KIBERGIGIYENA VA HUQUQIY MADANIYAT: O`ZBEKISTONDA KIBERHUQUQBUZARLIKLARNI OLDINI OLISH

Sherqo'ziyev Xolmuhammad Sharifjon o'g'li
Toshkent davlat yuridik universiteti
Ommaviy huquq fakulteti 2-bosqich talabasi
xolmuhammadsherqoziyev330@gmail.com

ANNOTATSIYA. Mazkur maqolada raqamli transformatsiya sharoitida kiber gigiyena va huquqiy madaniyatning jamiyat xavfsizligini ta'minlashdagi o'rni tahlil qilinadi. Kiber gigiyena tushunchasi, uning asosiy tamoyillari hamda kiberjinoyatchilikning oldini olishdagi ahamiyati ochib berilgan. Shuningdek, O'zbekiston Respublikasida kiberxavfsizlikni tartibga soluvchi normativ-huquqiy baza, xususan, shaxsiy ma'lumotlarni himoya qilish va axborot xavfsizligini ta'minlashga oid qonunlar tahlil qilinadi. Muallif kiberxavfsizlikni ta'minlashda davlat va jamiyatning o'zaro hamkorligi muhim ekanligini asoslab beradi.

Kalit so`zlar: kibergigiyena, huquqiy madaniyat, kiberxavfsizlik, shaxsiy ma'lumotlar, raqamli savodxonlik, kiberjinoyatchilik.

АННОТАЦИЯ. В статье рассматриваются вопросы кибергигиены и правовой культуры в условиях цифровой трансформации общества. Раскрывается сущность кибергигиены, ее основные принципы и роль в предупреждении киберпреступности. Особое внимание уделяется анализу нормативно-правовой базы Республики Узбекистан в сфере кибербезопасности и защиты персональных данных. Автор подчеркивает, что эффективная кибербезопасность возможна только при взаимодействии государства и общества.

Ключевые слова: кибергигиена, правовая культура, кибербезопасность, персональные данные, цифровая грамотность, киберпреступность.

ABSTRACT. This article examines the role of cyber hygiene and legal culture in ensuring societal security in the context of digital transformation. It explores the concept of cyber hygiene, its main principles, and its importance in preventing cybercrime. The study also analyzes the legal framework of the Republic of Uzbekistan in the field of cybersecurity and personal data protection. The author argues that effective cybersecurity requires a collaborative effort between the state and society.

Keywords: cyber hygiene, legal culture, cybersecurity, personal data, digital literacy, cybercrime prevention.

KIRISH

Bugungi globallashuv va raqamli transformatsiya davrida jamiyat hayotining barcha sohalari – davlat xizmatlari, bank tizimi, ta’lim va sog`liqni saqlash tizimi – jadal raqamlashtirilmoqda. Bu jarayon fuqarolarga qulayliklar yaratgan bo`lsa-da, yangi turdagi xavf-xatarlarni ham keltirib chiqarmoqda. Xususan, kiberjinoyatchilik, ma’lumotlarning sizib chiqishi, firibgarlik va noqonuniy kirish kabi holatlar tobora kengayib bormoqda. Shu sababli, bugungi kunda raqamli muhitda xavfsizlikni ta’minlash masalalarining dolzarbligi kundan kunga ortib bormoqda desak adashmagan bo`lamiz.

Kiberxavfsizlik texnik va huquqiy infratuzilmasi qanchalik mukammal bo`lmasin, ***“inson omili”*** (human facto) har doim tizimning eng zaif bo`g`ini bo`lib qolmoqda. Dunyoga mashhur kiberxavfsizlik eksperti **Bryus Shnayer** o`zining “Sirlar va yolg`onlar” (Secrets and Lies) kitobida ta’kidlaganidek, “Xavfsizlik – bu mahsulot emas, balki jarayondir” va bu jarayonda insonlarning xulq-atvori hal qiluvchi ahamiyatga ega[1]

