

O'ZBEKISTON FUQAROLARI ORASIDA KIBERSAVODXONLIK DARAJASI TAHLILI

*Musabekova Zinnura *, To'raqulov Abror, To'raqulov Zafar*

Toshkent kimyo-texnologiya instituti, Qarshi davlat texnika universiteti

e-mail: asturaqulov@gmail.com

Annotatsiya: Ushbu maqolada O'zbekiston fuqarolari orasida kybersavodxonlik darajasi hamda uning shakllanish omillari tahlil qilingan. Raqamli texnologiyalar keng joriy etilayotgan sharoitda kybersavodxonlik shaxsiy ma'lumotlarni himoya qilish, internetdan xavfsiz va samarali foydalanish hamda kiberxavfsizlik qoidalariga rioya etishni o'z ichiga oladi. Tadqiqotda aholining turli yosh guruhlari bo'yicha kybersavodxonlik ko'rsatkichlari o'rganilib, mavjud muammolar aniqlangan. Yoshlar internetdan faol foydalansalar-da, kiberrisklarni baholashda bilim yetishmasligi qayd etilgan. Shuningdek, ayrim ijtimoiy qatlamlarda raqamli xavfsizlik ko'nikmalarining sustligi aniqlangan. Maqolada kybersavodxonlikni oshirish bo'yicha ta'limiy va tashkiliy tavsiyalar ishlab chiqilgan bo'lib, ular raqamli madaniyatni rivojlantirishga xizmat qiladi.

Kalit so'zlar: Kybersavodxonlik, kibermadaniyat, kiberxavfsizlik, raqamli texnologiyalar, raqamli bilim va ko'nikmalar, kiberrisklar, axborot xavfsizligi, raqamli tafakkur, onlayn ta'lim, internet xavfsizligi.

KIRISH

Zamonaviy jamiyatning barcha sohalarida raqamli texnologiyalarning keng qo'llanilishi insonlarning internet va axborot tizimlaridan to'g'ri, xavfsiz hamda samarali foydalanish ko'nikmalarini shakllantirishni talab etadi. Shu nuqtayi nazardan kybersavodxonlik tushunchasi muhim ijtimoiy zarurat sifatida namoyon bo'lmoqda. Kybersavodxonlik insonning raqamli muhitda axborotni izlash, qayta ishlash, uzatish, shaxsiy ma'lumotlarni himoya qilish, internet xavfsizlik qoidalariga rioya qilish hamda onlayn makonda sodir bo'ladigan tahdidlarni anglab, ularga to'g'ri javob bera olish qobiliyatini o'z ichiga oladi. Raqamli madaniyatning ushbu tarkibiy qismi nafaqat kompyuter savodxonligini, balki media madaniyat va kiberxavfsizlik bo'yicha ongli yondashuvni ham talab etadi. O'zbekiston Respublikasida raqamli iqtisodiyot va "Raqamli O'zbekiston – 2030" strategiyasi doirasida davlat xizmatlarini elektronlashtirish, onlayn ta'limni rivojlantirish, axborot-kommunikatsiya texnologiyalarining ijtimoiy hayotga jadal kirib borishi kybersavodxonlik darajasini oshirishni yanada dolzarb masalaga aylantirdi. Biroq aholining turli qatlamlari o'rtasida kybersavodxonlik darajasi bir xil emas. Yoshlar internetdan faol foydalansalar-da, ularda shaxsiy ma'lumotlarni himoya qilish yoki kiberhujumlardan ehtiyot bo'lish madaniyati yetarli darajada shakllanmagan holatlar kuzatilmoqda. Aholining o'rta va katta yoshdagi qatlami esa ko'pincha internet resurslaridan foydalanishda qiyinchiliklarga duch kelmoqda, bu esa kiberjinoyatchilikka uchrash

ehtimolini oshiradi. So'nggi yillarda mamlakatimizda firibgarlikning onlayn shakllari, shaxsiy ma'lumotlarni o'g'irlash, bank kartalari orqali kiberjinoyatlar, soxta axborot tarqatish va ruhiy manipulyatsiya kabi tahdidlar ko'paymoqda. Ushbu holat kybersavodxonlikni nafaqat texnik bilim sifatida, balki ijtimoiy ong, axborot madaniyati va mas'uliyatning muhim unsuri sifatida qarashni talab etadi. Shu sababli fuqarolar o'rtasida kybersavodxonlikni rivojlantirish bo'yicha tizimli yondashuv va samarali o'quv-uslubiy mexanizmlar zarur.

