Kiberfiribgarliklardan himoyalanişida kibergigiyena va kiberprofilaktika integratsiyasi

Quvandiqov Şahzod Burxon öğli
Özbekiston Respublikasi Içki işlar vazirligi Akademiyasi 3-öquv kurs 329-guruh kursanti

Isaqov Abror Faxriddinoviç
IIV Akademiya Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boşliği örinbosari

Annotatsiya: Mazkur maqolada kibergigiyena madaniyatini şakllantiriş, kiberfiribgarliklarning oldini oliş hamda aholining axborot savodxonligini oşiriş masalalari yoritilgan. Raqamli texnologiyalar jadal rivojlanayotgan hozirgi davrda internet va elektron xizmatlardan foydalaniş kengayib borişi bilan bir qatorda kiberxavflar, xususan, kiberfiribgarlik, şaxsiy ma'lumotlarni öğirlaş, zararli dasturlar va moliyaviy jinoyatlar soni ham ortib borayotgani tahlil qilingan. Maqolada kibergigiyena tuşunçasining mazmuni, uning profilaktik ahamiyati hamda foydalanuvçilarni raqamli muhitda xavfsiz harakatlanişga örgatişning muhim jihatlari oçib berilgan.

Şuningdek, kibergigiyena madaniyatining asosiy qoidalari, jumladan, kuçli parollardan foydalaniş, antivirus dasturlarini qöllaş, xavfsiz veb-saytlarni tanlaş, şaxsiy ma'lumotlarni himoya qiliş va internetdagi şubhali havolalardan ehtiyot böliş kabi çoralar bayon etilgan. Kibergigiyenaning xabardorlik, öqitiş, amaliyot va nazorat bosqiçlari asosida şakllaniş jarayoni izohlangan.

Maqolada Özbekistonda kiberjinoyatlar sonining ortib borayotgani, aholi orasida raqamli savodxonlikni oşiriş zarurati hamda mahalla darajasida profilaktik tarğibot işlarini kuçaytirişning dolzarbligi asoslab berilgan. Bundan taşqari, Özbekiston Respublikasida axborot xavfsizligi va kiberxavfsizlikni ta'minlaşga qaratilgan davlat siyosati, Prezident

farmon va qarorlarining mazkur yönalişdagi ahamiyati yoritilgan. Tadqiqot natijalari kibergigiyena madaniyatini rivojlantiriş jamiyatda xavfsiz raqamli muhitni şakllantirişning muhim omili ekanini körsatadi.

Kalit sözlar: kibergigiyena, kiberxavfsizlik, kiberfiribgarlik, axborot xavfsizligi, profilaktika, media savodxonlik.

Annotation: This article discusses the issues of forming a cyber hygiene culture, preventing cyber fraud, and increasing the information literacy of the population. In the current era of rapid development of digital teçnologies, along with the expansion of the use of the Internet and electronic services, the number of cyber threats, in particular, cyber fraud, theft of personal information, malicious programs, and financial crimes, is also increasing. The article reveals the content of the concept of cyber hygiene, its preventive importance, and important aspects of teaching users to navigate safely in the digital environment.

It also outlines the basic rules of cyber hygiene culture, including the use of strong passwords, the use of antivirus programs, the selection of safe websites, the protection of personal data, and the avoidance of suspicious links on the Internet. The process of forming cyber hygiene based on the stages of awareness, training, practice, and control is explained.

The article substantiates the growing number of cybercrimes in Uzbekistan, the need to increase digital literacy among the population, and the urgency of strengthening preventive propaganda at the mahalla level. In addition, the state policy aimed at ensuring information security and cybersecurity in the Republic of Uzbekistan, the importance of presidential decrees and resolutions in this direction are highlighted. The results of the study show that the development of a culture of cyber hygiene is an important factor in forming a safe digital environment in society.

Keywords: cyber hygiene, cybersecurity, cyber fraud, information security, prevention, media literacy.

