ISSN: 3030-3346

O‘ZBEKISTONDA KIBERJINOYATCHILIK PROFILAKTIKASIDA AHOLINING KIBERXAVFSIZLIK MADANIYATINI BAHOLASHNING KONSEPTUAL-METODIK MODELI

Iminov Abdurasul Abdulatipovich[1], O‘rinkulov Odiljon Naziraliyevich[1]

[1]O‘zbekiston Respublikasi IIV Akademiyasi
E-mail: ourinkulov@gmail.com
https://orcid.org/0000-0003-2392-9309

K E Y W O R D S

kiberxavfsizlik madaniyati, kiber gigiyena, kiberjinoyatchilik profilaktikasi, phishing xabardorligi, ijtimoiy muhandislik, inson omili, raqamli savodxonlik

A B S T R A C T

Raqamli xizmatlar, onlayn to‘lovlar, elektron hukumat platformalari va ijtimoiy tarmoqlardan foydalanish kengaygani sari kiberjinoyatchilik profilaktikasida inson omili hal qiluvchi ahamiyat kasb etmoqda. Maqolaning maqsadi O‘zbekiston sharoitida aholining kiberxavfsizlik madaniyatini baholashga xizmat qiluvchi konseptual-metodik modelni ishlab chiqishdan iborat. Tadqiqotda normativ-huquqiy tahlil, ilmiy adabiyotlarni tizimli tahlil qilish, komparativ yondashuv va indikatorli modellashtirish usullaridan foydalanildi. Natijada kiberxavfsizlik xabardorligi, parol va autentifikatsiya madaniyati, phishing va ijtimoiy muhandislikni aniqlash, shaxsiy ma’lumotlarni himoya qilish, qurilma-ilova gigiyenasi, xavfli onlayn xatti-harakatlardan qochish hamda kiberhodisaga javob berish ko‘nikmalarini birlashtiruvchi Kiberxavfsizlik madaniyati indeksi taklif etildi. Model profilaktik ta’lim, segmentlangan treninglar va monitoring tizimini dalillarga asoslangan tarzda tashkil etish imkonini beradi. Maqolaning ilmiy yangiligi kiberxavfsizlik madaniyatini faqat nazariy xabardorlik emas, balki bilim, ko‘nikma, xavf idroki va amaliy xulq-atvor uyg‘unligi sifatida baholash mezonlarini taklif etishidadir.

KIRISH.

Raqamli transformatsiya jarayoni davlat xizmatlari, moliyaviy operatsiyalar, ta’lim, sog‘liqni saqlash va kundalik kommunikatsiyalarni onlayn muhitga ko‘chirmoqda. Bu jarayon xizmatlardan foydalanish qulayligini oshiradi, biroq foydalanuvchilarning shaxsiy ma’lumotlari, moliyaviy resurslari va raqamli identifikatsiyasi bilan bog‘liq xavflarni ham kuchaytiradi. Xalqaro amaliyotda kiberxavfsizlik faqat texnik infratuzilma masalasi emas, balki foydalanuvchi xulq-atvori, xabardorlik darajasi va xavfsiz odatlarga bog‘liq kompleks muammo sifatida qaraladi [2; 3].

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni kiberxavfsizlik sohasidagi munosabatlarni tartibga solish, kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilish hamda yagona davlat siyosatini shakllantirish uchun muhim huquqiy asos yaratdi [1]. Biroq huquqiy bazaning mavjudligi foydalanuvchilarning real kiber gigiyena ko‘nikmalari yetarli degani emas. Kiberjinoyatchilikning ko‘plab shakllari, ayniqsa

(cc) BY

ISSN: 3030-3346

phishing[1], smishing[2], vishing[3] va boshqa ijtimoiy muhandislik usullari, aynan insonning ishonchi, e'tiborsizligi yoki xavfni noto'g'ri baholashidan foydalanadi [3].

