KIBERJINOYATLAR PROFILAKTIKASINI TAKOMILLASHTIRISHNING NAZARIY-METODOLOGIK ASOSLARI

Mirzajonov Shoxruxbek Sobirjonovich

O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti mustaqil izlanuvchisi

Исследовательский институт криминологии Республики Узбекистан, независимый научный сотрудник

Independent researcher at the Research Institute of Criminology of the Republic of Uzbekistan

Annotatsiya. *Maqolada Yangi O‘zbekistonda kiberjinoyatchilikning oldini olishning normativ, uslubiy va doktrinal asoslari tahlil qilingan. Milliy strategiyalar hamda xorijiy (MDH, Osiyo, Yevropa, AQSh) yondashuvlarning qiyosiy tahlili asosida tadqiqotga situatsion profilaktika va politsentrik boshqaruv kabi zamonaviy konsepsiyalar integratsiya qilingan. Muallif “kibero‘g‘rilik” va “kiberfiribgarlik” tushunchalarining mualliflik ta’riflarini taklif etadi, shuningdek, kiberxavfsizlikni ta’minlash va raqamli huquqlarni himoya qilish prinsipini mustahkamlash zaruratini asoslaydi.*

Kalit so‘zlar: *kiberjinoyatlar profilaktikasi; kiberxavfsizlik; raqamli huquqlar; kibero‘g‘rilik; kiberfiribgarlik; situativ profilaktika; politsentrik boshqaruv; Budapesht konvensiyasi; NIS2.*

THEORETICAL AND METHODOLOGICAL FOUNDATIONS FOR IMPROVING CYBERCRIME PREVENTION

Abstract. *The article analyzes the regulatory, methodological, and doctrinal foundations of cybercrime prevention in New Uzbekistan. Based on national strategies and a comparative review of foreign approaches (CIS, Asia, Europe, USA), the study integrates contemporary concepts – such as situational prevention and polycentric governance – into the national criminological perspective. The author proposes original definitions for “cyber theft” and “cyber fraud” to be included in the Criminal Code, alongside codifying a distinct principle of ensuring cybersecurity and protecting digital rights.*

Keywords: *cybercrime prevention; cybersecurity; digital rights; cyber theft; cyber fraud; situational prevention; polycentric governance; Budapest Convention; NIS2.*

XXI asrning uchinchi o‘n yilligiga kelib, insoniyat sivilizatsiyasi o‘zining rivojlanish bosqichida tub burilish nuqtasiga – global raqamlashtirish davriga qadam qo‘ydi. Axborot-kommunikatsiya texnologiyalarining shiddatli rivojlanishi nafaqat iqtisodiy va ijtimoiy munosabatlarni, balki davlat boshqaruvi, milliy xavfsizlik va huquq-tartibot tizimining paradigmalarini ham tubdan o‘zgartirib yubordi. Ushbu global tendensiyalar fonida Yangi O‘zbekistonda amalga oshirilayotgan keng ko‘lamli islohotlar raqamli suverenitetni mustahkamlash va kibermakonda fuqarolarning huquq va erkinliklarini ishonchli himoya qilishga qaratilgan yangicha yondashuvlarni taqozo etayotgani hech kimga sir emas.

Shu o‘rinda, O‘zbekiston Respublikasi Prezident Sh.Mirziyoyev rahbarligida mamlakatimizda raqamli iqtisodiyotni rivojlantirish davlat siyosatining ustuvor yo‘nalishi sifatida belgilab olindi. Xususan, “Raqamli O‘zbekiston — 2030” strategiyasining qabul qilinishi [1] va uning doirasida amalga oshirilayotgan tizimli ishlar respublikani mintaqaviy IT-habga aylantirish, davlat xizmatlarini to‘liq raqamlashtirish va iqtisodiyotning barcha tarmoqlariga “aqlli” texnologiyalarni joriy etish maqsadini ko‘zlaydi [2]. Biroq, dialektik qonuniyatlarga ko‘ra, har qanday texnologik progress o‘zi bilan birga yangi turdagi xavf-xatarlarni ham olib keladi. Raqamlashuv jarayonlarining tezlashishi kibermakondagi jinoyatchilikning *(cybercrime)* misli ko‘rilmagan darajada o‘sishiga, uning shakllari va usullarining murakkablashuviga zamin yaratmoqda.

Jahon iqtisodiyoti va siyosatida yuz berayotgan geosiyosiy o‘zgarishlar sharoitida kiberxavfsizlik nafaqat texnik masala, balki milliy xavfsizlikning eng muhim tarkibiy qismiga aylandi. Xalqaro ekspertlarning baholashicha, kiberhujumlar natijasida jahon iqtisodiyotiga yetayotgan yillik zarar miqdori trillionlab AQSH dollarini tashkil etmoqda va bu ko‘rsatkich yil sayin ortib bormoqda [3]. O‘zbekistonda ham so‘nggi yillarda bank kartalaridan o‘g‘rilik, fishing hujumlari, ijtimoiy muhandislik *(social engineering)* asosidagi firibgarliklar va muhim axborot infratuzilmasiga qaratilgan kibertahdidlar soni keskin oshgani kuzatilmoqda. Bu esa, o‘z navbatida, huquqni muhofaza qiluvchi organlar va qonun chiqaruvchilar oldiga jinoyatchilikka qarshi kurashishning an’anaviy reaktiv *(jinoyat sodir etilgandan keyingi)* usullaridan voz kechib, proaktiv *(oldini oluvchi)* strategiyalarni ishlab chiqish vazifasini ko‘ndalang qo‘ymoqda.

