KIBERO‘G‘RILIK: ZAMONAVIY XAVF, HUQUQIY TAHDID VA OLDINI OLISH CHORA-TADBIRLARI

Kaxarova Munira Maxamadjanovna
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti ilmiy xodimi, siyosiy fanlar doktori

Annotatsiya. *Maqolada raqamli texnologiyalar orqali amalga oshiriladigan o‘g‘rilik – kibero‘g‘rilik tushunchasi, uning shakllari, tarqalishi, inson hayotiga ta’siri, huquqiy jihatlari va oldini olish mexanizmlari tahlil qilingan. Zamonaviy jamiyatda ma’lumotlar, moliyaviy resurslar va shaxsiy axborotlarni himoyalash yangi kiberxavfsizlik yondashuvlarini talab etmoqda. Shu nuqtai nazardan maqolada milliy va xalqaro tajriba misolida tahlillar berilgan.*

Kalit so‘zlar: *kibero‘g‘rilik, shaxsiy ma’lumot, raqamli xavf, kiberxavfsizlik, bank fishingi, huquqiy choralar, raqamli texnologiya, axborot, kiberhujum.*

КИБЕР КРАЖА: СОВРЕМЕННАЯ ОПАСНОСТЬ, ПРАВОВАЯ УГРОЗА И МЕРЫ ПРЕДУПРЕЖДЕНИЯ

Аннотация. *В статье анализируются понятие кибер кражи – хищений, совершаемых с использованием цифровых технологий, его формы, распространение, влияние на жизнь человека, правовые аспекты и механизмы предотвращения. Современное общество требует новых подходов к кибербезопасности для защиты данных, финансовых ресурсов и личной информации. С этой точки зрения в статье представлены аналитические обзоры на основе национального и международного опыта.*

Ключевые слова: *кибер кража, персональные данные, цифровая угроза, кибербезопасность, банковский фишинг, правовые меры, цифровые технологии, информация, кибератака.*

CYBER THEFT: MODERN DANGERS, LEGAL THREAT AND PREVENTIVE MEASURES

Abstract. *The article analyzes the concept of cyber theft – theft committed through digital technologies, its forms, prevalence, impact on human life, legal aspects, and prevention mechanisms. Modern society requires new approaches to cybersecurity to protect data, financial resources, and personal information. From this perspective, the article provides analytical insights based on national and international experiences.*

Keywords: *cyber theft, personal data, digital threat, cybersecurity, bank phishing, legal measures, digital technology, information, cyberattack.*

Hozirgi globallashuv va raqamli texnologiyalar shiddat bilan rivojlanayotgan zamonaviy jamiyatda axborot va ma’lumot asosiy boylik sifatida qaralmoqda. Raqamlashtirish jarayoni insoniyat faoliyatining barcha sohalariga kirib kelib, ma’lumotlarning qimmatli aktivga aylanishi bilan birga, ularning o‘g‘irlanish holatlari ham ortib bormoqda. Bu esa, o‘z navbatida, yangi turdagi jinoyatlarning, jumladan kibero‘g‘rilikning vujudga kelishiga zamin yaratmoqda. Kibero‘g‘rilik bugungi kunda jahon hamjamiyati uchun jiddiy xavf tug‘dirayotgan murakkab ijtimoiy-huquqiy muammolardan biriga aylangan.

Kibero‘g‘rilik – bu axborot-kommunikatsiya texnologiyalari vositasida boshqa shaxsning mul-

ki, shaxsiy ma’lumoti yoki mablag‘ini noqonuniy tarzda egallash. Bu turdagi jinoyatlar faqat moddiy zarar bilan chegaralanmasdan, ruhiy, huquqiy, ijtimoiy oqibatlarga ham olib keladi.

