SIMSIZ ALOQA TIZIMLARIDA AXBOROT RESURSLARINI HIMOYALASH: OCHIQ WI-FI TARMOQLARIDAGI XAVFLAR VA ULARDA MOLIYAVIY OPERATSIYALAR BAJARISHNING XATARLARI

Samarqand iqtisodiyot va servis instituti

"XALQARO IQTISODIY MUNOSABATLAR" fakulteti

Iqtisodiy xavfsizlik yo‘nalishi

IKX-123 4-KURS

Shodmonova Shahnozabonu Sayit qizi

+99894-104-31-75

shodmonovashahnozabonu04@gmail.com

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrasi asistenti

Rustamov Sherzod Norxudjayevich

Annotatsiya.

Maqolada simsiz aloqa tizimlarida axborot resurslarini himoyalash, ochiq Wi-Fi tarmoqlaridagi xavflar va ularda moliyaviy operatsiyalar bajarishning xatarlari tahlil qilingan. Mavzuning dolzarbligi raqamli to‘lovlar ko‘lamining kengayishi, kiberjinoyatlarning keskin o‘sishi va foydalanuvchilarning xavflarni yetarlicha anglamasligi bilan izohlanadi. Maqsad – ochiq Wi-Fi muhitidagi tahdidlar tasnifini ishlab chiqish, ularning moliyaviy xavfsizlikka ta’sirini baholash va himoya mexanizmlarini takomillashtirish bo‘yicha takliflar berishdir. Tadqiqotda normativ-huquqiy hujjatlar tahlili, qiyosiy-huquqiy usul, IEEE 802.11 protokollari va ilmiy adabiyotlarning tizimli tahlili hamda ochiq statistik ma’lumotlarni miqdoriy qayta hisoblash usullaridan foydalanildi. Natijada tahdidlarning uch qatlamli (kanal, tarmoq, ilova–foydalanuvchi) modeli asoslandi; shifrlash va autentifikatsiya alohida masalalar ekani, WPA3 va Enhanced Open ham soxta kirish nuqtasiga qarshi yagona yechim emasligi ko‘rsatildi; moliyaviy operatsiyalarni ochiq tarmoqda bajarmaslik, mobil tarmoqdan foydalanish va

ko‘p qatlamli himoyaga oid tavsiyalar hamda qonunchilikni takomillashtirish takliflari ishlab chiqildi. Olingan natijalar moliya tashkilotlari, tarmoq operatorlari, nazorat organlari, ta’lim muassasalari va fuqarolar uchun amaliy ahamiyat kasb etadi, shuningdek mavzu bo‘yicha keyingi tadqiqotlar uchun asos bo‘ladi.

Kalit so‘zlar: simsiz aloqa tizimlari, axborot xavfsizligi, ochiq Wi-Fi tarmoqlari, kiberxavfsizlik, soxta kirish nuqtasi hujumi, WPA3, moliyaviy operatsiyalar, elektron to‘lovlar, shaxsga doir ma’lumotlar, «o‘rtadagi odam» hujumi.

Abstract.

The article analyzes the protection of information resources in wireless communication systems, the risks of open Wi-Fi networks and the hazards of conducting financial transactions over them. Its relevance stems from the expanding scale of digital payments, the sharp growth of cybercrime and users’ insufficient awareness of risks. The aim is to develop a classification of threats in open Wi-Fi environments, assess their impact on financial security and propose improvements to protection mechanisms. The study uses analysis of legal acts, the comparative legal method, a systematic review of IEEE 802.11 protocols and scholarly literature, and quantitative recalculation of public statistics. A three-layer threat model (channel, network, application–user) is substantiated; encryption and authentication are shown to be separate problems, and WPA3 and Enhanced Open are not a sole remedy against rogue access points; recommendations on avoiding financial transactions over open networks, using mobile networks and multi-layered protection, as well as proposals for improving legislation, are developed.

Keywords: wireless communication systems, information security, open Wi-Fi networks, cybersecurity, evil twin attack, WPA3, financial transactions, electronic payments, personal data, man-in-the-middle attack.

