

O‘ZBEKISTONDA RAQAMLI INFRATUZILMANI DIVERSIFIKATSIYA QILISH: ZAMONAVIY KIBER TAHDIDLARGA QARSHI SINERGETIK MEXANIZM

SOBIROV ANVAR

Toshkent davlat iqtisodiyot universiteti

Falsafa kafedrasida mustaqil tadqiqotchisi

E-mail: dilmurodernazarov55@gmail.com

Mobile: +998997700429

Annotatsiya. Raqamli texnologiyalarning tez sur’atlarda rivojlanishi va kiberprostranstvoning kundalik hayotga chuqur integratsiyalanishi yoshlarni turli kiber tahdidlarga uchrash ehtimoliga olib keldi. Ushbu tadqiqot yoshlar kiber tahdidlar va kiberxavfsizlik haqidagi tushunchalarini shakllantirishdagi refleksiv jarayonlarni o‘rganadi, shuningdek raqamli savodxonlik, ta’lim muhiti, ijtimoiy aloqalar va shaxsiy tajribalarning ahamiyatiga e’tibor qaratilgan. Falsafa, psixologiya, sotsiologiya va axborot xavfsizligi tadqiqotlaridan olingan interdissiplinar adabiyotlar asosida, tadqiqot refleksiv fikrlash yoshlarga raqamli ma’lumotni tanqidiy baholash, ehtimoliy tahdidlarni aniqlash va mas’uliyatli onlayn xulq-atvorni qo‘llash imkonini berishi haqida ko‘rsatadi. Tadqiqot natijalari refleksiv ongning etik qirralar, raqamli barqarorlik va profilaktik kiberxavfsizlik amaliyotlari bilan yaqin aloqada ekanini ko‘rsatadi. Ushbu tadqiqot refleksiv fikrlashni rivojlantirish, kiberxavfsizlik ongini oshirish va yoshlarni murakkab raqamli muhitlarda xavfsiz va mas’uliyatli harakatlanish qobiliyatini kuchaytirish uchun kompleks ta’lim va ijtimoiy intervensiyalar zarurligini ta’kidlaydi.

Kalit so‘zlar. Kiberxavfsizlik, Refleksiv fikrlash, Yoshlar ongi, Raqamli savodxonlik, Kiber tahdidlar, Raqamli barqarorlik, Onlayn xulq-atvor, Axborot xavfsizligi ta’limi.

Kirish

Jamiyatning zamonaviy bosqichi raqamli texnologiyalarning tez rivojlanishi va kiberprostranstvoning kundalik hayotga chuqur integratsiyalanishi bilan tavsiflanadi. O‘zbekistonda raqamlilashtirish milliy rivojlanish strategiyalarining asosiy ustunlaridan biri bo‘lib, davlat xizmatlari, bank tizimlari, energetika, salomatlik, transport va ta’lim tizimlarini qamrab oladi (O‘zbekiston Respublikasi Davlat statistika qo‘mitasi, 2023). Raqamli infratuzilmaning rivojlanishi davlat va xususiy sektorlarda kirish imkoniyatlari, samaradorlik va shaffoflikni sezilarli darajada oshirdi.

Biroq, ushbu tez raqamli transformatsiya muhim axborot tizimlarida zaifliklarni ochib berdi. Fishing, rensamver (ransomware) hujumlari, ma’lumotlar buzilishi va

kibershpiionlik kabi kiber tahdidlar soni va murakkabligi tobora ortib bormoqda. (Kshetri 2021)ga ko'ra, O'zbekiston kabi rivojlanayotgan iqtisodiyotlar, kiberoxavfsizlik sohasidagi malakali kadrlarning yetishmasligi, texnologiyalarning turlicha joriy etilishi va tartib-taomildagi bo'shliqlar sababli kiber tahdidlarga alohida hassosdir. Ushbu tahdidlar nafaqat alohida foydalanuvchilar, balki muassasalar barqarorligi, milliy xavfsizlik va iqtisodiy barqarorlik uchun ham xatarlidir.

Kiber xatarlarni kamaytirishdagi muhim omil raqamli infratuzilmaning strategik diversifikatsiyasidir. Infratuzilmani diversifikatsiya qilish texnik, tashkilotchilik va funksional choralarni o'z ichiga oladi, bu esa axborot tizimlarida ehtiyotlik, barqarorlik va moslashuvchanlikni ta'minlaydi. Diversifikatsiya qilingan tizimlar kiber hodisalardan kelib chiqadigan zarbalarni o'zlari ulashlari, yagona nuqtalardagi buzilishlarni kamaytirishi va milliy kiberoxavfsizlik barqarorligini oshirishi mumkin (Al-Hadhrami & Alharthi, 2022).

Bundan tashqari, kiberoxavfsizlikda inson omilining ahamiyati markaziy ahamiyatga ega. Texnologiyalar hujumlarni aniqlash va oldini olish uchun zarur vositalarni taqdim etsa-da, ushbu choralarning samaradorligi shaxsiy va tashkilotchilik ong, refleksiv fikrlash va raqamli savodxonlikka bog'liqdir. Refleksiv jarayonlar shaxs va tashkilotlarga tahdidlarni tanqidiy baholash, ehtimoliy xatarlarni oldindan kuzatish va faol ravishda javob berish imkonini beradi (Livingstone & Helsper, 2007). O'zbekiston kontekstida raqamli boshqaruv va ta'lim dasturlariga refleksiv fikrlashni integratsiya qilish kiberbarqaror jamiyatni rivojlantirishda muhim ahamiyatga ega.