Ma’lumki, raqamli makondagi jinoyatlar an’anaviy o‘g‘rilik turlaridan keskin farq qiladi. Agar an’anaviy o‘g‘rilik jismoniy mol-mulkka nisbatan amalga oshirilsa, kibero‘g‘rilik ko‘proq elektron ma’lumotlar, bank plastik kartalari, shaxsiy ma’lumotlar, internet to‘lov tizimlari orqali amalga oshiriladi. Ayniqsa, davlat va xususiy sektorlarda axborot tizimlari keng qo‘llanilayotgan bir paytda, ushbu tizimlarni himoya qilish masalasi jahon miqyosida muhim vazifaga aylanmoqda.

Kiberjinoyatchilikning ushbu turi nafaqat iqtisodiy zarar yetkazadi, balki fuqarolarning shaxsiy hayoti daxlsizligiga, davlat institutlariga bo‘lgan ishonch va jamiyatdagi huquqiy madaniyatga ham salbiy ta’sir ko‘rsatadi. Bugungi raqamlashtirilgan jamiyatda ma’lumotlar va moliyaviy aktivlar internet tarmoqlari orqali boshqarilmoqda. Bunday sharoitda ma’lumotlarning xavfsizligini ta’minlash nafaqat texnik masala, balki huquqiy, ijtimoiy va axloqiy mas’uliyat ham hisoblanadi. Shuningdek, bu jinoyat turi davlat organlari, biznes subyektlari va fuqarolar uchun ham katta muammoga aylanmoqda. Demak, kibero‘g‘rilik muammosiga tizimli yondashuv talab etiladi.

Kibero‘g‘rilikka oid ilmiy tadqiqotlar so‘nggi yigirma yil ichida alohida ilmiy yo‘nalish sifatida shakllandi. Bu jinoyat turi raqamli muhitning rivojlanishi, internet platformalarining kengayishi va fuqarolarning raqamli faolligi ortishi bilan bog‘liq holda dolzarb ahamiyat kasb etmoqda.

Dunyo miqyosida kiberjinoyatchilik, xususan, kibero‘g‘rilik bo‘yicha yetakchi tadqiqotchi olimlar o‘z ishlarida kibero‘g‘rilikni nafaqat huquqiy, balki ijtimoiy va psixologik nuqtai nazardan ham tahlil qiladilar. Masalan, Lids universitetining kriminolog-professori David S. Wall o‘zining asarida kibero‘g‘rilikni raqamli muomala muhitidagi yangi jinoiy xatar sifatida tavsiflaydi va uning transmilliy xususiyatiga alohida e’tibor qaratadi. Olim kibero‘g‘rilik nafaqat texnologik jinoyat, balki ijtimoiy muammo bo‘lib, u insonlarning shaxsiy va moliyaviy xavfsizligiga jiddiy tahdid solishini yozadi.

Hindistonlik professor Karuppannan Jaishankar fikriga ko‘ra, kibero‘g‘rilik, ayniqsa, shaxsiy ma’lumotlarni o‘g‘irlash va moliyaviy kiberjinoyatlar, odamlarning onlayn muhitdagi erkinligi bilan bog‘liq. Uning “Space Transition Theory” nazariyasiga ko‘ra, insonlar onlaynda real hayotdagidan farqli ravishda harakat qilishga moyil bo‘ladilar, bu esa o‘g‘rilikni osonlashtiradi.

Michigan State University (AQSH) professori Dr. Thomas Holt esa kibero‘g‘rilikka aynan iqtisodiy manfaat qozonishga qaratilgan raqamli faoliyat deb qarash kerakligini va bu turdagi jinoyatlarda ko‘p hollarda jinoyatchilar rasmiy himoyasiz platformalardan foydalanishi mumkinligini yozadi.

Yaponiyaning Waseda universiteti professori Dr. Pauline Reich kibero‘g‘rilik transmilliy muammoga aylangani, texnologik globallashuv jinoyatchilarga turli yurisdiksiyalarda harakat qilish imkonini berayotgani, bu esa, huquqni muhofaza qiluvchi organlar ishini murakkablashtirganini ta’kidlaydi.