Muammoning dolzarbligi shundaki, O'zbekiston sharoitida aholining kiberxavfsizlik madaniyatini tizimli o'lchash, xavfli raqamli xatti-harakatlarni aniqlash va profilaktik ta'limni dalillarga asoslangan holda rejalashtirish bo'yicha metodik yondashuvlar yetarli darajada shakllanmagan. Shu bois ushbu maqolada kiberxavfsizlik madaniyatini baholash uchun indikatorlar tizimi va profilaktik ta'lim modeli ishlab chiqiladi.

Tadqiqotning maqsadi — O'zbekiston foydalanuvchilari orasida kiberxavfsizlik madaniyatini baholashga, zaif xulq-atvor omillarini aniqlashga va kiberjinoyatchilik profilaktikasini kuchaytirishga xizmat qiluvchi konseptual-metodik modelni taklif etishdan iborat.

Tadqiqot vazifalari quyidagilardan iborat: kiberxavfsizlik madaniyati tushunchasining ilmiy mazmunini aniqlash; inson omiliga oid mavjud yondashuvlarni tahlil qilish; baholash indikatorlarini ishlab chiqish; indekslash formulasini taklif etish; profilaktik ta'lim modelining bosqichlarini asoslash; modelning ilmiy-amaliy ahamiyatini ko'rsatish.

ADABIYOTLAR TAHLILI VA NAZARIY ASOS.

Kiberxavfsizlik xulq-atvorini o'rganishda inson omili, kiberxavfsizlikdan xabardorlik, himoyani rag'batlantirish nazariyasi (PMT), rejalashtirilgan xatti-harakatlar nazariyasi (TPB), fishing bo'yicha trening va kibergigiyena yo'nalishlari muhim o'rin tutadi. Tadqiqotlarda foydalanuvchining xavfni idrok etishi, himoyalanish samaradorligiga ishonchi, o'zini himoya qila olishiga bo'lgan ishonchi va xavfsiz harakat qilish niyati kiberxavfsizlik xulq-atvorini shakllantiruvchi asosiy omillar sifatida talqin qilinadi [5; 6; 7].

Taherdoost kiberxavfsizlik xabardorligi va trening modellari bo'yicha tadqiqotlarni tahlil qilib, faqat ma'lumot berishga asoslangan yondashuvlar har doim ham barqaror xulq-atvor o'zgarishini ta'minlamasligini ko'rsatadi [8]. Prümmer, van Steen va van den Berg esa trening metodlarining samaradorligi kontekst, motivatsiya, takroriy mashq va real vaziyatga yaqin ssenariylar bilan bog'liq ekanini ta'kidlaydi [9].

Phishingga qarshi tayyorgarlik bo'yicha tadqiqotlar foydalanuvchilarga real xabarlarga o'xshash topshiriqlar berish, xatolarni darhol tushuntirish va o'quv jarayonini takroriy tashkil etish samarali ekanini ko'rsatadi [10-12]. Shu bilan birga, generativ sun'iy intellektning rivojlanishi phishing xabarlarining grammatik, vizual va psixologik jihatdan yanada ishonarli bo'lishiga olib kelmoqda [13]. Demak, kiberxavfsizlik madaniyati statik bilim emas, balki doimiy yangilanadigan kompetensiya sifatida shakllantirilishi kerak.

Xalqaro elektr aloqa ittifoqi Global Cybersecurity Index metodologiyasida davlatlarning kiberxavfsizlik salohiyatini huquqiy, texnik, tashkiliy, salohiyatni rivojlantirish va hamkorlik mezonlari asosida baholaydi [2]. Bu yondashuv makro darajadagi milliy tayyorgarlikni o'lchasa, ushbu maqolada taklif etilayotgan model mikro darajada — foydalanuvchi xulq-atvori va kiber gigiyena amaliyotlarini baholashga qaratiladi.

TADQIQOT METODOLOGIYASI.

[1] Phishing — foydalanuvchini aldash orqali uning login-paroli, bank karta ma'lumotlari, SMS-kodlari yoki boshqa maxfiy axborotlarini qo'lga kiritishga qaratilgan kiberfiribgarlik usuli. Odatda soxta veb-sayt, elektron pochta yoki xabar orqali amalga oshiriladi.

