KIBERJINOYATLAR PROFILAKTIKASI SUBYEKTLARI TIZIMI VA ULARNING O‘ZARO HAMKORLIGI: MILLIY AMALIYOT, XORIJIY TAJRIBA VA HUQUQIY TAKLIFLAR

Mirzajonov Shoxruxbek Sobirjonovich
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti mustaqil izlanuvchisi

Annotatsiya: *Maqolada kiberjinoyatlar profilaktikasini amalga oshiruvchi subyektlar tizimi va ularning o‘zaro hamkorlik mexanizmlari ilmiy-amaliy jihatdan tahlil qilingan. Milliy modelda vakolatli organlar, huquqni muhofaza qiluvchi idoralar, raqamli transformatsiya subyektlari hamda bank-moliya sektorining o‘rni yoritilib, xususiy sektor (IT-kompaniyalar, provayderlar) bilan tezkor axborot almashinuvini ta’minlashdagi institutsional muammolar asoslantirilgan.*
Kalit so‘zlar: *kiberjinoyatlar profilaktikasi, subyektlar tizimi, subyektlararo hamkorlik, davlat-xususiy sheriklik, kiber-insident, majburiy xabardor qilish, elektron dalillarni tezkor saqlash, bankning kiberjavobgarligi,kiber-sug‘urta, sun’iy intellekt.*

Аннотация: *В статье анализируется система субъектов профилактики киберпреступности и механизмы их межведомственного/межсекторного взаимодействия. Раскрывается роль уполномоченных органов, правоохранительных структур, институтов цифрового развития и банковско-финансового сектора, а также проблематика оперативного обмена информацией с частным сектором (IT-компании, провайдеры).*
Ключевые слова: *профилактика киберпреступности, субъекты профилактики, межсекторное взаимодействие, государственно-частное партнёрство, киберинцидент, обязательное уведомление, ускоренное сохранение данных, ответственность банка, киберстрахование, искусственный интеллект.*

Abstract: *This article examines the system of actors responsible for cybercrime prevention and the effectiveness of their cooperation mechanisms. It outlines the roles of competent authorities, law-enforcement bodies, digital transformation institutions, and the banking/financial sector, while highlighting institutional bottlenecks in rapid information sharing with the private sector (IT companies and service providers).*
Keywords: *cybercrime prevention, prevention actors, inter-agency cooperation, public-private partnership, cyber incident, mandatory reporting, expedited data preservation, bank liability, cyber insurance, artificial intelligence*

Insoniyat sivilizatsiyasining hozirgi bosqichida raqamli transformatsiya jarayonlari jamiyat hayotining barcha jabhalarini qamrab oldi. Biroq, axborot texnologiyalarining jadal rivojlanishi nafaqat ijtimoiy-iqtisodiy yuksalishga, balki transchegaraviy xarakterga ega bo‘lgan yangi turdagi tahdid – kiberjinoyatchilikning ildiz otishiga ham zamin yaratdi. Shu o‘rinda, O‘zbekiston Prezidenti Shavkat Mirziyoyev ta’kidlaganidek, *“bugungi kunda dunyoda axborot sohasidagi tahdidlar kuchayib borayotgani, ayrim kuchlar internet va ijtimoiy tarmoqlar orqali odamlar ongiga salbiy ta’sir o‘tkazishga urinayotgani bizdan doimiy ogohlik va hushyorlikni talab etadi”* [1]. Davlat rahbari 2025 yil noyabr oyida o‘tkazilgan maxsus yig‘ilishda ham kiberxavfsizlik masalasiga alohida to‘xtalib, *“raqamlashtirish jarayoni har bir sohada shaffoflik va samaradorlikni ta’minlashi kerak, ammo bu jarayonda kiberjinoyatlarga qarshi*

kurashish tizimi ham texnologik, ham uslubiy jihatdan mukammal bo‘lishi shart” ekanligini ta’kidladi [2]. Mazkur ko‘rsatmalardan kelib chiqib, kiberjinoyatlar profilaktikasini amalga oshiruvchi subyektlar tizimini tahlil qilish va ularning o‘zaro hamkorlik mexanizmlarini takomillashtirish bugungi kunning eng dolzarb ilmiy-amaliy vazifalaridan biri hisoblanadi.