Kibero‘g‘rilik murakkab va ko‘p qirrali masala bo‘lib, olimlar uning texnologik, ijtimoiy psixologik, huquqiy va axloqiy jihatlarini keng yoritmoqda. Ularning umumiy xulosasi – kibero‘g‘rilikka qarshi kurashda faqatgina texnik vositalar emas, balki inson omili, targ‘ibot va xalqaro hamkorlik muhim ahamiyatga ega. Kibero‘g‘rilikning o‘sishiga global raqamli transformatsiya sabab bo‘lmoqda. Har bir yangi texnologiya jinoyatlar uchun yangi imkoniyatlar yaratadi.

Ilmiy adabiyotlarda kibero‘g‘rilikning shaxsiy ma’lumotlarni, bank rekvizitlarini o‘g‘irlash, korporativ ma’lumotlar bazasini buzish va dasturiy ta’minotdan noqonuniy foydalanish kabi ko‘p turlari ta’riflanadi. Tergov jarayonlarida raqamli izlarni saqlash va tahlil qilish muhim ahamiyatga ega. Buning uchun maxsus kompyuter forenzikasi *(Computer Forensics – bu raqamli dalillarni – fayllar, elektron xatlar, loglar, tarixlar, internet faoliyati, USB ma’lumotlari va boshqalar. Ilmiy va huquqiy tartibda tiklash va tahlil qilish usullarining*

majmuasi) usullari rivojlanmoqda. Kibero‘g‘rilikka qarshi kurashda xalqaro qonunchilik va hamkorlikning hali yetarli darajada yaratilmaganligini katta muammo sifatida keltirishimiz mumkin.

O‘zbekistonda ham oxirgi yillarda kiberjinoyatchilik bo‘yicha ilmiy tadqiqotlar ko‘paymoqda. Xususan, N.Salayev va R.Ro‘ziyev axborot xavfsizligiga tahdid soluvchi, bevosita kompyuter vositalari orqali yoki axborot texnologiyalari vositasida sodir etiladigan qonunga xilof ijtimoiy xavfli qilmishni axborot texnologiyalari sohasidagi jinoyatlar ekanini tushuntiradilar. Ammo olimlar tomonidan hali kibero‘g‘rilik jinoyati yetarlicha o‘rganilmagan.

Ayrim tadqiqotlar bu boradagi statistik ma’lumotlarni tahlil qilib, kibero‘g‘rilikning o‘sish dinamikasi, uning sabablari va profilaktik choralarini ham ko‘rsatib bergan. Shu bilan birga, O‘zbekistonda kiberjinoyatlar bo‘yicha maxsus mutaxassis kadrlar yetishmasligi va texnik imkoniyatlarning cheklanganligi ham muammo sifatida tilga olinadi.

Kibero‘g‘rilik jinoyati zamonaviy texnologiyalarning zaif tomonlaridan foydalanish orqali amalga oshiriladigan xavfli jinoyat turi hisoblanadi. Uning metodologiyasi yuqori darajadagi texnik tayyorgarlik, axborot muhitini teran anglash va inson psixologiyasini bilishni talab qiladi. Shu sababli, jamiyatda raqamli savod-xonlikni oshirish, kiberxavfsizlik sohasidagi huquqiy bazani mustahkamlash va profilaktik tadbirlarni takomillashtirish jinoyatning oldini olishda hal qiluvchi omillardandir. Xususan, bank kartalarining nusxasini yasash, elektron to‘lovlar hamyonini soxtalashtirish kabi yangi usullar paydo bo‘lmoqda. Shunday sharoitda raqamli dalillar sudlov amaliyotida muhim rol o‘ynaydi.

O‘zbekistonda bu sohani tartibga solish maqsadida 2024-yil 21-noyabrda “O‘zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi qonun qabul qilindi.

O‘zbekiston Respublikasining Jinoyat kodeksi, Ma’muriy javobgarlik to‘g‘risidagi kodeksi, elektron hujjat aylanmasi va elektron imzolar to‘g‘risidagi qonunlar, shuningdek, kiberxavfsizlik sohasidagi maxsus normativ-huquqiy hujjatlar tahlil qilindi. Ushbu tahlil milliy qonunchilikning kibero‘g‘rilikka nisbatan qonunchilik jihatidan qanday choralar ko‘rishi va kamchiliklarini aniqlash imkonini beradi. So‘nggi yillarda qonun ijodkorligi va huquqni muhofaza qilish organlarining tajribasi, shu jumladan sud qarorlari va jinoyat ishlari tahlil qilindi. Bu amaliy tahlil kibero‘g‘rilikka qarshi kurashishga oid qonunlarning amaliy samaradorligi va ulardagi muammolarni aniqlashga yordam berdi.