Annotatsiya: В данной статье рассматриваются вопросы формирования культуры кибергигиены, предотвращения кибермошенничества и повышения информационной грамотности населения. В современную эпоху стремительного развития цифровых технологий, наряду с расширением использования Интернета и электронных услуг, растет и число киберугроз, в частности, кибермошенничества, кражи личной информации, вредоносных программ и финансовых преступлений. В статье раскрывается содержание концепции кибергигиены, ее профилактическое значение и важные аспекты обучения пользователей безопасному взаимодействию в цифровой среде.

Также изложены основные правила культуры кибергигиены, включая использование надежных паролей, использование антивирусных программ, выбор безопасных веб-сайтов, защиту персональных данных и избегание подозрительных ссылок в Интернете. Объясняется процесс формирования кибергигиены на основе этапов осведомленности, обучения, практики и контроля.

В статье обосновывается растущее число киберпреступлений в Узбекистане, необходимость повышения цифровой грамотности населения и насущная необходимость усиления профилактической пропаганды на уровне махалл. Кроме того, подчеркивается государственная политика, направленная на обеспечение информационной безопасности и кибербезопасности в Республике Узбекистан, а также важность президентских указов и постановлений в этом направлении. Результаты исследования показывают, что развитие культуры кибергигиены является важным фактором формирования безопасной цифровой среды в обществе.

Ключевые слова: кибергигиена, кибербезопасность, кибермошенничество, информационная безопасность, профилактика, медиаграмотность.

KIRIŞ

XXI asr “Raqamli davr” sifatida e’tirof etilmoqda. Internet, bulutli texnologiyalar, sun’iy intellekt va mobil qurilmalar inson hayotini tubdan özgartirdi. Biroq texnologiyalar

rivoji bilan birga kiberxavflar ham murakkablaşib bormoqda. Bugungi kunda oddiy foydalanuvçidan tortib yirik kompaniyalargaça turli tahdidlarga duç kelmoqda: ma'lumotlar öğirlanişi, akkauntlar buzilişi, moliyaviy firibgarlik va boşqalar.Şu sababli, xavfsizlikni faqat texnik vositalar orqali emas, balki inson omili orqali ham ta'minlaş muhimdir. Aynan şu yerda kibergigiyena madaniyati asosiy rol öynaydi.

Kibermakonda şaxs, jamiyat va davlat manfaatlarini taşqi va içki tahdidlardan himoya qiliş davlatning kiberxavfsizligini ta'minlaşda ustuvor hisoblanadi. Kiberxavfsizlik sohasini tartibga solişga nisbatan yagona yondaşuv ma'lumotlarga işlov beriş hamda himoya qiliş böyiça dasturiy va texnik vositslarni işlab çiqariş hamda joriy etiş jarayonini taşkil etiş, uning monitoringini va nazoratini amalga oşirişga qaratilgan axborot tizimlarini hamda resurslarini kiberhimoya qilişning yagona davlat tizimi taşkil etilgan holda ta'minlanadi. Kiberxavfsizlikni ta'minlaş uşbu sohadagi munosabatlarni huquqiy, ma'muriy va texnik jihatdan tartibga soliş tizimini şakllantirişda yagona yondaşuvlar asosida amalga oşirilişi kerak

Kibergigiyena va kiberprofilaktikaning integratsiyasi kiberfiribgarliklarga qarşi kuraşişda samarali mexanizm hisoblanadi. Çunki faqat texnik himoya vositalarining özi yetarli emas; foydalanuvçilarning ongli ravişda xavfsizlik qoidalariga amal qilişi ham muhim omil sanaladi. Integratsiyalaşgan yondaşuv orqali bir tomondan foydalanuvçilarda xavfsiz raqamli xulq-atvor şakllantirilsa, ikkinçi tomondan davlat va taşkilotlar tomonidan profilaktik nazorat hamda himoya tizimlari kuçaytiriladi. Natijada kiberhujumlarning oldi olinadi, foydalanuvçilarning axborot xavfsizligi ta'minlanadi va raqamli muhitning barqarorligi oşadi.

