TOSHKENT DAVLAT YURIDIK UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.07/2025.27.12.Yu.01.04 RAQAMLI ILMIY KENGASH

TOSHKENT DAVLAT YURIDIK UNIVERSITETI

DO‘SMATOV DURBEK RUSTAMJON O‘G‘LI

KIBERJINOYATCHILIKKA QARSHI KURASHNING JINOYAT-HUQUQIY VA KRIMINOLOGIK JIHATLARI

12.00.08 – Jinoyat huquqi. Jinoyat-ijroiya huquqi
12.00.15 – Kriminologiya

Yuridik fanlari bo‘yicha falsafa doktori (Doctor of Philosophy) dissertatsiyasi AVTOREFERATI

Toshkent – 2026

UDK: 343.711:004.056(575.1)

Falsafa doktori (PhD) dissertasiyasi avtoreferati mundarijasi
Оглавление автореферата диссертации доктора философии (PhD)
Content of the abstract of the dissertation of the Doctor of Philosophy (PhD)

TOSHKENT DAVLAT YURIDIK UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.07/2025.27.12.Yu.01.04 RAQAMLI ILMIY KENGASH

TOSHKENT DAVLAT YURIDIK UNIVERSITETI

DO‘SMATOV DURBEK RUSTAMJON O‘G‘LI

KIBERJINOYATCHILIKKA QARSHI KURASHNING JINOYAT-HUQUQIY VA KRIMINOLOGIK JIHATLARI

12.00.08 – Jinoyat huquqi. Jinoyat-ijroiya huquqi
12.00.15 – Kriminologiya

Yuridik fanlari bo‘yicha falsafa doktori (Doctor of Philosophy) dissertatsiyasi AVTOREFERATI

Toshkent – 2026

Falsafa doktori (Doctor of Philosophy) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Fanlar akademiyasi huzuridagi Oliy attestatsiya komissiyasida B2023.3.PhD/Yu1168 raqam bilan ro‘yxatga olingan.

Dissertatsiya Toshkent davlat yuridik universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz, (rezyume)) Ilmiy kengash veb-sahifasida (https://tsul.uz/uz/fan/avtoreferatlar) va “Ziyonet” Axborot ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Abzalova Xurshida Mirziyatovna** yuridik fanlar doktori (DSc), professor
Rasmiy opponentlar:	**Rasulev Abdulaziz Karimovich** yuridik fanlari doktori (DSc), professor
	Kamalova Dildora Gayratovna yuridik fanlar doktori (DSc), professor
Yetakchi tashkilot:	**O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi**

Dissertatsiya himoyasi Toshkent davlat yuridik universiteti huzuridagi Ilmiy darajalar beruvchi DSc.07/2025.27.12.Yu.01.04 raqamli Ilmiy kengashning 2026-yil “7”-avgust soat 14^{30} dagi majlisida bo‘lib o‘tadi (Manzil: 100047, Toshkent shahar, Sayilgoh ko‘chasi, 35-uy. Tel.: +99871 233-66-36; faks: +99871 233-37-48; e-mail: info@tsul.uz).

Dissertatsiya bilan Toshkent davlat yuridik universiteti Axborot-resurs markazida tanishish mumkin (343.9-raqami bilan ro‘yxatga olingan). (Manzil: Toshkent shahar, Amir Temur ko‘chasi, 13-uy. Tel: +99871 233-66-36).

Dissertatsiya avtoreferati 2026-yil “22”-iyul kuni tarqatildi.
(2026-yil “22”-iyuldagi 6-raqamli reyestr bayonnomasi)

R.A.Zufarov
Ilmiy darajalar beruvchi Ilmiy kengash raisi, yuridik fanlar doktori, professor

N.K.Xojiyev
Ilmiy darajalar beruvchi Ilmiy kengash kotibi, yuridik fanlar bo‘yicha falsafa doktori, dotsent v.b.

