WI-FI TARMOQLARINING XAVFSIZLIGINI TA’MINLASH USULLARI VA ULARNING SAMARADORLIGINI TAHLIL QILISH

F. O‘.Toshboltayev
Farg‘ona davlat universiteti, Axborot texnologiyalari kafedrasi, katta o‘qituvchi, p.f.b.f.d.
E-mail: toshboltayevfaxriddin88@gmail.com
Abdusamadova Ma’sumaxon Abdulhamid qizi
Farg‘ona davlat universiteti talabasi
E-mail:abdusamatovamasumaxon1014@gmail.com
Husanova Shahloxon Zokirjon qizi
Farg‘ona davlat universiteti talabasi
E-mail:shahloxon821@gmail.com

Annotatsiya: ushbu maqolada simsiz (Wi-Fi) tarmoqlarning xavfsizligini ta’minlash muammolari, xavfsizlik protokollarining turlari hamda ularning ishlash mexanizmlari tahlil qilinadi. Maqolada WEP, WPA, WPA2 va WPA3 protokollarining afzallik va kamchiliklari solishtirib, ularning samaradorligi amaliy jihatdan yoritilgan. Tadqiqot natijalari asosida Wi-Fi tarmoqlarining himoya darajasini oshirish bo‘yicha takliflar ishlab chiqilgan.

Kalit so‘zlar: Wi-Fi, xavfsizlik, WEP, WPA, WPA2, WPA3, tarmoq himoyasi, autentifikatsiya, kriptografiya**.**

Аннотация: в данной статье рассматриваются проблемы обеспечения безопасности беспроводных (Wi-Fi) сетей, анализируются типы протоколов безопасности и механизмы их работы. В статье сравниваются преимущества и недостатки протоколов WEP, WPA, WPA2 и WPA3, а также приводится практический анализ их эффективности. На основе проведённых исследований разработаны предложения по повышению уровня защиты Wi-Fi сетей.

Ключевые слова: Wi-Fi, безопасность, WEP, WPA, WPA2, WPA3, защита сети, аутентификация, криптография

Abstract : this article examines the issues of ensuring the security of wireless (Wi-Fi) networks, analyzing the types of security protocols and their operating mechanisms. The advantages and disadvantages of WEP, WPA, WPA2, and WPA3 protocols are compared, and their effectiveness is analyzed in practice. Based on the research results, recommendations have been developed to enhance the protection level of Wi-Fi networks.

Keywords: Wi-Fi, security, WEP, WPA, WPA2, WPA3, network protection, authentication, cryptography

Kirish

ISSN 3030-3907

Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda simsiz aloqa tizimlarining ham keng qo‘llanilishi kuzatilmoqda. Wi-Fi texnologiyasi foydalanuvchilarga qulaylik yaratgan bo‘lsa-da, u orqali uzatilayotgan ma’lumotlarning xavfsizligi masalasi dolzarb bo‘lib qolmoqda. Bugungi kunda axborot tarmoqlariga nisbatan tahdidlar — parol o‘g‘irlash, ruxsatsiz kirish, “man-in-the-middle” (MITM) hujumlari, “sniffing” va “spoofing” kabi usullar orqali amalga oshirilmoqda. Shu sababli, Wi-Fi tarmoqlarini himoyalash mexanizmlarini chuqur o‘rganish va ularning samaradorligini tahlil qilish zamonaviy axborot xavfsizligi siyosatining muhim yo‘nalishidir

Adabiyotlar tahlili

IEEE 802.11 standarti Wi-Fi tarmoqlari uchun rasmiy texnik hujjat hisoblanadi. U simsiz tarmoqlarda ma’lumotlarni uzatish, autentifikatsiya va xavfsizlik protokollarini (WEP, WPA, WPA2, WPA3) batafsil yoritadi. Ushbu manba tarmoqlarni loyihalash va xavfsizlikni tashkil etishda asosiy qo‘llanma vazifasini bajaradi. Standartning kuchli tomonlari – rasmiy va ishonchli bo‘lishi, texnik detalni aniq taqdim etishi. Biroq, murakkabligi va texnik tili sababli yangi o‘quvchilar uchun tushunishi qiyin bo‘lishi mumkin.

Stallingsning kitobi tarmoq xavfsizligi nazariyasi va amaliyotini o‘zida jamlagan. Kitobda WEP, WPA/WPA2, WPA3 kabi xavfsizlik protokollarining ishlash prinsiplari, autentifikatsiya va kriptografiya asoslari batafsil tushuntiriladi. Bu manba nazariy bilimlarni amaliy misollar bilan boyitadi, protokollarni solishtirish imkonini beradi. Kamchilik sifatida, kitob Wi-Fi standartlarining texnik tafsilotlariga chuqur kirib bormaydi.

