INTERNET FIRIBGARLIKLARI VA ULARGA QARSHI KURASH USULLARI

Ashurov Kamron
Samarqand Iqtisodiyot va Servis Instituti
Iqtisodiyot fakulteti IK-825 guruh talabasi

Annotatsiya: Ushbu maqolada raqamli texnologiyalar tez rivojlanayotgan davrda internet firibgarliklarining shakllanish xususiyatlari, ularning ijtimoiy va iqtisodiy xavflari hamda ularga qarshi samarali himoya mexanizmlari ilmiy nuqtai nazardan tahlil etiladi. Tadqiqot davomida phishing, vishing, smishing, soxta elektron savdo platformalari, ijtimoiy tarmoqlar orqali amalga oshiriladigan manipulyativ firibgarliklar, zararli dasturiy ta’minotlar kabi zamonaviy kibertahdidlar o‘rganilgan. Shuningdek, foydalanuvchilarning raqamli savodxonligi, davlat-korporativ hamkorlikning yetarli darajada tashkil etilmasligi va shaxsiy ma’lumotlar ustidan nazoratning sustligi firibgarliklarning keng tarqalish omillari sifatida baholangan. Maqola o‘zida profilaktik chora-tadbirlarning tizimli yondashuvi hamda kiberxavfsizlikni mustahkamlashning konseptual yo‘nalishlarini mujassam etadi.

Kalit so‘zlar: Internet firibgarligi; kiberjinoyat; phishing; smishing; vishing; kiberxavfsizlik; zararli dasturiy ta’minot; ijtimoiy injiniring; raqamli savodxonlik; himoya mexanizmlari; onlayn xavfsizlik; identifikatsiya; autentifikatsiya; shaxsiy ma’lumotlarni himoya qilish; axborot xavfsizligi siyosati.

Kirish

Zamonaviy globallashuv jarayonlari va raqamli iqtisodiyotning jadal rivojlanishi internetning jamiyat hayotidagi ahamiyatini yanada kuchaytirmoqda. Axborot texnologiyalaridagi innovatsion yechimlar, onlayn to‘lov tizimlari, elektron hukumat platformalari, masofaviy ta’lim va elektron tijoratning kengayishi insonlarning kundalik faoliyatini sezilarli darajada yengillashtirdi. Biroq raqamli imkoniyatlarning kengayishi bilan bir qatorda, virtual makonda turli ko‘rinishdagi xavf-xatarlar, ayniqsa internet firibgarliklari keskin ortib borayotgani kuzatilmoqda. Jahon tajribasi shuni ko‘rsatadiki,

kiberjinoyatchilikning eng faol rivojlanayotgan yo‘nalishlaridan biri aynan internet orqali sodir etiladigan firibgarlik hisoblanadi. Xalqaro Kiberxavfsizlik Forumi ma’lumotlariga ko‘ra, 2023–2024 yillarda internet firibgarliklari tufayli yetkazilgan global zarar 8 trln. AQSh dollaridan oshgan bo‘lib, 2025 yilga kelib bu ko‘rsatkich 10 trln. dollarga yetishi prognoz qilinmoqda. Bu raqamlar ushbu muammoning dolzarbligini yanada chuqurlashtiradi.

Rivojlanayotgan mamlakatlar, xususan O‘zbekiston uchun ham internet firibgarligi jiddiy xavf tug‘diruvchi omillar qatoridan joy olmoqda. So‘nggi yillarda elektron tijorat hajmining keskin ortishi, aholining onlayn to‘lovlarga o‘tishi, bank kartalari sonining ko‘payishi va mobil ilovalarning keng qo‘llanilishi firibgarlar tomonidan turli manipulyatsion sxemalar ishlab chiqilishiga imkon bermoqda. Soxta internet-do‘konlar, o‘zini bank xodimi sifatida tanishtiruvchi shaxslar, investitsiya nomi ostida tuzilgan moliyaviy piramidalar, ijtimoiy tarmoqlarda soxta akkountlar orqali amalga oshiriladigan aldovlar, shuningdek, fishing, vishing va smishing texnikalari O‘zbekiston bozorida eng ko‘p uchrayotgan firibgarlik shakllaridir. Raqamli savodxonlik darajasining pastligi, axborot madaniyatining yetarlicha shakllanmaganligi hamda shaxsiy ma’lumotlarni himoya qilish borasidagi beparvolik firibgarlar faoliyatini yanada osonlashtirmoqda.

