O‘ZBEKISTONDA KIBERJINOYATCHILIK PROFILAKTIKASIDA AHOLI KIBERXAVFSIZLIK MADANIYATINING ROLI

Urinkulov Odiljon Naziraliyevich

O‘zbekiston Respublikasi IIV Akademiyasi
E-mail: ourinkulov@gmail.com
ORCID: 0000-0003-2392-9309

K E Y W O R D S

kiberjinoyatchilik, kiberxavfsizlik madaniyati, raqamli savodxonlik, kiberfiribgarlik, phishing, profilaktika

A B S T R A C T

Mazkur maqolada O‘zbekiston Respublikasida kiberjinoyatchilikning oldini olishda aholining kiberxavfsizlik madaniyatini oshirishning ilmiy-amaliy ahamiyati tadqiq etiladi. Raqamli xizmatlar, mobil banking, elektron to‘lovlar va ijtimoiy tarmoqlardan foydalanish ko‘lamining kengayishi fuqarolar uchun qulaylik yaratish bilan birga, kiberfiribgarlik, phishing, zararli havolalar, soxta mobil ilovalar, shaxsiy ma’lumotlarni qo‘lga kiritish va ijtimoiy muhandislikka asoslangan jinoyatlar xavfini ham kuchaytirmoqda. Tadqiqotning asosiy maqsadi kiberjinoyatchilik oqibatlarini bartaraf etishdan ko‘ra, uning oldini olishda fuqarolarning kiberxavfsizlik bo‘yicha bilim, ko‘nikma va xulq-atvorini shakllantirish samaraliroq ekanligini asoslashdan iborat.

Kirish. Raqamli texnologiyalarning jamiyat hayotiga chuqur kirib borishi fuqarolarning bank, davlat xizmatlari, savdo, aloqa va ta’lim xizmatlaridan masofaviy foydalanish imkoniyatlarini kengaytirdi. Shu bilan birga, fuqarolarning shaxsiy ma’lumotlari, bank karta rekvizitlari va raqamli identifikatsiya vositalariga nisbatan tahdidlar kuchaydi. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunida kiberjinoyatchilik axborotni egallash, o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi sifatida izohlanadi.

O‘zbekistonda 2024-yilda milliy internet segmentida 12 milliondan ortiq kiberhujum urinishlari qayd etilgan, firibgarlik holatlari esa 2023-yilga nisbatan 34 foizga oshgani xabar qilingan. To‘lov kartalari bilan bog‘liq firibgarlik shikoyatlari barcha firibgarlik murojaatlarining taxminan 35 foizini tashkil qilgan. Bundan tashqari, 2024-yilning birinchi choragida UzCERT monitoringi davomida milliy internet segmentida 3 290 860 dan ortiq kiberhujum qayd etilgan, 70 ta zaiflik aniqlanib bartaraf etilgan va 369 660 dan ortiq kibertahdid bo‘yicha tegishli tashkilotlarga axborot yuborilgan.

Mazkur holat kiberjinoyatchilikka qarshi kurashda faqat texnik vositalar, huquqiy javobgarlik yoki tergov harakatlari yetarli emasligini ko‘rsatadi. Chunki ko‘plab kiberfiribgarlik holatlarida jinoyatchi texnik himoyani buzishdan ko‘ra, foydalanuvchining ishonchi, shoshqaloqligi yoki bilim yetishmasligidan foydalanadi. Xalqaro tadqiqotlarda ham kiberxavfsizlik bilimlari va xabardorlik darajasi fuqarolarning xavfsiz xulq-atvorini shakllantirishda muhim omil ekani ko‘rsatilgan.

Adabiyotlar tahlili. So‘nggi yillardagi ilmiy adabiyotlar kiberjinoyatchilikni oldini olishda uch asosiy yondashuvni ajratib ko‘rsatadi: texnik himoya, huquqiy-profilaktik choralar va inson omiliga asoslangan kiberxavfsizlik madaniyati. Ho, Ko va Mazerolle tomonidan olib borilgan tizimli tahlilda situatsion jinoyatchilik profilaktikasi kiberjinoyatlarga ham tatbiq etilishi, bunda jinoyat

(cc) BY

sodir etish imkoniyatini kamaytirish muhimligi qayd etilgan.

