ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

GLOBAL RAQAMLI TAHDIDLAR SHAROITIDA MEDIASAVODXONLIK VA KIBERXAVFSIZLIK MADANIYATI

Xabiba Zoirova Xamrokulovna
Samarqand viloyati Favqulodda vaziyatlar boshqarmasi
Hayot faoliyati xavfsizligi o'quv markazi katta o'qituvchisi.

https://doi.org/10.5281/zenodo.19858482

Annotatsiya. *Ushbu maqolada globallashuv va raqamli transformatsiya sharoitida shaxs, jamiyat va davlat xavfsizligini ta'minlashning ustuvor yo'nalishlari tahlil qilingan. Tadqiqotda mediasavodxonlik axborot manipulyatsiyasiga qarshi turish mexanizmi sifatida, kiberxavfsizlik esa raqamli infratuzilmani himoya qilishning texnik asosi sifatida o'rganilgan. Maqolada kiberhujumlarning zamonaviy turlari, xususan, ijtimoiy muhandislik va fishing kabi tahdidlarning psixologik hamda texnologik jihatlari ochib berilgan. Shuningdek, davlat xizmatchilari va aholi o'rtasida kibergigiyena madaniyatini shakllantirish, axborot oqimini tanqidiy tahlil qilish ko'nikmalarini rivojlantirish bo'yicha ilmiy-amaliy tavsiyalar ishlab chiqilgan. Raqamli savodxonlikni oshirish favqulodda vaziyatlarning axborot komponentini boshqarishda strategik ahamiyatga ega ekanligi dalillangan.*

Kalit so`zlar. *Mediasavodxonlik, kiberxavfsizlik, axborot xavfsizligi, ijtimoiy muhandislik, kibergigiyena, raqamli transformatsiya, feyk xabarlar, fishing, kiberhujum.*

MEDIA LITERACY AND CYBERSECURITY CULTURE IN THE CONTEXT OF GLOBAL DIGITAL THREATS

Abstract. *This article analyzes the priority areas for ensuring the security of individuals, society, and the state in the context of globalization and digital transformation. The research examines media literacy as a mechanism for countering information manipulation, and cybersecurity as the technical foundation for protecting digital infrastructure. The article reveals modern types of cyberattacks, particularly the psychological and technological aspects of threats such as social engineering and phishing. Furthermore, it develops scientifically grounded recommendations for fostering a culture of cyber hygiene among civil servants and the general public, as well as enhancing critical information analysis skills. It is substantiated that digital literacy is of strategic importance in managing the information component of emergency situations.*

Keywords. *Media literacy, cybersecurity, information security, social engineering, cyber hygiene, digital transformation, fake news, phishing, cyberattack.*

МЕДИАГРАМОТНОСТЬ И КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛЬНЫХ ЦИФРОВЫХ УГРОЗ

Аннотация. *В данной статье анализируются приоритетные направления обеспечения безопасности личности, общества и государства в условиях глобализации и цифровой трансформации. В исследовании медиаграмотность рассматривается как механизм противодействия информационным манипуляциям, а кибербезопасность — как техническая основа защиты цифровой инфраструктуры. В статье раскрываются современные виды кибератак, в частности, психологические и технологические аспекты таких угроз, как социальная инженерия и фишинг.*

Также разработаны научно-обоснованные рекомендации по формированию культуры кибергигиены среди государственных служащих и населения, развитию навыков критического анализа информационных потоков. Обосновано, что цифровая грамотность имеет стратегическое значение в управлении информационной компонентой чрезвычайных ситуаций.

***Ключевые слова**. Медиаграмотность, кибербезопасность, информационная безопасность, социальная инженерия, кибергигиена, цифровая трансформация, фейковые новости, фишинг, кибератака.*

Kirish. Raqamli texnologiyalar insoniyat hayotining ajralmas qismiga aylangan hozirgi davrda axborot xavfsizligi tushunchasi o‘zining an’anaviy chegaralaridan chiqib, shaxs, jamiyat va davlat barqarorligini ta’minlovchi fundamental ustunga aylandi. To‘rtinchi sanoat inqilobi va global raqamli transformatsiya jarayonlari natijasida shakllangan yangi reallik, bir tomondan, cheksiz axborot almashinuvi va texnologik qulayliklarni taqdim etgan bo‘lsa, ikkinchi tomondan, kiberxavfsizlik va mediasavodxonlikni uzviy bog‘liq bo‘lgan yagona mudofaa tizimiga birlashtirish zaruriyatini keltirib chiqardi.