Kiberjinoyatchilikka qarshi kurashish va uning oldini olish tizimi ko‘p qirrali bo‘lib, u davlat organlari, xususiy sektor va fuqarolik jamiyatining jipslashgan faoliyatini talab qiladi. Ushbu maqolada biz kiberjinoyatlar profilaktikasi subyektlarining nazariy asoslarini, ular o‘rtasidagi hamkorlikning huquqiy jihatlarini hamda milliy va xorijiy tajribani atroflicha ko‘rib chiqamiz.

Hech kimga sir emaski, bugungi kunda kiberjinoyatlar profilaktikasining subyektlar tizimi va ularning vazifalari borasida huquqshunos olimlar o‘rtasida turlicha yondashuvlar mavjud. Professor M.H. Rustambayev kiberjinoyatlar profilaktikasini nafaqat jazo choralarini qo‘llash, balki tizimli va institutsional yondashuv asosida tashkil etilishi lozim bo‘lgan faoliyat sifatida tavsiflaydi [3]. Uning fikricha, profilaktika subyektlari tizimida ichki ishlar organlari markaziy o‘rin tutishi bilan birga, boshqa davlat organlari, mahalla va ta’lim muassasalari ham faol ishtirok etishi shart. Ushbu yondashuv *“ilmiy xulosa – tavsiya – natija”* tamoyiliga asoslanib, profilaktikaning barvaqt bosqichlarida ilmiy asoslangan choralarni qo‘llashni nazarda tutadi[4].

Rossiyalik olimlar kiberjinoyatchilikka qarshi kurashda subyektlarning integrativ va kompleks yondashuvini yoqlab chiqadilar. Jumladan, A.G. Volevodz xalqaro hamkorlikning ahamiyatiga to‘xtalib, kiberjinoyatlarning transchegaraviy tabiati sababli profilaktika subyektlari qatoriga xalqaro politsiya tashkilotlari va davlatlararo tuzilmalarni ham kiritishni taklif qiladi [5]. V.B. Vexov esa profilaktikani ikkita asosiy yo‘nalishga – *umumiy* va *maxsus* profilaktikaga ajratadi. Umumiy profilaktika subyektlari sifatida u axborot makonini tartibga soluvchi davlat idoralarini ko‘rsatsa, maxsus profilaktikada kiberxavfsizlik bo‘yicha mutaxassislar va raqamli kriminalistlarni e’tirof etadi [6].

Rivojlangan davlatlar olimlari, jumladan AQSH va Buyuk Britaniya vakillari *T.J. Xolt* [7] va *B.V. Reyns* [8] o‘z ilmiy tadqiqotlarida profilaktika tizimida *“Muntazam faoliyat nazariyasi” (Routine Activity Theory)* konsepsiyasini ilgari suradilar. Ularning fikricha, profilaktika subyekti sifatida nafaqat huquqni muhofaza qiluvchi organlar, balki *“raqamli vasiylar” (digital guardians),* ya’ni internetprovayderlar, IT-kompaniyalar va antivirus dasturlari ishlab chiquvchilar ham maydonga chiqishi kerak. Shuningdek, mazkur nazariyaga ko‘ra, jinoyatning oldini olish uchun jinoyatchining imkoniyatini cheklash, nishonning himoyasini kuchaytirish va nazorat qiluvchi subyektlarning sergakligini ta’minlash zarur.

S. Slonje va P. Smit esa profilaktikaning psixologik va ijtimoiy jihatlariga urg‘u beradilar. Ular kiberbulling va onlayn firibgarlikning oldini olishda ta’lim muassasalari va ijtimoiy xizmatlarni asosiy subyektlar deb hisoblashadi [9]. Bu esa profilaktika tizimi nafaqat texnik yoki huquqiy, balki pedagogik xarakterda ham bo‘lishi kerakligini anglatadi.