Kiberxavfsizlik bo‘yicha treninglar haqidagi tizimli tahlilda 16 771 ta dastlabki manbadan saralash orqali trening metodlari o‘rganilgan va ta’lim shakllari — video, matn, muhokama, o‘yinlashtirish, amaliy simulyatsiya kabi yondashuvlar — foydalanuvchi xatti-harakatiga turlicha ta’sir qilishi ko‘rsatilgan. Kiberxavfsizlik madaniyati bo‘yicha tezkor dalillar tahlilida esa 1 768 ta yozuvdan 59 ta tadqiqot yakuniy tahlilga kiritilgan va kiberxavfsizlik madaniyati faqat texnik masala emas, balki boshqaruv, xulq-atvor va tashkiliy qo‘llab-quvvatlash bilan bog‘liq jarayon ekani ta’kidlangan.

1-jadval. Adabiyotlar tahlili

Muallif / manba	**Metod**	**Asosiy xulosa**	**Maqolamizga ahamiyati**
Ho, Ko & Mazerolle, 2022	Tizimli sharh	Kiberjinoyatni profilaktika qilishda imkoniyatni kamaytirish muhim	Profilaktik model asoslanadi
Rohan va boshq., 2023	SLR	Axborot xavfsizligi xabardorligini o‘lchash shkalalari muhim	So‘rovnoma indikatorlari uchun asos
Lee & Chua, 2024	Empirik tahlil	Bilim va xabardorlik xulq-atvorga ta’sir qiladi	Aholi savodxonligi gipotezasini qo‘llab-quvvatlaydi
Prümmer va boshq., 2024	SLR	Trening metodlari turlicha samaradorlikka ega	Interaktiv o‘quv modelini asoslaydi
Sutton & Tompson, 2025	Rapid evidence review	Kiberxavfsizlik madaniyati ijtimoiy-boshqaruviy omil	“Madaniyat” tushunchasini kengaytiradi
Howell va boshq., 2024	Eksperimental/psixologik yondashuv	Cyber hygiene qaror qabul qilish bilan bog‘liq	Fuqarolar xulq-atvoriga ta’sir mexanizmini ko‘rsatadi

O‘zbekiston sharoitida kiberjinoyatchilikning texnik-huquqiy jihatlari bo‘yicha muhokamalar mavjud bo‘lsa-da, aholining yosh, raqamli tajriba, bank xizmatlaridan foydalanish darajasi va kiberxavfsizlik xulq-atvoriga moslashtirilgan profilaktik model yetarli darajada ishlab chiqilmagan.

Taklif etilayotgan profilaktik model. Kelgusida kiberjinoyatchilikning qurboniga aylanib qolmaslik va yangi turdagi firibgarliklarni erta aniqlay olish uchun quyidagi jarayonlarni amalga oshiruvchi profilaktik model taklif etiladi:

- Aholi kiberxavfsizlik bilim darajasini dastlabki baholash;
- Xavf guruhlarini aniqlash: yoshi kattalar, mobil bankingdan yangi foydalanuvchilar, raqamli savodxonligi past fuqarolar;
- Har bir guruh uchun moslashtirilgan o‘quv modullarini ishlab chiqish;
- Banklar, davlat xizmatlari va mahalla tizimi orqali ogohlantirish mexanizmini joriy qilish;
- Interaktiv test va real kiberfiribgarlik ssenariylari orqali bilimni mustahkamlash;
- O‘quvdan oldingi va keyingi natijalarni solishtirish;
- Kiberxavfsizlik madaniyati indeksini hisoblash.