Mazkur mavzuning dolzarbligi shundaki, milliy qonunchiligimizda va huquqiy fanda “kiberjinoyatlar profilaktikasi” tushunchasi, uning metodologik asoslari va amalga oshirish mexanizmlari haligacha to‘liq va tizimli ravishda tadqiq etilmagan. Amaliyotda ko‘rilayotgan choralar ko‘pincha tarqoq, texnik xarakterga ega bo‘lib, jinoyatning asl sabablarini *(kriminogen omillarni)* bartaraf etishga emas, balki oqibatlarini yumshatishga qaratilmoqda. Shu bois, ushbu maqolada biz kiberjinoyatlar profilaktikasining ilmiy-nazariy mohiyatini ochib berish, milliy va xorijiy tajribani qiyosiy tahlil qilish orqali O‘zbekiston uchun eng maqbul modelni taklif etishni maqsad qildik. Tahlil davomida Prezident Sh.Mirziyoyevning sohaga oid farmon va qarorlarida belgilangan vazifalar, jumladan, 2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi [4] va 2023-yil 31-mayda qabul qilgan “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi qarori asosiy metodologik yo‘nalish sifatida olindi [5].

Kiberjinoyatlar profilaktikasining mohiyatini tushunish uchun avvalo “kiberjinoyat” va “profilaktika” tushunchalarining o‘zaro dialektik bog‘liqligini tahlil qilish lozim. An’anaviy kriminologiyada profilaktika (prevention) deganda, shaxsda jinoyat sodir etish qasdi shakllanishining oldini olish, ijtimoiy muhitdagi salbiy omillarni bartaraf etish va jinoyat sodir etish uchun qulay sharoitlarni yo‘qotishga qaratilgan kompleks chora-tadbirlar tushuniladi. Biroq, kibermakon *(cyberspace)* o‘zining fizik va huquqiy tabiati bilan an’anaviy jinoyat maydonidan tubdan farq qiladi.

Shu o‘rinda, kiberjinoyatlar profilaktikasining an’anaviy profilaktikadan farqli jihatlarini belgilab beruvchi quyidagi asosiy omillarni sanab o‘tish lozim topdik:

1. Transchegaraviylik (Transnationality) omili. Bunda kiberjinoyatchi jismonan bir davlatda (masalan, Sharqiy Yevropa yoki Janubi-Sharqiy Osiyoda) bo‘lib turib, O‘zbekistondagi bank tizimiga yoki fuqarolarning elektron hamyonlariga hujum qilishi mumkin. Bu esa profilaktika choralarining faqat milliy chegaralar doirasida cheklanib qolishini samarasiz qiladi va xalqaro hamkorlikning yangi darajasini talab etadi. Xalqaro huquqda, xususan, Yevropa Kengashining *Budapesht konvensiyasida* bu masala markaziy o‘rin tutadi, biroq milliy qonunchilikda transchegaraviy profilaktika mexanizmlari hali to‘liq shakllanmagan [6].

2. Anonimlik va masofaviylik omili. Bunda jinoyatchi o‘z shaxsini yashirish uchun VPN, proksi-serverlar, TOR tarmoqlari va shifrlangan messenjerlardan foydalanadi. An’anaviy profilaktikada “profilaktik hisobda turuvchi shaxs” bilan yuzma-yuz ishlash mumkin bo‘lsa, kibermakonda

profilaktika obyekti (potensial jinoyatchi) ko‘pincha noma’lum bo‘ladi. Shu sababli, profilaktika markazi jinoyatchi shaxsidan *(offender-oriented)* jinoyat quroli va muhitiga *(environment-oriented)* ko‘chishi lozim.

3. Latentlik va avtomatlashtirish omili. Kiberjinoyatlarning aksariyati (masalan, kichik miqdordagi firibgarliklar) ro‘yxatga olinmaydi. Bundan tashqari, hujumlar avtomatlashtirilgan dasturlar *(botnetlar)* orqali amalga oshiriladi. Bu inson omilisiz, soniyasiga minglab hujumlarni amalga oshirish imkonini beradi. Shunga yarasha profilaktika tizimi tezkor va avtomatlashtirilgan bo‘lishi shart.