Mazkur tadqiqotning dolzarbligi shundan iboratki, O'zbekistonda kybersavodxonlik darajasining real holatini o'rganish, aholining internetdan foydalanish tajribasini tahlil qilish, muammo va zaif jihatlarni aniqlash hamda ushbu sohani rivojlantirishga qaratilgan ilmiy-amaliy tavsiyalar ishlab chiqish bugungi kunning muhim ehtiyojlaridan biridir. Tadqiqot natijalari raqamli xavfsizlik va axborot madaniyati bo'yicha ta'lim tizimini takomillashtirish, ommaviy axborot resurslarida ma'rifiy faoliyatni kuchaytirish hamda kibermadaniyat asosida ijtimoiy ongni rivojlantirishga xizmat qiladi.

ADABIYOTLAR TAHLILI

So'nggi yillarda raqamli texnologiyalarning jadal rivojlanishi jamiyat hayotining barcha jabhalariga, jumladan, ijtimoiy munosabatlar, iqtisodiyot, davlat boshqaruvi va ta'lim tizimiga chuqur kirib bormoqda. Ushbu jarayonda kibermakonning kengayishi bilan bir qatorda kiberxavfsizlik va kybersavodxonlik masalalari ham dolzarb ahamiyat kasb etmoqda [1]. Ayniqsa, raqamli xizmatlardan faol foydalanuvchi bo'lgan aholining kiberxavflarga tayyorgarligi masalasi ilmiy tadqiqotlarda muhim yo'nalish sifatida qaralmoqda [2].

Xalqaro tadqiqotlarda kybersavodxonlik tushunchasi shaxsning axborot texnologiyalaridan ongli, xavfsiz va samarali foydalanish ko'nikmalarining majmui sifatida talqin qilinadi [3]. UNESCO va ITU tashkilotlari hisobotlarida kybersavodxonlik raqamli kompetensiyaning ajralmas qismi ekanligi ta'kidlanib, aholining axborot xavfsizligi bo'yicha bilim darajasini oshirish barqaror rivojlanish omillaridan biri sifatida baholanadi [4, 5].

Bir qator xorijiy olimlar tomonidan olib borilgan tadqiqotlarda aholining kybersavodxonlik darajasi kiberjinoyatchilikka qarshi kurashishda muhim omil ekanligi isbotlangan [6]. Xususan, phishing, zararli dasturlar va shaxsiy ma'lumotlar o'g'irlanishiga qarshi samarali himoya avvalo foydalanuvchining bilim va hushyorligiga bog'liq ekanligi qayd etiladi [7, 8].

MDH davlatlari doirasida olib borilgan ilmiy izlanishlarda esa kybersavodxonlik masalasi ko'proq davlat siyosati va huquqiy mexanizmlar bilan bog'liq holda o'rganilgan [9]. Rossiya va Qozog'iston olimlari tomonidan ishlab chiqilgan konseptual yondashuvlarda aholini kybersavodxonlikka o'rgatish milliy kiberxavfsizlik strategiyasining muhim tarkibiy qismi sifatida ko'rsatilgan [10, 11].

O'zbekiston misolida kybersavodxonlik masalasi so'nggi yillarda davlat darajasida e'tibor qaratilayotgan yo'nalishlardan biri hisoblanadi. Raqamli iqtisodiyotni rivojlantirish va elektron hukumat tizimini joriy etish jarayonlarida

aholining raqamli madaniyati muhim omil sifatida qaralmoqda [12]. Prezident farmonlari va hukumat qarorlarida axborot xavfsizligi hamda aholining kiberxavfsizlik bo'yicha bilimlarini oshirish vazifalari belgilab berilgan [13, 14].

Mahalliy tadqiqotchilar tomonidan olib borilgan ilmiy ishlarda O'zbekiston fuqarolari orasida kybersavodxonlik darajasi notekis taqsimlanganligi, ayniqsa qishloq hududlarida va katta yoshdagi aholida bu borada muammolar mavjudligi ta'kidlanadi [15]. Ta'lim tizimida axborot xavfsizligi fanlarini joriy etish va ommaviy targ'ibot ishlarini kuchaytirish zarurligi qayd etilgan [16, 17].

