

“VPN TARMOQLARI VA XAVFSIZLIK MEXANIZMLARI”

O'qituvchi: Komilov Abdulajon

Ishtirokchilar: Nurulloxujayev Inomxo'ja,

Xoldorov Bahodir, Valiyev Muhammadqodir

Annotatsiya: Ushbu maqoladan VPN (Virtual Private Network) tarmoqlarining mohiyati, ularning ishlash tamoyillari va axborot xavfsizligini ta'minlashdagi o'rni yoritiladi. VPN texnologiyalari ochiq tarmoqlar orqali uzatilayotgan ma'lumotlarni himoyalash, foydalanuvchi shaxsiyligini saqlash hamda masofaviy kirishni xavfsiz tashkil etish imkonini beradi. Shuningdek, VPN tarmoqlarida qo'llaniladigan asosiy xavfsizlik mexanizmlari — shifrlash algoritmlari, autentifikatsiya usullari, tunnellash protokollari va ma'lumotlar yaxlitligini ta'minlash vositalari tahlil qilinadi. Mavzu axborot xavfsizligini oshirishda VPN texnologiyalarining ahamiyatini ochib beradi.

Аннотация: В данной статье рассматривается сущность VPN (виртуальных частных сетей), принципы их работы и роль в обеспечении информационной безопасности. Технологии VPN позволяют защищать данные, передаваемые по открытым сетям, сохранять конфиденциальность пользователей и безопасно организовывать удаленный доступ. Также анализируются основные механизмы безопасности, используемые в сетях VPN: алгоритмы шифрования, методы аутентификации, протоколы туннелирования и инструменты обеспечения целостности данных. Тема раскрывает важность технологий VPN в повышении информационной безопасности.

Annotation: This article discusses the essence of VPN (Virtual Private Network) networks, their principles of operation and their role in ensuring information security. VPN technologies allow you to protect data transmitted over open networks, preserve user privacy, and securely organize remote access. The main security mechanisms used in VPN networks are also analyzed - encryption algorithms, authentication methods, tunneling protocols, and data integrity tools. The topic reveals the importance of VPN technologies in improving information security.

Kalit soʻzlar: VPN, Virtual Private Network, axborot xavfsizligi, shifrlash, autentifikatsiya, tunnelling, IPsec, SSL/TLS, maʼlumotlar yaxlitligi, maxfiylik..

Zamonaviy dunyo internet muhitida axborot xavfsizligi va maxfiyligi tobora dolzarb masalaga aylanmoqda. Foydalanuvchilar shaxsiy maʼlumotlarini himoya qilish, internetga erkin kirish va cheklovlarni chetlab oʻtish uchun turli texnologiyalardan foydalanishadi. Virtual Shaxsiy Tarmoq (VPN – Virtual Private Network) hisoblanadi. VPN texnologiyasi foydalanuvchining internetga ulanayotgan maʼlumotlarini shifrlab, uni maxfiy va xavfsiz holda uzatishga imkon beradi. Ushbu texnologiya orqali foydalanuvchi oʻzining haqiqiy IP-manzilini yashirish va boshqa mamlakatlardagi serverlar orqali internetga ulanish imkoniyatiga ega boʻladi. Bu esa nafaqat internetda shaxsiy hayotni himoya qilishga, balki ochiq Wi-Fi tarmoqlari orqali ulanishda maʼlumotlarning oʻgʻirlanishining oldini olishga ham yordam beradi. VPN texnologiyasining ishlash tamoyillari, uning asosiy turlari va foydalanuvchilarga taqdim etadigan afzalliklari haqida batafsil maʼlumot beriladi. VPN (Virtual Private Network) – bu internet orqali shifrlangan va xavfsiz aloqa kanalini taʼminlaydigan texnologiya boʻlib, u foydalanuvchilarga shaxsiy maʼlumotlarini himoya qilish, geo-cheklovlarni aylanib oʻtish va anonimlikni taʼminlash imkonini beradi. VPN yordamida foydalanuvchining internetga kirish faoliyati shifrlanadi va maxsus serverlar orqali yoʻnaltiriladi, bu esa uning haqiqiy IP-manzilini yashirish imkonini beradi. Trafikni shifrlash – VPN foydalanuvchining qurilmasidan internetga yuborilayotgan maʼlumotlarni shifrlaydi, bu esa maʼlumotlarni uchinchi shaxslar tomonidan kuzatilishining oldini oladi. Trafikni yoʻnaltirish – Maʼlumotlar VPN serveri orqali yoʻnaltiriladi, bu esa foydalanuvchining haqiqiy IP-manzilini yashirish va boshqa mamlakatdagi server orqali ulanishni taʼminlaydi. Internetga kirish – VPN orqali foydalanuvchi oʻz manzilini yashirib, internetga boshqa joylashuvdan kirayotgan kabi koʻrinadi. Bu esa geo-cheklovlarni aylanib oʻtishga imkon beradi.