Bugungi kunda global raqamli tahdidlar shunchaki texnik dasturlar yoki kompyuter viruslari bilan cheklanib qolmay, balki inson ongi va jamiyatning kollektiv psixologiyasini nishonga oluvchi murakkab gibrid ko‘rinishga ega bo‘lmoqda. Aynan mana shu nuqtada, kiberxavfsizlikning texnik infratuzilmasi va mediasavodxonlikning tahliliy ko‘nikmalari o‘rtasidagi simbioz raqamli suverenitetning asosi bo‘lib xizmat qiladi.

Kiberxavfsizlik evolyutsiyasini tahlil qilar ekanmiz, sohaning dastlabki bosqichlarida asosiy e’tibor faqatgina tizimlarni ruxsatsiz kirishdan himoya qilishga qaratilganini ko‘ramiz, biroq zamonaviy kiberhujumlar strategiyasi tubdan o‘zgardi. Hozirgi kunda kiberjinoyatchilar eng murakkab texnik to‘siqlarni ham "ijtimoiy muhandislik" (social engineering) deb ataluvchi usullar orqali chetlab o‘tishmoqda. Mazkur jarayonning markazida inson omili (human factor) yotadi, chunki eng mukammal himoya tizimi ham mediasavodsiz yoki raqamli gigiyena qoidalaridan bexabar foydalanuvchining birgina ehtiyotsiz harakati bilan ishdan chiqishi mumkin.

Statistik ma’lumotlar shuni ko‘rsatadiki, global miqyosdagi kiberhujumlarning qariyb 90 foizi insonning psixologik zaifliklaridan foydalanish, masalan, fishing (phishing) xabarlariga ishonish yoki shubhali havolalarga kirish natijasida sodir bo‘ladi. Bu holat shuni anglatadiki, kiberxavfsizlik madaniyati shunchaki parollarni murakkablashtirish emas, balki axborot oqimini tanqidiy tahlil qilish, manipulyatsiyalarni aniqlash va raqamli dunyoda mas’uliyatli xulq-atvorni shakllantirishdir.

Mediasavodxonlik tushunchasi zamonaviy xavfsizlik arxitekturasida "axborot urushlari" (information warfare) va dezinformatsiya oqimiga qarshi "ijtimoiy immunitet" vazifasini o‘taydi.

Global miqyosda sodir bo‘layotgan geosiyosiy mojarolar, pandemiyalar va favqulodda vaziyatlar shuni ko‘rsatdiki, yolg‘on (feyk) xabarlar jamiyatda vahima uyg‘otish, davlat institutlariga bo‘lgan ishonchni pasaytirish va ijtimoiy barqarorlikni izdan chiqarishning eng samarali quroliga aylangan. Marshall Maklyuenning "Media — bu xabar" degan fundamental qarashi hozirgi kunda yangicha ahamiyat kasb etib, axborotni qabul qilish kanallarining xavfsizligi uning mazmuni kabi muhim ekanligini isbotlamoqda.

Mediasavodxon inson nafaqat axborotni iste'mol qiladi, balki uning manbasini tekshirish, ortidagi yashirin maqsadlarni aniqlash va o'zining raqamli izini (digital footprint) himoya qilish orqali umumiy axborot ekologiyasini saqlashga hissa qo'shadi. O'zbekiston Respublikasining raqamli strategiyasi va milliy manfaatlarini ko'rib chiqqanda, mamlakatimizdagi yosh aholi salmog'ining yuqoriligi ushbu masalani yanada dolzarblashtiradi. "Kiberxavfsizlik to'g'risida"gi Qonun va milliy strategiya hujjatlari kiber-makonda xavfsizlikni ta'minlashning huquqiy asosi bo'lsa-da, amaliy natijaga erishish uchun aholining barcha qatlamlarida, xususan, davlat xizmatchilari va strategik soha vakillarida yuqori kiber-madaniyatni shakllantirish talab etiladi.