[2] Smishing — SMS yoki messenjer xabarlari orqali amalga oshiriladigan phishing turi. Bunda foydalanuvchiga soxta havola, yolg'on ogohlantirish yoki "mukofot", "hisob bloklanadi", "kodni yuboring" kabi xabarlar yuborilib, maxfiy ma'lumotlarni olishga urinish bo'ladi.

[3] Vishing — telefon qo'ng'iroqlari orqali amalga oshiriladigan phishing turi. Firibgar o'zini bank xodimi, davlat tashkiloti vakili yoki texnik yordam mutaxassisi sifatida tanishtirib, foydalanuvchidan parol, karta raqami, SMS-kod yoki boshqa shaxsiy ma'lumotlarni olishga harakat qiladi.

(cc) BY

ISSN: 3030-3346

Maqola konseptual-metodik tadqiqot sifatida ishlab chiqildi. Unda empirik so‘rov natijalari taqdim etilmaydi; asosiy e’tibor kiberxavfsizlik madaniyatini o‘lchash uchun indikatorlar tizimini shakllantirish va kelgusidagi empirik tadqiqotlar uchun metodik asos yaratishga qaratildi.

Tadqiqotda quyidagi usullar qo‘llanildi: normativ-huquqiy tahlil — O‘zbekiston Respublikasining kiberxavfsizlikka oid huquqiy asoslarini o‘rganish; ilmiy adabiyotlarni tizimli tahlil qilish — cybersecurity awareness, phishing training, PMT, TPB va human factor yo‘nalishidagi tadqiqotlarni umumlashtirish; komparativ tahlil — xalqaro indekslar va amaliy yondashuvlarni mahalliy kontekst bilan solishtirish; indikatorli modellashtirish — kiberxavfsizlik madaniyatini baholovchi komponentlar va ularga og‘irlik koeffitsiyentlarini belgilash.

Modelni amaliy sinovdan o‘tkazishda kelgusida respondentlar bo‘yicha so‘rovnoma, phishingni aniqlash topshiriqlari, ssenariy asosidagi testlar, 2FA ishlatish holati, parol boshqaruvi amaliyoti va kiberhodisaga javob berish ko‘nikmalari bo‘yicha ma’lumotlar yig‘ilishi tavsiya etiladi. Shunday qilib, taklif etilayotgan model nazariy asoslangan indikatorlar majmuasi sifatida keyingi empirik tekshiruvlarga tayyor metodik konstruktsiya hisoblanadi.

KIBERXAVFSIZLIK MADANIYATI TUSHUNCHASI VA BAHOLASH MEZONLARI.

Ushbu tadqiqotda kiberxavfsizlik madaniyati foydalanuvchining kibermakondagi xavflarni tushunishi, xavfsiz raqamli xulq-atvorni ongli ravishda tanlashi, shaxsiy va moliyaviy ma’lumotlarni himoya qilishi, ijtimoiy muhandislik belgilarini aniqlashi hamda kiberhodisa yuz berganda to‘g‘ri harakat qila olishini ifodalovchi integratsiyalashgan kompetensiyalar tizimi sifatida talqin qilinadi.

Bu ta’rif kiberxavfsizlik madaniyatini faqat “bilim darajasi” bilan cheklamaydi. Chunki foydalanuvchi phishing nima ekanini nazariy bilishi mumkin, ammo real vaziyatda shoshilinchlik, qo‘rquv, rasmiylik yoki manfaat va’dasi orqali manipulyatsiyaga uchrashi mumkin. Shuning uchun baholash tizimi bilim, ko‘nikma, xavf idroki va amaliy odatlarni birgalikda qamrab olishi lozim.