Ushbu tadqiqot O'zbekistonda raqamli infratuzilmani diversifikatsiya qilishning zamonaviy kiber tahdidlarga qarshi sinergetik mexanizm sifatidagi rolini o'rganishga qaratilgan. Shuningdek, tadqiqot texnologiyaviy choralari, institut strategiyalari va insonning refleksiv jarayonlari o'rtasidagi o'zaro ta'sirni tahlil qilishni maqsad qilgan.

Adabiyotlar tahlili

Raqamli infratuzilmani diversifikatsiya qilish konsepsiyasi barqarorlik nazariyasiga asoslangan bo'lib, u tizimlarning noqulay sharoitlarda ham funkcionalligini saqlab qolish qobiliyatini ta'kidlaydi. (Walker va hamkasblari 2004) barqarorlikni ijtimoiy-texnik tizimlarning buzilishlarga chidamli bo'lib, moslashishi va samarali ishlab turuvchi qobiliyati sifatida ta'riflaydilar. Bu prinsipni raqamli infratuzilmalarga qo'llashda, diversifikatsiya strategiyalari texnologik va operatsion xatarni turli komponentlarga – tarmoqlar, serverlar, ma'lumot markazlari, bulut xizmatlari va inson operatorlariga – taqsimlashni maqsad qiladi.

Rivojlanayotgan iqtisodiyotlarda kiberoxavfsizlik bo'yicha o'tkazilgan tadqiqotlar kiber tahdidlarning ko'pqirrali tabiatini ta'kidlaydi. (Kshetri, 2021) kiber tahdidlar faqat texnik muammolar emas, balki ular tashkilotchilik, iqtisodiy va ijtimoiy qirralarni ham o'z ichiga olishi haqida yozadi. Masalan, yetarli tayyorgarlikning yo'qligi, past ong darajasi va markazlashtirilgan raqamli tizimlarga bog'liqlik kiberoxujumlarga

chidamsizlikni oshiradi. Shu nuqtai nazardan, diversifikatsiya xatarni kamaytirishda ham texnik, ham tashkilotchilik mexanizm sifatida xizmat qiladi.

O‘zbekiston kontekstida, hukumat raqamli transformatsiyani ustuvor vazifa sifatida belgilagan va barqaror kiberxavfsizlik tizimlarining zarurligini tan olgan. “Digital Uzbekistan 2030” strategiyasiga ko‘ra (O‘zbekiston Respublikasi Raqamli rivojlanish vazirligi, 2021), tadbirlar sirasida bulut infratuzilmasini kengaytirish, idoralararo raqamli platformalarni joriy etish va kiberxavfsizlik qobiliyatlarini rivojlantirish dasturlari mavjud. Ammo olimlar fikriga ko‘ra, faqat texnologik yangilanishlar yetarli emas; kiber xatarlarni samarali kamaytirish infratuzilmani diversifikatsiya qilish, huquqiy tartibga solish, ta’lim va jamoat ongini birlashtirgan integratsiyalangan yondashuvni talab qiladi (Al-Hadhrami & Alharthi, 2022); (Papadopoulos et al., 2020).

Sinergetik mexanizm tushunchasi texnologik, tashkilotchilik va inson omillarining o‘zaro bog‘liqligini hisobga olganda paydo bo‘ladi. Diversifikatsiya qilingan raqamli infratuzilmalar ehtiyotni ta’minlaydi, ammo ularning samaradorligi to‘g‘ri boshqaruv, monitoring va foydalanuvchi hamda administratorlarning refleksiv qobiliyatlariga bog‘liqdir (Castells, 2010). Refleksiv jarayonlar, masalan xavfsizlik protokollarini tanqidiy baholash, ssenariy asosida rejalashtirish va doimiy o‘rganish, raqamli tizimlarning barqarorligini oshiradi va muvaffaqiyatli kiberxujumlar ehtimolini kamaytiradi.

Shuningdek, tadqiqotlar diversifikatsiya bulut hisoblash, ko‘pqavatli xavfsizlik tizimlari va detsentralizovan tarmoqlarni o‘z ichiga olishi kerakligini ta’kidlaydi. Bulutni diversifikatsiya qilish tashkilotlarga ma’lumotlarni turli platformalar bo‘yicha taqsimlash imkonini beradi va mahalliy kiber hodisalar ta’sirini minimallashtiradi (Zubareva et al., 2020). Ko‘pqavatli kiberxavfsizlik arxitekturalari, shu jumladan faervollar, buzilishlarni aniqlash tizimlari va shifrlangan aloqa kanallari, zaiflikni cheklaydigan qo‘shma himoya choralarini yaratadi. Detsentralizatsiya yagona nuqtalarga bog‘liqlikni kamaytiradi, tizimni hujum va tabiiy buzilishlarga chidamli qiladi (Singer & Friedman, 2014).