Kiberjinoyatlar profilaktikasining nazariy asoslarini o‘rganishda milliy va xorijiy huquqshunos olimlarning tadqiqotlari muhim ahamiyatga ega. Ularning qarashlarini qiyosiy tahlil qilish orqali O‘zbekiston uchun maqbul ta’rifni shakllantirish mumkin. Hech kimga sir emaski, so‘nggi yillarda yangi O‘zbekistonda ham milliy huquqshunoslik yo‘nalishida kiberjinoyatlar profilaktikasi masalalari faol o‘rganilmoqda. Xususan, yuridik fanlar doktori A.K. Rasulev o‘z tadqiqotlarida kiberjinoyatlarga qarshi kurashishning jinoiy-huquqiy va kriminologik jihatlarini chuqur tahlil qilgan. Olimning fikricha, kiberjinoyatlar profilaktikasini “jinoyat sodir etilganidan keyingina javobgarlikni ta’minlash” vazifasi bilan cheklab bo‘lmaydi. U profilaktikani axborot xavfsizligi konsepsiyasining ajralmas qismi sifatida ko‘rib, tahdidlar monitoringi, axborot tizimlari zaifliklarini aniqlash va fuqarolarning raqamli huquqiy ongini yuksaltirishga qaratilgan uzluksiz siyosat sifatida talqin qiladi [7].

Shuningdek, A.K. Rasulev va G.A. Sa’dullayev hamkorlikdagi tadqiqot ishlarida “kadrlar salohiyati” omilini alohida ajratib ko‘rsatadilar. Ularning qarashlaricha, eng mukammal qonunlar va texnika ham, agar ularni ishlatadigan malakali mutaxassislar bo‘lmasa, profilaktikada o‘zining samarali natijasini bermaydi. Shu bois, ular profilaktikaning metodologik asoslari qatoriga “yuqori malakali kiberxavfsizlik kadrlarini tayyorlash” prinsipini kiritishni taklif qiladilar [8]. Tadqiqotchi D. Raxmanov esa kiberjinoyatlar profilaktikasini uch bosqichli tizim sifatida tasniflaydi. Bular:

umumiy ijtimoiy profilaktika – jamiyatda kibermadaniyatni shakllantirish, iqtisodiy va ijtimoiy sabablarni bartaraf etish;

maxsus-kriminologik profilaktika – bevosita axborot tizimlarini himoya qilish, monitoring va tezkor-qidiruv tadbirlarini amalga oshirish;

individual-viktimologik profilaktika – kiberhujum qurboni bo‘lish ehtimoli yuqori bo‘lgan guruhlar *(yoshlar, keksalar, kichik biznes)* bilan manzilli ishlash[9]. Bu yondashuv amaliyot uchun juda qulay bo‘lib, har bir bosqichda mas’ul subyektlarni aniq belgilash imkonini beradi.

J. Umurzakov esa masalaga makroiqtisodiy nuqtai nazardan yondashib, profilaktikani milliy kiberxavfsizlik strategiyalari va CERT *(Computer Emergency Response Team)* markazlari faoliyati bilan bog‘laydi. Uning fikricha, profilaktikaning bosh maqsadi – kiberjinoyatlardan ko‘riladigan global iqtisodiy zararni kamaytirishdir [10].

Rossiyalik olim K.N. Yevdokimov kompyuter jinoyatchiligiga qarshi kurashishning tashkiliy-huquqiy asoslarini ilmiy tadqiq etar ekan, profilaktika samarasizligining asosiy sababi sifatida qonunchilikdagi bo‘shliqlarni ko‘rsatadi. Uning ta’kidlashicha, Rossiya Federatsiyasi va MDH davlatlarida profilaktika ko‘pincha faqat huquqni muhofaza qiluvchi organlar vazifasi deb qaraladi. Shuningdek, K.N. Yevdokimov “Kompyuter jinoyatchiligiga qarshi kurashish to‘g‘risida” maxsus federal qonun qabul qilish va unda profilaktika subyektlari, xususan, internet-provayderlar va IT-kompaniyalarning majburiyatlarini aniq belgilashni taklif qiladi [11]. Bu yondashuv yangi O‘zbekiston uchun ham dolzarb, chunki xususiy sektorning profilaktikadagi o‘rni qonunchilikda yetarlicha aks ettirilmagan. V.G. Stepanov-Yegiyans va M.A. Prostoserdov esa profilaktikani jinoyat huquqi normalarini takomillashtirish bilan bog‘laydilar. Ularning fikricha, jinoyat qonunidagi jazo muqarrarligi va sanksiyalarning qat’iyligi (general deterrence) eng katta profilaktik kuchga ega [12].

Shu o‘rinda, G‘arb kriminologiyasida kiberjinoyatlar profilaktikasiga nazar tashlasak, yondashuv tubdan farq qiladi. Bu yerda “politsiya nazorati”dan ko‘ra “boshqaruv” (governance) va “ekologiya” (ecology) tushunchalari ustunlik qiladi.