Olimlarning qarashlarini umumlashtirgan holda, profilaktika subyektlarini quyidagi guruhlarga ajratish mumkin:

Davlat/ olimlar guruhi	Asosiy ilmiy qarashlari	Profilaktika subyektlariga bergan tavsifi
O‘zbekiston *(M.H. Rustambayewa boshqalar)*	Institutsional va tizimli profilaktika	Huquqni muhofaza qiluvchi organlar va jamoatchilik tuzilmalarining uzviyligi
Rossiya *(A.G. Volevodz, V.B. Vexov)*	Integrativ va kriminalistik yondashuv	Davlat organlarining texnik va huquqiy salohiyatini birlashtirish
AQSH va Buyuk Britaniya *(T.J. Xolt, B.V. Reyns)*	Muntazam faoliyat va viktimologikprofilaktika	Xususiy sektor *(IT-kompaniyalar)*va foydalanuvchilarning mas’uliyati
Shimoliy Yevropa davlatlari (S. Slonjeva boshqalar)	Ijtimoiy-pedagogik profilaktika	Ta’lim tizimi va ijtimoiy himoya organlarining faolligi

Ushbu nazariy qarashlar shuni ko‘rsatadiki, kiberjinoyatlar profilaktikasi subyekti tushunchasi kengayib bormoqda. Endilikda bu tizimga nafaqat huquqni muhofaza qiluvchi xizmatlar, balki iqtisodiy subyektlar va fuqarolik instituti vakillari ham kiritilmoqda.

O‘zbekiston Respublikasi qonunchiligida kiberjinoyatlar profilaktikasi subyektlari tizimi so‘nggi yillarda tubdan yangilandi. Xususan, 2022-yilda qabul qilingan *“Kiberxavfsizlik to‘g‘risida”*gi qonun ushbu sohadagi munosabatlarni tartibga soluvchi asosiy huquqiy hujjat bo‘lib xizmat qilmoqda [10]. Qonunga muvofiq, kiberxavfsizlik sohasidagi yagona davlat siyosatini amalga oshiruvchi va tizimni muvofiqlashtiruvchi vakolatli organ sifatida O‘zbekiston Respublikasi Davlat xavfsizlik xizmati (DXX) belgilangan.

Milliy qonunchilikda profilaktika subyektlari quyidagi iyerarxik tartibda yoritilgan:

1. ***Davlat xavfsizlik xizmati:*** Kibermakondagi tahdidlarni aniqlash, muhim axborot infratuzilmasi obyektlarini himoya qilish va boshqa organlar faoliyatini muvofiqlashtirish uchun mas’ul [11].

2. ***Ichki ishlar vazirligi (IIV)*** huzuridagi Kiberxavfsizlik markazi bevosita kiberjinoyatchilikka qarshi kurashish, tezkor-qidiruv tadbirlarini o‘tkazish va aholi o‘rtasida profilaktika ishlarini olib borish bilan shug‘ullanadi [12]. Prezident qarori bilan ushbu markazning vakolatlari kengaytirilib, yettita yangi turdagi ekspertiza turlari joriy etildi.

3. ***Raqamli texnologiyalar vazirligi*** axborot texnologiyalari infratuzilmasini rivojlantirish, kiberxavfsizlik standartlarini ishlab chiqish va raqamli savodxonlikni oshirishga mas’ul.

4. ***Markaziy bank va tijorat banklari*** bank-moliya tizimidagi kiberjinoyatlarning *(masalan, fishing yoki onlayn kredit firibgarligi)* oldini olish uchun anti-frod tizimlarini qo‘llash va shubhali tranzaksiyalarni nazorat qilish majburiyatiga ega [13].

5. ***Bosh prokuratura*** profilaktika sohasidagi qonunlar ijrosi ustidan nazoratni amalga oshiradi. Shuningdek, Prezident ko‘rsatmasiga binoan, davlat organlarining qarorlari qonuniyligini maso-faviy monitoring qiluvchi “raqamli nazorat” tizimi joriy etilmoqda [14].

Milliy qonunchilikda subyektlarning hamkorligi masalasiga ham alohida e’tibor qaratiladi. Xususan, Prezidentimizning 2025-yil noyabrdagi topshiriqlariga asosan, jinoyat haqida xabar berilgan paytdan boshlab sud qarori ijrosigacha bo‘lgan barcha jarayonlarni raqamlashtirish va sun’iy intellekt texnologiyalarini joriy etish vazifasi qo‘yilgan [15]. Bu esa subyektlar o‘rtasidagi axborot almashinuvini tezlashtiradi.