Kibero‘g‘rilik turlari juda xilma-xil bo‘lib, ularni amalga oshirish usuli, maqsadi va yo‘nalishiga qarab, turli shakllarda tasniflash mumkin. Quyida eng keng tarqalgan turlari keltiramiz:

Fishing (Phishing) – foydalanuvchining shaxsiy ma’lumotlarini (parollar, bank ma’lumotlari va h.k.) soxta veb-saytlar yoki elektron pochta xabarlari orqali qo‘lga kiritish usuli. Bunday hollarda qurbon o‘z ma’lumotini o‘z xohishi bilan kiritadi, biroq manzil qalbaki bo‘ladi.

Farming (Pharming) – kompyuter yoki ma’lumotlarni turli tarmoqlar orasida uzatishni boshqaruvchi qurilma (router)ni zaharlab, foydalanuvchini haqiqiy veb-sayt o‘rniga qalbaki sahifaga yo‘naltiradi. Bu orqali ham shaxsiy ma’lumotlar qo‘lga kiritiladi.

Malvar (Malware) orqali o‘g‘rilik – kompyuterga yoki mobil qurilmaga zararli dastur joylashtirish orqali ma’lumotlarni noqonuniy tarzda o‘g‘rilash. Bu turga keyloggerlar (keyboard sniffer), troyan viruslari va shantajchi dasturlar kiradi.

Ijtimoiy muhandislik (Social Engineering) foydalanuvchini psixologik aldash yo‘li bilan uning ishonchli ma’lumotlarini qo‘lga kiritish usuli. Masalan, operator yoki bank xodimi sifatida chaqiruv qilib ma’lumot so‘raydi.

Onlayn tijorat sohasidagi o‘g‘riliklar Internetdagi savdo platformalarida qalbaki to‘lovlar, mavjud bo‘lmagan mahsulotlarni sotish, to‘lovdan keyin mahsulot yetkazib berilmasligi va hokazolar ko‘rinishida namoyon bo‘ladi.

Shaxsiy akkauntlarni o‘g‘rilash – elektron pochta, ijtimoiy tarmoqlar, moliyaviy platforma-

lardagi foydalanuvchi hisoblarini buzib, ular orqali moddiy va axborot manfaatlarini qo‘lga kiritish.

Kibero‘g‘rilikning xavfli jihati shundaki, u nafaqat moliyaviy ziyon keltiradi, balki ishonch, maxfiylik va milliy xavfsizlik tizimlarini ham sinov ostiga qo‘yadi. Davlat tashkilotlari, xususiy korxonalar hamda jamoatchilik bu tahdidga qarshi mukammal raqamli profilaktika va *(sifrovoy)* xavfsizlik siyosatini amalga oshirishlari zarur.

1990-yillarda World Wide Web (WWW) paydo bo‘ldi va internet ommaviy foydalanishga ochildi. Bu kiberjinoyatlar uchun shaxsiy ma’lumotlarni o‘g‘irlash, firibgarlik va zararli dasturlarni tarqatish kabi yangi imkoniyatlar yaratdi.

1994-yilda Vladimir Levin ismli rossiyalik xaker Citibank tizimidan 10 million dollar o‘g‘riladi. Bu bank tizimlariga qarshi birinchi yirik kiberhujumlardan biri edi. 2000-yilda esa “I Love You” virusi tarqaldi, millionlab kompyuterni zararlab, global iqtisodiyotga milliardlab dollar zarar keltirdi.