Wi-Fi Alliance hujjati WPA3 protokolining yangi imkoniyatlari va xavfsizlikni oshirish usullarini ko‘rsatadi. Bu manba amaliy qo‘llanma sifatida muhim bo‘lib, protokolni joriy etishdagi tavsiyalarni beradi. Cheklovlari shundaki, hujjat faqat WPA3 ga yo‘naltirilgan bo‘lib, eski standartlar bilan solishtirishni to‘liq o‘z ichiga olmaydi.

Tanenbaumning kitobi tarmoqlar nazariyasi va arxitekturasini keng yoritadi. OSI modelidan boshlab protokollar, xavfsizlik mexanizmlari va tarmoq loyihalashtirish prinsiplari tushuntiriladi. Nazariy jihatdan eng mukammal manbalardan biri bo‘lib, Wi-Fi xavfsizligini tushunishda tizimli yondashuvni ta’minlaydi. Biroq, zamonaviy Wi-Fi xavfsizligi bo‘yicha amaliy tavsiyalarni kamroq beradi.

Keltirilgan adabiyotlar bir-birini to‘ldiradi: IEEE 802.11 va Wi-Fi Alliance rasmiy va amaliy standartlar bilan, Stallings nazariy va amaliy tahlil bilan, Tanenbaum esa tarmoqlar nazariyasi va tizimli yondashuv bilan boyitadi. Shu manbalar asosida Wi-Fi xavfsizligi protokollari (WEP, WPA/WPA2, WPA3) samaradorligi, afzallik va kamchiliklari aniqlanadi. Ular tarmoq xavfsizligini

ISSN 3030-3907

ta’minlash va Wi-Fi tarmoqlarini loyihalash uchun zarur bo‘lgan ilmiy asosni beradi.

Tadqiqot metodologiyasi

Ushbu tadqiqotning metodologiyasi Wi-Fi tarmoqlarining xavfsizlik darajasini baholash, qo‘llaniladigan himoya protokollarining samaradorligini aniqlash hamda ularning amaliy qo‘llanish holatini tahlil qilishga qaratilgan. Tadqiqot jarayoni nazariy-analitik, solishtirma tahlil, eksperimental sinov va statistik baholash kabi ilmiy metodlar asosida amalga oshirildi.

Birinchidan, ilmiy adabiyotlar, xalqaro standartlar (IEEE 802.11), Wi-Fi Alliance tomonidan ishlab chiqilgan xavfsizlik me’yorlari hamda WEP, WPA, WPA2 va WPA3 protokollarining texnik hujjatlari o‘rganildi. Ushbu bosqichda nazariy tahlil va dokumental tahlil metodlari qo‘llanildi.

Ikkinchidan, Wi-Fi xavfsizlik protokollarining imkoniyatlari, zaifliklari va kriptografik mexanizmlari solishtirma tahlil metodi orqali taqqoslandi. Tarmoqni himoyalashda ishlatiladigan shifrlash algoritmlari (RC4, AES-CCMP, SAE) funksional jihatdan o‘rganilib, ularning himoya darajasi bo‘yicha ilmiy xulosalar ishlab chiqildi.

Uchinchidan, amaliy tajribalar o‘tkazilib, turli xavfsizlik protokollaridan foydalanadigan Wi-Fi tarmoqlariga hujumlar (packet sniffing, deauthentication attack, brute-force attack) simulyatsiya qilindi. Bu jarayonda eksperimental metod va penetratsion testlash elementlaridan foydalanildi. Olingan natijalar asosida har bir himoya turining real sharoitdagi samaradorligi baholandi.

To‘rtinchidan, tajriba natijalari qayta ishlanib, samaradorlik ko‘rsatkichlari — hujumga qarshi chidamlilik, shifrlash kuchi, autentifikatsiya mexanizmining barqarorligi va foydalanish qulayligi — statistik tahlil metodi orqali umumlashtirildi. Natijalar asosida Wi-Fi tarmoqlarida qaysi protokolning afzal ekanligi yuzasidan ilmiy xulosa chiqarildi.