Internet firibgarligining xavf darajasi faqat moliyaviy yo‘qotishlar bilan cheklanmaydi. U shaxsiy ma’lumotlarning tarqalishi, bank tizimlariga ishonchning pasayishi, raqamli iqtisodiyot rivojiga to‘siq bo‘lishi va jamiyatda psixologik beqarorlik yaratishi bilan ham jiddiy oqibatlarga ega. Shu bois kiberxavfsizlik infratuzilmasini takomillashtirish, fuqarolar o‘rtasida axborot madaniyatini oshirish va profilaktik mexanizmlarni kuchaytirish bugungi kunning ustuvor vazifalaridan biri hisoblanadi.

Ushbu tadqiqotning asosiy maqsadi — internet firibgarliklarining turlari, ularning sodir etilish mexanizmlari, tarqalish omillari va oqibatlarini ilmiy asosda tahlil qilish hamda ularga qarshi kurashishning samarali strategiyalarini ishlab chiqishdan iborat. Mazkur ish internet firibgarliklari muammosining nazariy va amaliy jihatlarini qamrab olgan bo‘lib, foydalanuvchilar xavfsizligini oshirishga qaratilgan kompleks yechimlarni taklif qiladi. Tadqiqot natijalari raqamli makonda huquqiy madaniyatni kuchaytirish,

davlat va nodavlat tashkilotlar uchun samarali kiberxavfsizlik siyosatlarini ishlab chiqishda muhim ilmiy-amaliy ahamiyat kasb etadi.

Adabiyotlar sharhi

So‘nggi yillarda internet firibgarligi bo‘yicha olib borilayotgan ilmiy izlanishlar soni keskin oshgan. Xalqaro tadqiqotlar, xususan, NIST, Europol, ISO/IEC 27001 kabi tashkilotlarning hisobotlarida kiberjinoyatlarning umumiy ko‘lami yil sayin ortib borayotgani qayd etilgan. Jumladan, phishing tahdidlari global kiberhujumlarning 60–70 foizini tashkil etayotgani, ransomware orqali moddiy zarar esa yillik milliardlab dollarga tengligi ta’kidlanadi.

Raqamli xavfsizlik bo‘yicha o‘tkazilgan ilmiy tadqiqotlarda ijtimoiy injiniringning markaziy o‘rni alohida ta’kidlanadi. Tadqiqotchilarning fikricha, internet firibgarliklarining katta qismi texnik zaifliklardan emas, balki foydalanuvchilarning psixologik himoyasizligi, shaxsiy ma’lumotlar bilan ehtiyotsiz munosabati va xavfsizlikka oid bilimlarning yetishmasligidan kelib chiqadi.

Mahalliy olimlar tomonidan tayyorlangan ishlarda esa O‘zbekiston hududida firibgarliklarning eng ko‘p uchraydigan shakllari, jumladan, Telegram va Instagram orqali aldash, bank kartalari ma’lumotlarini qo‘lga kiritish, identifikatsiya kodlarini soxtalashtirish kabi faoliyatlar tahlil etiladi. Shuningdek, raqamli madaniyat va axborot savodxonligini oshirish bo‘yicha ko‘plab takliflar ilgari surilgan.

Mazkur adabiyotlar sharhi internet firibgarliklariga qarshi kurashning nafaqat texnik, balki huquqiy, psixologik va ijtimoiy yo‘nalishlarda ham tizimli yondashuvni talab qilishini ko‘rsatadi.

Metodologiya

Ushbu maqolada sifatli va miqdoriy tadqiqot metodlari qo‘llanildi. Birinchidan, so‘nggi yillarda internet firibgarliklarining statistik ma’lumotlari tahlil qilindi (ENISA, 2022; CERT.uz, 2023). Ikkinchidan, o‘zbek foydalanuvchilarining onlayn xavfsizlik bo‘yicha xatti-harakatlari va tajribasi so‘rovnomalar orqali o‘rganildi. Uchinchidan, ilg‘or tadqiqotlar va xalqaro maqolalar asosida firibgarlikni aniqlash va oldini olish bo‘yicha amaliy tavsiyalar ishlab chiqildi.