Mazkur maqola kiberfiribgarliklardan himoyalanişda kibergigiyena va kiberprofilaktika integratsiyasining nazariy hamda amaliy jihatlarini örganişga qaratilgan bölib, unda raqamli xavfsizlikni ta'minlaşning zamonaviy usullari, profilaktik çoralarning samaradorligi hamda foydalanuvçilarning kiberxavfsizlik madaniyatini şakllantiriş masalalari tahlil qilinadi

METODOLOGIYA VA MUHOKAMA

Bugungi kunda Özbekistonda 50 ga yaqin tölov tizimi bölib, ularning hammasi ham kiberxavfsizlik talablariga javob bermasligi qayd etildi. Mutasaddi vazirlik va idoralarga barça elektron tölov tizimlari uçun yagona kiberxavfsizlik talablarini işlab çiqiş va ijrosini qat'iy nazorat qiliş topşirildi. IT xizmatlari hajmini 20 trillion sömga, eksportni 800 million dollarga yetkaziş, tarmoqlarda 130 ta axborot tizimini joriy qiliş va 750 ta davlat xizmatini töliq raqamlaştiriş borasidagi rejalarni işlab çiqiş muhimligi qayd etildi. Firibgarlikdan himoyalanişda fuqarolarning özlari ham faol iştirok etişlari şartdir. Firibgarlik jinoyatining jabrlanuvçisi bölib qolişdan saqlaniş uçun quyidagilar töğrisida ogoh böliş zarur hisoblanadi:

Birinçidan, işontiriş maqsadida özini bank, huquqni muhofaza qiluvçi organ yoki biron savdo taşkilotining xodimi sifatida taniştiruvçi begona şaxslardan qönğiroq bölişi, SMS-xabarnoma yoki ijtimoiy tarmoqlar orqali turli xabarlarning kelib tuşişidan ogoh böliş;

Ikkinçidan, turli sovğalar ğolibiga aylaniş, sizning foydangizga har qanday mablağlarni ötkazib beriş yoki tovar va xizmatlarni jozibador şartlarda sotib oliş kabi göyoki juda foydali va kutilmagan imkoniyatlarning taklif etilişidan xuşyor böliş;

Uçinçidan, yutuqlarni keyinçalik bank kartasiga ötkazib beriş şarti bilan turli hil sörovlar va lotereyalarda iştirok etiş taklif qilinişidan ehtiyot böliş;

Törtinçidan, yutuqlarni qabul qiliş yoki tovar va xizmatlar uçun tölovlarni amalga oşiriş maqsadida turli mobil ilovalarni örnatiş yoki havolalar orqali bank kartangiz yohud şaxsiy ma'lumotlaringizni kiritiş töğrisida takliflar berilişidan ehtiyotkor böliş;

Beşinçidan, hisobvarağingizdagi pul mablağlari yöqolişi mumkinligi haqida qörqitiş va tezkor qaror qabul qilişga majburlovçi ruhiy bosim ötkaziş holatlaridan ogoh böliş;

Oltinçidan, hisobingizga xatolik bilan pul mablağı ötkazib yuborilganligi va uşbu mablağlarni qaytarişni sörab qönğiroq qiliş holatlari bölganida xuşyorlik çoralarini körilişi zarur.

Kibergigiyena – bu foydalanuvçilarning raqamli muhitda xavfsiz harakatlanişini ta'minlovçi bilim, könikma va odatlar yiğindisidir. U axborot xavfsizligi fanining amaliy yönalişlaridan biri hisoblanadi. Kibergigiyena oddiy qoidalar majmui bölib körinsa-da, u

insonlarning kundalik hayotida doimiy qöllanilişi kerak bölgan xavfsizlik madaniyatidir. Masalan, qanday qilib biz şaxsiy gigiyenaga amal qilsak (qöl yuviş, tozalik), xuddi şunday raqamli muhitda ham “tozalik”ni saqlaş zarur. Kibergigiyena madaniyati quyidagi asosiy qoidalarga asoslanadi:

Birinçi qoida. Parol va kodlaringizni heç kimga aytmang Kartaning PIN-kodi, CVC-/SVV-kodi (Visa va Mastercard uçun kartaning old tarafidagi maxfiy kodi), amal qiliş muddati va boşqa ma’lumotlarini heç kimga aytmang. Agar sizga bankning texnik qöllab-quvvatlaş xizmatidan yoki “Bank menejeri” qönğiroq qilib kartangiz bloklanganini aytib kartangiz ma’lumotlarini sörasa ehtiyot bölişingiz kerak. Bank xodimi heç qaçon kartaga boğliq ma’lumotlarni söramaydi. Xaridlar yoki hisobvaraq böyiça tölovni amalga oşirganingizda kartangizni sotuvçi yoki ofitsiantning qöliga bermang, PIN-kodini ularga aytmang. Parolingizni kiritişda tölov terminali yoki ATM bankomatlarida klaviaturasini har doim qölingiz bilan yopib turing. Bundan taşqari, nazorat kameralari siz PIN-kodingizni terayotgan jarayonni körmayotganiga işonç hosil qiling. Bank kartangiz va bank veb-saytidagi şaxsiy kabinetingizga kiriş uçun murakkab parolni yarating.

Ikkinçi qoida. Bank kartangizga SMS-xabarnomasini ulang. Har doim hisob operatsiyalaringizni kuzatib boring. Barça faol kartalaringiz böyiça SMS-xabarnoma xizmatini ulab qöying. Şunda har bir karta böyiça amalga oşirilgan operatsiyalar haqida xabarnoma olasiz. Buning uçun sizga xizmat körsatuvçi bankomatlarda «SMS xabarnoma»ni tanlab, mobil telefon raqamingizni kiritişingiz kerak.

Uçinçi qoida. Antiviruslardan foydalaning. Antivirus dasturini siz foydalanadigan barça moslamalarga – kompyuteringiz, planşetingiz va mobil telefoningizga örnatiş juda muhimdir. Antivirus dasturi firibgarlar pul öğirlaş uçun foydalanadigan dasturlar va veb-saytlardan himoya qiladi. Internetda funksiyalari çeklangan antivirus dasturlarining bepul versiyalarini topişingiz mumkin. Eng muhimi, ularni rasmiy ilovalar dökonlaridan yoki taniqli antivirus işlab çiquvçilarning veb saytlaridan yuklab olişdir.

Törtinçi qoida. Ma’lumotni qayta tekşiring Kartangizga boğliq bölgan muammolarni (blokirovka, tölovlar rad etilişi) qayta tekşiring. Buning uçun bankning işonç

telefoniga murojaat qiling. Telefon raqami xizmat körsatuvçi bankning rasmiy veb-saytida körsatilgan böladi.

Beşinçi qoida. Xavfsiz veb-saytlarni tanlang Faqat tasdiqlangan veb-saytlarga kiring. Sizga SMS-xabarlar orqali yoki elektron poçtangizga noma'lum «xayrixoh»lardan kelgan internet havolalarga kirmang. Firibgarlar taniqli rasmiy onlayn-dökonga öxşaş soxta veb-sayt yaratadi. Soxta veb-saytning nomi bir neçta harfdan taşqari deyarli rasmiy veb-sayt bilan bir xil böladi. Şuning uçun har doim brauzerning manzil satrini (veb-sayt manzili körsatilgan qatorni) diqqat bilan tekşirişingiz kerak. Rasmiy va işonçli veb-saytlar manzilini qölda tering yoki brauzerning saqlab qoliş funksiyasini işlating. Veb-sayt manziliga e'tibor bering. Xavfsiz sayt https:// bilan boşlanadi. Himoyalangan veb-sayt manzilida yopiq qulf belgisi böladi. Agar veb-sayt xavfsiz bölmasa, unga şaxsiy yoki kredit karta ma'lumotlarini kiritmaslik kerak. Har qanday veb-saytga bank kartasi yoki pasport hamda şaxsni tasdiqlovçi boşqa hujjatlarning ma'lumotlarini kiritişdan oldin, uni yaxşilab örganiş va internetda foydalanuvçilar qoldirgan fikrlarni körib çiqiş kerak.

Oltinçi qoida. Xaridlar va xizmatlar tölovi uçun faqat mobil qöllanmangizni işlating Xaridlar qiliş, bank veb-saytlariga yoki bank ilovalariga kiriş uçun faqat özingizning şaxsiy kompyuteringiz, planşet va telefoningizdan foydalaning. Barça mobil moslamalaringizga parollar qöying. Agar bank mobil ilovasi örnatilgan, SMS-xabarlari va parollari keladigan mobil telefoningizni yöqotsangiz, darhol sizga xizmat – 107 – körsatuvçi bankka xabar bering. SMS-xabarnoma funksiyasini va raqamga boğlangan bank xizmatlarini öçirib qöyişingiz kerak.