2000-yillardan boshlab kiberjinoyatlar yanada tizimli va murakkab tus oldi. Shaxsiy ma’lumotlarni o‘g‘rilash (phishing), ransomware (ma’lumotlarni shifrlab, pul talab qilish), DDoS hujumlari va davlatlararo kiber xavf-xatarlar keng tarqaldi.

2017-yilda WannaCry ransomware hujumi 150 dan ortiq mamlakatda 200.000 dan ziyod kompyuterni zararlab, global xavfsizlikka jiddiy tahdid soldi.

Hozirgi kunda kibero‘g‘rilik jinoyatlari sun’iy intellekt, blokcheyn va boshqa zamonaviy texnologiyalardan foydalangan holda yanada rivojlanmoqda. Masalan, deyepfake *(Deepfake – bu sun’iy intellekt (AI) yordamida haqiqatga juda o‘xshash soxta tasvirlar, videolar va audio yozuvlarni yaratish)* texnologiyasi yordamida firibgarlik yoki kriptovalyuta o‘g‘rilash kabi jinoyatlar ko‘paymoqda.

O‘zbekistonda internet 1990-yillarning oxirida keng tarqala boshladi. 2000-yillarda axborot texnologiyalarining rivojlanishi bilan birga, kiberjinoyatlar ham paydo bo‘ldi. 2010-yildan boshlab bank kartalari ma’lumotlarini o‘g‘irlash, onlayn firibgarlik va ijtimoiy tarmoqlardagi huquqbuzarliklar holatlari qayd etildi.

O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori bilan kibero‘g‘rilikka barham berish va uning barvaqt oldini olish tizimi doimiy ravishda takomillashtirilib, kiberxavfsizlikni ta’minlash choralari ko‘rilmoqda.

Steve Morgan muallifligidagi va Cybersecurity Ventures tashkiloti tomonidan 2021-yilda e’lon qilingan “C-Suitedagi kiberurush” (The Cyberwarfare in the C-Suite) nomli maxsus hisobotda kiberjinoyatlar orasida kibero‘g‘rilikning keng qamrovli va barqaror o‘sishi qayd etilgan. Unga ko‘ra:

- kibero‘g‘rilik orqali yetkazilayotgan global iqtisodiy zarar 2021-yilda 6 trln. dollarga yetgan bo‘lsa, bu ko‘rsatkich 2025-yilga borib 10,5 trln. dollarni tashkil etishi kutilmoqda. Bu – yillik 15% o‘sish demakdir;
- Har 11 soniyada dunyoda bitta kiberhujum amalga oshiriladi. Ulardan ko‘pchiligi moliyaviy ma’lumotlarni noqonuniy egallash yoki shaxsiy ma’lumotlarni o‘g‘rilashga qaratilgan bo‘ladi;
- AQSHda fuqarolarning deyarli barcha shaxsiy ma’lumotlari tor doiradagi “qorong‘i internet”da (dark web) tarqalgan va sotilayotganligi qayd etilgan. Bu kibero‘g‘rilikning tijoratlashgan xususiyatini ko‘rsatadi.

Kibero‘g‘rilik inson ruhiyatida ishonchsizlik, xavotir, depressiya, ijtimoiy izolyatsiya holatlarini yuzaga keltiradi. Odamlar raqamli platformalardan foydalanishga ehtiyot bo‘lib qarashni boshlaydilar va raqamli islohotlarga nisbatan ishonch pasayadi. Moliyaviy tomondan esa shaxsiy va korporativ hisoblarida katta yo‘qotishlar bo‘ladi.

Statistik ma’lumotlarga ko‘ra, O‘zbekistonda 2018–2023-yillarda kibero‘g‘rilik bilan bog‘liq holatlar soni 8 baravar oshgan. Moliyaviy yo‘qotishlarning 70% internet-bank foydalanuvchilari hisobiga to‘g‘ri keladi. Eng ko‘p qurbon bo‘luvchilar – 25-40 yoshli Internet foydalanuvchilar va onlayn tadbirkorlar.