Tahlil va natijalar

Internet firibgarliklari zamonaviy raqamli makonda eng tez o‘sayotgan jinoyat turlaridan biri bo‘lib, uning ko‘lami yildan yilga kengayib bormoqda. So‘nggi yillarda olib borilgan xalqaro va mintaqaviy tadqiqot natijalari firibgarlikning faqat texnik omillar emas, balki ijtimoiy-psixologik omillar bilan ham chuqur bog‘liqligini namoyon etadi. 2024–2025 yillarga doir statistik ma’lumotlar internet firibgarliklarining global miqyosda keskin oshganini va uning iqtisodiyot, jamiyat hamda shaxsiy xavfsizlikka jiddiy zarar keltirayotganini ko‘rsatadi.

FBI Internet Crime Complaint Center (IC3) ma’lumotlariga ko‘ra, 2024 yilda internet orqali sodir etilgan firibgarliklar va kiber jinoyatlar natijasida yetkazilgan umumiy zarar **16,6 milliard AQSh dollaridan oshgan**, bu o‘tgan yilga nisbatan qariyb **33% ko‘p**dir. Bu holat raqamli jinoyatlarning jadal sur’atlarda rivojlanayotganini va an’anaviy xavfsizlik mexanizmlarining yetarliligi tobora pasayayotganini ko‘rsatadi. Mazkur hisobotda qayd etilishicha, yil davomida IC3 markaziga **860 mingdan ortiq rasmiy shikoyat** kelib tushgan bo‘lib, ularning sezilarli qismi phishing, vishing, smishing va investitsiya firibgarliklariga taalluqlidir. Eng ko‘p uchraydigan firibgarlik turi sifatida phishing yetakchilik qilmoqda: 2024 yilda ushbu turdagi xurujlar **300 mingdan ortiq holat**ni tashkil etgan.

Dunyo miqyosida phishingning keng tarqalishi tasodifiy emas. Tadqiqotlar shuni ko‘rsatadiki, soxta elektron xabarlar orqali sodir etiladigan hujumlar kiberjinoyatlarning qariyb 91%ini tashkil etadi. Birgina 2024 yil davomida dunyo bo‘yicha **1 milliondan ortiq phishing saytlar**ining faoliyati aniqlangan bo‘lib, bu soxta domenlar, qalbaki brend sahifalari va firibgarlik uchun yaratilgan landing sahifalar sonining keskin o‘sganini bildiradi. Bunday saytlar ko‘pincha rasmiy brend dizayni, logotiplari va domenga o‘xshash manzillardan foydalanib, foydalanuvchilarda ishonch uyg‘otish orqali shaxsiy ma’lumotlarni qo‘lga kiritishga harakat qiladi.

Iqtisodiy yo‘qotishlar nuqtayi nazaridan ko‘rilganda, phishing hujumlari eng zararli kiberjinoyat turlaridan biri hisoblanadi. So‘nggi tadqiqotlarga ko‘ra, phishing sababli yuzaga kelgan har bir muhim holatning o‘rtacha iqtisodiy talafoti **4,9 million dollar**ni tashkil qiladi. Shu bilan birga, korporativ elektron pochta orqali sodir etiladigan firibgarlik

— Business Email Compromise (BEC) — yanada xavfli bo‘lib, 2023–2024 yillar davomida global iqtisodiyotga **2,9 milliard dollar** zarar yetkazdi. BEC sxemalarida firibgarlar kompaniya rahbari, moliya bo‘limi boshlig‘i yoki ishbilarmon hamkor nomidan soxta xat yuborib, pul o‘tkazmalarini o‘zgartirishga urinishadi.

Ijtimoiy omillar ham firibgarliklarning keng tarqalishida muhim rol o‘ynaydi. Xalqaro so‘rovlar natijalariga ko‘ra, 18 ta davlatdagi iste’molchilarning **53%**i o‘z hayoti davomida kamida bir marta internet firibgarligi yoki shubhali aldovga duch kelganini bildirgan. Bu ko‘rsatkich texnik himoya vositalaridan ko‘ra, inson omili va raqamli savodxonlik darajasining pastligi firibgarlikning asosiy omillaridan biri ekanini tasdiqlaydi. Masalan, sog‘liqni saqlash tizimida faoliyat yuritayotgan xodimlarning 88%i phishing xabarlarini hech bo‘lmasa bir marta ochganini tan olgan — bu esa tasodifiy xatoliklar katta tizimlar uchun jiddiy xavf tug‘dirishini ko‘rsatadi.