Kibergigiyena birdan şakllanmaydi, u bosqiçma-bosqiç rivojlanadi:

1. Xabardorlik (awareness) - Foydalanuvçilarga xavflar haqida ma'lumot beriş. Masalan, noma'lum havolalarni bosmaslik, begona fayllarni yuklab olmaslik yoki şaxsiy ma'lumotlarni işonçsiz saytlarga kiritmaslik kabi oddiy xavfsizlik qoidalariga amal qiliş odati paydo böladi.

2. Öqitiş (education) – Kiberxavfsizlik xodimlari, profilaktika inspektorlari va jamoatchilik iştirokida aholiga kiberfiribgarliklardan himoyalaniş böyiça treninglar ötkaziş.

3. Amaliyot (practice) - Olingan bilimlarni kundalik hayotda qöllaş ya'ni murakkab va xavfsiz parollardan foydalaniş, parollarni boşqalarga bermaslik, qurilmalarni muntazam yangilab boriş, şubhali sayt va ilovalardan ehtiyot böliş, internetda axborot almaşişda ehtiyotkorlikka rioya qiliş.

4. Nazorat (control) - bu bosqiçda taşkilot va muassasalarda axborot xavfsizligi siyosatiga amal qilinişi monitoring qilinadi. Nazorat quyidagi yönalişlarda olib boriladi: xavfsizlik qoidalariga rioya etilişini tekşiriş, foydalanuvçi faoliyatini monitoring qiliş, xavfsizlik tizimlarini yangilaş, ehtimoliy tahdidlarni aniqlaş, xodimlar uçun muntazam instruktsiya joriy etiş. Nazorat orqali kiberxavfsizlikdagi kamçiliklar aniqlanadi va ularni bartaraf etiş çoralari köriladi.

Kiberprofilaktika (inglizça, "cyber" raqamli muhit, yunonça, "profilaktikos" saqlovçi, oldini oluvçi) — bu axborot-kommunikatsiya texnologiyalari va internet muhitida yuzaga kelişi mumkin bölgan kiberxavflar, kiberfiribgarliklar hamda kiberjinoyatlarning oldini olişga qaratilgan taşkiliy, texnik, huquqiy va ijtimoiy çora-tadbirlar tizimidir. Kibergigiyena aynan şu vazifani bajaradi. Masalan kuçli parol işlatiş orqali akkaunt buzilişining oldi olinadi, şubhali fayllarni yuklamaslik orqali viruslardan himoyalaniş mumkin, ikki bosqiçli parol xavfsizligini yoqiş orqali hisobni qöşimça himoya qiliş ta'minlanadi. Agar foydalanuvçilar kibergigiyena qoidalariga amal qilsa, köplab kiberjinoyatlar sodir bölmaydi. Şu sababli kiberprofilaktika kiberjinoyatchilikka qarşi eng samarali "profilaktik vosita" hisoblanadi.

Özbekistonda kiberjinoyatlar soni ortib borayotganligi sababli (2025-yilda jami jinoyatlarning 44.4% i), aholining kiberxavfsizlik savodxonligini oşiriş davlat siyosati darajasiga kötarilgan. Hozirgi vaqtda yurtimizda quyidagi muammolar mavjud. Bular, fuqarolarning beparvoligi va e'tiborsizligi; raqamli savodxonlik darajasining pastligi; yangi tahdidlarning tez paydo bölişi; Ijtimoiy tarmoqlarda ortiqça ma'lumot ulaşiş. Bu muammolar kibergigiyenani yanada rivojlantiriş zarurligini körsatadi.