Kibergigiyena (Cyber Hygiene) – bu raqamli muhitda xavfsizlikni ta’minlashga qaratilgan muntazam va odatiy harakatlar majmui bo`lib, u parollarni tez-tez o`zgartirish, ikki faktorli autentifikatsiyadan foydalanish, shubhali havolalarni ochmaslik va dasturiy ta’minotni o`z vaqtida yangilashni o`z ichiga oladi[2]

O‘zbekiston Respublikasida kiberxavfsizlikni tartibga soluvchi huquqiy baza mustahkam shakllangan. “Kiberxavfsizlik to‘g‘risida”gi Qonun, “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun va “Axborotlashtirish to‘g‘risida”gi Qonun raqamli tizimlarda ma’lumotlarni himoya qilish va axborot resurslaridan foydalanishning huquqiy asoslarini belgilab beradi. Bundan tashqari, Jinoyat kodeksida axborot texnologiyalaridan foydalangan holda sodir etilgan jinoyatlar uchun javobgarlik belgilangan. Shu bilan birga, amaliyot shuni ko`rsatadiki, ko`plab kiberjinoyatlar texnik nosozliklardan ko`ra, inson omili – bilim yetishmasligi va e’tiborsizlik – sababli sodir bo`ladi.

Shu nuqtai nazardan, kiberxavfsizlikni ta’minlashda nafaqat qonuniy mexanizmlar, balki jamiyatning huquqiy madaniyati va foydalanuvchilarning raqamli savodxonligi muhim rol o`ynaydi. Mazkur maqolaning maqsadi – O‘zbekistonda kibergigiyena va huquqiy madaniyatning o`zaro bog`liqligini o`rganish va kiberjinoyatchilikni oldini olish mexanizmlarini tahlil qilishdir. Shu maqsadga erishish uchun maqolada kibergigiyena va huquqiy madaniyat nazariy asoslari, O‘zbekiston Respublikasidagi kiberxavfsizlik huquqiy bazasi va kiberjinoyatchilikka qarshi amaliy strategiyalar tahlil qilinadi.

METODLAR

[1] Schneier, B. (2000). Secrets and Lies: Digital Security in a Network World. Wiley. (Kiberxavfsizlik falsafasi bo`yicha klassik asar)

[2] Kiber huquq: o`quv qo`llanma / Abdixakimov Islombek Bahodir o`g`li. – T.: TDYU nashriyoti, 2025. – 418 b.

Ushbu tadqiqotda O`zbekiston sharoitida kibergigiyena va huquqiy madaniyatning kiberjinoyatchilikni oldini olishdagi rolini o`rganish maqsadida bir nechta ilmiy-uslubiy yondashuvlar qo`llangan.

Birinchidan, ***normativ-huquqiy tahlil*** metodi yordamida O‘zbekiston Respublikasining kiberxavfsizlik va shaxsiy ma’lumotlarni himoya qilishga oid qonunlari, jumladan, “Kiberxavfsizlik to`g`risida”gi Qonun (2022), “Shaxsiy ma’lumotlar to`g`risida”gi Qonun (2019), “Axborotlashtirish to`g`risida”gi Qonun va Jinoyat kodeksi tahlil qilindi. Ushbu tahlil kiberxavfsizlikni ta’minlash mexanizmlarini huquqiy jihatdan aniqlash va ularning samaradorligini o`rganishga imkon berdi.

Ikkinchidan, ***solishtirma tahlil*** metodi orqali O‘zbekiston va rivojlangan davlatlarning kiberxavfsizlik strategiyalari, kibergigiyena qoidalari va foydalanuvchilarning raqamli savodxonligini oshirish tajribasi taqqoslandi. Bu metod O`zbekistonning amaliyoti va xalqaro standartlar o`rtasidagi o`xshashliklar va farqlarni aniqlashga yordam berdi.

Uchinchidan, ***empirik kuzatuv va amaliy misollar tahlili*** ishlatildi. Bu doirada foydalanuvchilarning kundalik raqamli faoliyatida kiberhujumlarga duch kelish holatlari, masalan, SMS orqali firibgarlik, soxta saytlar orqali ma’lumotlarni oshkor qilish kabi holatlar tahlil qilindi. Ushbu metod inson omilining kiberxavfsizlikdagi rolini chuqurroq tushunishga imkon berdi.