Ijtimoiy va ta’lim qirralari ham muhim ahamiyatga ega. Livingstone & Helsper (2007)ning tadqiqotlariga ko‘ra, yosh foydalanuvchilar orasida raqamli savodxonlik va refleksiv ong kiber tahdidlarga bog‘liq xatarlarni sezilarli darajada kamaytiradi. Kiberxavfsizlik, etik raqamli xulq-atvor va kiber hodisalarni boshqarish bo‘yicha amaliy mashqlarga qaratilgan ta’lim dasturlari shaxsiy va tashkilotchilik barqarorlikni mustahkamlaydi. O‘zbekistonda bunday dasturlar oliy ta’lim muassasalarida, kasbga yo‘naltirilgan markazlarda va jamoat ongini oshirish kompaniyalarida bosqichma-bosqich joriy etilmoqda.

Natijada, raqamli infratuzilmani diversifikatsiya qilishga sinergetik yondashuv doimiy monitoring, baholash va moslashuvni talab qiladi. ISO/IEC 27032 (2012) va

milliy kiberxavfsizlik ramkalari xatarlarni boshqarish dinamik bo‘lishi, tahdid aqlini, tizim auditini va siyosat yangilanishini integratsiya qilishi kerakligini taklif qiladi. Texnologik, institutsional va inson komponentlarini muvofiqlashtirib, mamlakatlar zamonaviy kiber tahdidlarni kamaytirish uchun barqaror mexanizmlar rivojlantirishi mumkin.

Metodologiya

Tadqiqot dizayni

Ushbu tadqiqotda aralash metodologiya – sifatli va miqdoriy yondashuvlarni birlashtirish – qo‘llanildi. Bu yondashuv O‘zbekistonda kiber tahdidlarni kamaytirishda raqamli infratuzilmani diversifikatsiya qilish mexanizmining rolini o‘rganishga imkoniyat beradi. Aralash metod tadqiqot ma’lumotlarini triangulyatsiya qilish orqali natijalarning ishonchliligi va to‘g‘riligini oshiradi (Creswell & Creswell, 2018).

Ishtirokchilar

Tadqiqot namunalariga 450 kishi kiritilgan, jumladan oliygoh talabalari, IT mutaxassislari va davlat IT administratorlari. Ishtirokchilar turli yosh guruhlari, ta’lim darajalari va kasbiy faoliyatni inobatga olgan holda stratifikatsiyalangan tasodifiy usul bilan tanlangan. Ishtirokchilarning 55% erkak, 45% ayol bo‘lib, yoshi 18–35 yil oraliq‘ida edi.

Ma’lumot to‘plash usullari (Data Collection Methods)

Ma’lumot to‘plash uch bosqichda amalga oshirildi:

1. **So‘rovnomalar (Surveys)** – Struktur so‘rovnomalar orqali ishtirokchilarning raqamli savodxonligi, kiberxavfsizlik choralari bilan tanishligi va kiber tahdidlarga oid qarashlari baholandi. Savollar kiberxavfsizlik va raqamli savodxonlik tadqiqotlari asosida ishlab chiqildi (Livingstone & Helsper, 2007; Kshetri, 2021).

2. **Suhbatlar (Interviews)** – 50 asosiy respondent bilan yarim-strukturalangan suhbatlar o‘tkazildi, jumladan IT administratorlari, kiberxavfsizlik mutaxassislari va pedagoglar. Suhbatlar reflektiv fikrlash, infratuzilmani diversifikatsiya qilish strategiyalari va kiber tahdidlarni kamaytirish bo‘yicha institutsional amaliyotlarni tadqiq qilish maqsadida o‘tkazildi.

3. **Hujjatlarni tahlil qilish (Document Analysis)** – O‘zbekistondagi milliy siyosatlar, raqamli transformatsiya strategiyalari va kiberxavfsizlik tartiblari tahlil qilindi (O‘zbekiston Respublikasi Raqamli rivojlanish vazirligi, 2021); (O‘zbekiston Respublikasi Davlat statistika qo‘mitasi, 2023).

Ma’lumotlarni tahlil qilish (Data Analysis)

Miqdoriy so‘rovnomalar ma’lumotlari tasviriy statistika, korrelyatsiya tahlili va regressiya modellari orqali tahlil qilindi, bu raqamli savodxonlik, infratuzilmani anglash va kiber tahdidlarga oid reflektiv fikrlash o‘rtasidagi bog‘liqlikni aniqlash imkonini berdi. Statistik tahlil uchun SPSS dasturi (versiya 28) qo‘llanildi.

Sifatli intervyu ma'lumotlari mavzuviy kontent tahlili orqali tahlil qilindi, bu ishtirokchilar javoblaridagi patternlar va mavzularni aniqlash imkonini berdi (Braun & Clarke, 2006). Kodlash kategoriyalari: raqamli savodxonlik, xatarni anglash, reflektiv jarayonlar, institutsional strategiyalar va texnologik diversifikatsiya choralari.

Sifatli va miqdoriy ma'lumotlarni triangulyatsiya qilish O'zbekistonda diversifikatsiya qilingan raqamli infratuzilmani inson va institutsional omillar bilan o'zaro ta'sirini chuqur tushunish imkonini berdi.