Shuningdek, statistik ma'lumotlarga asoslangan tadqiqotlarda internet foydalanuvchilarining shaxsiy ma'lumotlarni himoyalash borasidagi bilimlari yetarli emasligi aniqlangan [18]. Bu holat ijtimoiy tarmoqlar va onlayn xizmatlardan foydalanishda xavf-xatarlarni oshirishi mumkinligi ko'rsatilgan [19].

Umuman olganda, mavjud adabiyotlar tahlili shuni ko'rsatadiki, kybersavodxonlik masalasi kompleks yondashuvni talab etadi va u texnik, huquqiy hamda pedagogik omillar uyg'unligida rivojlantirilishi lozim [20, 21]. Shu sababli O'zbekiston sharoitida aholining kybersavodxonlik darajasini tahlil qilish va uni oshirish mexanizmlarini ishlab chiqish ilmiy-amaliy ahamiyatga ega hisoblanadi.

METODOLOGIYA

Ushbu tadqiqot O'zbekiston sharoitida aholining kiberxavfsizlikka oid xabardorlik darajasi, kibermadaniyatning shakllanish jarayoni hamda fuqarolarning raqamli makondagi o'zini tutish xatti-harakatlarini o'rganishga qaratildi. Tadqiqotning asosiy maqsadi kiberxavflar haqida ogohlik darajasini aniqlash, himoya strategiyalarining shakllanganlik darajasini baholash hamda kybersavodxonlikni oshirish bo'yicha amaliy takliflar ishlab chiqishdan iborat bo'ldi. Tadqiqot usuli sifatida ijtimoiy so'rovnoma metodi qo'llanildi. Ushbu usul kybersavodxonlikni bevosita shaxsiy tajriba va kundalik raqamli faoliyat kontekstida o'rganish imkonini berdi. Savolnoma foydalanuvchilarning axborot xavfsizligiga munosabati, onlayn faoliyatdagi himoya odatlari, kiberjinoyatlarga duch kelgan yoki duch kelish ehtimolini sezgan holatlari haqida ma'lumot olishga yo'naltirilgan. So'rovnoma savollarini tuzishda tadqiqot quyidagi uch asosiy yo'nalishga tayanib ishlab chiqildi:

1. Institutsional sharoitlar va tashkiliy madaniyat. Bu yo'nalishda tashkilot va muassasalarda axborot xavfsizligiga oid ichki siyosat mavjudligi, xodimlar uchun kiberxavfsizlik bo'yicha o'quv-seminarlar, treninglar va ogohlantirish tizimlarining joriy etilganlik darajasi baholandi. Shuningdek korxonalarda xavfsizlik protokollariga rioya etilish tizimi, ma'lumotlarni himoya qilish bo'yicha mas'ul shaxslar faoliyati, xavf haqida o'z vaqtida axborot berish mexanizmlari kabi omillar ham o'rganildi.

2. Kundalik raqamli xatti-harakatlar va himoya strategiyalari. So'rovnoma foydalanuvchilar internet va raqamli qurilmalardan foydalanish jarayonida qanday himoya tadbirlarini qo'llashini aniqlashga qaratildi. Jumladan: parollarni yaratish va yangilash odatlari, ikki bosqichli autentifikatsiya (2FA) dan foydalanish, jamoat Wi-Fi tarmoqlaridan foydalanishdagi ehtiyot choralar, mobil ilovalarga ruxsatlar berishdagi ehtiyotkorlik, havola va fayllarning xavfsizligini tekshirish kabi ko'rsatkichlar tahlil

qilindi. Ushbu parametrlar foydalanuvchilarning amaliy kibermadaniyat darajasini aniqlashda muhim omil bo'lib xizmat qildi.

3. Yangi kiberxatarlarni idrok etish va ularga munosabat: Raqamli makonda so'nggi yillarda keng tarqalgan yangi turdagi kiberjinoyatlar — sun'iy intellekt orqali yaratiladigan soxta kontent (deepfake), fishing xabarlar, bank tizimlariga qaratilgan kiberhujumlar va onlayn ruhiy zo'ravonlikka nisbatan fuqarolarning xabardorligi baholandi. Bunda: tahdidni anglash qobiliyati, riskni baholash madaniyati, onlayn muhitdagi o'zini himoya qilish strategiyalarini tanlash mexanizmini aniqlashga yordam berdi.