Kiberxavfsizlik madaniyatini o‘lchash uchun Kiberxavfsizlik madaniyati indeksi (KMI) taklif etiladi. Indeks 0 dan 100 ballgacha bo‘lgan integral ko‘rsatkich sifatida hisoblanadi. Umumiy formula quyidagicha ifodalanadi:

$$KMI = \sum_{i=1}^{n} W_i * I_i$$

Bunda,

KMI— kiberxavfsizlik madaniyati indeksi, W_i — indikatorning og‘irlik koeffitsiyenti, I_i — indikator bo‘yicha 0–100 oralig‘idagi baho, KMI— indikatorlar soni, n — indikatorlar soni, i — indikatorlar tartib raqami.

Indikatorlar og‘irligi xavf darajasi, foydalanuvchi xulq-atvoriga ta’siri va kiberjinoyatchilik profilaktikasidagi amaliy ahamiyatidan kelib chiqib belgilanadi. Jadvalda modelning asosiy komponentlari keltirilgan.

1-jadval.

Kiberxavfsizlik madaniyati indeksining asosiy indikatorlari

№	Indikator	Mazmuni	Baholash usuli	Og‘irlik
1	Xabardorlik	Asosiy tahdidlar, xavfsizlik qoidalari va huquqiy mas’uliyatni bilish	Test va so‘rovnoma	15%
2	Parol va autentifikatsiya madaniyati	Kuchli parol, parolni takrorlamaslik, 2FA/MFAdan foydalanish	Amaliy savollar, o‘zini baholash	15%

(cc) BY

ISSN: 3030-3346

№	Indikator	Mazmuni	Baholash usuli	Og‘irlik
3	Phishing va ijtimoiy muhandislikni aniqlash	Soxta havola, domen, shoshilinchlik, manipulyativ xabar belgilarini topish	Ssenariy va topshiriq	20%
4	Shaxsiy ma’lumotlarni himoya qilish	Bank karta, SMS-kod, pasport va akkaunt ma’lumotlarini ehtiyot qilish	Vaziyatli savollar	15%
5	Qurilma va ilova gigiyenasi	Yangilanish, antivirus, ruxsatlar, rasmiy manbadan yuklash	Checklist va test	10%
6	Xavfli xatti-harakatlardan qochish	Shubhali fayl/havola, pirat dastur, noma’lum Wi-Fi, ortiqcha ulashishdan saqlanish	So‘rov va ssenariy	10%
7	Kiberhodisaga javob berish	Hisob buzilganda parolni almashtirish, bankka murojaat qilish, dalillarni saqlash	Vaziyatli test	10%
8	Uzluksiz o‘rganish	Yangi tahdidlar haqida xabardor bo‘lish va xavfsizlik sozlamalarini yangilash	So‘rovnoma	5%

PROFILAKTIK TA’LIM MODELI.

Taklif etilayotgan KMI baholash modeli faqat diagnostika vositasi emas, balki kiberjinoyatchilik profilaktikasi uchun amaliy boshqaruv mexanizmi hamdir. Model asosida foydalanuvchilar xavf profili bo‘yicha segmentlanadi, ularga mos trening mazmuni tanlanadi va treningdan keyingi o‘zgarishlar qayta baholanadi.

Profilaktik ta’lim modeli besh bosqichdan iborat: dastlabki diagnostika, xavf bo‘yicha segmentlash, moslashtirilgan o‘quv modullari, amaliy simulyatsiya va natijani qayta o‘lchash. Bunday yondashuv umumiy ma’ruzadan ko‘ra samaraliroq, chunki u foydalanuvchining real zaif tomonini aniqlaydi va o‘quv jarayonini shu ehtiyojga yo‘naltiradi.

2-jadval.

Kiberxavfsizlik madaniyatini oshirish bo‘yicha profilaktik ta’lim modeli

Bosqich	Mazmuni	Vositalar	Kutiladigan natija
1. Diagnostika	Foydalanuvchining KMI bo‘yicha boshlang‘ich darajasini aniqlash	Test, so‘rovnoma, phishing topshirig‘i	Zaif indikatorlar aniqlanadi
2. Segmentlash	Yosh, kasb, platforma, raqamli tajriba va xavf profilini ajratish	Klasterlash yoki oddiy guruhlash	Maqsadli auditoriya belgilanadi