Natijalar (Results)

Miqdoriy natijalar (Quantitative Findings)

So'rovnomma ma'lumotlari ishtirokchilarning raqamli savodxonligi, raqamli infratuzilmani diversifikatsiya qilish haqidagi anglashlari va kiber tahdidlarga oid reflektiv fikrlash o'rtasida sezilarli bog'liqlikni ko'rsatdi. Tasviriy statistika ma'lumotlariga ko'ra, ishtirokchilarning 72% o'rtacha va yuqori darajada raqamli savodxonlikka ega bo'lgan, ammo faqat 54% ishtirokchi tashkilotlaridagi infratuzilmani diversifikatsiya qilish strategiyalari haqida to'liq ma'lumotga ega edi.

Korrelyatsiya tahlili raqamli savodxonlik va kiber tahdidlarga oid reflektiv ong o'rtasida kuchli ijobiy bog'liqlikni ko'rsatdi ($r = .68, p < .001$). Bu natija yuqori texnik malaka kiber xatarlarni tanqidiy baholash va profilaktik choralarni qo'llash qobiliyati bilan bog'liqligini ko'rsatadi. Shuningdek, ishtirokchilarning diversifikatsiya qilingan raqamli infratuzilma bilan tanishligi ham reflektiv fikrlash bilan ijobiy bog'liq edi ($r = .55, p < .01$), bu esa institutsional va texnologik choralarni tushunish xatarni anglash va strategik qarorlar qabul qilishni oshiradi degan ma'noni anglatadi.

Regressiya tahlili raqamli savodxonlik va infratuzilmani anglash birgalikda yoshlar va IT mutaxassislar orasida reflektiv ongning o'zgarishining 48% ni tushuntirishini ko'rsatdi ($R^2 = .48, F(2, 447) = 206.15, p < .001$). Ikki ko'rsatkich ham statistik ahamiyatli bo'lib, raqamli savodxonlik ta'siri kuchliroq edi ($\beta = .49, p < .001$) va infratuzilmani anglash nisbatan kamroq ta'sir ko'rsatdi ($\beta = .34, p < .01$). Bu natijalar kiberxavfsizlik bilimlarini shakllantirishda texnik malaka va kontekstual tushunishning muhimligini ko'rsatadi.

Sifatli natijalar (Qualitative Findings)

Suhbat ma'lumotlari mavzuviy tahlil natijalari beshta asosiy mavzularni ko'rsatdi:

1. **Refleksiv ong va raqamli savodxonlik.** Ishtirokchilar internetdagi ma'lumotni tanqidiy baholash va ehtimoliy kiber tahdidlarni oldindan anglash qobiliyati muhimligini ta'kidladilar. Bir IT mutaxassisi shunday dedi: "Turli tizimlar qanday bog'langanini va zaifliklar qacda ekanini tushunish bizga oldindan fikrlash va ma'lumotlarni samarali himoya qilish imkonini beradi." Refleksiv ong ishtirokchilarning raqamli vositalar va platformalar bo'yicha o'zlari bildirgan malakasi bilan uzviy bog'liq edi.

2. Infratuzilmani diversifikatsiya qilish ta'siri

Suhbat qatnashchilari diversifikatsiya qilingan raqamli infratuzilma – ehtiyot serverlar, bir nechta bulut provayderlari va detsentralizovan tarmoqlar – kiber hodisalar ta'sirini kamaytiradi, deb ta'kidladilar. Bir universitet IT administratori shunday dedi: “Resurslarimizni turli tizimlarga taqsimlash orqali, agar bir qism hujumga uchrasa ham, boshqalari xavfsiz qoladi, bu esa bizga xavfsiz raqamli amaliyotlarni qo'llashga yordam beradi.” Bu mavzu texnologik strategiyalar va inson refleksivligi o'rtasidagi sinergiyani ko'rsatadi.

3. **Institutsional qo'llab-quvvatlash va ta'lim.** Ta'lim dasturlari, seminarlar va institutsional yo'riqnomalar refleksiv fikrlashni rivojlantirishda asosiy omillar sifatida aniqlandi. Ishtirokchilar kiberxavfsizlik bo'yicha tuzilgan ta'lim va ong oshirish kampaniyalari yosh foydalanuvchilarga noqonuniy raqamli xulq-atvorning ehtimoliy oqibatlarini tushunishga yordam berishi haqida fikr bildirdilar.

4. **Ijtimoiy va hamkasb ta'siri** Yosh ishtirokchilar hamkasblar bilan suhbatlar, onlayn jamoalarda ishtirok va voqeaviy kiber hodisalar ta'sirini refleksiv ongni shakllantirishda muhimligi haqida xabar berdilar. Fishing, hakerlik yoki ijtimoiy muhandislik hujumlari haqidagi hamkasblar hikoyalari ongni oshirib, shaxsiy raqamli amaliyotlarni qayta ko'rib chiqishga undaydi.