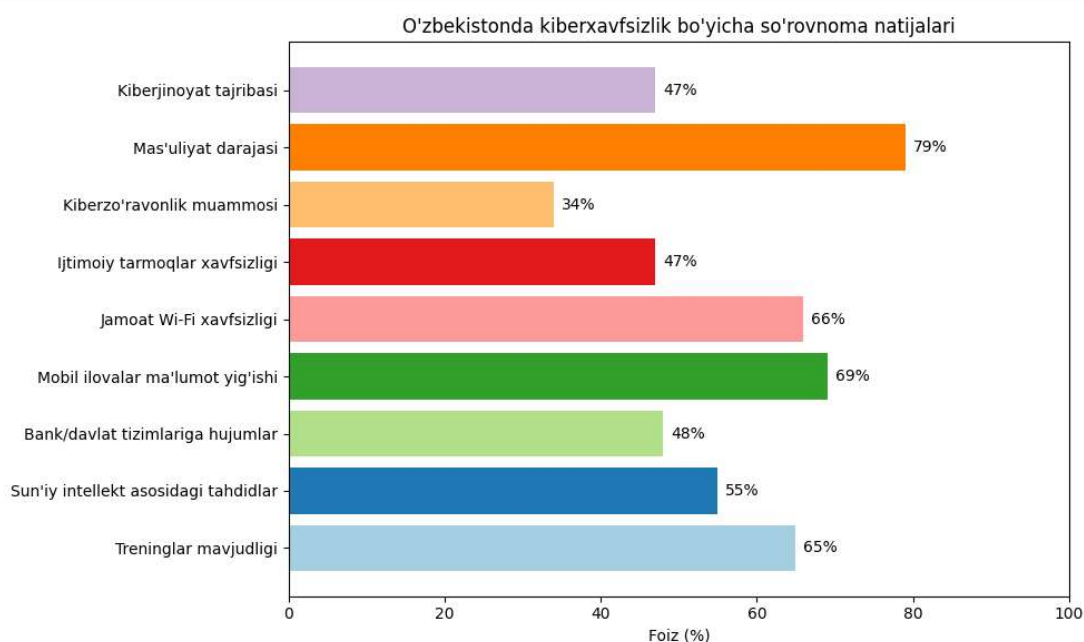
So'rovnoma o'tkazish tartibi. So'rovnoma onlayn shaklda o'tkazildi va anonim tarzda ma'lumotlar yig'ildi.

Bu ishtirokchilarga o'z fikrlarini erkin ifodalash imkonini berdi hamda natijalarning ob'ektivligi oshirdi. Jami 116 nafar respondent tadqiqot jarayoniga jalb qilindi. Ular turli yosh toifalarini (16 yoshdan 55 yoshgacha), kasbiy guruhlarni (talabalar, xizmatchilar, pedagoglar, tadbirkorlar), hududlarni (Toshkent shahri va viloyatlar) qamrab oldi. Olingan ma'lumotlar qayta ishlanishi.

Yig'ilgan javoblar kodlash orqali tizimlashtirildi, foiz ko'rsatkichlari, chastota taqsimoti va o'rtacha qiymatlar hisoblandi. Keyinchalik natijalar taqqoslash va umumlashtirish metodi orqali talqin qilindi.

NATIJALAR VA MUHOKAMA

Tadqiqot jarayonida O'zbekiston fuqarolari o'rtasida kibersavodxonlik va kiberxavfsizlik bo'yicha o'tkazilgan so'rovnoma natijalari jamiyatda kiberxavfsizlik madaniyati yetarli darajada shakllanmaganligini ko'rsatdi. Diagrammada aks ettirilgan ma'lumotlar shuni anglatadiki, aholining raqamli texnologiyalardan foydalanishi keng tarqalgan bo'lsa-da, ularning xavfsiz foydalanish bo'yicha amaliy bilim va ko'nikmalari bir xil emas.