Tadqiqotning doirasi O‘zbekiston Respublikasi hududida amalga oshirilgan bo`lib, asosan davlat organlari, ta’lim muassasalari va keng jamoatchilik foydalanuvchilarining raqamli xulq-atvori asosiy obyekt sifatida olingan. Ma’lumot manbalari sifatida rasmiy qonunlar, strategik hujjatlar, ilmiy maqolalar va xalqaro tashkilotlarning hisobotlari ishlatilgan.

Kibergigiyenaning asosiy ***tamoyillari*** quyidagilardan iborat:

kuchli autentifikatsiya tizimlaridan foydalanish. Murakkab parollar yaratish va ikki bosqichli autentifikatsiyani joriy etish hisoblarni himoya qilishda samarali vosita hisoblanadi.
dasturiy ta’minotni muntazam yangilab borish. Chunki yangilanishlar orqali tizimdagi zaifliklar bartaraf etiladi.
foydalanuvchilarning hushyorligi. Shubhali havolalar, noma’lum manbalardan kelgan xabarlar yoki qo`ng`iroqlarga ehtiyotkorlik bilan yondashish zarur.
shaxsiy ma’lumotlarni himoya qilish. Foydalanuvchilar o`z ma’lumotlarini begona shaxslarga oshkor qilmasliklari lozim

Ushbu metodlar va tamoyillar kombinatsiyasi tadqiqotga ilmiy asos va amaliy ahamiyat beradi, shuningdek, O`zbekiston sharoitida kiberxavfsizlikni oshirish bo`yicha samarali tavsiyalar ishlab chiqishga imkon yaratadi.

NATIJALAR

Ushbu tadqiqotning natijalari shuni ko`rsatdiki, **kiberjinoyatchilik va raqamli tahdidlar butun dunyoda jadal sur'atlarda o`sib bormoqda**, bu esa kibergigiyena va huquqiy madaniyatni mustahkamlash zaruratini yanada oshirmoqda. Global tadqiqotlar bo`yicha har bir internet foydalanuvchisi har kuni o`rtacha yuzlab tahdidlarga duch keladi, va bu raqam 2025-yilda sezilarli darajada oshgani qayd etilgan (*masalan, o`rtacha fuqaro bir kunida 66 ta xavf-tahdid bilan duch keladi*).

O`zbekiston Respublikasida kiberhuquqbuzarliklarni oldini olishga doir bir nechta qonunlar va qonunosti hujjatlar qabul qilindi. Bunga misol qilib, O'zbekiston Respublikasining **Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to`g`risidagi 38-son** Prezident Farmonini keltirishimiz mumkin. Ushbu farmonnning 1-ilovasida **2026-2030-yillarga** mo`ljallangan kiberxavfsizlik strategiyalari mustahkamlab qo`yilgan bo`lib, davlat organlari va tashkilotlarining axborot tizimlari va resurslarini hamda muhim axborot infratuzilmasi obyektlarini kibertahdidlardan himoya qilishni nazarda tutuvchi davlat himoya tizimini yanada rivojlantirish, axborot texnologiyalari orqali sodir etiladigan jinoyatlar va boshqa huquqbuzarliklarni aniqlash va ularning oldini olish, ushbu maqsadda raqamli kriminalistikani keng qo`llash, muhim axborot infratuzilmasi obyektlarida kiberxavfsizlik talablariga qat'iy rioya etilishi ustidan nazoratni kuchaytirish hamda kiberxavfsizlik sohasidagi qonunchilik talablarini buzganlik uchun javobgarlikni belgilash va boshqa strategiyaning maqsadiga erishish uchun vazifalar keltirib o`tilgan[3]