Media savodxonlik - turli axborot vositalarini (internet, ijtimoiy tarmoqlar, elektron resurslar) tanqidiy baholaş, töğri va notöğri axborotni ajrata oliş, onlayn muhitda xavfsiz va

mas’uliyatli faoliyat yuritiş qobiliyati. Media savodxonlik öquvçilarga kiberxavflardan himoyalaniş va axborot oqimini ongli boşqariş imkonini beradi. Kiberxavfsizlik - raqamli muhitdagi şaxsiy va ijtimoiy ma’lumotlarni, qurilmalarni va tizimlarni zararli ta’sirlardan himoya qiliş tizimi. Bu tuşunça öquvçilarning internet va raqamli texnologiyalardan xavfsiz foydalanişini, ma’lumotlarni yöqotiş, öğirlaş yoki notöğri işlatişdan saqlanişini öz içiga oladi. Algoritm - ma’lum bir vazifani yoki jarayonni ketma-ket va tizimli qadamlar orqali bajariş tartibi. Mazkur tadqiqot kontekstida pedagogik algoritm öquvçilarning axloqiy ong va media savodxonligini rivojlantiriş, şuningdek, kiberxavflardan himoya qiliş böyiça bosqiçma-bosqiç amaliy tavsiyalar va ta’limiy usullarni ifodalaydi.

Raqamli texnologiyalar hayotimizni osonlaştirayotgan bir paytda, fuqarolarni kiberxavfsizlik madaniyatiga örgatiş — nafaqat huquq-tartibot organlarining, balki butun mahalla jamoatchiligining vazifasidir. Şu sababli “Kiberfiribgarliklar va ularning mahalla darajasida profilaktikasi” mavzusi bugungi kun uçun ijtimoiy, huquqiy va ma’naviy jihatdan nihoyatda dolzarbdir. Bu nafaqat jinoyatchilikni kamaytiriş, balki xavfsiz, ogoh va mas’uliyatli fuqarolik jamiyatini şakllantiriş sari muhim qadamdir. Şuningdek yuqoridagi holatlar vujudga kelişi jadal avj olayotgani kiberfiribgarliklarning oldini oliş, fuqarolarning axborot savodxonligini oşiriş va internet xavfsizligini ta’minlaş masalalari davlat siyosatining ustuvor yönalişiga aylantirildi. Özbekiston Respublikasi Prezidenti Şavkat Mirziyoyev öz nutqlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlaş — milliy xavfsizlikning ajralmas qismi ekanini alohida ta’kidlab kelmoqda. Xususan, 2025 -yil 30-apreldagi PQ-153-sonli “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarşi kuraşiş faoliyatini yanada kuçaytirişga qaratilgan çoratadbirlar töğrisida”gi qarorlarida axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarşi kuraşiş faoliyatini yanada kuçaytiriş maqsadida davlat organlari va fuqarolik jamiyati institutlari hamkorligida axborot xavfsizligi madaniyatini oşiriş, kiberfiribgarliklarning oldini oliş böyiça tarğibot işlarini kuçaytiriş vazifasi belgilangan. Bundan taşqari, Özbekiston Respublikasi Prezidentining Farmoni, 05.10.2020 yildagi PF6079-son “Raqamli Özbekiston — 2030” strategiyasini tasdiqlaş va uni samarali amalga oşiriş çora-tadbirlari töğrisidagi farmonda

ham bugungi dolzarb mavzuyimizga daxldorlik joyi mavjud. Mazkur hujjatlar mahalla darajasida kiberfiribgarliklar profilaktikasini yölga qöyiş, fuqarolar örtasida axborot savodxonligini oşiriş, internetda xavfsiz muhitni yaratiş zarurligini davlat darajasida tan olinganini körsatadi. Şu boisdan “Kiberfiribgarliklar va ularning mahalla darajasida profilaktikasi: axborot savodxonligi, internet xavfsizligi böyiça tarğibot işlari” mavzusi mamlakatimizda olib borilayotgan islohotlar mazmuni bilan uzviy boğliq bölib, Prezident siyosati va strategik hujjatlarida belgilangan ustuvor yönalişlarning amaliy ifodasi sifatida nihoyatda dolzarbdir.