Biroq, so‘nggi besh yillikda respublikada kiberjinoyatlar yil sayin keskin ortib bormoqda. Xususan, 2021–2025-yillarda mamlakatda jami kiberjinoyatlar soni *4 865 tadan 62 440 tagacha*, ya’ni qariyb *13 barobarga* o‘sishi [16] raqamli makondagi jinoyatchilikning transformatsiya-lashuv jarayoni naqadar shiddatli kechayotganini ko‘rsatadi. Ayniqsa, yetkazilgan umumiy moddiy zarar *(3 trln 730 mlrd so‘m)ning* salkam yarmi – *1 trln 890 mlrd so‘mi* aynan 2025-yilning 11 oyiga to‘g‘ri kelayotgani kibertahdidlarning nafaqat miqdor, balki sifat jihatidan ham ijtimoiy xavflilik darajasi ortib borayotganidan dalolat beradi.

Kriminologik vaziyatning bunday murakkab-lashuvi milliy qonunchilikda profilaktika subyektlari o‘rtasidagi o‘zaro hamkorlikning institutsional asoslari, xususan, *xususiy sektor (IT kompaniya-lar) va huquqni muhofaza qiluvchi organlar o‘rta-sidagi tezkor axborot almashinuvining protsessual tartiblari* yetarli darajada reglamentatsiya qilin-maganidan dalolat.

Mazkur huquqiy bo‘shliqlar amaliyotda axbo-rot texnologiyalari subyektlarining viktimologik profilaktikadagi mas’uliyatini cheklab, jinoyatlarni “issiq izidan” fosh etishda *idoraviy byurokratizm va vaqt yo‘qotishlariga* olib kelmoqda. Bu esa kiberjinoyatchilikka qarshi kurashishning tashkiliy-huquqiy mexanizmlarini takomillashtirish hamda xususiy sektorning ijtimoiy mas’uliyatini qonun darajasida mustahkamlash zaruratini dolzarb masala sifatida kun tartibiga qo‘ymoqda.

Shu o‘rinda, rivojlangan davlatlar tajribasiga nazar tashlasak, ularda kiberjinoyatlar profilak-tikasi subyektlari tizimining yuqori darajadagi ixtisoslashuvi va institutsional jipsligi bilan ajralib turadi. Xususan:

Buyuk Britaniya modelining asosini 2016-yilda tashkil etilgan Milliy kiberxavfsizlik markazi *(National Cyber Security Centre – NCSC)* tashkil etadi. NCSC Hukumat aloqalari markazi tarkibiga kiradi va Britaniyani onlayn rejimda yashash va

ishlash uchun eng xavfsiz joyga aylantirish missiyasini bajaradi [17]. Uning o‘ziga xos jihati shundaki, NCSC nafaqat davlat idoralari, balki kichik biznes va oddiy fuqarolar bilan ham bevosita hamkorlik qiladi. Ular uchun maxsus *“Cyber Assessment Framework”* va *“Cyber Action Toolkit”* kabi vositalar ishlab chiqilgan bo‘lib, bu profilaktikaning avtomatizatsiya darajasini oshiradi [18].

Amerika Qo‘shma Shtatlarida esa profilaktika tizimi ko‘p qatlamli bo‘lib, asosiy rol Kiberxavfsizlik va infratuzilma xavfsizligi agentligi (CISA) zimmasiga yuklatilgan [19]. CISA Milliy xavfsizlik departamenti (DHS) tarkibida faoliyat yuritib, federal agentliklar va muhim infratuzilma operatorlari o‘rtasida ma’lumot almashinuvini ta’minlaydi. 2022-yilda qabul qilingan CIRCIA *(Cyber Incident Reporting for Critical Infrastructure Act)* qonuni muhim infratuzilma subyektlarini kiberhujum sodir bo‘lganligi haqida 72 soat ichida CISA ga xabar berishga majbur qiladi [20]. Shuningdek, FQB (FBI) va Maxfiy xizmat (Secret Service) transmilliy kiberjinoyatlarni tergov qilish va operativ profilaktika ishlarini olib boradi [21].

