley, 2001.*
6. *Frankel S., Krishnan S. IP Security (IPsec) and VPNs. Internet Engineering Task Force, 2011.*
7. *Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel. 2017.*
8. *OpenVPN Project Documentation. OpenVPN Technologies Inc., 2020.*
9. *RFC 4301. Security Architecture for the Internet Protocol. IETF, 2005.*
10. *RFC 5246. The Transport Layer Security (TLS) Protocol Version 1.2. IETF, 2008.*