5. **Etik qarashlar.** Ko'pchilik respondentlar etik refleksivlikni mas'uliyatli onlayn xulq-atvorning ajralmas qismi sifatida ta'kidladilar. Ishtirokchilar shaxsiy ma'lumotlar, raqamli huquqlar va bee'tibor harakatlarining ehtimoliy zarari haqida ongli bo'lishdi. Bir talabaning fikri: “Bu faqat o'zimni himoya qilish haqida emas; shuningdek, men onlayndagi harakatlarim boshqalarga qanday ta'sir qilishi mumkinligini ham hisobga olaman.”

Miqdoriy va sifatli ma'lumotlarni integratsiya qilish (Integration of Quantitative and Qualitative Data)

So'rovnoma natijalari va suhbat ma'lumotlarini triangulyatsiya qilish refleksiv ongning ham kognitiv, ham ijtimoiy konstruksiya ekanligini tasdiqladi, u ta'lim, hamkasblar bilan aloqa, shaxsiy tajriba va institutsional strategiyalar ta'sirida shakllanadi. Natijalar texnik malaka va infratuzilma hamda ijtimoiy kontekstlar haqida tanqidiy fikrlashni birlashtirgan shaxslar kiber tahdidlarga nisbatan yuqori barqarorlikka ega ekanligini ko'rsatdi.

Asosiy kuzatuvlar (Key Observations)

- Raqamli savodxonlik refleksiv ongning asosiy belgisi bo'lib, kiber tahdidlarni oldindan aniqlash va kamaytirish imkonini beradi.
- Raqamli infratuzilmani diversifikatsiya qilish foydalanuvchilarga tizimli zaifliklar va xavfsizlik choralari tushunish imkonini beruvchi aniq mexanizm sifatida xizmat qiladi.

- Ta'lim va institutsional qo'llab-quvvatlash reflektiv jarayonlarni kuchaytiradi, xavfsiz va etik onlayn xulq-atvorni mustahkamlaydi.
- Ijtimoiy tarmoqlar va hamkasblar bilan aloqa kollektiv reflektiv fikrlashga hissa qo'shadi, mas'uliyatli raqamli faoliyat uchun normalarni shakllantiradi.
- Etik ong texnik va kognitiv strategiyalarni to'ldirib, raqamli ekosistemada mas'uliyatli ishtirokni ta'minlaydi.

Etik qarashlar (Ethical Considerations)

Tadqiqot uchun etik ruxsat O'zbekiston Respublikasi Oliy va o'rta maxsus ta'lim vazirligi Milliy etika qo'mitasidan olindi. Ishtirokchilardan ma'lum rozilik olindi va ularning maxfiyligi va noma'lumliligi ta'minlandi.

Munozara

Ushbu tadqiqot natijalari O'zbekistonda yoshlar tomonidan kiberxavflarning anglanishi va kiberxavfsizlikni yaxshilashda raqamli infratuzilmani diversifikatsiya qilishning sinergetik mexanizmi rolini tushunishda muhim ma'lumotlar taqdim etadi. Yoshlar orasida reflektiv fikrlash ko'p o'lchovli konstruktsiya sifatida namoyon bo'lib, uning shakllanishi kognitiv, ta'limiy, ijtimoiy va institutsional omillar bilan belgilanadi, bu esa adabiyot tahlilida ko'rib chiqilgan nazariy nuqtai nazarlar bilan muvofiq keladi (Livingstone & Helsper, 2007; Castells, 2010).

Refleksiv anglash va raqamli savodxonlik. Asosiy topilmalardan biri – raqamli savodxonlik va kiberxavflarga nisbatan reflektiv anglash o'rtasidagi mustahkam bog'lanishdir. Ilgari olib borilgan tadqiqotlar bilan muvofiq ravishda (Kshetri, 2021; Papadopoulos et al., 2020), yuqori darajada raqamli kompetensiyaga ega shaxslar raqamli ma'lumotni tanqidiy baholay olishadi, ehtimoliy zaif nuqtalarni aniqlay olishadi va profilaktik choralarni qo'llay olishadi. Bu topilma raqamli savodxonlik nafaqat texnik ko'nikma emas, balki reflektiv baholash va strategik qaror qabul qilish imkoniyatini beruvchi kognitiv quvvat ekanini ko'rsatadi. Bu ma'noda, reflektivlik raqamli kompetensiyaning natijasi va mas'uliyatli onlayn harakatlarning orqa-mediaci sifatida faoliyat ko'rsatadi.

Infratuzilmani diversifikatsiya qilish – reflektivlikni rag'batlantiruvchi omil. Tadqiqot shuni ko'rsatdiki, diversifikatsiya qilingan raqamli infratuzilma reflektiv anglashni oshiradi. Ishtirokchilar bir nechta ehtiyot tizimlar, bulut platformalari va detsentralizatsiya qilingan tarmoqlar bilan tanishlik ularni kiberxavflarga nisbatan faol yondashishga undaydi, deb qayd etishdi. Bu topilmalar tizimli ehtiyot va texnologiyali diversifikatsiya kiberxavflarni kamaytirishda muhim ahamiyatga ega ekanini ko'rsatuvchi tadqiqotlar bilan muvofiq (O'zbekiston Respublikasi Raqamli rivojlanish vazirligi, 2021). Infratuzilmani diversifikatsiya qilish reflektiv kognitsiya bilan sinergetik tarzda ishlab, foydalanuvchilarga ehtimoliy zaif nuqtalarni kengroq tushunish imkonini beradi va oldindan fikrlashni rag'batlantirib, kiberhodisalar ehtimolini kamaytiradi.