Shuningdek, bugungi kunda dunyoda kibermakondagi tahdidlarga qarshi kurashishda ijobiy tajribani aynan Skandinaviya mamlakatlari va Finlyandiya davlati eng samarali tizimlardan birini yaratgan. Xususan, ***Finlandiya*** Xalqaro elektr aloqa ittifoqi (ITU) tomonidan e’lon qilinadigan Global kiberxavfsizlik indeksida *(Global Cybersecurity Index — GCI)* izchil ravishda yuqori natijalarni qayd etib kelmoqda *(masalan, oxirgi hisobotlarda 95.78 ball bilan top-reytinglarda turadi)* [22]. Finlandiya modelining o‘ziga xosligi – kiberxavfsizlikni ta’minlashda nafaqat davlat organlari, balki xususiy sektor va fuqarolik jamiyatining *“milliy yakdilligi”*ga asoslanishidadir.

Mintaqaviy darajada ***Skandinaviya*** davlatlari *(Norvegiya, Daniya, Shvetsiya va Finlandiya) “Nordic National CERT Collaboration”* platformasi doirasida faol hamkorlik qiladi. Mazkur tuzilma texnik ma’lumotlarni *(insidentlar haqidagi xabarlarni)* real vaqt rejimida almashish, transchegaraviy kiberhujumlarga qarshi qo‘shma kibermashqlar o‘tkazish va profilaktikaning yagona standartlarini ishlab chiqish bilan shug‘ullanadi [23].

Norvegiya tajribasida esa Milliy kiberjinoyatchilikka qarshi kurash markazi *(NCIS — National Cyber Crime Centre)* yetakchilik rolini o‘ynaydi. Ushbu markazning o‘ziga xosligi shundaki, u nafaqat milliy darajada, balki xalqaro operativ maydonda, xususan, Yevropol qoshidagi *J-CAT (Joint Cybercrime Action Taskforce)* tizimi bilan uzviy bog‘langan. Bu mexanizm Norvegiya huquqni muhofaza qilish organlariga xalqaro kiberguruhlarni aniqlash va ularga qarshi tezkor choralar ko‘rishda keng imkoniyat yaratadi [24].

Fransiya davlatida Milliy tizimlar xavfsizligi agentligi (ANSSI) kiberxavfsizlik siyosatini belgilaydi va muhim ahamiyatga ega operatorlarni himoya qiladi [25]. ***Ispaniyada*** esa Milliy kiberxavfsizlik instituti (INCIBE) fuqarolar va tadbirkorlar uchun asosiy profilaktika subyekti hisoblanadi [26]. Uning *“017”* ishonch telefoni kibertahdidlarga qarshi tezkor maslahat berish tizimi sifatida dunyoda tan olingan [27].

Quyidagi jadvalda rivojlangan davlatlarning profilaktika subyektlari va hamkorlik mexanizmlari qiyoslangan:

Davlat	Asosiy profilaktika subyekti	Hamkorlik mexanizmining o‘ziga xos jihati
Buyuk Britaniya	NCSC *(Milliy kiberxavfsizlik markazi)*	Davlat va sanoat o‘rtasidagi *“yagona oyna”* tizimi [28]
AQSH	CISA *(Kiberxavfsizlik agentligi)*	Hodisalar haqida majburiy hisobot berish (CIRCIA)[29]
Finlandiya	NCSC-FI *(Transport va aloqa agentligi)*	Mintaqaviy (Nordic) va yuqori texnologik hamkorlik[30]
Shveysariya	NCSC *(sobiq MELANI)*	Davlat va xususiy sektorning strategik sheriklig[31]
Ispaniya	INCIBE *(Milliy kiberxavfsizlik instituti)*	Fuqarolik jamiyati va KO‘B uchun keng qamrovli xizmatla[32]

Ushbu davlatlarda hamkorlik nafaqat davlat idoralari o‘rtasida, balki davlat va xususiy sektor *(Public-Private Partnership)* o‘rtasida ham yuqori darajada yo‘lga qo‘yilgan. Bu kiberjinoyatlarni barvaqt aniqlash va ularning oqibatlarini yumshatish imkonini beradi. Shuningdek, mavzu doirasida kibermakondagi huquqbuzarliklar profilaktikasini amalga oshiruvchi subyektlar tizimini o‘rganishda, xalqaro tan olingan Finlandiya tajribasi *(GCI – 95,78)* alohida ahamiyatga ega. Mazkur davlatda profilaktikaning muvaffaqiyati *“Nordic National CERT Collaboration” va NCIS (Norvegiya)* kabi tizimlar doirasida davlat va xususiy sektorning real vaqt rejimidagi hamkorligiga asoslangan [33]. Biroq, milliy amaliyot va Andijon viloyati misolida o‘rganilgan jinoyat ishlari fabulalari tahlili bizda profilaktika subyektlari o‘rtasidagi hamkorlikda jiddiy institutsional muammolar mavjudligini ko‘rsatmoqda. Bularga:

Birinchidan, subyektlararo hamkorlikning huquqiy mexanizmi detallashtirilmagan. O‘rganilgan jinoyat ishlari tahlili shuni ko‘rsatadiki, *“Uzum nasiya”* kabi IT-platformalar va banklar jinoyat alomatlarini aniqlagan taqdirda ham ularni IIOga tezkorlik bilan uzatish bo‘yicha protsessual majburiyatga ega emas. Bu esa xususiy sektorning *(IT-kompaniyalar)* profilaktika tizimidan uzilib qolishiga sabab bo‘lmoqda.

Ikkinchidan, axborot almashinuvidagi “byurokratik lag” (vaqt yo‘qotish) muammosi. Jinoyatchilar mablag‘larni masofaviy boshqarish orqali bir necha soniya ichida o‘zlashtirmoqdalar. Amalda esa IIO va bank tizimlari o‘rtasida ma’lumot almashish an’anaviy so‘rovnomalar asosida amalga oshirilmoqda. Shimoliy Yevropa davlatlaridagi *J-CAT* tizimidan farqli o‘laroq, bizda shubhali tranzaksiyalarni avtomatik to‘xtatish va real vaqtda xabar berish mexanizmi yo‘qligi sababli yetkazilgan 3,7 trln so‘mlik zararning aksariyati qaytarilmay qolmoqda [34].

Uchinchidan, viktimologik profilaktikaning sustligi. Fuqarolarning ishonuvchanligi natijasida mablag‘larini boy berishi profilaktika subyektlari tomonidan aholining kiber-savodxonligini oshirish bo‘yicha tarqoq, tizimsiz harakat qilinayotganidan dalolat beradi.

Milliy va xorijiy davlatlarning kiberxavfsizlik sohasidagi huquqiy normalarini ilmiy-qiyosiy tahlil qilish shuni ko‘rsatadiki, O‘zbekiston Respublikasi qonunchiligi rivojlangan davlatlar tajribasini o‘zlashtirishda muayyan yutuqlarga erishgan bo‘lsa-da, profilaktika subyektlarining hamkorlik mexanizmlarida hali ham tizimli huquqiy bo‘shliqlar mavjudligi kuzatilmoqda. Nazarimizda, ushbu bo‘shliqlarni quyidagi to‘rtta konseptual yo‘nalishda klassifikatsiyalash maqsadga muvofiq. Bular:

1. Insidentlar haqida majburiy xabardor qilish (Mandatory Reporting) institutining shakllanmaganligi. Xorijiy tajribada, xususan, AQSHning *“Kiberxavfsizlik bo‘yicha muhim infratuzilma insidentlari to‘g‘risida xabar berish to‘g‘risida”*gi qonunida (CIRCIA) muhim infratuzilma obyektlari kiberhujum sodir etilgan vaqtdan boshlab qat’iy belgilangan muddatda xabar berishi shartligi belgilangan [35]. O‘zbekiston qonunchiligida bunday majburiyat asosan davlat organlariga tegishli bo‘lib, xususiy sektor, ayniqsa, moliyaviy tashkilotlar va aloqa provayderlari uchun insidentlar haqida tezkor xabar berishning aniq huquqiy mexanizmi hamda uni bajarmaganlik uchun sanksiyalar tizimi yetarli darajada detallashtirilmagan. Bu esa kiberjinoyatlar profilaktikasida subyektlararo axborot almashinuvining sustligiga olib kelmoqda.