Kanadalik olim, Monreal universiteti professori Benua Dyupon o‘zining “Politsentrik boshqaruv” (Polycentric Governance) nazariyasini ilgari suradi. Uning fikriga ko‘ra, kibermakon infratuzilmasi (serverlar, kabellar, dasturlar) asosan xususiy sektorga tegishli bo‘lganligi sababli, davlat (politsiya) yolg‘iz o‘zi jinoyatchilikni nazorat qila olmaydi. Profilaktika markazlashgan emas, balki “politsentrik” bo‘lishi, ya’ni davlat, biznes, nodavlat tashkilotlar va xalqaro tuzilmalarning teng huquqli tarmog‘iga asoslanishi kerak. Shuningdek, B.Dyuponning fikricha, kibermakonda eng samarali profilaktika – bu *“fragmented networks of cooperation”* (tarqoq hamkorlik tarmoqlari)ni birlashtirish va muvofiqlashtirishdir [13].

Shuningdek, Kembrij va Edinburg universitetlari tadqiqotchilari bo‘lgan Ben Kolyer va Elis Xatchings o‘zlarining “Kiberjinoyatlarning ijtimoiy ekologiyasi” (Social Ecology of Cybercrime) nazariyasini ishlab chiqqanlar. Ular kiberjinoyatchilikni alohida individlarning harakati emas, balki murakkab ekotizim sifatida ko‘rishadi. Bu ekotizimda xakerlik forumlari, qora bozorlar (Darknet), o‘qitish xizmatlari va pul yuvish mexanizmlari o‘zaro bog‘liq holda ishlaydi. Bundan tashqari, aynan B. Kolyerning fikricha, profilaktika jinoyatchini jazolashdan ko‘ra, “zararni kamaytirish” (harm reduction) va yoshlarni jinoiy yo‘ldan qaytarish (divert)ga qaratilishi kerak [14].

Avstraliyalik olim H. Ho va uning hamkasblari “Situativ jinoyat profilaktikasi” (Situational Crime Prevention – SCP) nazariyasini kibermakonga tatbiq etish bo‘yicha keng ko‘lamli tadqiqotlar olib borishgan. Ularning tizimli tahlili (systematic review) shuni ko‘rsatadiki, kiberjinoyatlarni oldini olishning eng samarali yo‘li – bu jinoyat sodir etish imkoniyatlarini texnik jihatdan cheklash (masalan, ikki faktorli autentifikatsiya, murakkab parollar, tarmoq monitoringi) [15].

Yuqoridagi tahlillardan kelib chiqib, shuni xulosa qilish mumkinki, O‘zbekiston sharoitida kiberjinoyatlar profilaktikasiga beriladigan ta’rif ham huquqiy, ham texnik, ham ijtimoiy jihatlarni qamrab olishi zarur. Biz olib borilgan o‘rganishlardan kelib chiqib quyidagi ta’rifni taklif qilamiz:

*“**Kiberjinoyatlar profilaktikasi** – bu kibermakonda shaxs, jamiyat va davlatning qonuniy manfaatlariga tahdid soluvchi jinoiy qilmishlarning sabablari va sharoitlarini aniqlash, bartaraf etish hamda ularning sodir etilishiga yo‘l qo‘ymaslik maqsadida davlat organlari, xususiy sektor, fuqarolik jamiyati institutlari va xalqaro tashkilotlar tomonidan politsentrik hamkorlik asosida amalga oshiriladigan huquqiy, tashkiliy, texnik, viktimologik va ma’rifiy chora-tadbirlarning yagona va uzluksiz tizimi”.*

Mazkur ta’rifda profilaktikaning subyekti sifatida nafaqat davlatni, balki xususiy sektorni ham kiritdik (B. Dyupon nazariyasiga muvofiq) va choralar tizimiga “viktimologik” (qurbonlarni himoya qilish) va “texnik” (SCP nazariyasiga muvofiq) elementlarni qo‘shdik.

Shuni alohida ta’kidlash joizki, profilaktika faoliyatining samaradorligi uning metodologik bazasi qanchalik to‘g‘ri tanlanganiga bog‘liq. Jahon amaliyotida sinovdan o‘tgan va ilmiy asoslangan bir nechta metodologik yondashuvlar mavjud bo‘lib, ularni milliy tizimga implementatsiya qilish bugungi kun davr talabiga aylanmoqda.

Yuqorida ta’kidlanganidek, B. Dyupon tomonidan asoslangan metodologiya kiberxavfsizlikni ta’minlashda davlat monopoliyasidan voz kechishni talab qiladi [13]. Bu metodologiya yangi O‘zbekiston uchun quyidagi jihatlari bilan muhimdir:

❖ *Reallikka moslashish.* O‘zbekistonda Internet provayderlar, mobil operatorlar (Ucell, Beeline, Uzmobile va boshqalar) va to‘lov tizimlari (Click, Payme va boshqalar) xususiy yoki aksionerlik jamiyatlari shaklida faoliyat yuritadi. Kiberjinoyatlarning katta qismi (fishing, kartadan

o‘g‘rilik) aynan ularning infratuzilmasida sodir etiladi. IIV Kiberxavfsizlik markazi ushbu subyektlar bilan to‘g‘ridan-to‘g‘ri, byurokratiyasiz hamkorlik qilmasdan turib, jinoyatlarning oldini ololmaydi.