Favqulodda vaziyatlar organlari kabi tizimlarda axborotning tezkorligi va aniqligi insonlar hayotiga to'g'ridan-to'g'ri ta'sir ko'rsatadi, demak, ushbu soha vakillari uchun mediasavodxonlik xizmat vazifasining ajralmas qismidir. 1980-yillarning oxirida, xususan, 1988-yilda internet tarixidagi birinchi yirik kiberhujum — "Morris qurti" (Morris Worm) sodir bo'lganda, dunyo hamjamiyati tarmoq xavfsizligi qanchalik zaif ekanligini anglab yetdi. O'shanda kiberxavfsizlik tushunchasi faqat texnik nosozliklarni bartaraf etish bilan cheklangan edi. Biroq, 2010-yildagi "Stuxnet" virusining paydo bo'lishi kiber-qurollar real dunyo infratuzilmasini (energetika tizimlarini) jismonan yo'q qilish kuchiga ega ekanligini isbotladi. Ushbu evolyutsiya kiber-tahdidlarning murakkablashuvini ko'rsatibgina qolmay, balki ularning asosiy nishoni — insoniyat tomonidan boshqariladigan strategik qarorlar ekanligini oydinlashtirdi.

Binobarin, kiberxavfsizlik endilikda faqat "IT mutaxassislari ishi" emas, balki mediasavodxonlik orqali shakllanadigan umummilliy mudofaa strategiyasidir.

Mediasavodxonlikning psixologik va sotsiologik jihatlarini o'rganar ekanmiz, kiberjinoyatchilar ko'p hollarda inson ongining "tasdiqlash moyilligi" (confirmation bias) kabi zaifliklaridan foydalanishini ko'ramiz. Inson o'z qarashlariga mos keladigan axborotni, uning rost yoki yolg'onligini tekshirmasdan qabul qilishga moyildir. Bu holat raqamli muhitda "axborot pufakchalari" (echo chambers) hosil bo'lishiga olib keladi. Natijada, mediasavodxonligi past bo'lgan foydalanuvchi nafaqat kiber-tuzoqqa (masalan, fishing havolasiga) osonlikcha tushadi, balki o'zi bilmagan holda dezinformatsiya tarqatuvchi vositaga aylanadi. Shu sababli, zamonaviy kiberxavfsizlik madaniyati inson psixologiyasini tushunishni va unga qarshi tanqidiy fikrlashni (critical thinking) qalqon sifatida qo'llashni talab etadi. Bu jarayonni ilmiy adabiyotlarda "raqamli kognitiv xavfsizlik" deb ham atashmoqda.

Xalqaro huquqiy maydonda ham kiberxavfsizlik va mediasavodxonlik masalasi ustuvor yo'nalishga aylandi. Yevropa Kengashining Kiberjinoyatchilik bo'yicha Budapesht konvensiyasi va BMTning Axborot xavfsizligi bo'yicha ishchi guruhlari rezolyutsiyalari raqamli makonda xulq-atvor me'yorlarini belgilab beradi.

O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni aynan shu kabi xalqaro standartlarga tayangan holda, milliy axborot makonini himoya qilishning huquqiy mexanizmlarini yaratdi. Biroq, qonunning samaradorligi bevosita jamiyatning mediasavodxonlik darajasiga bog'liq.

Chunki har qanday kiber-jinoyatni tergov qilishdan ko'ra, aholi o'rtasida kiber-gigiyena madaniyatini shakllantirish orqali uning oldini olish davlat uchun iqtisodiy va ijtimoiy jihatdan foydalidir. Favqulodda vaziyatlar boshqarmasi va boshqa huquqni muhofaza qiluvchi organlar uchun raqamli xavfsizlik madaniyati operatsion barqarorlikni anglatadi.