2. Elektron dalillarni “tezkor saqlash” (Preservation of Data) mexanizmining yo‘qligi. Kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasiga a’zo davlatlar *(masalan, Fransiya, Germaniya)* qonunchiligida *“ma’lumotlarni tezkor saqlash”* (*expedited preservation of stored computer data*) mexanizmi mavjud bo‘lib, u raqamli izlar yo‘q qilinishidan oldin ma’lumotlarni ma’lum muddatga blokda saqlab turish imkonini beradi [36]. O‘zbekiston Jinoyat-protsessual kodeksida bunday tezkor choralarning yo‘qligi, profilaktika va surishtiruv jarayonining an’anaviy *“tintuv”* va *“olib qo‘yish”* normalari bilan cheklanib qolgani raqamli makonda dalillar bazasini shakllantirish samaradorligini pasaytiradi.

3. Kiber-sug‘urta va jabrlanuvchiga zararni qoplash tizimining nomukammalligi. Kanadaning PIPEDA qonuni kabi xalqaro andozalarda shaxsga doir ma’lumotlar xavfsizligini ta’minlamagan tashkilotlarning qat’iy mas’uliyati va jabrlanuvchiga zararni qoplashning sug‘urtaviy mexanizmlari rivojlangan [37]. Milliy amaliyotda

esa, bank kartalaridan mablag‘lar noqonuniy yechib olinganda, zararni qoplash mas’uliyati ko‘pincha jabrlanuvchining zimmasida qolmoqda. Bu esa tijorat banklarining kiberprofilaktika sohasidagi ijtimoiy va huquqiy mas’uliyatini oshirish uchun maxsus sug‘urta fondlarini tashkil etish zaruratini tug‘diradi.

4. Sun’iy intellektdan (AI) profilaktika maqsadida foydalanishning huquqiy chegaralari belgilanmaganligi. Ilmiy tadqiqotlar shuni ko‘rsatadiki, sun’iy intellekt nafaqat jinoyat sodir etish vositasi, balki preventiv monitoringning muhim instrumenti hamdir. Biroq, profilaktika maqsadida AI yordamida aholini monitoring qilishning inson huquqlari va shaxsiy hayot daxlsizligi bilan bog‘liq muvozanati milliy qonunchilikda o‘z ifodasini topmagan [38]. Bu esa raqamli texnologiyalarni profilaktikaga joriy etishda *“huquqiy xavfsizlik”* tamoyilining buzilishiga sabab bo‘lishi mumkin.

Yuqoridagi tahlillardan kelib chiqib, milliy qonunchilikni xalqaro standartlarga muvofiqlashtirish nafaqat davlat organlarining, balki xususiy sektorning ham profilaktik funksiyalarini kengaytirishni taqozo etadi.

Xulosa qilib aytganda, kiberjinoyatlar profilaktikasi subyekti sifatida faqat davlat organlariga tayanish yetarli emas. Global tajriba *(Finlandiya va Shimoliy Yevropa mamlakatlari)* va olib borilgan ilmiy tahlillar shuni ko‘rsatadiki, samarali tizim faqatgina *davlat, biznes va fuqarolarning* texnologik va huquqiy jihatdan birlashgan makonida *(Public-Private Partnership)* shakllanishi mumkin.