(cc) BY

Muhokama. O‘zbekistonda kiberhujumlar va kiberfiribgarliklar ko‘lami ortib bormoqda. 2024-yilda mamlakatda 12 milliondan ortiq kiberhujum urinishlari qayd etilgan, bu 2023-yildagi 11 million ko‘rsatkichdan yuqori. 2024-yil birinchi choragida milliy internet segmentida 3 290 860 dan ortiq kiberhujum qayd etilgan, 19 ta davlat organi va tashkiloti veb-resurslarida 70 ta zaiflik aniqlanib bartaraf etilgan. Ochiq xabarlarga ko‘ra, 2024-yilda O‘zbekistonda kiberjinoyatlar soni 2023-yilga nisbatan 9,1 barobarga oshgan, 2019-yilda 863 ta kiberjinoyat qayd etilgan bo‘lsa, 2024-yilda bu ko‘rsatkich 58,8 mingtaga yetgan. Bank kartalari bilan bog‘liq kiberjinoyatlar asosiy xavf omili sifatida ajralib turadi: ochiq manbalarda kiberjinoyatlarning 98 foizi bank kartalari orqali sodir etilgani, 60 foizi zararli havola va dasturlar orqali karta yoki mobil qurilma boshqaruvini qo‘lga kiritish bilan bog‘liqligi keltirilgan. O‘zbekiston Respublikasining 2026–2030-yillarga mo‘ljallangan kiberxavfsizlik strategiyasida fuqarolar, xususiy sektor va davlatning raqamli xavfsizlik darajasini oshirish, kiberjinoyatchilikka qarshi faol kurashish va raqamli kriminalistika imkoniyatlarini kuchaytirish strategik vazifalar sifatida belgilangan.

Natijalar kiberjinoyatchilikning oldini olishda texnik himoya choralaridan tashqari, aholining kiberxavfsizlik madaniyatini oshirish zarurligini ko‘rsatadi. O‘zbekistonda bank kartalari va mobil ilovalar bilan bog‘liq firibgarliklarning ulushi yuqori bo‘lgani fuqarolarning raqamli moliyaviy xavfsizlik bo‘yicha amaliy bilimlarini kuchaytirishni talab qiladi. Ayniqsa, zararli havolalar, APK fayllar, SMS-kodlarni qo‘lga kiritish, soxta bank xodimi yoki davlat tashkiloti nomidan qo‘ng‘iroq qilish kabi ijtimoiy muhandislik usullari inson omili bilan bevosita bog‘liq.

Xalqaro tadqiqotlarda ham kiberxavfsizlik xabardorligi foydalanuvchining xavfsiz xulq-atvori bilan bog‘liq ekani qayd etiladi. Lee va Chua tadqiqotida kiberxavfsizlik bilimi va xabardorlik darajasi fuqarolarning kiberxavfsizlik niyati va xatti-harakatiga ta’sir qiluvchi omil sifatida tahlil qilingan. Prümmer va hammualliflar esa kiberxavfsizlik treninglari samaradorligi ularning shakli, davomiyligi, foydalanuvchiga moslashtirilgani va xatti-harakatga yo‘naltirilganligi bilan bog‘liq ekanini ko‘rsatadi.

O‘zbekiston sharoitida kiberxavfsizlik madaniyatini oshirish bo‘yicha umumiy ma’ruzalar yoki ogohlantirishlar yetarli bo‘lmasligi mumkin. Chunki yoshi katta fuqarolar, mobil bankingdan yangi foydalanuvchilar, talabalar, tadbirkorlar va davlat xizmatlaridan faol foydalanuvchilarning xavf profili bir xil emas. Shu sababli profilaktik mexanizm segmentlangan, interaktiv, doimiy yangilanadigan va real firibgarlik ssenariylariga asoslangan bo‘lishi kerak.

Xulosa

Tadqiqot natijalari O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashda aholining kiberxavfsizlik madaniyatini oshirish strategik ahamiyatga ega ekanini ko‘rsatadi. Kiberjinoyatlar ko‘lamining ortishi, bank kartalari orqali sodir etilayotgan firibgarliklarning yuqori ulushi va zararli havolalar hamda ijtimoiy muhandislik usullarining keng qo‘llanishi profilaktika choralarini kuchaytirishni talab qiladi.