Natijalar va ularning tahlili

Tadqiqot jarayonida Wi-Fi tarmoqlarining xavfsizligini ta’minlovchi WEP, WPA, WPA2 va WPA3 protokollarining texnik imkoniyatlari, ularning himoya darajasi, zaifliklari va amaliy sharoitdagi samaradorligi har tomonlama o‘rganildi. O‘tkazilgan eksperimental sinovlar va solishtirma tahlillar ushbu protokollar orasidagi farqlarni aniq ko‘rsatdi. WEP protokoli eng eski va zaif himoya vositasi ekani ma’lum bo‘ldi. RC4 shifrlash algoritmi, kalit uzunligining qisqaligi va ivning takrorlanishi tufayli paketlarni yig‘ish va tahlil qilish orqali tarmoqni bir necha daqiqada buzish mumkinligi tajribada tasdiqlandi. Shu sababli WEP zamonaviy Wi-Fi tarmoqlari uchun yaroqsiz hisoblanadi. WPA protokoli WEPga qaraganda yaxshiroq himoya taqdim etsa-da, TKIP algoritmidagi zaifliklar, paketlarni manipulyatsiya qilish imkoniyati va PSK kalitlarini topishga doir hujumlar uning

ISSN 3030-3907

samaradorligini cheklab qo‘yadi. Amaliy sinovlar WPA himoyasining hozirgi kunda yetarli emasligini ko‘rsatdi. WPA2 protokoli AES-CCMP shifrlashiga asoslangan bo‘lib, tajriba natijalarida yuqori darajadagi barqarorlik namoyish etdi. Biroq PSK kaliti murakkab bo‘lmagan holatlarda tarmoqka kirish xavfi ortishi qayd etildi. Shu bilan birga, WPA2-Enterprise rejimi korporativ tarmoqlar uchun yanada kuchli himoya ta’minlashi aniqlandi. Eng yuqori samaradorlik WPA3 protokolida kuzatildi. SAE autentifikatsiya mexanizmi offline brute-force hujumlarga imkon qoldirmadi, forward secrecy funksiyasi esa ma’lumotlarni qo‘shimcha himoya qildi. Tajribalar WPA3 protokolining amaliy jihatdan eng ishonchli himoya vositasi ekanini ko‘rsatdi.

Penetratsion testlar natijalarida Wi-Fi tarmoqlarining umumiy xavfsizligiga ta’sir qiluvchi omillar ham aniqlab olindi. Murakkab va uzun parollardan foydalanish, routerda faqat zamonaviy shifrlash protokollarini yoqish, tarmoqni segmentlarga ajratish, firmware yangilab borish va xavfsizlik siyosatini to‘g‘ri tashkil etish tarmoqni sezilarli darajada mustahkamlaydi. Shuningdek, MAC filtering yoki SSID yashirish kabi oddiy usullar real xavfsizlik darajasini kuchaytirmasligi amaliy sinovlarda tasdiqlandi.

Umuman olganda, tadqiqot natijalari shuni ko‘rsatadiki, Wi-Fi tarmoqlarida xavfsizlikni ta’minlashda asosiy rolni ishlatilayotgan shifrlash protokoli va autentifikatsiya mexanizmi bajaradi. WEP va WPA protokollari zamonaviy tahdidlar qarshisida zaif bo‘lsa, WPA2 nisbatan barqaror, WPA3 esa hozirda eng samarali va ishonchli himoya tizimi hisoblanadi. Tahlil qilingan ma’lumotlar Wi-Fi tarmoqlarining xavfsizligini oshirishda texnik chora-tadbirlarni to‘g‘ri tanlash hamda muntazam qo‘llash zarurligini ko‘rsatdi.

Xulosa

Wi-Fi tarmoqlarining xavfsizligini ta’minlash zamonaviy axborot infratuzilmasining ajralmas qismidir. Tahlillar shuni ko‘rsatadiki, eski protokollar (WEP, WPA) bugungi tahdidlar uchun yetarli emas. Shuning uchun foydalanuvchilar va tashkilotlar Wi-Fi tarmoqlarida WPA3 standartini qo‘llashlari, VPN texnologiyalaridan foydalanishlari va autentifikatsiya siyosatini kuchaytirishlari lozim. Bu nafaqat foydalanuvchi ma’lumotlarini himoya qiladi, balki milliy axborot xavfsizligi tizimini mustahkamlashga ham xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Coleman, D., Westcott, D. CWNA: Certified Wireless Network Administrator Study Guide. Sybex, 2020.
2. Wi-Fi Alliance. WPA3 Security Enhancements Overview, 2020.
3. Tanenbaum A. S. Computer Networks. 6th Edition, Pearson, 2021.
4. Cisco Systems. Wireless LAN Design Guide: 802.11ac and 802.11ax Best Practices, 2022.

ISSN 3030-3907

5. Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2022.

ISSN 3030-3907