Foydalanilgan manbalar

1.Matbuot va ommaviy axborot vositalari xodimlariga bayram tabrigi //https://president.uz/uz/lists/view/6442
2.Uzbekistan to intensify fight against drug and cybercrime, expand digital oversight system // https://daryo.uz/en/2025/11/04/uzbekistan-to-intensify-fight-against-drug-and-cybercrime-expand-digital-oversight-system/
3.Cybercrime Prevention: Theory and Applications | Request PDF – ResearchGate // https://www.researchgate.net
4.Scientific approach to early crime prevention in Surkhandarya mahallas // https://proacademy.uz/en/news/view?alias=2784
5.Parhomenko S.V., Evdokimov K.N. Prevention of cybercrime in the Russian federation: An integrative and comprehensive approaches // July 2015 Криминологический журнал Байкальского государственного университета экономики и права 9(2):265-276 / DOI:10.17150/1996-7756.2015.9(2).265-276
6.Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. – Волгоград: ВА МВД России, 2004. – С. 154–158.
7.Holt, T. J. "Examining the Applicability of Routine Activity Theory to Explain Victimization Online" // Deviant Behavior / 2008, Volume 30, Issue 1. – P. 1–25
8.Reins B.H. “Cyberbolt: A Systemic Approach to Cybercrime” ёки “Cybercrime: A Reference Handbook” ABC-CLIO. – P. 84–87.
9.Slonje S., Smith P. K. Cyberbullying: Another main type of bullying? // Scandinavian Journal of Psychology. – 2008. – Vol. 49. – Iss. 2. – P. 152.
10.O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son qonuni // https://lex.uz/docs/5960604
11. O‘zbekiston Respublikasining “O‘zbekiston Respublikasi Davlat xavfsizlik xizmati to‘g‘risida”gi O‘RQ-471-son qonunning 5-moddasi // https://www.lex.uz/acts /3610935
12.O‘zbekiston Respublikasi Prezidentining “Raqamli mahsulotlarning kiberxavfsizligini ta’minlash va kriminalistik tadqiqotlarni takomillashtirish chora-tadbirlari to‘g‘risida”gi PQ-209-son qarori // Qonunchilik ma’lumotlari milliy bazasi, 03.07.2023-y., 07/23/209/0438-son.
13.O‘zbekiston Respublikasining “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi. O‘RQ-578-son qonuni.
14.O‘zbekiston Respublikasi Prezidentining “Raqamli texnologiyalar sohasida jinoyatchilikka qarshi kurashish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PQ-381-son qarori // https://lex.uz/docs/6681111
15.O‘zbekiston Respublikasi Prezidentining “Sud hokimiyati organlari faoliyatini raqamlashtirish chora-tadbirlari to‘g‘risida”gi PQ-4818-son qarori / https://lex.uz/docs/4979896
16.https://kun.uz/kr/63123328

17.National Cyber Security Centre - GOV.UK //https://www.gov.uk
18.National Cyber Security Centre - NCSC.GOV.UK // https://www.ncsc.gov.uk/
19.Combatting Cyber Crime – CISA // https://www.cisa.gov/ combatting-cyber-crime
20.Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) – CISA // https://www.cisa.gov
21.Combatting Cyber Crime – CISA // https://www.cisa.-gov/combatting-cyber-crime
22.International Telecommunication Union (ITU). Global Cybersecurity Index 2024 Report. – Geneva: ITU Publications.
23.Nordic CSIRTs Collaboration. Annual Report on Regional Cooperation in Cybersecurity. – Oslo/Helsinki: Nordic National CERTs.
24.Europol. Joint Cybercrime Action Taskforce (J-CAT) Operational Overview. – The Hague: European Cybercrime Centre (EC3).
25.France - NCC - European Cybersecurity Competence Centre and Network // https://cybersecurity-centre.europa.eu/ france-ncc_en
26.NCC-ES – INCIBE // https://www.incibe.es/en/incibe/corporate-information/who-we-work-with/european-projects/NCC-ES
27.SIC-SPAIN 3.0 – INCIBE // https://www.incibe.es/en/incibe /corporate-information/who-we-work-with/european-projects/ sic-spain3
28.What we do at the NCSC - NCSC.GOV.UK // https://www.ncsc.-gov.uk
29.Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) – CISA // https://www.cisa.gov/topics/cyber-threats-and-advisories/information -sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
30.Global Cybercrime Report 2024: Which Countries Face the Highest Risk? – MixMode // https://www.mixmode.ai/ blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk
31.Europe's commitment in cybersecurity – ITU // https://www.itu.int/en/-ITUD/Cybersecurity/Documents/GCI_EUROPE_ITUwebinar.pdf
32.SIC-SPAIN 3.0 - INCIBE // https://www.incibe.es/en/incibe/ corporate-information/who-we-work-with/european-projects/sic-spain3
33.International Telecommunication Union (ITU). Global Cybersecurity Index 2024 Report. – Geneva, 2024.
Andijon shahri bo‘yicha IIOFMB huzuridagi Tergov bo‘limi materiallari: 2025-yildagi 56633, 56864, 54732, 54583-sonli jinoyat ishlari fabulalari.
34.Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). – Public Law No. 117-103.
35.Council of Europe. Convention on Cybercrime (Budapest Convention). ETS No.185. – Article 16.
36.Personal Information Protection and Electronic Documents Act (PIPEDA). – S.C. 2000, c. 5.
37.European Commission. Ethics guidelines for trustworthy AI. – Brussels, 2019.