(cc) BY

ISSN: 3030-3346

Bosqich	Mazmuni	Vositalar	Kutiladigan natija
3. O‘qitish	Parol, 2FA, phishing, shaxsiy ma’lumotlar va mobil xavfsizlik modullari	Mikrodars, video, infografika	Bilim va motivatsiya oshadi
4. Simulyatsiya	Real hayotga yaqin xabar, havola va firibgarlik ssenariylarini yechish	Phishing simulation, case-study	Amaliy qaror qabul qilish ko‘nikmasi shakllanadi
5. Monitoring	Treningdan keyingi KMI o‘zgarishini o‘lchash va dasturlarni yangilash	Qayta test, statistik tahlil	Profilaktika natijasi baholanadi

MUHOKAMA.

Taklif etilayotgan modelning asosiy afzalligi shundaki, u kiberxavfsizlik madaniyatini keng va noaniq tushuncha sifatida emas, balki o‘lchanadigan indikatorlar majmuasi sifatida talqin qiladi. Bu davlat organlari, ta’lim muassasalari, bank sektori va raqamli xizmat ko‘rsatuvchi tashkilotlarga profilaktik ishlarni dalillarga asoslangan tarzda rejalashtirish imkonini beradi.

Modeldan foydalanishda auditoriyani bir xil guruh sifatida qabul qilish metodik xato bo‘ladi. Yoshlar, katta yoshdagi foydalanuvchilar, davlat xizmatchilari, talabalar, tadbirkorlar va bank mijozlarining xavf profili turlicha. Masalan, yoshlar ijtimoiy tarmoqlarda shaxsiy ma’lumotlarni ortiqcha ulashish xavfiga, katta yoshdagilar esa soxta qo‘ng‘iroq va SMS orqali manipulyatsiyaga ko‘proq duch kelishi mumkin. Shu sababli treninglar segmentlangan, qisqa, amaliy va mahalliy misollar bilan boyitilgan bo‘lishi zarur.

Model O‘zbekiston sharoitida mahalliy til, mahalliy raqamli xizmatlar, bank ilovalari, elektron hukumat tizimlari, mobil operatorlar va messenjerlardan foydalanish amaliyotini hisobga olishi bilan ahamiyatlidir. Ayniqsa “SMS-kodni hech kimga bermaslik”, “havola domenini tekshirish”, “bank xodimi PIN-kod so‘ramasligi”, “2FAni yoqish” kabi sodda, takroriy va vaziyatga mos profilaktik xabarlar aholi orasida xavfsiz odatlarni shakllantirishga yordam beradi.

Shu bilan birga, model hozircha konseptual-metodik shaklda taklif etilmoqda. Uning ishonchliligini oshirish uchun turli hududlar, yosh guruhlari va kasbiy segmentlar bo‘yicha empirik sinov o‘tkazish, indikatorlarning ichki izchilligini baholash, treningdan oldingi va keyingi natijalarni statistik solishtirish zarur.

ILMIY YANGILIK VA AMALIY AHAMIYAT.

Maqolaning ilmiy yangiligi O‘zbekiston sharoitida kiberxavfsizlik madaniyatini baholash uchun indikatorli KMI modelini taklif etishida namoyon bo‘ladi. Model cybersecurity awareness tushunchasini kengaytirib, foydalanuvchining amaliy xatti-harakati, xavf idroki, ijtimoiy muhandislikka chidamliligi va kiberhodisaga javob berish qobiliyatini yagona baholash tizimida birlashtiradi.

Amaliy ahamiyati shundaki, model asosida ta’lim muassasalari, banklar, davlat idoralari, mahalla va jamoatchilik tashkilotlari uchun maqsadli kiber gigiyena dasturlari ishlab chiqish mumkin. Bundan tashqari, indeks natijalari kiberjinoyatchilik profilaktikasida eng zaif xulq-atvor omillarini aniqlash, profilaktik materiallarni moslashtirish va trening samaradorligini monitoring qilishga xizmat qiladi.