KIRISH

Raqamlashtirish jarayonlarining jadallashuvi moliyaviy munosabatlarni tubdan o‘zgartirmoqda: bank xizmatlari, elektron to‘lovlar va davlat xizmatlari tobora ko‘proq

mobil qurilmalar orqali, simsiz aloqa vositasida amalga oshirilmoqda. Wi-Fi kafe, mehmonxona va aeroportlarda kundalik vositaga aylandi, biroq parolsiz yoki hamma biladigan parolli ommaviy tarmoqlar ma’lumotlarning uchinchi shaxslar qo‘liga tushish ehtimolini oshiradi. Shu bois axborot resurslarini simsiz muhitda himoyalash nafaqat texnik, balki ilmiy-huquqiy muammodir. Mavzuning dolzarbligi, avvalo, konstitutsiyaviy mohiyatga ega: O‘zbekiston Respublikasi Konstitutsiyasining 31-moddasida har bir inson shaxsiy hayotining daxlsizligi, shaxsiy va oilaviy sirga ega bo‘lish, o‘z sha’ni va qadr-qimmatini himoya qilish huquqiga ega ekanligi mustahkamlangan.[1] Ma’lumotning ushlab olinishi shaxsiy sirga tajovuz, moliyaviy operatsiyalarda esa mulkka tahdiddir.

Davlat siyosati darajasida ham mavzu ustuvor: Prezidentning 2022-yil 28-yanvardagi PF-60-son Farmoni bilan tasdiqlangan 2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi iqtisodiyot va ijtimoiy sohani raqamlashtirishni ustuvor yo‘nalish sifatida belgilagan,[2] raqamli transformatsiya esa xavfsizlik poydevorisiz barqaror bo‘lmaydi. Sohaning asosiy huquqiy asosini 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonun tashkil etadi: u 40 ta moddadan iborat bo‘lib, 2022-yil 17-iyuldan kuchga kirgan, kiberhujum va muhim axborot infratuzilmasi kabi tushunchalarni aniqlashtirgan, vakolatli organ sifatida Davlat xavfsizlik xizmatini belgilagan.[3] Foydalanuvchi ma’lumotlari 2019-yil 2-iyuldagi O‘RQ-547-sonli «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun bilan himoyalanadi: u subyekt, mulkdor va operator tushunchalarini hamda bazalarning davlat reyestrini belgilaydi.[4]

So‘nggi yillarda qabul qilingan hujjatlar orasida Prezidentning 2025-yil 30-apreldagi PQ-153-son qarori alohida o‘rin tutadi: unga ko‘ra Ichki ishlar vazirligi kiberjinoyatlarga

[1] O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahrir), 31-modda. – Lex.uz

[2] O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son Farmoni «2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida». – Lex.uz

[3] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – Lex.uz

[4] O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-sonli «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. – Lex.uz

qarshi kurash bo‘yicha vakolatli organ etib belgilangan, mijozlarning moliyaviy xavfsizligini ta’minlash banklar va to‘lov tashkilotlarining ustuvor vazifasi deb e’tirof etilgan, o‘z nomidagi bank kartasi, SIM-kartasi yoki hamyonini kiberjinoyatda foydalanishga qo‘ygan shaxslar uchun javobgarlik, shuningdek axborot xavfsizligi talablariga rioya etmagan tashkilotlar hisobidan zararni undirish tartibi nazarda tutilgan.[5] Jinoiy-huquqiy himoya Jinoyat kodeksining XX bobidagi 278^1–278^6-moddalari hamda firibgarlikka oid 168-modda orqali ta’minlanadi.[6]

Shunga qaramay, biz ko‘rib chiqqan ochiq manbalarda ochiq Wi-Fi tarmoqlari alohida xavf manbai sifatida tizimli o‘rganilmagan, kiberjinoyatlar statistikasida ularning ulushi ajratib ko‘rsatilmagan. Maqsad – ochiq Wi-Fi tarmoqlaridagi xavflar tasnifini ishlab chiqish va moliyaviy operatsiyalar xatarlarini baholab, ularni kamaytirish bo‘yicha takliflarni asoslashdir. Ilmiy yangilik – xavflarni kanal, tarmoq va ilova–foydalanuvchi qatlamlariga ajratuvchi model hamda moliyaviy xavf asosan texnik zaiflikdan ko‘ra ijtimoiy-texnik omillar bilan belgilanadi, degan ishchi gipotezaning asoslanishidir.