Bundan tashqari, 2022-yil 17-iyulda kuchga kirgan **Kiberxavfsizlik to`g`risidagi** qonunni qabul qilinishi ham kiberhuquqbuzarliklarni oldini olinishiga va davlat organlariga va mansabdor shaxslariga bir qancha vazifalarni yuklatilishiga sabab bo`ldi. Xususan ushbu qonunning **1-moddasida** ushbu qonunning maqsadi keltirilgan bo`lib unga ko`ra, kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat ekanligi belgilab qo`yilgan[4]. Bundan tashqari ushbu qonun davlat organlari va tashkilotlariga o`z xodimlari orasida kiberxavfsizlik madaniyatini shakllantirish va ularning malakasini oshirish majburiyatini yuklaydi. Bu shuni anglatadiki, agar buxgalter oddiy kibergigiyena qoidasini buzib (masalan, parolni monitorga yopishtirib qo`yib), tashkilotga zarar yetkazsa, bu shunchaki ehtiyotsizlik emas, balki mehnat majburiyatlarini qo`pol ravishda buzish va intizomiy javobgarlikka tortishga asos bo`ladi.

Bunga qo`shimcha ravishda, texnologiyalarnig tobora rivojlanib borishi natijasida ularni oldini olish maqsadida qonunchilikka ham bir qancha o`zgartirishlar

[3] Qonunchilik millliy bazasi O`zbekiston Respublikasi Prezidentining Farmoni, 10.03.2026 yildagi PF-38-son https://lex.uz/uz/docs/-8079286#-8084459
[4] Qonunchilik milliy bazasi O`zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O`RQ-764-son https://lex.uz/uz/docs/-5960604

kiritilishini taqazo etdi. Bunga misol qilib, 2022-yil 19-oktabr O`RQ-794-sonli qonun tahriri asosida Jinoyat kodeksiga bir qancha o`zgartirishlar kiritildi[5]. Jumladan, Kodeksning *168-moddasi 2-qismiga* yangi band sifatida (g) **firibgarlik axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan bo`lsa** kodeksning shu bandi bilan javobgarlikka tortiladigan bo`ldi. Natijada, kiberhuquqbuzarliklar bu o`zgartirishlar kiritilishidan oldingi statistikaga qaraganda ancha miqdorga yaxshilandi. Bu esa o`z navbatida kiberjinoyatchiliklarni oldini olsihga qo`yilgan ilk qadamlardan biri desak adashmagan bo`lamiz.

Yuqorida ta'kidlaganimizdek, kiberhujumlar orqali shaxsga doir ma'lumotlarni qo`lga kiritilishi va noqonuniy maqsadlarda foydalanishini oldini olish uchun alohida tartiblarni belgilanishi bugungi kunda alohida zarurat sifatida e'tirof etildi. Bunga misol qilib, 2021-yil 14-yanvardagi 666-sonli qonuniga asosan Shaxsga doir ma'lumotlar to`g`risidagi qonunga kiritilgan o`zgartirishlarni misol qilib keltirishimiz mumkin. Ushbu qonunga asosan 27-moddaning davomi sifatida 27 prim 1 -modda kiritildi. Unga ko`ra, "mulkdor va (yoki) operator O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga axborot texnologiyalaridan foydalangan holda ishlov berishda, shu jumladan Internet jahon axborot tarmog'ida ishlov berishda ularning jisman O'zbekiston Respublikasi hududida joylashgan texnik vositalarda hamda belgilangan tartibda Shaxsga doir ma'lumotlar bazalarining davlat reyestrida ro'yxatdan o'tkazilgan shaxsga doir ma'lumotlar bazalarida yig'ilishini, tizimlashtirilishini va saqlanishini ta'minlashi shart[6]". Natijada, O`zbekiston Respublikasi hududida rasmiy ravishda serverlari bo`lmagan tashkilot va korxonalarning mamlakat hududida foydalanishi cheklandi. Bu esa o`z navbatida O`zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlarini bevosita boshqa davlat hududida bo`lishi va ularni boshqa maqsadlarga ishlatilishini oldini oladi.