XULOSA

Kiberjinoyatchilikka qarshi kurashda texnik himoya, huquqiy tartibga solish va tashkiliy nazorat muhim bo‘lsa-da, foydalanuvchi xavfsiz qaror qabul qilmasa, kiberjinoyatchilar uchun imkoniyat saqlanib qoladi. Shu sababli aholining kiberxavfsizlik madaniyatini oshirish yordamchi

(cc) BY

emas, balki strategik profilaktika yo‘nalishi sifatida qaralishi kerak.

Tadqiqotda O‘zbekiston sharoitida kiberxavfsizlik madaniyatini baholash uchun Kiberxavfsizlik madaniyati indeksi konseptual-metodik model sifatida ishlab chiqildi. Model xabardorlik, parol va autentifikatsiya madaniyati, phishingni aniqlash, shaxsiy ma’lumotlarni himoya qilish, qurilma-ilova gigiyenasi, xavfli xatti-harakatlardan qochish, kiberhodisaga javob berish va uzluksiz o‘rganish kabi indikatorlarni qamrab oladi.

Kelgusida ushbu modelni empirik sinovdan o‘tkazish, respondentlar kesimida statistik tahlil qilish, indikatorlar og‘irligini ekspert baholash orqali aniqlashtirish va trening samaradorligini oldin-keyin dizayni asosida o‘lchash tavsiya etiladi. Bu yondashuv O‘zbekistonda kiberxavfsizlik madaniyatini tizimli rivojlantirish va kiberjinoyatchilik profilaktikasini kuchaytirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni. 15.04.2022. URL: https://lex.uz/docs/-5960604
2. International Telecommunication Union. Global Cybersecurity Index 2024. Geneva: ITU, 2024. URL: https://www.itu.int
3. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Athens: ENISA, 2024. URL: https://www.enisa.europa.eu
4. Verizon. 2025 Data Breach Investigations Report. Verizon Business, 2025. URL: https://www.verizon.com/business/resources/reports/dbir/
5. Alsharida R.A. et al. A systematic review of multi-perspectives on human cybersecurity behavior // Technology in Society. 2023. Vol. 73. Article 102258. DOI: 10.1016/j.techsoc.2023.102258.
6. Kiran U., Khan N.F., Murtaza H., Farooq A., Pirkkalainen H. Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory // Computers & Security. 2025. Vol. 149. Article 104204. DOI: 10.1016/j.cose.2024.104204.
7. Li L., Xu L., He W. The effects of antecedents and mediating factors on cybersecurity protection behavior // Computers in Human Behavior Reports. 2022. Vol. 5. Article 100165. DOI: 10.1016/j.chbr.2021.100165.
8. Taherdoost H. A critical review on cybersecurity awareness frameworks and training models // Procedia Computer Science. 2024. DOI: 10.1016/j.procs.2024.04.156.
9. Prümmer J., van Steen T., van den Berg B. A systematic review of current cybersecurity training methods // Computers & Security. 2024.
10. Yeoh W., Huang H., Lee W.-S., Al Jafari F., Mansson R. Simulated phishing attack and embedded training campaign // Journal of Computer Information Systems. 2022. Vol. 62, No. 4. P. 802–821. DOI: 10.1080/08874417.2021.1919941.
11. Hillman D., Harel Y., Toch E. Evaluating organizational phishing awareness training on an enterprise scale // Computers & Security. 2023. Vol. 132. Article 103364. DOI: 10.1016/j.cose.2023.103364.
12. Sutter T., Bozkir A.S., Gehring B., Berlich P. Avoiding the hook: influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception // IEEE Access. 2022. DOI: 10.1109/ACCESS.2022.3207272.
13. Jabir R. et al. Phishing attacks in the age of generative artificial intelligence: a systematic review of human factors // AI. 2025. Vol. 6, No. 8. Article 174.
14. Argyridou E. et al. Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: concept study // Journal of Medical Internet Research. 2023. Vol. 25. Article e41294. DOI: 10.2196/41294.
15. World Economic Forum. Global Cybersecurity Outlook 2024. Geneva: WEF, 2024. URL: https://www.weforum.org

(cc) BY