Simsiz tarmoqlarni himoyalash tarixi – himoya va hujum usullari o‘rtasidagi uzluksiz raqobat tarixi. IEEE 802.11 standartidagi dastlabki WEP mexanizmi tez orada buzilgan; WPA2 uzoq vaqt asosiy standart bo‘lib qoldi, biroq Vanhoef va Piessens (2017) KRACK hujumlarida to‘rt bosqichli qo‘l siqish jarayonida kalitni qayta o‘rnatishga majburlash orqali nonce qiymati takrorlanishi, bu esa trafikni deshifrlash yoki o‘zgartirish imkonini berishini isbotladi.[7] 2018-yilda joriy etilgan WPA3 SAE protokoli orqali oflayn lug‘at hujumlariga chidamlilikni va oldinga yo‘naltirilgan maxfiylikni ta’minladi, ammo Vanhoef va Ronen «Dragonblood» tadqiqotida yon kanal oqishlari hamda WPA2/WPA3

[5] O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son qarori «Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida» (mazmuni Anhor.uz materiali orqali tahlil qilindi)

[6] O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr): Maxsus qism, XX bob (278^1–278^6-moddalar), 168-modda. – Lex.uz

[7] Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS ’17). – New York: ACM, 2017. – P. 1313–1328.

aralash rejimida quyi versiyaga o‘tkazish hujumlarini ko‘rsatdi.[8] Halbouni va hammualliflarning 36 ta maqola tizimli sharhi WPA3 avvalgilaridan ustun, biroq hal etilmagan zaifliklar saqlanishini ko‘rsatgan.[9] Demak, himoya ko‘p qatlamli bo‘lishi lozim.

Ochiq Wi-Fi bu yutuqlardan to‘liq foydalana olmaydi. Klassik ochiq tarmoqda autentifikatsiya yo‘q va kadrlar kanal darajasida shifrlanmaydi, shuning uchun radio qamrovidagi oddiy adapter paketlarni ushlab olishi mumkin; umumiy parolli WPA2-Personal tarmog‘ida esa parolni bilgan va qo‘l siqishni kuzatgan shaxs boshqa foydalanuvchining seans kalitlarini hisoblay oladi. Buni yumshatish uchun RFC 8110 hujjatida Opportunistic Wireless Encryption (OWE) taklif etilgan: Diffie–Hellman almashinuvi orqali har bir qurilma uchun alohida kalit hosil qilinadi va parolsiz tarmoqda ham kanal shifrlanadi.[10] Biroq OWE kirish nuqtasining haqiqiyligini tasdiqlamaydi: passiv tinglash qiyinlashadi, lekin soxta kirish nuqtasiga ulanish xavfi saqlanadi. Tarmoq nomi (SSID) noyob identifikator emas va qurilmalar oldin ulangan nomni avtomatik tanib ulanadi, shuning uchun shifrlash va autentifikatsiya bir narsa emas, ochiq muhitda ishonch esa tashkiliy vositalar (xodim tasdig‘i) orqali o‘rnatilishi kerak.

Shu asosda tahdidlarning uch qatlamli tasnifini taklif etamiz. Kanal qatlamida passiv tinglash, himoyalanmagan boshqaruv kadrlari orqali ulanishni uzish va «soxta egizak» (evil twin) turidagi soxta kirish nuqtalari asosiy xavf. Tarmoq qatlamida ARP/DNS soxtalashtirish va fishing vositasiga aylantirilgan «captive portal» sahifalari xavfli. Ilova va foydalanuvchi qatlamida hujum shifrlangan seansga emas, foydalanuvchi qaroriga qaratiladi: Marlinspike ommalashtirgan SSL stripping HTTPS ga o‘tishni yashirincha

[8] Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // 2020 IEEE Symposium on Security and Privacy (SP). – IEEE, 2020. – P. 517–533.

[9] Halbouni A. et al. Wireless Security Protocols WPA3: A Systematic Literature Review // IEEE Access. – 2023. – Vol. 11. – P. 112438–112450.