Xizmat faoliyati davomida foydalaniladigan maxfiy ma’lumotlarning himoyasi, xodimlarning ijtimoiy tarmoqlardagi faolligi va aholini xabardor qilishda foydalaniladigan raqamli kanallarning xavfsizligi — bularning barchasi mediasavodxonlikning amaliy ko‘rinishidir. Agar mutaxassis kelayotgan axborotning manipulyativ ekanini tushuna olmasa yoki kiber-gigiyena qoidalariga rioya qilmasa, bu butun boshli davlat tizimining falajlanishiga olib kelishi mumkin.

Shu nuqtai nazardan, kiberxavfsizlik va mediasavodxonlik simbiozi nafaqat nazariy tadqiqot ob’ekti, balki zamonaviy davlat boshqaruvining hayotiy zaruratidir. Maqolaning ushbu kirish qismida qo‘yilgan masalalar, raqamli tahdidlarning murakkablashib borishi sharoitida O‘zbekistonning barqaror rivojlanishi uchun intellektual poydevor bo‘lib xizmat qiladi.

Asosiy qism. Zamonaviy kiberxavfsizlik arxitekturasini tahlil qilishda "Inson omili" tushunchasi endilikda tizimning zaif nuqtasi emas, balki uning eng strategik himoya qatlami sifatida qayta talqin etilmoqda. Texnologik taraqqiyotning hozirgi bosqichida kiberhujumlarning vektori binar kodlardan kognitiv jarayonlarga ko‘chganini ko‘rishimiz mumkin. Bu jarayonni ilmiy nuqtai nazardan "Kognitiv kiber-urush" (Cognitive Cyber Warfare) deb atash o‘rinli.

Mazkur urushda asosiy qurol — dezinformatsiya, manipulyatsiya va ijtimoiy muhandislik bo‘lsa, asosiy qalqon — mediasavodxonlikdir. Maqolaning ushbu qismida biz kiberxavfsizlik va mediasavodxonlik integratsiyasini to‘rtta fundamental yo‘nalishda: texnik-psixologik manipulyatsiyalar, O‘zbekiston kiberhududidagi real xavflar, sun’iy intellekt asosidagi tahdidlar va amaliy kiber-gigiyena madaniyati misolida tahlil qilamiz. Birinchi navbatda, kiberhujumlarning texnik-psixologik tasnifiga to‘xtalib o‘tish joiz. Ijtimoiy muhandislikning zamonaviy usullari foydalanuvchining ishonch, qo‘rquv yoki qiziqish kabi bazaviy instinktlariga asoslanadi. Masalan, "Pretexsting" (Pretexting) usulida jinoyatchi o‘zi uchun soxta, lekin ishonarli shaxsiyat yaratadi.

U foydalanuvchiga tizim administratori, huquqni muhofaza qiluvchi organ xodimi yoki bank menejeri sifatida murojaat qiladi. Bunday vaziyatda kiberxavfsizlikning texnik vositalari (antiviruslar yoki firewall) ojiz qoladi, chunki foydalanuvchi o‘z ixtiyori bilan tizimga kirish huquqini (login, parol yoki OTP kodni) jinoyatchiga beradi. Mediasavodxonlik foydalanuvchiga axborotning "metama’lumotlarini" — jo‘natuvchi elektron pochta manzilining haqiqiyligini, xatdagi mantiqiy xatoliklarni va murojaat uslubini tahlil qilish ko‘nikmasini beradi. Har bir raqamli signalni shubha ostiga olish va uni rasmiy manbalar orqali kross-tekshiruvdan (cross-referencing) o‘tkazish zamonaviy raqamli madaniyatning birinchi qoidasidir.