Ulanish protokoliga koʻra 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 trafiginı 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.

Korporatsiyalar — bu katta hajmdagi korxonalar va kompaniyalar tomonidan yuritilayotgan biznes faoliyati bo'yicha, unda bir nechta bo'limlar, doimiy va keng biznesdagi mavjud. Korporativ biznesning maqsadi ko'pincha katta foyda, bozorda imkoniyatlarni qo'lga kiritish, va o'z qobiliyatini global darajada olishdir. Bu biznes turida yuqori boshqaruv, strategik qaror, va operatsion samaradorlik muhim o'rin tutadi. Korporativ biznesning asosiy harakatlari: Korporativ biznes ko'plab bo'limlar va yangilanishni o'z ichiga oladi. Bunda marketing, ishlab chiqarish, moliya, HR (inson resurslari), logistika, sotuvlar va boshqa bo'limlar mavjud. Har bir'lim o'zidan foydalanishni, lekin umumiy foydalanish uchun ular'zaro mumkin bo'lishi mumkin.

VPN xavfsizligi va shifrlash usullari: VPN texnologiyasida xavfsizlikni ta'minlash uchun ishlatiladigan shifrlash usullari va autentifikatsiya mexanizmlari haqida ko'plab tadqiqot ishlari mavjud. Bruce Schneier'ning "Applied Cryptography" kitobi shifrlash algoritmlari, VPN'da qo'llaniladigan AES-256, RSA, SHA-2 kabi xavfsizlik mexanizmlarini tahlil qiladi. IEEE Xplore va SpringerLink kabi ilmiy ma'lumotlar bazalarida VPN xavfsizligi bo'yicha qator maqolalar mavjud. Xususan, VPN texnologiyasining kiberxavfsizlikdagi roli, uning zaif tomonlari va potentsial hujum usullari (MITM – Man-in-the-Middle, DNS hijacking, IP leak) haqida ilmiy tahlillar keltirilgan. So'nggi yillarda VPN texnologiyasining rivojlanishi, uning biznes, ta'lim va

kundalik hayotda keng qo'llanilishi haqida qator tadqiqot ishlari olib borilgan. Gartner Research va Statista kabi tashkilotlarning tahliliy hisobotlarida VPN xizmatlarining bozordagi o'sishi va tendensiyalari yoritiladi. Shuningdek, "The Internet Freedom & Privacy Report" kabi tadqiqotlarda VPN texnologiyasining erkin internetga kirishdagi roli, davlat nazoratidan qochish va senzuralangan kontentga ulanish imkoniyatlari haqida batafsil ma'lumotlar keltirilgan. Shaxsiy VPN va tijorat VPN xizmatlari bo'yicha TechRadar, CNET, PCMag kabi texnologik portallarning sharhlari foydalanuvchilar uchun juda muhim. Ushbu saytlarda turli VPN xizmatlari, ularning tezligi, xavfsizligi, foydalanish qulayligi va narx-sifat nisbati tahlil qilinadi.