❖ *Javobgarlikni taqsimlash*. Polisentrik modelda kiberxavfsizlik uchun javobgarlik faqat davlat zimmasida emas, balki xizmat ko‘rsatuvchi provayderlar zimmasiga ham yuklatiladi.

Bugungi kunda Jahon Iqtisodiy Forumi (WEF) tomonidan ishlab chiqilgan “Internet provayderlari uchun kiberjinoyatlar profilaktikasi prinsiplari” (Cybercrime Prevention Principles for ISPs) ushbu metodologiyaning amaliy ko‘rinishidir. Ushbu hujjat quyidagi to‘rtta asosiy tamoyilni o‘zida qamrab oladi [16]:

1) sukut bo‘yicha himoyalanish (Protect consumers by default). Provayderlar foydalanuvchilardan xavfsizlikni sozlashni kutib o‘tirmasdan, tarmoq darajasida ma’lum bo‘lgan tahdidlarni (botnetlar, fishing saytlar) bloklashi shart;

2) xabardorlikni oshirish (Raise awareness). Provayderlar o‘z mijozlarini mavjud tahdidlardan oldindan ogohlantirib borishi kerak;

3) ishlab chiqaruvchilar bilan hamkorlik. Uskunalar (routerlar, modemlar) xavfsizligini ta’minlash;

4) marshrutlash xavfsizligi (Secure routing). Internet trafikning xavfsizligini ta’minlash.

Mazkur tamoyillarni bugungi kunda yangi O‘zbekistonda milliy qonunchiligiga singdirish va provayderlar uchun majburiy litsenziya talabiga aylantirish profilaktika samaradorligi keskin oshirishga xizmat qiladi.

Shu o‘rinda, Ben Kolyer va Elis Xatchings o‘zlarining “Ijtimoiy ekologiya” metodologiyasida kiberjinoyatchilikni texnik muammo sifatida emas, balki ijtimoiy jarayon sifatida ko‘radilar. Bu metodologiya bugungi kunda yangi O‘zbekistondagi yoshlar siyosati bilan bog‘liq muammolarning oldini olishga to‘g‘ridan-to‘g‘ri xizmat qiladi [17]. Xususan, dolzarb muammo sifatida yangi O‘zbekistonda IT sohasiga qiziquvchi yoshlar ko‘p, lekin ularning hammasi ham etik (oq qalpoqli) xaker bo‘lish yo‘lini tanlashmayapti. Aksincha, *“Telegram”* messenjeridagi yopiq guruhlarda “kading” (karta ma’lumotlarini o‘g‘irlash) yoki Distributed Denial of Service (ishlashini izdan chiqarishni) hujumlarini o‘rgatuvchi elektron qo‘llanmalar tarqalishi yoshlarni jinoyat olamiga tortmoqda. Shu kabi salbiy holatlar profilaktikasini kuchaytirish maqsadida kiberjinoyatchilikka moyil yoki “kam darajali” kiberhuquqbuzarlikka aralashgan o‘smir-yoshlarga nisbatan jazoga tayangan reaktiv yondashuv o‘rniga diversiya (yo‘naltirish) dasturlarini joriy etish ilmiy-amaliy jihatdan maqbul hisoblanadi. Bunda asosiy g‘oya – yoshning raqamli ko‘nikmalarini kriminal trayektoriyadan chiqarib, huquqiy maydonga qayta yo‘naltirish, ya’ni majburiy huquqiy-axloqiy (kiberetika) savodxonlik, kiberxavfsizlik kompetensiyalarini oshirish, mentorlik va ta’lim-kasbga yo‘naltirishi orqali legitim mehnat bozoriga integratsiya qilishdan iborat. Mazkur yondashuvning institutsional namunasi sifatida Buyuk Britaniyada “National Crime Agency” (NCA) tomonidan muvofiqlashtiriladigan *Cyber Choices* kabi profilaktik dasturlar ko‘rsatiladi. Mazkur hujjat qonunbuzarlikka olib boruvchi omillarni barvaqt aniqlash hamda ularni ta’lim va qonuniy kasbiy imkoniyatlarga yo‘naltirishga qaratilgandir.

Bugungi kunda ushbu ijobiy amaliyotni yangi O‘zbekiston sharoitida “One Million Uzbek Coders” tashabbusi va IT Park ekotizimi imkoniyatlari bilan uyg‘unlashtirish maqsadga muvofiqdir. Xususan, xavf guruhidagi yoshlarni erta bosqichda aniqlash, ularni maqsadli qayta tayyorlash dasturlari, stajirovkalar va legal startap yo‘laklarini ishga tushirish zarur. Bunda diversiya mexanizmlari faqat “ishga joylashtirish” emas, balki qonuniylik, mas’uliyat va raqamli madaniyatni shakllantiruvchi kompleks reabilitatsion model sifatida normativ-tashkiliy jihatdan mustahkamlansa, mamlakatda kiberjinoyatchilikning yoshlar orasida takrorlanish xavfi pasayishiga xizmat qiladi.