O‘zbekiston kiberhududidagi oxirgi ikki yillik holat kiber-ogohlikning nafaqat shaxsiy, balki milliy xavfsizlik masalasi ekanligini ko‘rsatdi. 2024-yil boshida kuzatilgan "Click-phishing" va Telegram messenjeri orqali amalga oshirilgan keng ko‘lamli xurujlar buni isbotladi. Jinoyatchilar tomonidan yaratilgan soxta botlar va havolalar orqali foydalanuvchilarga "Prezident qarori bilan kompensatsiya to‘lanishi" haqida yolg‘on ma’lumotlar tarqatildi. Bu yerda biz mediasavodxonlikning "Axborot manbasi autentifikatsiyasi" bosqichi oqsayotganini ko‘ramiz.

Foydalanuvchilar axborotning "gov.uz" yoki "lex.uz" kabi rasmiy domenlarda mavjudligini tekshirmasdan, anonim kanallardagi ma’lumotlarga tayangan holda o‘z shaxsiy ma’lumotlarini kiritishdi. Kiberxavfsizlik tizimi texnik jihatdan ushbu soxta domenlarni bloklashi mumkin, biroq jinoyatchilar bir necha daqiqa ichida yangi domenlarni ro‘yxatdan o‘tkazish imkoniga ega. Binobarin, yagona samarali yechim — aholida "axborot filtri"ni shakllantirishdir.

Bu esa davlat idoralari xodimlari va oddiy fuqarolar uchun doimiy kiber-mashqlarni (cyber-drills) o‘tkazishni taqozo etadi. Ikkinchi strategik yo‘nalish — sun’iy intellekt va "Deepfake" texnologiyalari bilan bog‘liq tahdidlardir. Bugungi kunda generativ AI tizimlari yordamida insonning ovozi va qiyofasini 99% aniqlikda soxtalashtirish imkoniyati mavjud.

O‘zbekistonning raqamli segmentida yirik davlat arboblari va tadbirkorlar nomidan odamlarni shubhali investitsiya loyihalariga chorlovchi deepfake videolarining tarqalishi "vizual savodxonlik" (visual literacy) tushunchasini kun tartibiga chiqardi. Mediasavodxon kishi bunday videolarni ko‘rganda uning biometrik nomutanosibliklariga — ko‘z qisish chastotasi, lab harakatining ovoz bilan mos kelmasligi va piksellarning chegaralaridagi g‘alizlikka e’tibor berishi lozim. Bundan tashqari, kognitiv xavfsizlikning muhim qismi bu — emotsional kontrol. Agar axborot o‘ta yuqori foyda yoki favqulodda qo‘rqinchli xabar berayotgan bo‘lsa, bu manipulyatsiyaning birinchi belgisidir. Mediasavodxonlik insonni "tezkor mantiq" (System 1) dan "chuqur mahlil" (System 2) tizimiga o‘tishga majbur qiladi. Uchinchi bo‘limda kiber-gigiyena va "Raqamli daxlsizlik" (Privacy) masalasini amaliy jihatdan tahlil qilishimiz lozim. O‘zbekistonlik foydalanuvchilar orasida kuzatilayotgan "Oversharing" (haddan tashqari ko‘p shaxsiy ma’lumotlarni ulashish) holati kiber-josuslik va maqsadli hujumlar (Spear Phishing) uchun zamin yaratadi.

Ijtimoiy tarmoqlarda xizmat joyidan rasm qo‘yish, ish stoli yoki hujjatlarni ko‘rsatish — bu jinoyatchilar uchun tayyor "razvedka ma’lumotlari"dir. Raqamli gigiyena madaniyati foydalanuvchiga murakkab parollar menejmenti (Password Managers) va ikki bosqichli autentifikatsiya (2FA) tizimlaridan foydalanishni odatga aylantirishni o‘rgatadi. Statistikaga ko‘ra, faqatgina 2FA (SMS emas, balki maxsus autentifikator ilovalar)ni yoqish kiberhujumlar xavfini 80% ga kamaytiradi.

Biroq, ko‘pchilik buni "noqulaylik" deb bilishi mediasavodxonlikning yetishmasligidan dalolat beradi. Bizning vazifamiz — xavfsizlikni noqulaylik emas, balki raqamli hayotda omon qolishning yagona yo‘li ekanligini jamiyatga singdirishdir. To‘rtinchi va eng muhim yo‘nalish — kiberxavfsizlik va mediasavodxonlikning davlat boshqaruvi tizimidagi strategik ahamiyatidir.