Kiberxavfsizlik madaniyatini oshirish va shakllantirishda xalqaro standartlarni roli beqiyos. *ISO/IES 27001* xalqaro standarti (Axborot xavfsizligini boshqarish tizimlari) kiberhuquqbuzarlikdan himoyalanishdagi texnik choralar va tashkiliy choralarni tartibga soladi. Bu shartlarga ko`ra, axborot xavfsizligi siyosati tashkilotning barcha bo`g`inlariga singdirilgan bo`lishi shart. O`zbekiston Respublikasining bank tizimi va elektron hukumat loyihalarida ushbu standart talablari majburiy deb belgilangan. Bunga misol qilib, *"toza stol" (clean desk) va "toza ekran"* (clean screen) siyosati xodimlardan ish joyini tark etganda maxfiy hujjatlarni qoldirmaslikni va kompyuterni bloklashni talab qiladi[7]. Bu oddiy qoida bo`lib ko`rinsa-da, huquqiy jihatdan u tijorat siri va shaxsga doir ma'lumotlarni himoya qilishning eng

[5] Qonunchilik milliy bazasi O`zbekiston Respublikasining Jinoyat kodeksi https://lex.uz/docs/-111453
[6] Qonunchilik milliy bazasi, O`zbekiston Respublikasining Qonuni, 02.07.2019 yildagi O`RQ-547-son https://lex.uz/docs/-4396419
[7] Kiber huquq: o`quv qo`llanma / Abdixakimov Islombek Bahodir o`g`li. – T.: TDYU nashriyoti, 2025. – 418 b.

birlamchi pog`onasi hisoblanadi. G‘arb tadqiqotlari shuni ko‘rsatadiki, kiberhujumlarning 90 foizdan ortig‘i ***phishing*** — ya’ni xodimlarning e’tiborsizligidan foydalanib, zararli havolalar orqali tizimga kirish bilan boshlanadi[8]. Shu sababli, kiberhuquq sohasida xavfsizlik bo‘yicha xabardorlik (Security Awareness) treninglarini tashkil etish hamda xodimlarning hushyorligini tekshirish maqsadida ularga muntazam ravishda sinov tariqasida phishing xatlari yuborish muhim va zarur choralar qatoriga kiradi. Jahon miqyosida kiberjinoyatchiliklar asosan **ma’lumotlar o`g`irlanishi, identifikatsiya firibgarligi va shaxsiy ma’lumotlarning suiiste’mol qilinishi** ko`rinishida sodir bo`lmoqda. *McAfee* va boshqa xalqaro statistik tadqiqotlarda global zararlarning 2021-yilda yiliga trillionlab dollarni tashkil etganligi, 2025-yilgacha bu ko`rsatkichning 10,5 trillion dollargacha yetishi bashorat qilinganligi, kiberjinoyatlar iqtisodiyot va jamiyat uchun jiddiy xavf bo`lib qolayotganini tasdiqlaydi[9].

Natijalar shuni ko`rsatadiki, kiberjinoyatchilikning asosiy sababi inson omili ekanligi nafaqat nazariy, balki amaliy misollarda ham o`z tasdig`ini topadi. Jumladan, 2013-yilda sodir bo‘lgan *Target Data Breach* hodisasi foydalanuvchilarning kibergigiyena qoidalariga rioya qilmasligi jiddiy oqibatlarga olib kelishini ko`rsatdi[10]. Ushbu hujum natijasida millionlab foydalanuvchilarning bank kartalari ma’lumotlari o‘g‘irlangan bo‘lib, bunga sabab sifatida phishing orqali uchinchi tomon tizimlariga noqonuniy kirish qayd etilgan.

Bunga yana bir misol qilib, 2017-yilda sodir bo`lgan *WannaCry Ransomware* Attack global kiberhujumi kibergigiyenaning ahamiyatini yana bir bor isbotlab berdi[11]. Ushbu hujum dunyoning 150 dan ortiq davlatida yuz minglab kompyuter tizimlarini ishdna chiqargan. Tahlil shuni ko`rsatdiki, ushbu hujumning asosiy sababi operatsion tizimlarning o`z vaqtida yangilanmaganligi bo`lib, oddiy xavfsizlik choralariga amal qilish orqali kiberhujumlarni oldini olish mumkin edi.