[10] Harkins D., Kumari W. Opportunistic Wireless Encryption. RFC 8110. – Internet Engineering Task Force (IETF), March 2017. – https://www.rfc-editor.org/info/rfc8110

HTTP ga tushirib ma’lumotni ochiq matnda ushlab olishga imkon bergan,[11] HSTS va TLS 1.3 buni kamaytiradi, ammo foydalanuvchi soxta portalga ma’lumot kiritsa, texnik himoya yordam bermaydi.

Inson omili ham hal qiluvchi: Klasnja va hammualliflar odamlar ochiq Wi-Fi xavflarini cheklangan anglashini ko‘rsatgan.[12] Moliyaviy operatsiyalarda xatar yuqori: hujumchi karta rekvizitlari, kirish ma’lumotlari va bir martalik kodlarni olib, mablag‘ni to‘g‘ridan-to‘g‘ri o‘zlashtira oladi. PCI DSS 4.0 standarti ochiq jamoat tarmoqlari orqali uzatiladigan karta ma’lumotlarini himoyalash uchun kuchli kriptografiya talab qiladi;[13] biroq kuchli autentifikatsiya ham mutlaq kafolat emas: IIV ma’lumotlariga ko‘ra, O‘zbekistonda bank kartalari bilan bog‘liq jinoyatlarning bir qismi aldov yo‘li bilan SMS-tasdiqlash kodini olish orqali sodir etiladi, ya’ni ikkinchi omil ham ijtimoiy muhandislik oldida zaif.[14]

Statistika muammo miqyosini ko‘rsatadi, biroq e’lon qilingan raqamlar kiberjinoyatlarni umumiy holda aks ettiradi va Wi-Fi vektorini ajratmaydi. Ommaviy axborot vositalari huquqni muhofaza qilish organlariga tayanib, 2019-yilda 863 ta, 2024-yilda esa 58 800 ta kiberjinoyat qayd etilganini xabar qilgan.[15] O‘sish koeffitsiyenti 58 800 : 863 ≈ 68,1, o‘rtacha yillik o‘sish ≈ 2,33 barobar (muallif hisobi). IIV ma’lumotiga ko‘ra, jinoyatlarning 98 foizi bank kartalari bilan bog‘liq, 1 trillion 909 milliard so‘mdan ortiq mablag‘ talon-taroj qilingan; zararli havola va dastur yuborish 60 foiz, aldov bilan SMS-kod olish 16 foizni tashkil etgan. Demak, jinoyatlarning asosiy qismi foydalanuvchi harakati orqali, ya’ni ilova–foydalanuvchi qatlamida amalga oshadi; soxta kirish nuqtasi

[11] Marlinspike M. New Tricks for Defeating SSL in Practice // Black Hat DC. – 2009.

[12] Klasnja P., Consolvo S., Jung J. et al. “When I Am on Wi-Fi, I Am Fearless”: Privacy Concerns and Practices in Everyday Wi-Fi Use // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’09). – New York: ACM, 2009. – P. 1993–2002.

[13] PCI SSC. PCI DSS: Requirements and Testing Procedures, v4.0. – 2022. – Req. 4.2.1.

[14] IIV Kiberxavfsizlik markazi press-tur materiallari, 2025-yil 29-may. – gov.uz/oz/iiv/news/view/57775

[15] O‘zbekistonliklar so‘nggi besh yilda kiberfiribgarliklarga 159 million dollar yo‘qotgan // Zamin.uz, 2025-yil 3-noyabr.

va captive portal esa aynan shu fishing usullarini jinoyatchi nazorat qiladigan muhitda yetkazib beradi. Shu bois ochiq Wi-Fi mustaqil xavf manbai emas, balki firibgarlik samaradorligini oshiruvchi omil sifatida baholanadi; bu gipoteza Wi-Fi vektorini ajratuvchi statistika bilan tasdiqlanishi kerak.