Ta'limiy va institutsional ta'sir. Ta'limiy dasturlar va institutsional strategiyalar reflektiv jarayonlarni shakllantirishda muhim qo'llab-quvvatlovchi omil sifatida aniqlandi. Bu McGrew va hamkasblari (2018) topilmalari bilan muvofiq, ular ta'limiy intervensiyalar raqamli ma'lumotni tanqidiy tahlil qilishni yaxshilashini va kiberxavflardan xabardorlikni oshirishini ko'rsatadi. O'zbekiston kontekstida universitet ta'lim dasturlariga kiberxavfsizlik modullarini integratsiya qilish, seminarlar va jamoat xabardorlik kampaniyalari reflektiv fikrlash uchun qulay muhit yaratadi. Bunday intervensiyalar nafaqat texnik malakani oshiradi, balki etik xabardorlikni ham rivojlantirib, raqamli muhitda mas'uliyatli harakat qilishni ta'kidlaydi.

Ijtimoiy va hamkasb kontekstlar. Ijtimoiy muhit, ayniqsa hamkasb tarmoqlar va onlayn jamoalar, reflektiv anglashni shakllantirishda muhim ahamiyatga ega. Ishtirokchilar kiberxodisalar haqidagi umumiy tajribalar, hikoyalar va ijtimoiy tarmoqlardagi muhokamalar orqali o'rganishganini qayd etishdi. Bu topilmalar Vigotskiyning ijtimoiy-farsal nazariyasi bilan muvofiq bo'lib, kognitiv rivojlanish ijtimoiy aloqalar orqali ro'y beradi (Vygotsky, 1978). Kiberxavflarning kollektiv tajribasi guruh darajasida reflektivlikni rivojlantirib, onlayn muhitda xavfsiz va mas'uliyatli harakat qilish uchun ijtimoiy normalarni o'rnatadi.

Reflektiv anglashning etik o'lchami. Tadqiqotda yana bir muhim mavzulardan biri reflektiv jarayonlarning etik jihati bo'ldi. Reflektiv fikrlash yoshlarning raqamli harakatlarining boshqalarga ta'sirini hisobga olishini, maxfiylikka hurmat qilishini va onlayn jamoalarda mas'uliyatli ishtirok etishini rag'batlantiradi. Bu zamonaviy raqamli etikaga oid yondashuvlar bilan muvofiq keladi, ular kiberxavfsizlik ta'limida ma'naviy mas'uliyatni muhim qism sifatida ta'kidlaydi (Floridi, 2014). Etik reflektivlik texnik va kognitiv strategiyalarni qo'llab-quvvatlab, profilaktik choralarni nafaqat xavfdan qochish, balki ijtimoiy mas'uliyat asosida amalga oshirishni ta'minlaydi.

Shaxsiy tajriba va raqamli barqarorlik. Shaxsiy kiberxodisalar tajribasi reflektiv anglashni rag'batlantirishi aniqlandi, bu Kolbning tajribaviy o'rganish nazariyasiga muvofiq (Kolb, 1984). Fishing hujumlari, hakerlik yoki shaxsiyat o'g'irlanishiga duchor bo'lgan ishtirokchilarda yuqori diqqat va profilaktik harakatlar kuzatildi. Bu tajribaviy o'lcham raqamli barqarorlikni rivojlantirishga hissa qo'shadi, ya'ni kiberxavflarni oldindan baholash, unga javob berish va tiklanish qobiliyatini yaratadi. Raqamli barqarorlik real hayotda reflektiv jarayonlarning amaliyotda qo'llanilishini ko'rsatadi va kognitiv, ijtimoiy hamda infratuzilmaviy strategiyalarning ahamiyatini ta'kidlaydi.

Global kiberxavfsizlik nuqtai nazarlari bilan integratsiya. Topilmalar shuningdek kiberxavfsizlik tadqiqotlaridagi global tendensiyalar bilan muvofiq. Yevropa va Shimoliy Amerika tadqiqotlari raqamli savodxonlik, reflektiv fikrlash va

infratuzilma xabardorligi o'rtasidagi bog'lanishni kiberxavflarni kamaytirishda asosiy omil sifatida ko'rsatadi (Singer & Friedman, 2014; Wellman, 2001). O'zbekistonning yondashuvi, infratuzilmani diversifikatsiya qilishni ta'lim va jamoat xabardorligi bilan birlashtirish, milliy kiberxavfsizlik siyosatida texnologiya va kognitiv strategiyalarni integratsiya qilish uchun namuna bo'lib xizmat qiladi.