Tahlil shuni ko`rsatdiki, kiberhujumlar texnik vositalardan ko`ra **inson omili** orqali ko`proq amalga oshiriladi. Phishing kabi ijtimoiy muhandislik usullari foydalanuvchilarni aldash orqali shaxsiy ma’lumotlar va bank rekvizitlarini olish guruhlarini yaratgan. Bu foydalanuvchilarning raqamli savodxonligi past bo`lgan taqdirda sodir bo`ladigan eng keng tarqalgan xuruj turlaridan biri hisoblanadi. Bu esa o`z navbatida insonlarda kibergigiyenani va kibehujumlardan himoyayalanishga bo`lgan huquqiy madaniyatni oshirish kerakligini ko`rsatadi.

Xalqaro tajribalarda (masalan, NIST va ISO kabi standartlar asosida) kibergigiyena — foydalanuvchilarning **parollarni murakkab va noyob qilish, ikki**

[8] Якубова, М.А. Киберстрахование: учобное пособие / Мадинабону Абдумаликовна Якубова. - Ташкент: Издво ТГЮУ, 225. - 184 с.
[9] Cybercrime Magazine https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025
[10] KrebsonSecurity https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[11] Britannica https://www.britannica.com/topic/WannaCry-ransomware-attack

bosqichli autentifikatsiyani yoqish, antivirus va operatsion tizimlarni yangilab borish kabi kundalik xavfsizlik qoidalariga rioya etishi — tahdidlarni sezilarli darajada kamaytirishi ko`rsatilgan. Ammo ko`plab tashkilotlar va foydalanuvchilar bu qoidalarga to`liq amal qilmaydi. Masalan, global korxonalar orasida 92 % hollarda kiberhujumlar **yaxshi kibergigiyena choralari qo‘llanilganda oldini olinish mumkinligi** bildirildi, lekin faqat 32 % kompaniyalar bu amaliyotlarni strategik darajada joriy qilgan[12].

Bu natijalar shuni ko`rsatadiki, **kiberjinoyatchilikning o`sish sur’ati nafaqat texnik tizimlar zaifligidan, balki odamlarning raqamli xulq-atvori va huquqiy madaniyati pastligidan ham kelib chiqadi**. Shu sababli kibergigiyena bo`yicha bilimlarni oshirish va huquqiy madaniyatni mustahkamlash jamiyat xavfsizligini ta’minlash uchun muhim ahamiyat kasb etadi.

O`zbekiston kontekstida ham kiberjinoyatchilik amaliyotlari tobora murakkablashgan. Bu mamlakatda “Kiberxavfsizlik to`g`risida”gi qonun qabul qilinishi bilan birga, kiberjinoyatchilikni aniqlash va oldini olish tizimlarini takomillashtirish bo`yicha kompleks yo`nalishlar belgilanganligi qayd etilgan. Shu bilan birga, kiberhujum va tahdidlarni aniqlash uchun maxsus tizimlar joriy etilishi, yoshlar va fuqarolarni kiberxavfsizlik bo`yicha o`qitish tadbirlari tashkil etilishi rejalashtirilmoqda. Ushbu qonun qabul qilinishi bilan ushbu sohada maxsus vakolatli organ bo`lgan davlat xavfsizlik xizmatiga ham nbir qancha vakolat va vazifalar yuklatildi. Bularga misol qilib, kiberxavfsizlik sohasida tadqiqotlar o`tkazilishini va monitoringlar tashkil etilishi, muhim axborot infratuzilmalari obyektlarining kiberxavfsizligini ta’minlashga doir talablarni belgilash, muhim axborot infratuzilmasi obyektlariga bo‘lgan kiberhujumlarga urinishlarning oldini olishga doir rejalarni ishlab chiqish va ularni bevosita amalga oshirish va boshqalarni keltirishimiz mumkin.