1-rasm. O'zbekistonda kiberxavfsizlik bo'yicha so'rovnoma natijalari jadvali

Mas'uliyat darajasi – 79% Respondentlarning katta qismi (79%) internetdan foydalanishda shaxsiy ma'lumotlar xavfsizligi uchun ma'lum darajada mas'uliyat sezishini bildirgan. Biroq ushbu mas'uliyat amaliy ko'rinishda hamisha aks etmaydi, chunki xavfsizlik choralari yetarli qo'llanilmaydi. Mobil ilovalar orqali ma'lumot yig'ilishi – 69%. Ishtirokchilarning 69% i mobil ilovalar tomonidan shaxsiy ma'lumotlarning yig'ilishi va qayta ishlanishidan xavotir bildirgan. Bu aholining shaxsiy hayot daxlsizligi borasida ong darajasi oshayotganini ko'rsatadi. Jamoat Wi-Fi xavfsizligi – 66%. Jamoat Wi-Fi tarmoqlaridan foydalanish xavfi ko'pchilik tomonidan tan olingan bo'lsa-da, amaliy ehtiyot choralariga rioya qilmaslik yuqori darajada qolmoqda. Bu foydalanuvchilarning nazariy xabardorligi yuqori, biroq amaliy ko'nikmalari zaif ekanini anglatadi. Treninglar mavjudligi – 65%. Respondentlarning 65% ta'lim muassasalari yoki ish joylarida kiberxavfsizlik bo'yicha ma'lum darajada treninglar o'tkazilayotganini qayd etgan. Ammo treninglarning ko'lami va sifatining yetarli emasligi ham alohida muammo bo'lib qolmoqda. Sun'iy intellekt asosidagi tahdidlar – 55%. So'rovda qatnashganlarning yarmidan ko'pi sun'iy intellekt yordamida amalga oshiriladigan "deepfake" video, audio va matnli soxtalashtirish tahdidlarini tan olgan. Bu kibertahdidlarning shakli zamonaviylashib borayotganini ko'rsatadi. Bank va davlat tizimlariga hujumlar – 48% Respondentlarning deyarli yarmi moliyaviy tizimlar kiberhujumlar uchun nisbatan zaif bo'lishi mumkinligini ta'kidlagan. Shunga qaramay, ko'plab foydalanuvchilar o'z hisoblarini himoya qilishda yetarlicha ehtiyotkor emas. Kiberjinoyat tajribasi – 47%. Ishtirokchilarning 47% i hayotida kamida bir marta raqamli firibgarlik yoki hisob buzilishi kabi kiberjinoyatga duch kelganini bildirgan. Bu kiberjinoyatlarning keng tarqalganligini va real xavf ekanini ko'rsatadi. Kibero'rganish muammosi – 34%. Eng past ko'rsatkich kibermadaniyatni o'rganishdagi tizimli yondashuvning yetishmasligi bilan bog'liq. Aksariyat respondentlar kiberxavfsizlikni mustaqil o'rganishga vaqt, imkon yoki manba yetishmasligini qayd etgan.

XULOSA

Tadqiqot natijalari shuni ko'rsatdiki, O'zbekiston fuqarolari orasida kipersavodxonlik va kiberxavfsizlik madaniyati shakllanayotgan bo'lsada, uning darajasi bir xil emas va hali yetarli darajada mukammal emas. Aholining aksariyati (79%) raqamli xavfsizlikka nisbatan shaxsiy mas'uliyat borligini anglaydi, biroq ularning amaliy himoyalani sh ko'nikmalari to'liq shakllanmagan. Mobil ilovalar orqali shaxsiy ma'lumotlarning yig'ilishi va jamoat Wi-Fi tarmoqlaridan foydalanish xavfi ko'pchilik tomonidan sezilayotgan bo'lsa-da, kundalik foydalanish jarayonida ehtiyot choralariga yetarli e'tibor berilmayotgani aniqlandi. Sun'iy intellekt asosidagi soxta kontent, fishing hamda bank tizimlariga qaratilgan kiberhujumlar haqidagi xabardorlik o'rtacha darajada bo'lib, aholining yarmi bu kabi xavf-xatarlarni real muammo sifatida baholaydi. Shu bilan birga, kiberjinoyatlarga duch kelganlar sonining 47% bo'lgani kiberxavfsizlikni bevosita hayotiy zaruratga aylanganini ko'rsatadi. Tahlil natijalari shuni anglatadiki, kipersavodxonlikni oshirish uchun mavjud resurslar yetarli bo'lsa-da, ular muntazam va tizimli shaklda qo'llanilmayapti. Ta'lim muassasalari, korxona

va tashkilotlarda o'tkazilayotgan treninglar ko'proq nazariy xususiyatga ega bo'lib, amaliy himoya ko'nikmalarini shakllantirishga yetarlicha e'tibor qaratilmagan. Demak, O'zbekistonda kibermadaniyatni rivojlantirish jarayoni davom etayotgan bo'lsada, uni kuchaytirish uchun quyidagilarni amalga oshirish lozim:

• **Ta'lim tizimiga** raqamli xavfsizlik asoslari bo'yicha **majburiy kurslar joriy etish;**

• **Jamoatchilik uchun onlayn va oflayn treninglar sonini oshirish;**

• **Mobil ilovalar, bank tizimlari va internet xizmatlari foydalanuvchilari uchun aniq amaliy qo'llanmalar ishlab chiqish;**

• **Ommaviy axborot vositalari orqali keng qamrovli tushuntirish kampaniyalarini tashkil etish.**

Shunday qilib, kibersavodxonlikni oshirish jamiyatda raqamli texnologiyalardan xavfsiz, samarali va ongli foydalanish madaniyatini shakllantirishga xizmat qiladi hamda mamlakatning raqamli transformatsiya jarayonini tezlashtirishda muhim omil sifatida namoyon bo'ladi.

FOYDALANILGAN ADABIYOTLAR

1. S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and prevention of spear phishing attacks: A comprehensive survey," *Comput. Secur.*, vol. 151, p. 104317, Apr. 2025, doi: 10.1016/j.cose.2025.104317.
2. G. W. Giumetti and R. M. Kowalski, "Cyberbullying via social media and well-being," *Curr. Opin. Psychol.*, vol. 45, p. 101314, Jun. 2022, doi: 10.1016/j.copsyc.2022.101314.
3. Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, and Chinonye Esther Ugochukwu, "Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio," *World J. Adv. Res. Rev.*, vol. 21, no. 3, pp. 625–643, Mar. 2024, doi: 10.30574/wjarr.2024.21.3.0707.
4. Кибербезопасность: учебное пособие / под ред. А. А. Иванова. — Москва: Юрайт, 2020. — 256 с.
5. Солдатов А. И. Информационная безопасность личности. — Москва: Академия, 2019. — 192 с.
6. OECD. Digital Security Risk Management. — Paris: OECD Publishing, 2015. — 128 p.
7. UNESCO. Digital Literacy in Education. — Paris: UNESCO, 2018. — 64 p.
8. ITU. Global Cybersecurity Index. — Geneva: ITU, 2021. — 96 p.
9. Wall D. Cybercrime: The Transformation of Crime in the Information Age. — Cambridge: Polity Press, 2007. — 220 p.
10. Hadnagy C. Social Engineering: The Science of Human Hacking. — Indianapolis: Wiley, 2018. — 320 p.
11. Kaspersky Lab. Cybersecurity Awareness Report. — Moscow, 2020. — 54 p.
12. Марков А. С. Киберпространство и национальная безопасность. — Москва: Наука, 2017. — 210 с.

13. Лопатин В. Н. Основы кибербезопасности. — Москва: Инфра-М, 2019. — 240 с.
14. Нургалиев Е. А. Информационная безопасность в Республике Казахстан. — Алматы: Экономика, 2020. — 180 с.
15. Ўзбекистон Республикаси Президенти. Рақамли иқтисодиётни ривожлантириш стратегияси. — Тошкент, 2020. — 32 б.
16. Ўзбекистон Республикаси Президентининг фармони. Ахборот хавфсизлигини таъминлаш чора-тадбирлари тўғрисида. — Тошкент, 2019.
17. Ўзбекистон Республикаси Вазирлар Маҳкамаси қарори. Электрон ҳукумат тизимини ривожлантириш. — Тошкент, 2021.
18. Раҳимов Б. Б. Ўзбекистонда ахборот хавфсизлиги муаммолари // Ахборот жамияти. — 2020. — №2. — Б. 45–52.
19. Саидов Ж. К. Кибертаълим асослари. — Тошкент: Фан, 2021. — 168 б.
20. Юлдашев Ш. Рақамли маданият ва жамият. — Тошкент: Innovatsiya, 2022. — 144 б.
21. World Bank. Digital Development Report. — Washington: World Bank, 2020. — 110 p.