Masalan: ExpressVPN va NordVPN – eng xavfsiz va tezkor xizmatlar sifatida taqdim etiladi. ProtonVPN – maxfiylikka urg'u beradi, shifrlash darajasi yuqori. Bepul VPN xizmatlari – aksariyati ma'lumotlarni saqlashi yoki uchinchi tomonlarga sotishi mumkinligi ta'kidlanadi.

Xulosa

VPN texnologiyasining asosiy vazifalaridan biri internet trafigini shifrlash va IP-manzilni yashirish orqali foydalanuvchining shaxsiy hayotini himoya qilishdir. Internet-provayderlar, hukumat organlari yoki kiberjinoyatchilar foydalanuvchining qaysi veb-saytlarga tashrif buyurayotganini yoki qanday ma'lumotlar almashayotganini ko'ra olmaydi. Ayniqsa, ommaviy Wi-Fi tarmoqlarida VPN foydalanish muhim, chunki bunday tarmoqlarda kiberxavfsizlik tahdidlari yuqori bo'lishi mumkin. Shuningdek, VPN geo-checklovlarni chetlab o'tish imkoniyatini beradi. Masalan, ayrim davlatlarda ijtimoiy tarmoqlar yoki axborot saytlariga cheklovlar qo'yilgan bo'lsa, VPN yordamida foydalanuvchilar cheklangan resurslarga erkin kirishlari mumkin. Bundan tashqari, xalqaro video va musiqa platformalarida mavjud bo'lgan mintaqaviy cheklovlarni ham aylanib o'tish imkonini beradi.

VPN texnologiyasida xavfsizlik darajasi qo'llanilayotgan shifrlash usullariga bog'liq. Eng ishonchli VPN xizmatlari AES-256 shifrlash algoritmidan foydalanadi, bu esa zamonaviy hisoblash texnologiyalariga asoslangan hujumlarga bardosh bera oladigan

darajada kuchli. Bundan tashqari, VPN orqali ulanayotgan foydalanuvchilar turli protokollar yordamida internetga chiqadi. Masalan, OpenVPN, WireGuard va IPSec kabi protokollar yuqori darajadagi xavfsizlik va tezkor ishlash imkonini beradi. Bugungi kunda VPN texnologiyasi nafaqat oddiy foydalanuvchilar, balki korporativ bizneslar uchun ham juda muhim

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Кодиров, Ф. Э., and О. Д. Дониёров. "ЭФФЕКТИВНЫЕ МОДЕЛИ РАЗВИТИЯ МЕДИЦИНСКОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ КАШАКАДЬИНСКОЙ ОБЛАСТИ." Символ науки 7-2 (2022): 15-17.
2. Zoxidov, J. B., F. E. Qodirov, and I. J. Bozorova. "QUARTUS II PROJECT CONCEPT AND ITS OPPORTUNITIES AND PROBLEMS." АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕХНИЧЕСКОГО И ТЕХНОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ. 2019.
3. Uzakov, Gulom, et al. "Simulation of a tubular pyrolysis reactor using comsol multiphysics software." International Scientific and Practical Conference Digital and Information Technologies in Economics and Management. Cham: Springer Nature Switzerland, 2023.
4. Кодиров, Ф. "ЎУДУДУЛАРДА ТИББИЙ ХИЗМАТЛАРНИ ДАСТУРИЙ ПАКЕТЛАР ЁРДАМИДА ЭЛЕКТРОН ТИББИЙ БАЗАСИНИ ЯРАТИШ." О'zbekiston Respublikasi Oliy Va o'rta Maxsus ta'lim Vazirligi Namangan Muhandislik-Qurilish Instituti (2022).
5. Qodirov, F. E., O. D. Doniyorov, and H. Shokirov Sh. "Basic concepts of information security in information systems. Wide threats and their consequences." концепции устойчивого развития науки в современных условиях (2021): 153-155.