Kibero‘g‘rilik – bu raqamli texnologiyalar jadal rivojlanayotgan hozirgi zamonda jamiyat xavfsizligi va shaxsning huquqiy kafolatlariga tahdid solayotgan jiddiy jinoiy muammolardan biri. Bu jinoyat turi nafaqat moddiy ziyon keltiradi, balki shaxsiy ma’lumotlar, maxfiy axborotlar, moliyaviy tizimlar va davlat infratuzilmalariga ham daxl qilishi bilan o‘ta xavfli tusga ega.

Tahlillar shundan dalolat beradiki, kibero‘g‘rilik ko‘lami kengayib borayotganiga sabab bo‘luvchi asosiy omillar – bu axborot xavfsizligi madaniyatining pastligi, huquqiy bazaning to‘liq shakllanmagani, texnik nazorat vositalarining samarasizligi hamda huquqni muhofaza qiluvchi organlarning kiberjinoyatchilikka qarshi kurashishdagi malaka va imkoniyatlarining cheklanganligi. Uning oldini olish uchun quyidagi *amaliy va tizimli takliflarni* berish mumkin:

– kibero‘g‘rilikka oid alohida modda va ta’riflarni Jinoyat kodeksida aniq belgilash, jinoyatni sodir etish vositalari va oqibatlarini chuqur qamrab olgan normalarni joriy etish lozim;

– davlat miqyosida milliy kiberxavfsizlik strategiyasini qabul qilish va uni amaliyotga tatbiq etish orqali kibertahdidlarga qarshi tizimli yondashuv yaratilishi zarur;

– har bir hududiy ichki ishlar boshqarmalari qoshida malakali kadrlardan iborat maxsus kiberjinoyatlarga qarshi bo‘linmalarni tashkil etish maqsadga muvofiq;

– keng jamoatchilikka kibero‘g‘rilik xavflari, shaxsiy ma’lumotlarni muhofaza qilish, fishing va zararli dasturlardan himoyalanish usullari haqida muntazam ravishda ommaviy axborot vositalari orqali ma’lumot berib borish kerak;

– transmilliy kiberjinoyatlarga qarshi samarali kurash olib borish uchun xalqaro tashkilotlar, qo‘shni va rivojlangan davlatlar bilan ma’lumot almashish, qo‘shma tergovlar o‘tkazish va ilg‘or tajribalarni joriy etish zarur;

– moliyaviy tashkilotlar, davlat idoralari va xususiy sektorda axborot tizimlarini muhofaza qiluvchi zamonaviy kriptografik va biometrik texnologiyalarni joriy etish muhim hisoblanadi;

– ilmiy manbalar tahlili shuni ko‘rsatadiki, kibero‘g‘rilik jahon ilm-fanida keng o‘rganilmoqda, ammo O‘zbekistonda ushbu mavzu bo‘yicha tadqiqotlarni yanada chuqurlashtirish, qiyosiy tahlillar olib borish, amaliyot va nazariya uyg‘unligini ta’minlash talab etiladi. Ayniqsa, xalqaro tajriba va milliy huquqiy muhit o‘rtasidagi farqni aniqlab, samarali modellarni joriy etish muhim hisoblanadi;

– kibero‘g‘rilik – bu faqat kompyuterga bog‘liq muammo emas, balki inson huquqlari, shaxsiy daxlsizlik, moliyaviy xavfsizlik va jamiyat barqarorligiga taalluqli dolzarb muammo. Davlat, jamoatchilik va fuqarolar o‘rtasidagi hamkorlikkina ushbu tahdidni kamaytirishda asosiy omil bo‘la oladi. Zamonaviy jamiyat faqat axborot emas, balki xavfsizlik madaniyatini ham shakllantirishi lozim. Maktab va universitetlarda majburiy kiberxavfsizlik kurslarini joriy etish zarur;

– televideniye, radio, ijtimoiy tarmoqlar orqali “Onlaynda xavfsiz bo‘ling” kampaniyalarini yo‘lga qo‘yish ham o‘z samarasini beradi;

– ota-onalar uchun bolalarni internet xavflaridan himoya qilishga bag‘ishlangan broshyuralar va video darslarni bolalar kontentlariga joylab borish kerak;