Shuningdek, Heemeng Ho tadqiqotlari asosida yaratilgan SCP metodologiyasiga asoslangan nazariya bugungi kunda eng pragmatik va texnik yondashuvdir[18]. U beshta asosiy strategiyaga tayanadi:

– *harakatni qiyinlashtirish (Increase the Effort)* – tizimlarga kirishni murakkablashtirish (2FA, biometriya;

– *xavfni oshirish (Increase the Risks)* – jinoyatchining aniqlanish ehtimolini oshirish (kuzatuv, jurnallarni yuritish);

– *foydani kamaytirish (Reduce the Rewards)* – o‘g‘irlangan ma’lumotni ishlatib bo‘lmaydigan qilish (shifrlash, kartalarni tezkor bloklash);

– *provokatsiyalarni kamaytirish (Reduce Provocations)* – foydalanuvchilarni xato qilishga undamaslik.

– *bahonalarni yo‘qotish (Remove Excuses)* – qoidalarni aniq va tushunarli qilish (hech kim “bilmovdim” deya olmasligi uchun).

O‘zbekistonda bank sektorida ushbu metodologiya qisman qo‘llanilmoqda (SMS xabarnomalar, Face-ID), lekin davlat tashkilotlari va kichik biznes faoliyatida bu ko‘rsatkich juda kam.

Shu o‘rinda, so‘nggi yillarda mamlakatda amalga oshirilayotgan islohotlar tufayli Prezident Sh. Mirziyoyevning tashabbusi bilan 2022-yil 15-aprelda “Kiberxavfsizlik to‘g‘risida”gi qonun qabul qilindi [19]. Mazkur Qonunda “kibermakon”, “kiberjinoyatchilik”, “kiberhimoya” kabi tushunchalar ilk bor qonun darajasida mustahkamlandi. Shuningdek, Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi etib belgilandi. Bundan tashqari, davlat organlari va tashkilotlariga o‘z tizimlarining xavfsizligini ta’minlash majburiyatlari yuklatildi.

Bundan tashqari, mazkur islohotning mantiqiy davomi sifatida 2023 yil 31-mayda Prezident Sh. Mirziyoyev tashabbusi bilan mamlakatda “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi qarori qabul qilindi [20]. Mazkur Qaror bilan “Muhim axborot infratuzilmasi” tushunchasi va uni himoya qilish mexanizmlari joriy etildi. Bu qaror profilaktika nuqtai nazaridan inqilobiy ahamiyatga ega, chunki birinchi marta davlat nazorati nafaqat davlat organlariga, balki strategik ahamiyatga ega bo‘lgan xususiy sektor (banklar, aloqa operatorlari, energetika) obyektlariga ham tatbiq etildi. Qaror doirasida:

- muhim axborot infratuzilmasi obyektlarining yagona reyestri shakllantirildi;
- ularni toifalash (o‘ta muhim, muhim, o‘rta) tartibi belgilandi;
- “kiberxavfsizlik markazi” tomonidan muntazam audit o‘tkazish tizimi yo‘lga qo‘yildi.

Biroq, tahlillar mavjud qonunchilikda quyidagi huquqiy bo‘shliqlar mavjudligini ko‘rsatmoqda:

birinchidan, bugungi kunda “Kiberxavfsizlik to‘g‘risida”gi qonunda “profilaktika” so‘zi deyarli ishlatilmaydi. Qonun ko‘proq texnik himoya va insidentlarga reaksiya qilishga (response) qaratilgan. Kriminologik profilaktika (sabablarni o‘rganish) chetda qolgan;

ikkinchidan, Jinoyat kodeksining 168-moddasi (Firibgarlik) va 169-moddasi (O‘g‘rilik) kiberjinoyatlarning o‘ziga xos xususiyatlarini (masalan, kriptovalyuta o‘g‘riligi, o‘yin akkauntlarini buzib kirish) to‘liq qamrab olmaydi. Bu amaliyotda jinoyatlarni noto‘g‘ri malakalashga sabab bo‘lmoqda;

uchinchidan, muhim axborot infratuzilmasi obyektlaridan tashqari bo‘lgan xususiy kompaniyalar (internet do‘konlar, yetkazib berish xizmatlari) uchun mijozlar ma’lumotlarini himoya qilish bo‘yicha aniq profilaktik majburiyatlar Yevropa Ittifoqida amal qiladigan GDPR (General Data Protection Regulation)da belgilanmagan [21].