XULOSA

Xulosa qilib aytganda, zamonaviy axborotlaşgan jamiyatda kiberfiribgarliklar insonlar, taşkilotlar va davlat xavfsizligi uçun eng jiddiy tahdidlardan biriga aylanib bormoqda. Internet texnologiyalari va raqamli xizmatlarning keng rivojlanişi inson hayotini qulaylaştirgan bölsa-da, şu bilan birga kiberjinoyatchilar uçun ham yangi imkoniyatlarni yaratmoqda. Ayniqsa, phişing, zararli dasturlar, ijtimoiy muhandislik, bank kartalari orqali firibgarlik va şaxsiy ma’lumotlarni öğirlaş kabi holatlar kundan-kunga ortib borayotgani kiberxavfsizlikka bölgan e’tiborni yanada kuçaytirişni talab etadi. Bunday şaroitda foydalanuvçilarning raqamli savodxonligini oşiriş va kiberxavflarning oldini oliş böyiça tizimli çoralarni amalga oşiriş muhim ahamiyat kasb etadi.

Kiberfiribgarliklarga qarşi samarali kuraşişda kibergigiyena va kiberprofilaktika özaro uzviy boğliq tuşunçalar hisoblanadi. Kibergigiyena foydalanuvçilarning kundalik xavfsiz raqamli odatlarini şakllantirişga xizmat qilsa, kiberprofilaktika esa tahdidlarni oldindan aniqlaş va ularning oldini olişga qaratilgan taşkiliy, texnik hamda ma’rifiy çoralarni öz içiga oladi. Uşbu ikki yönalişning integratsiyasi natijasida nafaqat texnologik himoya kuçayadi, balki inson omili bilan boğliq zaifliklar ham kamayadi. Çunki aksariyat kiberfiribgarlik holatlarining asosiy sababi foydalanuvçilarning ehtiyotsizligi, yetarli bilim va tajribaga ega emasligi bilan boğliqdir.

Umuman olganda, kibergigiyena va kiberprofilaktikaning integratsiyasi kiberfiribgarliklardan himoyalanişning eng samarali yöllaridan biri bölib, u

foydalanuvçilarning raqamli madaniyatini oşiriş, axborot xavfsizligini mustahkamlaş hamda kiberjinoyatchilikning oldini olişda muhim ahamiyatga ega. Mazkur yönalişlarni kompleks ravişda rivojlantiriş orqali xavfsiz va barqaror raqamli muhitni şakllantiriş mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. An’anaviy va kiber firibgarliklardan himoyalaniş usullari [Matn]: uslubiy qöllanma / H.P. Abulkasimov, M.H. Abulkasimov. – Toşkent: Bookmany print, 2024. – 130 b.
2. “Kiberxavfsizlik asoslari” öquv qöllanmasi S.K. Ganiyev, A.A. Ganiyev Toşkent, 2020.
3. “Kiberxavfsizlik” öquv qöllanmasi R.Y. Mamajonov, T.J. Rajabov, E.I. Saidaxmedov, I.U.Xuşboqov, Toşkent, 2024.
4. Salayev N.S., Ro‘ziyev R.N Kiberjinoyatchilikka qarşi kuraşişga oid milliy va xalqaro standartlar. Monografiya ., – T.: TDYU, 2018, 139-b
5. Özbekiston Respublikasi “Kiberxavfsizlik töğrisida”gi Qonuni, ÖRQ–764-son, 2022-yil 15-aprel.
6. Özbekiston Respublikasi “Huquqbuzarliklar profilaktikasi töğrisida”gi Qonuni, ÖRQ–371-son, 2014-yil 14-may.
7. Özbekiston Respublikasi Prezidentining “Raqamli Özbekiston – 2030” strategiyasi töğrisidagi PF–6079-son Farmoni, 2020-yil 5-oktyabr.
8. Özbekiston Respublikasi Prezidentining “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarşi kuraşiş faoliyatini yanada kuçaytirişga qaratilgan çoratadbirlar töğrisida”gi 2025 -yil 30-apreldagi PQ-153-sonli qarori.
9. “Kibermakondagi firibgarlik turlari va ulardan himoyalanişning zarurati, tajribasi, ahamiyati” ilmiy maqola Ş.B.Quvandiqov 12.05.2026 yil https://doi.org/10.5281/zenodo.20134429
10. Anorboyev A.U Kiberjinoyatchilik, unga qarşi kuraşiş muammolari va kiberxavfsizlikni ta’minlaş istiqbollari. Monografiya – T.: Milliy gvardiya instituti, 2020. – 324 b.