Ahamiyat va tavsiyalar. Natijalarni muhokama qilish ko'rsatadiki, reflektiv jarayonlar statik xususiyatlar emas, balki kontekstga bog'liq dinamik kognitiv mexanizmlardir. Reflektiv anglashni rivojlantirish uchun ko'p o'lchovli intervensiyalar talab etiladi, jumladan raqamli savodxonlik dasturlari, infratuzilma ta'limi, hamkasblardan o'rganish, ssenariy asosidagi mashqlar va etik yo'riqlar. Texnologik diversifikatsiyani inson markazli ta'lim bilan birlashtirgan milliy strategiyalar sinergetik ta'sir ko'rsatib, nafaqat shaxsiy kiberxavfsizlik harakatlarini, balki kollektiv raqamli barqarorlikni ham oshirishi mumkin. Umuman olganda, ushbu tadqiqot yoshlar orasida reflektiv fikrlash samarali kiberxavfsizlik amaliyotlarining muhim determinanti ekanini ko'rsatadi. Raqamli infratuzilmani diversifikatsiya qilish nafaqat himoya mexanizmi, balki reflektiv kognitsiyani rag'batlantiruvchi omil sifatida xizmat qiladi. Bu esa siyosat va ta'limiy tuzilmalarda kognitiv, texnik, ijtimoiy va etik o'lchamlarni integratsiya qilishning ahamiyatini ta'kidlaydi.

Xulosa

Ushbu tadqiqotning maqsadi yoshlar orasida kiberxavflar haqidagi reflektiv jarayonlarni va raqamli infratuzilmani diversifikatsiya qilishning sinergetik mexanizm sifatida kiberxavfsizlikni yaxshilashdagi rolini o'rganish edi. Natijalar nazariy va amaliy jihatdan bir qator muhim topilmalarni ochib berdi.

Birinchidan, reflektiv fikrlash yoshlar tomonidan kiberxavflarga nisbatan tushuncha va munosabatlarni shakllantiruvchi asosiy kognitiv mexanizm sifatida aniqlandi. Reflektiv jarayonlar yoshlarga raqamli ma'lumotni tanqidiy baholash, ehtimoliy xavflarni oldindan baholash va himoya choralarini qabul qilish imkonini beradi. Tadqiqot ko'rsatdiki, bu jarayonlar ko'p o'lchovli bo'lib, kognitiv ko'nikmalar, ta'limiy tajriba, ijtimoiy aloqalar va institutsional tuzilmalar bilan bog'liq (Livingstone & Helsper, 2007; Castells, 2010).

Ikkinchidan, raqamli savodxonlik reflektiv anglashning muhim determinanti sifatida namoyon bo'ldi. Texnik malakalari va ma'lumotni baholash ko'nikmalari yuqori bo'lgan ishtirokchilar profilaktik va faol kiberxavfsizlik harakatlarini amalga oshirishda yuqori qobiliyatga ega ekanliklari aniqlandi. Bu topilma oldingi tadqiqotlar bilan muvofiq keladi, ular raqamli savodxonlikni nafaqat kognitiv, balki mas'uliyatli onlayn xulq-atvorni qo'llab-quvvatlovchi omil sifatida ta'kidlaydi (Kshetri, 2021; Papadopoulos et al., 2020).

Uchinchidan, tadqiqot shuni ko'rsatdiki, infratuzilmani diversifikatsiya qilish reflektiv anglash va kiberxavfsizlik barqarorligini sezilarli darajada oshiradi. Bir

nechta platformalar, ehtiyot tizimlar va detsentralizatsiya qilingan tarmoqlar bilan tanishlik oldindan fikrlash va xavfni kamaytirish strategiyalarini rag‘batlantiradi. Infratuzilmani diversifikatsiya qilish reflektiv kognitsiya bilan sinergetik tarzda ishlab, texnologik himoya va ehtimoliy kiberxavflarni tanqidiy baholash uchun asosiy strukturani ta’minlaydi (O‘zbekiston Respublikasi Raqamli rivojlanish vazirligi, 2021).

To‘rtinchidan, ta’lim muhiti reflektiv jarayonlarni rivojlantirishda muhim rol o‘ynaydi. Kiberxavfsizlik ta’lim dasturlaridagi strukturalangan modullar, seminarlar va ssenariy asosidagi mashqlar tanqidiy fikrlash, etik anglash va amaliy ko‘nikmalarni rivojlantirishni qo‘llab-quvvatlaydi. Shu bilan birga, ijtimoiy kontekstlar, jumladan hamkasb tarmoqlar va onlayn jamoalar, kollektiv reflektivlikni shakllantirishga hissa qo‘shib, raqamli xavfsizlik bo‘yicha normativ xulq-atvorni rivojlantirishga yordam beradi (McGrew et al., 2018; Vygotsky, 1978).

Beshinchidan, etik reflektivlik mas’uliyatli raqamli xulq-atvorning muhim o‘lchami sifatida aniqlandi. Reflektiv yoshlar nafaqat o‘zlarini kiberxavflardan himoya qiladi, balki o‘z harakatlarining boshqalarga ta’sirini ham hisobga olib, maxfiylik, intellektual mulk va jamoat normalariga hurmat ko‘rsatadi. Ta’lim dasturlari va jamoat xabardorlik kampaniyalariga etik reflektivlikni integratsiya qilish individual va ijtimoiy kiberxavfsizlikni mustahkamlaydi (Floridi, 2014).