Favqulodda vaziyatlar boshqarmasi kabi tizimlar uchun axborotning daxlsizligi — bu insonlar hayoti bilan bog‘liq masala. Agar krizis vaziyatida tizimga dezinformatsiya kirib kelsa yoki xodimlarning akkauntlari orqali soxta buyruqlar tarqatilsa, bu butun boshli mintaqaning barqarorligiga putur yetkazishi mumkin. Shu sababli, davlat xizmatchilari uchun "Axborot immuniteti" moduli ishlab chiqilishi lozim. Bu modul doirasida xodimlarga nafaqat texnik kiberxavfsizlik, balki "kognitiv psixologiya" darslari o‘tilishi, ularning axborot manipulyatsiyasiga bo‘lgan chidamliligi (Resilience) sinovdan o‘tkazilishi shart. Xalqaro tajriba (masalan, Estoniyaning "Cyber Hygiene" kursi) shuni ko‘rsatadiki, ogoh aholi har qanday antivirusdan ko‘ra samaraliroq himoya vositasidir.

Kiberxavfsizlik va mediasavodxonlikning integratsiyasi raqamli ekotizimda "yaxlit qalqon" (The Holistic Shield) hosil qiladi. Texnik qatlamlar hujumlarni to‘xtatib tursa, intellektual qatlam ularni fosh etadi. Bu ikki soha endilikda alohida o‘rganilishi mumkin emas. Sun’iy intellekt qanchalik aqlli bo‘lmasin, qaror qabul qiluvchi yakuniy nuqta — inson ongi bo‘lib qoladi. Biz algoritmlar tomonidan boshqariladigan jamiyatga emas, balki algoritmlarni mediasavodxonlik orqali boshqaradigan jamiyatga aylanishimiz kerak.

O‘zbekiston Respublikasining 2030-yilgacha bo‘lgan rivojlanish strategiyasida raqamli iqtisodiyot va kiber-xavfsizlik ustuvor yo‘nalish etib belgilangan. Ushbu maqsadga erishishning yagona yo‘li — texnologik infratuzilmaga sarmoya kiritish bilan bir qatorda, jamiyatning intellektual salohiyatini, ya’ni mediasavodxonligini yuksaltirishdir.

Kiberxavfsizlik muammosi — bu muhandislik muammosi emas, balki psixologik va sotsiologik muammodir. Biz raqamli dunyoda "zirh"imizni (texnologiya) qanchalik mustahkam qilmaylik, uni kiygan "jangchi" (inson) ojiz bo‘lsa, mudofaa samarasiz bo‘lib qolaveradi. Shuning uchun, milliy kiberxavfsizlik strategiyasi doirasida mediasavodxonlik markazlarini tashkil etish, aholining barcha qatlamlari uchun kiber-gigiyena bo‘yicha interaktiv qo‘llanmalarni ishlab chiqish va axborot makonini doimiy monitoring qilib borish hayotiy zaruratdir. Faqatgina texnik mukammallik va intellektual onglilik birlashgan nuqtadagina biz global raqamli tahdidlar sharoitida o‘z raqamli suverenitetimizni saqlab qola olamiz. Kelajak xavfsizligi — bu mukammal kodlar emas, balki har bir raqamli qadamini o‘ylab bosadigan, axborotni filtrlay oladigan va o‘z daxlsizligini qadrlaydigan mediasavodxon jamiyatdir.