Mazkur huquqiy bo‘shliqlarni bartaraf etish maqsadida bugungi kunda Yevropa Ittifoqining yangi NIS2 direktivasi (Network and Information Security Directive) kiberxavfsizlik sohasidagi eng ilg‘or hujjat hisoblanadi [22]. Mazkur xalqaro hujjatning milliy qonunchilikdan farqi shundaki, NIS2 da “Risk-based approach” (Riskka asoslangan yondashuv) markaziy o‘rinda turadi. O‘zbekistonda xavfsizlik talablari ko‘pincha “qolip” (checklist) asosida belgilanadi. NIS2 da esa tashkilotlar avval o‘zlariga xos risklarni baholashi va shunga mos choralarni ishlab chiqishi shart. Bu resurslarni tejash va samaradorlikni oshirishga xizmat qiladi. Shuningdek, NIS2 da rahbarlarning shaxsiy javobgarligi (hatto lavozimdan chetlatishgacha) belgilangan. Bizda esa javobgarlik ko‘pincha IT-mutaxassis darajasida qolib ketmoqda.

Bundan tashqari, O‘zbekiston hali Yevropa Kengashining “Kiberjinoyatchilik to‘g‘risida”gi konvensiyasiga qo‘shilmagan. Shu o‘rinda, rossiyalik olim K.N. Yevdokimovning tanqidiy qarashlariga qaramay, ushbu Konvensiya transchegaraviy dalillarni olish va ekstraditsiya masalalarida eng samarali xalqaro vosita hisoblanadi [23]. O‘zbekistonning ushbu Konvensiyaga qo‘shilishi yoki uning normalarini milliy qonunchilikka to‘liq implementatsiya qilishi profilaktika imkoniyatlarini kengaytirgan bo‘lar edi.

Yuqorida bayon etilgan tahlil natijalariga tayanilgan holda, kiberjinoyatlar profilaktikasini takomillashtirishga qaratilgan bir qator kompleks takliflarni ilgari surishni maqsadga muvofiq deb bildik. Takliflar konseptual jihatdan *“jazodan keyin emas, jinoyatdan oldin”* (prevention-first) tamoyiliga asoslanib, huquqbuzarlik yuzaga kelishidan oldin uning sabab va shart-sharoitlarini bartaraf etishga qaratilgan tizimli yondashuvni nazarda tutadi.

Jumladan, Jinoyat kodeksining “Atamalarning huquqiy ma’nosi” bo‘limiga kiberjinoyatchilik sohasida qo‘llaniladigan qator yangi tushuncha va ta’riflarni kiritish taklif etiladi. Mazkur normalarni qonun darajasida aniq belgilash amaliyotchi xodimlar uchun kiberhuquqbuzarliklarni huquqiy jihatdan to‘g‘ri kvalifikatsiya qilish, ularning o‘zaro farqlarini aniq ajratish hamda profilaktika chora-tadbirlarini maqsadli va manzilli tashkil etishda muhim metodologik asos bo‘lib xizmat qiladi.

Kibero‘g‘rilik (Cyber-theft) *– axborot tizimlari, telekommunikatsiya tarmoqlari yoki raqamli to‘lov vositalaridan foydalanish orqali, jabrlanuvchining ishtirokisiz yoki uning roziligisiz, texnik vositalar (zararli dasturlar, maxsus kodlar) yordamida o‘zganing mulkini yoki mulkiy huquqlarini (shu jumladan raqamli aktivlarni) yashirin ravishda talon-toroj qilish.*

Kiberfiribgarlik (Cyber-fraud): *– kibermakonda ijtimoiy muhandislik usullari, soxta veb-resurslar (fishing), elektron to‘lov tizimlaridagi zaifliklardan foydalangan holda, o‘zgani aldash yoki ishonchini suiiste’mol qilish yo‘li bilan mulkni yoki mulkiy huquqni qo‘lga kiritish.*

Shuningdek, Jinoyat kodeksining I bobiga (Vazifalar va prinsiplar) quyidagi yangi prinsipni kiritish maqsadga muvofiq:

“10[1]-modda. Kiberxavfsizlikni ta’minlash va raqamli huquqlarni himoya qilish prinsipi

Jinoyat qonunchiligi va huquqni qo‘llash amaliyoti davlat, jamiyat va shaxsning kibermakondagi xavfsizligini ta’minlashga, kiberjinoyatlarning sabab va sharoitlarini proaktiv aniqlashga, risklarni boshqarishga hamda jabrlanuvchilarning raqamli huquqlarini tiklashga ustuvorlik beradi.”

Ushbu prinsip davlat organlarining e’tiborini jazolashdan ko‘ra himoya qilish va oldini olishga buradi.

Xulosa o‘rnida shuni ta’kidlash joizki, kiberjinoyatlar profilaktikasi – bu murakkab, ko‘p qirrali va doimiy yangilanib turuvchi jarayon. Amalga oshirilgan tahlillar shuni ko‘rsatdiki, yangi O‘zbekistonda kiberxavfsizlik sohasida mustahkam siyosiy va huquqiy poydevor yaratilgan. Biroq, tez o‘zgaruvchan tahdidlar mavjud mexanizmlarni yanada takomillashtirishni, xususan, profilaktikaning nazariy va metodologik asoslarini qonunchilikda aniq belgilashni talab qilmoqda.