MUHOKAMA

Natijalar shuni ko`rsatdiki, kiberjinoyatchilikning asosiy sababi texnik nosozliklardan ko`ra, inson omili hisoblanadi. Ko`plab foydalanuvchilar shaxsiy ma’lumotlarni himoya qilish bo`yicha zarur choralarni yetarlicha bilmaydi yoki ularga rioya qilmaydi. Shu jihatdan, kibergigiyena va huquqiy madaniyat jamiyat xavfsizligi uchun muhim vosita sifatida namoyon bo`ladi.

Xalqaro tajriba ham bu fikrni tasdiqlaydi. Masalan, AQSh va Yevropa mamlakatlarida NIST va ISO standartlari asosida foydalanuvchilarni kiberxavfsizlik bo`yicha muntazam o`qitish, parollarni murakkab qilish, ikki bosqichli autentifikatsiya va antivirus yangilanishlarini majburiy qilish orqali kiberhujumlarning *70–90 %* holatini oldini olish mumkinligi ko`rsatilgan. Shu bilan birga, bu davlatlarda ***jamiyatning huquqiy madaniyati*** ham yuqori darajada, ya’ni foydalanuvchilar qonun

[12] Kiber huquq: o`quv qo`llanma / Abdixakimov Islombek Bahodir o`g`li. – T.: TDYU nashriyoti, 2025. – 418 b.

va xavfsizlik qoidalariga e’tiborli munosabatda bo`lishadi.

O`zbekiston sharoitida ham kiberxavfsizlikni oshirish bo‘yicha qonuniy baza mavjud, ammo amaliy natijalar ko`rsatadiki, foydalanuvchilar orasida raqamli savodxonlik darajasi yetarli emas. Shu sababli, nafaqat texnik choralar, balki ***muntazam targ`ibot, ta’lim va huquqiy madaniyatni oshirish*** tadbirlari ham zarur. Misol uchun, yoshlar va katta yoshdagi aholi uchun kibergigiyena bo`yicha seminarlar, davlat va nodavlat tashkilotlari tomonidan raqamli xavfsizlik kampaniyalari olib borilishi kiberhujumlarni sezilarli darajada kamaytirishi mumkin.

Natijalar shuni ham ko`rsatadiki, kiberjinoyatchilikni oldini olishda davlat va jamiyatning o‘zaro hamkorligi eng samarali usul hisoblanadi. Davlat organlari qonunlarni ishlab chiqadi, tizimlarni nazorat qiladi, ammo foydalanuvchilarning huquqiy madaniyati va raqamli savodxonligi yuqori bo‘lmasa, kiberxavfsizlik tizimi to‘liq samarador bo‘la olmaydi. Shu nuqtai nazardan, 2020-yil 5-oktabrda qabul qilingan **“Raqamli O`zbekiston – 2030”** strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to`g`risidagi 6079-son Preziden Farmonida ushbu strategiya doirasida kiberxavfsizlikni mustahkamlash raqamli savodxonlikni oshirish ustuvor yo`nalish sifatida belgilangan[13]. O`zbekistonning “Raqamli O`zbekiston – 2030” strategiyasi va kiberxavfsizlikni ta’minlash bo`yicha rejalari nafaqat texnik, balki huquqiy va madaniy omillarni ham qamrab olishi lozim.

Shu asosda, muallif tavsiyasi shuki: kiberxavfsizlikni mustahkamlash uchun kompleks yondashuv zarur bo`lib, u **texnik vositalar, qonuniy mexanizmlar va jamiyatning huquqiy madaniyati**ni birlashtirishi kerak. Bu yondashuv nafaqat kiberjinoyatchilikning oldini olish, balki barqaror va xavfsiz raqamli muhit yaratish imkonini beradi.

XULOSA

Xulosa qilib aytganda, ***kiberxavfsizlik*** zamonaviy jamiyat uchun eng muhim vazifalardan biri hisoblanadi. Tadqiqot natijalari shuni ko`rsatdiki, kiberjinoyatchilikning asosiy sababi texnik nosozliklar emas, balki ***inson omili*** – bilim yetishmasligi va e’tiborsizlikdir. Shu sababli, *kibergigiyena* va *huquqiy madaniyat* jamiyat xavfsizligini ta’minlashda asosiy vosita sifatida namoyon bo`ladi.