Xulosa. Global raqamli transformatsiya va sun’iy intellekt texnologiyalarining shiddatli taraqqiyoti sharoitida kiberxavfsizlik va mediasavodxonlik o‘rtasidagi bog‘liqlikni tadqiq etish shuni ko‘rsatadiki, raqamli xavfsizlik endilikda tor doiradagi texnik tushuncha emas, balki milliy xavfsizlikning fundamental ustuniga aylandi. Mazkur ilmiy maqola doirasida amalga oshirilgan tahlillar kiber-mudofaaning samaradorligi faqatgina dasturiy ta’minot yoki texnik filtrlar bilan emas, balki bevosita inson omili — foydalanuvchining axborotni qabul qilish va tahlil qilish salohiyati bilan belgillanishini isbotladi. O‘zbekiston tajribasi, xususan, so‘nggi yillarda bank-moliya tizimi va davlat axborot resurslariga qilingan kiber-hujumlar kiberxavfsizlik madaniyatini shakllantirishda "Insoniy firewall" (Insoniy qalqon) konsepsiyasining naqadar hayotiy ekanligini ko‘rsatdi. Texnik jihatdan mukammal himoyalangan tizimlar ham mediasavodxonligi past bo‘lgan foydalanuvchining birgina ehtiyotsiz harakati yoki manipulyatsiyaga uchrashi natijasida falajlanishi mumkin. Bu esa, mamlakatimizda kiber-profilaktika ishlarini yangi bosqichga ko‘tarishni, ya’ni aholi orasida "axborot immuniteti"ni shakllantirishni strategik vazifa qilib qo‘yadi.

Tadqiqot natijalariga ko‘ra, O‘zbekistonning raqamli suverenitetini mustahkamlash uchun quyidagi strategik takliflarni ilgari surish maqsadga muvofiq:

Ta’lim integratsiyasi: Mediasavodxonlik va kiber-gigiyena asoslarini nafaqat oliy ta’lim, balki maktabgacha va maktab ta’limi dasturlariga "raqamli omon qolish ko‘nikmasi" sifatida integratsiya qilish.

Davlat xizmatchilari tayyorgarligi: Favqulodda vaziyatlar boshqarmasi va boshqa strategik idoralar xodimlari uchun muntazam ravishda simulyatsiya qilingan kiber-hujumlar va mediasavodxonlik testlarini o‘tkazish tizimini yo‘lga qo‘yish.

Milliy kontent xavfsizligi: Deepfake va AI-manipulyatsiyalarini aniqlash bo‘yicha milliy texnik bazani yaratish va aholini ushbu tahdidlardan xabardor qilishning tezkor mexanizmlarini ishlab chiqish.

Ijtimoiy hamkorlik: Davlat, xususiy sektor (banklar, IT-kompaniyalar) va fuqarolik jamiyati o‘rtasida kiber-ogohlikni oshirish bo‘yicha yaxlit platforma yaratish.

Xulosa qilib aytganda, raqamli dunyoda "mutloq xavfsizlik" mavjud emas, biroq "maksimal barqarorlik"ka erishish mumkin. Bu barqarorlikning kaliti esa — texnik mukammallik va intellektual uyg‘oqlikning simbiozidadir. O‘zbekistonning raqamli kelajagi faqatgina kuchli serverlar yoki yuqori tezlikdagi internet bilan emas, balki har bir axborotni tanqidiy filtrdan o‘tkaza oladigan, o‘z raqamli huquq va daxlsizligini qadrlaydigan mediasavodxon jamiyat bilan kafolatlanadi. Zero, kiber-makondagi eng kuchli qurol — bu erkin va tahliliy fikrlaydigan inson ongidir.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining Farmoni. "O‘zbekiston – 2030" strategiyasi to‘g‘risida (PF-158-son). – Toshkent, 2023-yil 11-sentyabr.
2. O‘zbekiston Respublikasining Qonuni. "Axborotlashtirish to‘g‘risida". – Toshkent, 2003 (yangi tahriri bilan).
3. UNESCO. Media and Information Literacy: Policy and Strategy Guidelines. – Paris, 2021.
4. Csutak, Z. "Media Literacy and Cyber Security: Theory and Practice in Education". Journal of Digital Security, 2022.
5. ENISA (European Union Agency for Cybersecurity). Cybersecurity Culture in Organizations report. – 2023.
6. O‘zbekiston Respublikasi Kiberxavfsizlik markazi. "Kiberxavfsizlikning yillik tahliliy hisoboti (2023-2024)".