Sh.Dj.Xaydarov
Ilmiy darajalar beruvchi Ilmiy kengash qoshidagi Ilmiy seminar raisi, yuridik fanlar doktori, professor

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Dunyoda iqtisodiyotning jadal raqamlashuvi sharoitida kiberjinoyatchilik tashkilotlar va davlatlarning barqaror rivojlanishiga asosiy global tahdidlardan biriga aylanmoqda. Cybersecurity Ventures ma'lumotlariga ko'ra, 2024-yilda kiberjinoyatlardan ko'rilgan umumiy global zarar 9,5 trillion AQSH dollarga yetgan bo'lsada, 2025-yilda esa 10,5 trillion AQSH dollariga etgan. Muammoning ahamiyati bulutli texnologiyalar, masofaviy xizmatlar, global internet va ma'lumotlar hajmining o'sishi tufayli raqamli hujumlarning kengayishi natijasida kuchaymoqda. Ayniqsa, tovlamachilik dasturlari xavf tug'diradi, ulardan ko'rilgan zarar 2024-yilda 42 milliard AQSH dollariga baholanmoqda. Kiberxavfsizlik sohasida 3,5 million bo'sh ish o'rinlarini tashkil etuvchi global kadrlar tanqisligi qo'shimcha xavf omili hisoblanadi. Ushbu holatlar tashkilotlarning kiberbarqarorligini ta'minlashning samarali mexanizmlarini ishlab chiqishga qaratilgan tadqiqotlarning yuqori ilmiy va amaliy dolzarbligini tasdiqlaydi[1].

Jahonda konseptual jihatdan, kiberjinoyatchilikka qarshi kurashning jinoyat-huquqiy va kriminologik jihatlari global taraqqiyotning fundamental tendensiyalari ta'sirida shakllanmoqda. Insoniyat rivojining hozirgi bosqichi iqtisodiyot va davlat boshqaruvidan tortib shaxsiy muloqot hamda ijtimoiy munosabatlargacha bo'lgan ijtimoiy hayotning barcha sohalarini misli ko'rilmagan darajada raqamli o'zgartirish bilan tavsiflanadi. Ijtimoiy borliqning tamomila yangi o'lchami sifatida global kibermakoning shakllanishi jinoyatchilik fenomenologiyasining sifat jihatidan o'zgarishi bilan birga kechmoqda: sanoat davrida shakllangan klassik jinoyat-huquqiy va kriminologik tushunchalarga sig'maydigan o'ziga xos ontologik xususiyatlarga ega ijtimoiy xavfli qilmishlarning mustaqil turi – kiberjinoyatchilik vujudga kelmoqda.

O'zbekiston Respublikasi davlat boshqaruvi tizimi, iqtisodiyot, bank sohasi, ta'lim va sog'liqni saqlashga axborot-kommunikatsiya texnologiyalarini (AKT) faol joriy etar ekan, ayni vaqtda kompyuter tizimlari va tarmoqlaridan foydalangan holda sodir etilayotgan jinoyatlarning o'sishiga ham duch kelmoqda. Respublika Ichki ishlar vazirligi ma'lumotlari raqamli muhitda jinoyatchilik muttasil ortib borayotganidan dalolat beradi. Birgina 2023-yilning o'zida huquqni muhofaza qilish organlari tomonidan 8 mingdan ortiq kiberjinoyatlar qayd etilgan bo'lib, ular orasida fishing sxemalari, kompyuterlarni buzib kirish, onlayn firibgarlik, axborot resurslariga ruxsatsiz kirish va virusli dasturiy ta'minotni tarqatish kabi qilmishlar mavjud. Shu bilan birga, bunday jinoyatlarni fosh etish darajasi pastligicha qolmoqda, bu holat ularni tergov qilishning texnologik jihatdan murakkabligi hamda ushbu sohadagi mavjud huquqiy tartibga solishning yetarlicha samarali emasligi bilan izohlanadi. Mamlakatimizda kiberjinoyatchilikka qarshi kurashish bo'yicha muhim ishlar olib borilmoqda, qonunchilik darajasida kiberxavfsizlik sohasidagi huquqiy asosni mustahkamlash chora-tadbirlari ko'rilmoqda. Shunga qaramay, ko'rib chiqilayotgan sohadagi jinoyat-huquqiy tartibga solish hanuz bir qator jiddiy