O`zbekiston sharoitida kiberxavfsizlikni ta’minlash uchun mustahkam huquqiy baza yaratilgan: “Kiberxavfsizlik to`g`risida”gi Qonun, “Shaxsiy ma’lumotlar to`g`risida”gi Qonun, “Axborotlashtirish to`g`risida”gi Qonun va Jinoyat kodeksi. Shu bilan birga, natijalar shuni ko`rsatadiki, qonuniy mexanizmlar samarali ishlashi uchun foydalanuvchilarning **raqamli savodxonligi va huquqiy madaniyati**ni oshirish zarur.

Xalqaro tajriba shuni ko`rsatadiki, rivojlangan davlatlarda kiberxavfsizlik faqat texnik vositalar bilan emas, balki keng qamrovli ta’lim va targ`ibot ishlari orqali

[13] Qonunchilik milliy bazasi O‘zbekiston Respublikasi Prezidentining Farmoni, 05.10.2020 yildagi PF-6079-son https://lex.uz/ru/docs/-5030957

ta’minlanadi. Shu sababli O‘zbekistonda ham yoshlar va katta yoshdagi aholi orasida kiberxavfsizlik bo`yicha muntazam o`qitish, seminarlar va targ`ibot tadbirlarini kuchaytirish muhim ahamiyat kasb etadi.

Natijada, kiberjinoyatchilikni oldini olish va barqaror raqamli muhit yaratish faqatgina ***davlat va jamiyatning o`zaro hamkorligi*** orqali mumkin. Foydalanuvchilarning shaxsiy mas’uliyati, huquqiy madaniyat va texnik vositalar birgalikda ishlaganda kiberxavfsizlikning samaradorligi sezilarli darajada oshadi. Shu bilan birga, kelajakda O‘zbekistonda **sun’iy intellekt, moliyaviy texnologiyalar va IoT tizimlari bilan bog`liq yangi tahdidlar**ni oldini olish uchun doimiy monitoring va strategik yangilanishlar talab etiladi.

FOYDALANILGAN ADABIYOTLAR

1. Kaspersky. Cybersecurity Awareness and Cyber Hygiene Report. – 2023.
2. ENISA (European Union Agency for Cybersecurity). Cyber Hygiene Practices. – 2022.
3. NIST (National Institute of Standards and Technology). Cybersecurity Framework. – USA, 2018.
4. Yakubova N. Kiberstraxovaniya. – Toshkent, 2025.
5. OECD. Digital Security Risk Management in a Global Economy. – Paris, 2020.
6. Abduxakimov I. Kiber huquq o`quv qo`llanma. – Toshkent, 2025. (308-312)
7. ISO/IEC 27001:2013. Information Security Management Systems – Requirements.
8. Whitman, M.E., Mattord, H.J. Principles of Information Security. – Cengage Learning, 2021.
9. Solove, Daniel J. Understanding Privacy. – Harvard University Press, 2008.
10. O‘zbekiston Respublikasi “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonuni. 01.10.2019. https://lex.uz/docs/-4396419
11. O‘zbekiston Respublikasi Jinoyat kodeksi 01.04.1995. https://lex.uz/docs/-111453
12. O`zbekiston Respublikasi “Kiberxavfsizlik to`g`risida”gi qonun. 17.07.2022. https://lex.uz/uz/docs/-5960604
13. O‘zbekiston Respublikasi Prezidentining Farmoni, 10.03.2026 yildagi PF-38-son. 11.03.2026. https://lex.uz/uz/docs/-8079286#-8084459
14. O‘zbekiston Respublikasi Prezidentining Farmoni, 05.10.2020 yildagi PF-6079-son. 06.10.2020. https://lex.uz/ru/docs/-5030957
15. ITU (International Telecommunication Union). Global Cybersecurity Index. – 2023.
16. Hadnagy, Christopher. Social Engineering: The Science of Human Hacking. – Wiley, 2018.