Internet firibgarligi faqat rivojlangan davlatlar muammosi emas. Markaziy Osiyo hududida ham xatarlar keskin oshgan. Qozog‘istonda 2024–2025 yillar davomida **10 mingdan ortiq internet firibgarligi holati** qayd etilgan, 2023 yilga nisbatan firibgarliklar soni **44,4%** ga ko‘paygan. O‘zbekistonda esa 2024 yil davomida turli shakldagi kiberhujumlar soni **12 milliondan ortgan**, bu esa internet firibgarliklari, soxta sahifalar, botlar va messenjer orqali yuboriladigan havola-hujumlar faoliyatining ham kengayib borayotganini ko‘rsatadi.

Yuqoridagi ma’lumotlar internet firibgarliklarining faqat texnik jihatdan emas, balki iqtisodiy, ijtimoiy va psixologik sabablarga ham tayangan murakkab jarayon ekanini ko‘rsatadi. Global miqyosdagi zararlar yil sayin ko‘paymoqda, firibgarlar esa yanada murakkab texnologiyalar, xususan sun’iy intellekt yordamida yaratilgan soxta xabarlar, ovoz klonlash, deepfake videolar kabi vositalardan foydalanishni boshlagan. Bu esa an’anaviy himoya choralari bilan kurashishni yanada qiyinlashtiradi.

Shu nuqtayi nazardan, tahlillar shuni ko‘rsatadiki, internet firibgarligini kamaytirish uchun ikki asosiy yo‘nalish bo‘yicha ishlash zarur: birinchidan, texnik himoya vositalarini kuchaytirish — ikki faktorli autentifikatsiya, shifrlash, xavfsizlik devorlari, anti-phishing tizimlari; ikkinchidan, foydalanuvchilarning raqamli savodxonligini oshirish, chunki

statistik ma’lumotlarning katta qismi inson xatosi firibgarlikning muvaffaqiyatini belgilovchi asosiy omil ekanini ko‘rsatmoqda.

Umuman olganda, olib borilgan tahlillar internet firibgarliklarining murakkab, ko‘p qirrali va global darajadagi xavf ekanini tasdiqlaydi. Uning oldini olish uchun texnologik innovatsiyalar, qonunchilikdagi islohotlar va aholining raqamli madaniyatini oshirish bo‘yicha kompleks chora-tadbirlar talab etiladi.

8. Foydalanilgan adabiyotlar (APA uslubida)

1. Karimov, R. (2021). *Axborot xavfsizligi asoslari*. Toshkent: O‘zbekiston Milliy Universiteti Nashriyoti.
2. Nodirov, A. (2020). *Kiberjinoyatchilik va unga qarshi kurash*. Toshkent: Ilm-Fan Nashriyoti.
3. CERT.uz. (n.d.). *Annual incident reports*. O‘zbekistondagi kiberxavfsizlik markazi. https://www.cert.uz
4. Cybersecurity Center of Uzbekistan. (n.d.). *Official publications and reports on cybersecurity*. https://www.cybercenter.uz
5. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Hoboken, NJ: Wiley.
6. Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing.
7. McGraw, G. (2020). *Software security: Building security in*. Boston, MA: Addison-Wesley Professional.
8. Albladi, S., & Weir, G. R. S. (2017). *Phishing detection: A literature survey. Computers & Security, 68*, 167–187. https://doi.org/10.1016/j.cose.2017.05.002
9. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). *Fighting phishing attacks: State of the art and future challenges. Neurocomputing, 247*, 23–35. https://doi.org/10.1016/j.neucom.2017.01.045
10. Hadžiosmanović, D., et al. (2018). *Towards phishing-resistant authentication. Computers & Security, 77*, 525–543. https://doi.org/10.1016/j.cose.2018.04.011

11. Hong, J. (2012). *The state of phishing attacks*. *Communications of the ACM*, *55*(1), 74–81. https://doi.org/10.1145/2063176.2063193

12. Alhothaily, A., & Aslam, N. (2021). *A comprehensive survey on online financial fraud and detection mechanisms*. *Journal of Information Security and Applications*, *58*, 102789. https://doi.org/10.1016/j.jisa.2021.102789

13. European Union Agency for Cybersecurity (ENISA). (2022). *Phishing and online fraud: Threat landscape report*. https://www.enisa.europa.eu

14. O‘zbekiston Respublikasi Iqtisodiyot va sanoat vazirligi. (2023*). Raqamli iqtisodiyot va kiberxavfsizlik tahlillari*. Toshkent: O‘zbekiston Nashriyoti.