Natijada, tadqiqot reflektiv kognitsiya, raqamli savodxonlik, infratuzilmani diversifikatsiya qilish va ijtimoiy-etik ta’limni milliy kiberxavfsizlik strategiyalariga integratsiya qilish muhimligini ta’kidlaydi. Bu elementlar orasidagi sinergetik aloqa raqamli barqarorlikni oshiradi, ya’ni kiberxodisalarni oldindan baholash, unga javob berish va tiklanish qobiliyatini mustahkamlaydi. O‘zbekiston kontekstida diversifikatsiya qilingan raqamli infratuzilmani inson markazli ta’lim bilan birlashtirish zamonaviy kiberxavflarni kamaytirishda barqaror yondashuvni ta’minlaydi.

Tavsiyalar va takliflar

1. **Siyosat va boshqaruv:** Milliy kiberxavfsizlik strategiyalari infratuzilmani diversifikatsiya qilish va ta’lim dasturlarini birlashtirishni afzal ko‘rsatishi lozim. Siyosatchilar asosiy axborot tizimlarida ehtiyot va detsentralizatsiyalangan texnologiyalarni joriy qilish, raqamli savodxonlik va reflektiv anglashni rivojlantirishni ta’minlashi zarur.

2. **Ta’lim va trening:** Universitetlar va oliy o‘rta ta’lim muassasalari kiberxavfsizlik modullari, ssenariy asosidagi o‘rganish va etik refleksiya mashqlarini integratsiya qilishi kerak, bu reflektiv jarayonlar va mas’uliyatli raqamli xulq-atvorni rivojlantiradi.

3. **Jamoat ishtirokchiligi:** Hamkasb tarmoqlar, onlayn jamoalar va jamoat xabardorlik kampaniyalaridan kollektiv refleksivlikni rivojlantirish va onlayn xavfsizlik bo'yicha ijtimoiy normalarni mustahkamlash uchun foydalanish kerak.

4. **Kelgusi tadqiqotlar:** Keyingi tadqiqotlar refleksiv anglashning kiberxavflarga barqarorlikka uzoq muddatli ta'sirini, refleksiv kognitsiyaning madaniy farqlarini va infratuzilmani diversifikatsiya qilishning kiberxavflarni kamaytirishdagi samaradorligini o'rganishi mumkin.

Xulosa qilib aytganda, refleksiv jarayonlar yoshlar orasida kiberxavflar haqidagi tushuncha va mas'uliyatli raqamli xulq-atvorning fundamental qismi hisoblanadi. Raqamli infratuzilmani diversifikatsiya qilish bu kognitiv jarayonlarni rag'batlantiruvchi sinergetik mexanizm sifatida xizmat qiladi va individual hamda ijtimoiy darajada kiberxavfsizlikni mustahkamlaydi. Kognitiv, texnologik, ijtimoiy va etik o'lchamlarning integratsiyasi O'zbekiston va shunga o'xshash kontekstlarda kiberxavfsizlik barqarorligini mustahkamlash uchun kompleks asosni ta'minlaydi.

Adabiyotlar ro'yxati

1. Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
2. Floridi, L. (2014). *The ethics of information*. Oxford University Press.
3. Kshetri, N. (2021). Cybersecurity management in developing countries: Challenges and opportunities. *Journal of Global Information Technology Management*, 24(2), 85–102. <https://doi.org/10.1080/1097198X.2021.1878241>
4. Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, 9(4), 671–696. <https://doi.org/10.1177/1461444807080335>
5. Ministry of Digital Development of the Republic of Uzbekistan. (2021). *National digital transformation strategy of Uzbekistan*. Tashkent: Government Press.
6. McGrew, S., Ortega, T., Breakstone, J., & Wineburg, S. (2018). The challenge that's bigger than fake news: Civic reasoning in a digital world. *American Educator*, 42(3), 4–11.
7. Papadopoulos, T., Oikonomou, A., & Fragidis, G. (2020). Cybersecurity awareness and behavior among adolescents: A systematic review. *Computers & Security*, 95, 101859. <https://doi.org/10.1016/j.cose.2020.101859>
8. Piaget, J. (1972). *Psychology and epistemology: Towards a theory of knowledge*. Penguin Books.
9. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
10. Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

11. Wellman, B. (2001). Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research*, 25(2), 227–252. <https://doi.org/10.1111/1468-2427.00309>
12. Chebotaryova, A. A. (2019). Reflexive processes in the cognition of information security. *Journal of Information Security Studies*, 7(1), 45–62.
13. Zubareva, I. V., Zhidkova, I. V., & Kadushkin, I. V. (2017). Cybersecurity of automated control systems of military purposes. *Cybersecurity Journal*, 4(2), 11–29.
14. Kershisnig, G. (2018). Typologies of cyber threats: Risk assessment and classification. *International Journal of Cybersecurity Research*, 5(1), 30–47.
15. ISO/IEC 27032:2012. (2012). *Information technology – Security techniques – Guidelines for cybersecurity*. International Organization for Standardization.
16. Federal Law of the Russian Federation № 149-FZ. (2005, April 3). *On information, information technologies and protection of information*.
17. Castells, M. (2001). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press.
18. Wellman, B., & Haythornthwaite, C. (2002). *The Internet in everyday life*. Blackwell Publishing.
19. Singer, P. W. (2010). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin.
20. Kshetri, N. (2010). The global cybercrime industry: Economic, institutional and strategic perspectives. *Springer*.