– kibero‘g‘rilikka oid jinoyatlar dinamikasini aniqlash, tahlil qilish va profilaktika ishlarini samarali tashkil etish uchun maxsus elektron statistik platformani shakllantirish lozim. Bu orqali muammoning qaysi hududlarda, qaysi sohalarda ko‘proq uchrayotganini o‘rganish mumkin bo‘ladi;

– yuristlar, ayniqsa tergovchilar, prokurorlar va sudyalar zamonaviy raqamli jinoyatlarga qarshi huquqiy bilimlarga ega bo‘lishlari lozim. Shu bois, yuridik OTMlarda kiberhuquq, raqamli dalillar va kiberhimoyaga oid fanlar o‘qitilishi muhim;

– fintex va axborot tizimlarida shaxsiy ma’lumotlar, operatsiyalar va foydalanuvchi faoliyatini kuzatuvchi sun’iy intellekt (AI) yordamida jinoyatni sodir etishdan oldin aniqlash imkoniyatlari yaratilishi kerak. Bu himoyada “proaktiv yondashuv”ni ta’minlaydi;

– kiberhimoya bo‘yicha milliy dasturiy ta’minot va IT mahsulotlarini ishlab chiqish uchun

mahalliy startaplar, innovatsion markazlar va IT mutaxassislariga davlat grantlari ajratilishi maqsadga muvofiq;

– kibero‘g‘rilik ko‘pincha ijtimoiy tarmoqlar orqali amalga oshirilayotganini hisobga olib, mazkur platformalarda shaxsiy ma’lumotlarni muhofaza qilish bo‘yicha monitoring mexanizmlari yaratilishi, huquqiy asoslar kuchaytirilishi darkor.

Xullas, kibero‘g‘rilik – raqamli asrning eng xavfli jinoyat turlaridan biri sifatida nafaqat shaxsiy, balki milliy xavfsizlikka ham jiddiy tahdid solayotgan murakkab ijtimoiy-huquqiy muammo. Ushbu jinoyat turining sur’at bilan o‘sib borishi, jinoyatchilarning transmilliy xarakterga ega bo‘lishi va aniqlashdagi qiyinchiliklar uning zamonaviy jihatdan jiddiy tahlil etilishini talab etmoqda.

Fuqarolarning raqamli savodxonligini oshirish, huquqni muhofaza qiluvchi organlarning texnik salohiyatini mustahkamlash, huquqiy bazani xalqaro standartlarga mos ravishda takomillashtirish va sun’iy intellekt imkoniyatlaridan samarali foydalanish ushbu muammoning oldini olishda hal qiluvchi omillardan sanaladi.

Shu nuqtai nazardan, kibero‘g‘rilikka qarshi kurashda integral yondashuv, ya’ni huquqiy, texnologik, ta’limiy va profilaktik mexanizmlarni uyg‘unlashtirish asosidagi strategiya ishlab chiqilishi hamda amaliyotga tatbiq etilishi maqsadga muvofiqdir.

Foydalanilgan manbalar

1. O‘zbekiston Respublikasining Jinoyat kodeksi. – T., 2024. https://lex.uz.
2. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-son qonuni, 02.07.2019-yil. https://lex.uz.
3.“O‘zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi qonun. 2024-yil 21-noyabr https://lex.uz.
4. O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori. 2025-yil 30-aprel. https://lex.uz.
5. Salayev N.S., Ro‘ziyev R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar: Monografiya. – T.: TDYUU, 2018. – 139-b.
6. David S. Wall “Cybercrime: The Transformation of Crime in the Information Age” 2007. – C. 94.
7. Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In Criminology and Criminal Justice (Ҳиндистон).
8. Holt, T. J., & Bossler, A. M. (2020). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses (АҚШ).
9. Reich, P., et al. (2021). Law, Policy, and Technology: Cyberterrorism, Information Warfare and Internet Immobilization (Япония).
10. Brenner S. (2021). Cybercrime and the Digital Economy. Routledge.
11. INTERPOL. (2023). Global Cyber Threat Assessment.