Maqolaning asosiy ilmiy xulosasi shundan iboratki, kiberjinoyatchilikning oldini olishda faqat texnik himoya, huquqiy javobgarlik yoki tergov choralariga tayanish yetarli emas. Fuqarolarning raqamli savodxonligi, shubhali axborotni farqlash qobiliyati, bank karta ma’lumotlarini himoya qilish ko‘nikmasi va kiberhodisa yuz berganda to‘g‘ri harakat qilish madaniyati kompleks profilaktik tizimning ajralmas qismi bo‘lishi kerak.

Tadqiqotning amaliy ahamiyati aholining turli guruhlari uchun moslashtirilgan kiberxavfsizlik o‘quv modullari, ogohlantiruvchi axborot platformalari va bank-davlat xizmatlari bilan integratsiyalashgan profilaktik mexanizm ishlab chiqish zarurligini asoslashdan iborat. Tadqiqotning cheklovi shundaki, hozirgi bosqichda empirik so‘rovnoma va eksperimental o‘quv natijalari kiritilmagan. Kelgusida respondentlar ishtirokida kiberxavfsizlik madaniyati indeksini ishlab chiqish va o‘quvdan oldingi hamda keyingi natijalarni statistik solishtirish tavsiya etiladi.

(cc) BY

Foydalanilgan dabiyotlar ro'yxati

1. Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security, 115*, 102611. https://doi.org/10.1016/j.cose.2022.102611
2. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234
3. Lee, C. S., & Chua, Y. T. (2024). The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States. *Crime & Delinquency, 70*(9). https://doi.org/10.1177/00111287231180093
4. Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585. https://doi.org/10.1016/j.cose.2023.103585
5. Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, 148*, 104110. https://doi.org/10.1016/j.cose.2024.104110
6. Mutlutürk, M., Wynn, M., & Metin, B. (2024). Phishing and the human factor: Insights from a bibliometric analysis. *Information, 15*(10), 643. https://doi.org/10.3390/info15100643
7. Howell, C., Maimon, D., Muniz, C., Kamar, E., & Berenblum, T. (2024). Engaging in cyber hygiene: The role of thoughtful decision-making and informational interventions. *Frontiers in Psychology, 15*, 1372681. https://doi.org/10.3389/fpsyg.2024.1372681
8. Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614. https://doi.org/10.1016/j.compind.2022.103614
9. Frauenstein, E. D., Flowerday, S., Mishi, S., & Warkentin, M. (2023). Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing Model. *Information & Management, 60*, 103858. https://doi.org/10.1016/j.im.2023.103858
10. Bognar, L., & Bottyan, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588. https://doi.org/10.3390/educsci14060588
11. Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education. *Education and Information Technologies, 29*, 3699–3727. https://doi.org/10.1007/s10639-023-11973-5
12. Kävrestad, J., Burvall, F., & Nohlberg, M. (2024). A taxonomy of factors that contribute to organizational cybersecurity awareness. *Information and Computer Security, 33*(3). https://doi.org/10.1108/ICS-11-2023-0209
13. Sur, A., DeLiema, M., Vock, D. M., & Boyle, P. (2023). A microsimulation of well-being and literacy interventions to reduce scam susceptibility in older adults. *Journal of Applied Gerontology, 42*(12), 2360–2370. https://doi.org/10.1177/07334648231196850
14. INTERPOL. (2024). *Be Cyber Aware / Think Twice campaign materials*. INTERPOL.
15. O'zbekiston Respublikasi. (2022). *Kiberxavfsizlik to'g'risida: O'RQ-764-son Qonun*. Lex.uz.
16. O'zbekiston Respublikasi Prezidenti. (2026). *O'zbekiston Respublikasining 2026–2030-yillarga mo'ljallangan kiberxavfsizlik strategiyasi*. Prezident farmoni PF–38-son.
17. Abdullayev, Murodjon. Urinkulov, Odiljon. "Analysis Of Cybersecurity Issues In Social Networks." TLEP–International Journal of Multidiscipline 2.5 (2025): 164-167.

(cc) BY