Taklif etilayotgan polisentrik boshqaruv modeli, ijtimoiy ekologiya yondashuvi va situativ profilaktika (SCP) metodlarining milliy qonunchilikka integratsiya qilinishi, O‘zbekistonning global kibermakondagi pozitsiyasini mustahkamlashga, eng muhimi, fuqarolarning raqamli dunyodagi ishonchi va xavfsizligini ta’minlashga xizmat qiladi. Prezident Shavkat Mirziyoyev ta’kidlaganidek: “Raqamli iqtisodiyotsiz mamlakat iqtisodiyotining kelajagi yo‘q”, xavfsiz raqamli iqtisodiyot esa samarali profilaktika tizimisiz mavjud bo‘la olmaydi.

Foydalanilgan manbalar / References

1. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son farmoni // https://lex.uz/docs/-5030957
2. JSST va O'zbekiston Respublikasining 2025–2030 yillarga mo'ljallangan o'zaro hamkorlik strategiyasi – IRIS // https://iris.who.int/bitstreams/c6c42bfa-d5f4-420f-a434-d3a3c4514881/download
3. O'zbekistonda raqamli ekotizimni shakllantirish: davlat xizmatlaridan biznesgacha (IT platformalar tahlili) Qurvonaliyev Lazizbe, accessed January 24, 2026, https://interspp.com/index.php/vsi/article/download/2846/2063/4048
4. “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-167-son qaror// https://lex.uz/docs/-6479190
5. “Muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta'minlash” / Kiberxavfsizlik markazi // https://csec.uz/uz/news/-seminarlar/muhim-axborot-infratuzilmasi-obyektlari-kiberxavfsizli-gini-ta-minlash-mavzusida-seminar-tadbiri-bo-l/
6. Problematic aspects of international cooperation of the Russian Federation on the fight against cybercrime: Текст научной статьи по специальности «Право – КиберЛенинка» // https://cyberlenin-ka.ru/article/n/problematic-aspects-of-international-cooperation-of-the-russian-federation-on-the-fight-against-cybercrime
7. Расулев А.К. Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларга қарши курашишнинг жиноят-ҳуқуқий ва криминологик чораларини такомиллаштириш: Юрид. фан. д-ри (DSc) ... дис. автореф. – Тошкент, 2018. – 22–23-б.
8. Расулев А.К., Саъдуллаев Г.А. Кибер жиноятчилик ва ахборот хавфсизлиги: кадрлар тайёрлаш ва қайта тайёрлаш масалалари //Ўзбекистон Республикаси Судьялар олий мактаби илмий журнали. – 2021. –№ 1(48). –Б.61
9. Рахманов Д. Профилактика киберпреступности. Изучение национального и международного опыта // Bulletin of Science and Practice. – 2024. – Т. 10. – № 1. – С. 449–456.
10. Умурзаков Ж. Профилактика киберпреступности: нынешнее состояние и перспективы развития // Russian Journal of Education and Psychology. – 2024. – Т. 15. – № 1. – С. 1–10.
11. Евдокимов К. Н «Противодействие компьютерной преступности: теория, законодательство, практика». – Москва, 2021. – С. 27–28. // https://cyberleninka.ru
12. Степанов-Егиянц В.Г., Простосердов М.А. Prevention of cybercrime in the Russian federation: An integrative and comprehensive approaches // Криминологический журнал Байкальского государственного университета экономики и права 9(2):265-276 DOI:10.17150/1996-7756.2015.9(2).265-276
13. Benoit Dupont “The Polycentric Governance of Cybercrime: The Fragmented Networks of International Cooperation” // https://shs.cairn.info
14. Ben Collier, Alice Hutchings “Cybercrime: A social ecology” / Chapter in Book/Report/ Conference proceeding › Chapter (peer-reviewed) › peer-review // https://www.research.ed.ac.uk/
15. Heemeng Ho, Ryan Ko, Lorraine Mazerolle, John Gilmour Cheng Miao “Using Situational Crime Prevention (SCP)-C 3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes” // https://watermark02.silverchair.com
16. World Economic Forum 2020: Cybercrime Prevention Principles For ISPs // https://www. issan.org.ng/
17. Ben Collier, Alice Hutchings “Cybercrime: A social ecology” // School of Social and Political Science / https://www.research.ed.ac.uk
18. Heemeng Ho, Ryan Ko, Lorraine Mazerolle, John Gilmour Cheng Miao “Using Situational Crime Prevention (SCP)-C 3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes” // https://watermark02.silverchair.com
19. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni // O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi // https://lex.uz/docs/5960604
20. “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-167-son qaror // O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi / https://lex.uz /docs/6479190
21. “Muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta'minlash” // https://csec.uz /uz/news
22. The NIS 2 Directive, Final Text // Article 21, Cybersecurity risk-management measures / https://www.nis-2-directive.com/NIS_2_Directive_-Article_21.html
23. Makushev D.I. Problematic aspects of international cooperation of the Russian Federation on the fight against cybercrime // https://cyberleninka.ru