Xalqaro tajribada Budapesht konvensiyasi (2001) noqonuniy kirish, noqonuniy ushlab olish va kompyuter vositasida firibgarlikni jinoyat deb kvalifikatsiya qilishni talab qilgan;[16] bu JK 278^2, 278^6 va 168-moddalar mantiqiga yaqin. Jinoiy javobgarlik hujumdan keyin ishlaydi, profilaktikani esa PQ-153 kuchaytirdi; ochiq Wi-Fi operatorlari uchun minimal xavfsizlik talablariga oid aniq normani aniqlay olmadik. Himoya uch darajada quriladi: foydalanuvchi moliyaviy operatsiyalarni ochiq tarmoqda bajarmaydi va mobil operator tarmog‘idan foydalanadi (VPN ishonchni provayderga ko‘chiradi, soxta portal oldidagi qaror xatosini bartaraf etmaydi), avtomatik ulanishni o‘chiradi; operator mijozlarni izolyatsiya qiladi, WPA3 yoki OWE va PMF ni joriy etadi; banklar xavfga asoslangan autentifikatsiya va g‘ayrioddiy tranzaksiyalarni aniqlashni qo‘llaydi.

XULOSA

Tadqiqot quyidagi xulosalarga olib keldi. Birinchidan, protokollar WEPdan WPA3 gacha takomillashgan bo‘lsa-da, har biri zaifliklarga duch kelgan, shuning uchun himoya ko‘p qatlamli bo‘lishi shart. Ikkinchidan, ochiq tarmoqda shifrlash va autentifikatsiya alohida masalalar: OWE passiv tinglashga qarshi samarali, lekin soxta kirish nuqtasini bartaraf etmaydi. Uchinchidan, uch qatlamli model xavflarni tizimlashtirib, choralarni qatlamlarga bog‘laydi. To‘rtinchidan, O‘zbekistonda kiberjinoyatlar 2019–2024-yillarda 863 tadan 58 800 tagacha o‘sgani va asosiy qismi bank kartalari bilan bog‘liqligi moliyaviy xavfsizlikni milliy ustuvorlikka aylantiradi; ochiq Wi-Fi fishing samaradorligini oshiruvchi muhit sifatida qaralishi mumkin, biroq bu maxsus statistika bilan tasdiqlanishi lozim.

[16] Convention on Cybercrime. ETS No. 185. – Budapest, 2001.

Mualliflik takliflari: ochiq Wi-Fi operatorlari uchun minimal xavfsizlik talablarini idoraviy hujjat bilan belgilash; IIV va Markaziy bank statistikasida jinoyat sodir etilgan tarmoq turini ajratish; SMS-kodlardan ilova yoki apparat tasdiqlashiga bosqichma-bosqich o‘tish; raqamli gigiyena dasturlarini kengaytirish. Fuqarolar uchun asosiy qoida: to‘lovlarni ochiq Wi-Fi orqali bajarmaslik.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahrir), 31-modda. – Lex.uz

2. O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son Farmoni «2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida». – Lex.uz

3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – Lex.uz

4. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-sonli «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. – Lex.uz

5. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son qarori «Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida» (mazmuni Anhor.uz materiali orqali tahlil qilindi)

6. O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr): Maxsus qism, XX bob (278^{1}–278^{6}-moddalar), 168-modda. – Lex.uz

7. Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS ’17). – New York: ACM, 2017. – P. 1313–1328.

8. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // 2020 IEEE Symposium on Security and Privacy (SP). – IEEE, 2020. – P. 517–533.

9. Halbouni A. et al. Wireless Security Protocols WPA3: A Systematic Literature Review // IEEE Access. – 2023. – Vol. 11. – P. 112438–112450.

10. Harkins D., Kumari W. Opportunistic Wireless Encryption. RFC 8110. – Internet Engineering Task Force (IETF), March 2017. – https://www.rfc-editor.org/info/rfc8110

11. Marlinspike M. New Tricks for Defeating SSL in Practice // Black Hat DC. – 2009.

12. Klasnja P., Consolvo S., Jung J. et al. “When I Am on Wi-Fi, I Am Fearless”: Privacy Concerns and Practices in Everyday Wi-Fi Use // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’09). – New York: ACM, 2009. – P. 1993–2002.

13. PCI SSC. PCI DSS: Requirements and Testing Procedures, v4.0. – 2022. – Req. 4.2.1.

14. IIV Kiberxavfsizlik markazi press-tur materiallari, 2025-yil 29-may. – gov.uz/oz/iiv/news/view/57775

15. O‘zbekistonliklar so‘nggi besh yilda kiberfiribgarliklarga 159 million dollar yo‘qotgan // Zamin.uz, 2025-yil 3-noyabr.

16. Convention on Cybercrime. ETS No. 185. – Budapest, 2001.