[1] Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024

kamchiliklarga ega. Xususan, O‘zbekiston Respublikasining Jinoyat kodeksida kibermuhitda sodir etiladigan jinoyatlarni tasniflashga nisbatan tizimli yondashuv mavjud emas. Bundan tashqari, qonunchilikda kriptoaktivlar, internet-firibgarlik, muhim infratuzilmalarga qilingan hujumlar bilan bog‘liq kiberjinoyatlarning o‘ziga xos jihatlari inobatga olinmagan. Bu, o‘z navbatida, huquqni qo‘llash amaliyotini murakkablashtiradi, huquqiy noaniqlikka olib keladi hamda bu kabi ishlarni tergov qilish va sudda ko‘rib chiqish samaradorligini pasaytiradi. Kriminologik nuqtayi nazardan, kiberjinoyatchilikning rivojlanishiga imkon beruvchi sabablar va shart-sharoitlar yetarlicha o‘rganilmagan. Hozirgi kunga qadar uning oldini olishning samarali mexanizmi ishlab chiqilmagan, statistik ma’lumotlarni to‘plash va tahlil qilish bo‘yicha yaxlit tizim yo‘q, aholining raqamli madaniyat darajasi esa qoniqarsizligicha qolmoqda. Kiberjinoyatlarga qarshi kurashishning jinoyat-huquqiy va kriminologik mexanizmlarini takomillashtirishga qaratilgan ilmiy asoslangan tavsiyalarni ishlab chiqish alohida ahamiyat kasb etmoqda. Kiberjinoyatchilikning jinoyat-huquqiy va kriminologik jihatlarini, jumladan, huquqiy bo‘shliqlarni aniqlash, sabab va shart-sharoitlarni tahlil qilish, profilaktika yo‘nalishlarini belgilash hamda qonunchilikni takomillashtirish bo‘yicha takliflar tayyorlashni o‘z ichiga olgan kompleks tadqiqot raqamli davrda huquqiy tartibotni mustahkamlashga va davlatning axborot xavfsizligini ta’minlashga hissa qo‘shadigan, bugungi kunda talab yuqori va dolzarb ilmiy yo‘nalish hisoblanadi.

Ushbu tadqiqot ishi O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi 439-II-son, O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonunlari, O‘zbekiston Respublikasi Prezidentining 2019-yil 14-sentabrdagi “Axborot texnologiyalari va kommunikatsiyalarini joriy etishni nazorat qilish, ularning himoyasini tashkil etish tizimini takomillashtirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ–4452-son, 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, 2026-yil 5-yanvardagi “Respublika mahallalarida xavfsiz muhitni yaratish yo‘nalishida manzilli ishlarning yaxlit tizimini joriy etishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ–1-son Qarorlari, 2026-yil 3-martdagi “Ayollar va bolalar huquqlarining himoyasini kuchaytirish hamda ularga nisbatan tazyiq va zo‘ravonlik holatlarining oldini olish bo‘yicha qo‘shimcha tashkiliy-huquqiy choralar to‘g‘risida”gi PF–33-son, 2026-yil 10-martdagi “O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida”gi PF–38-son Farmonlari hamda sohaga doir boshqa me’yoriy-huquqiy hujjatlarda belgilangan ustuvor vazifalarni amalga oshirish mexanizmlarini yaratishga muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining asosiy ustuvor yo‘nalishlariga mosligi. Mazkur dissertatsiya ishi Respublika fan va texnologiyalar rivojlanishining “I. Axborotlashgan jamiyat va demokratik davlatni ijtimoiy, huquqiy, iqtisodiy, madaniy, ma’naviy-ma’rifiy rivojlantirishda innovatsion g‘oyalar tizimini shakllantirish va ularni amalga oshirish yo‘llari” ustuvor yo‘nalishiga muvofiq bajarilgan.

Muammoning o‘rganilganlik darajasi. Respublikamizda kiberjinoyatchilikka qarshi kurashishning jinoyat-huquqiy va kriminologik jihatlari bugungi kunga qadar kompleks monografik tarzda ishlab chiqilmagan. Axborot munosabatlarini muhofaza qilish, raqamli muhitda jinoyatlarni kvalifikatsiya qilish va jinoyat qonunchiligini takomillashtirishning ayrim masalalari mamlakatimiz olimlari - M.X. Rustambayev, A.Anorbayev, N.S. Salayev, X.R. Ochilov, A.K. Rasulev, A.S. Tursunov va boshqa olimlarimizning asarlarida o‘rganilgan bo‘lsa-da, ushbu asarlarda JK Maxsus qismining tuzilishini kiberjinoyatchilikka nisbatan jinoiy xulq-atvorning mustaqil turi sifatida tizimli ravishda qayta ko‘rib chiqish yoritilmagan.

MDHga a’zo davlatlarda birinchi yo‘nalishda kiberjinoyatlarning tarkibi, dogmatik-jinoiy-huquqiy tahlili, ularni malakalash va maxsus jinoyat-huquqiy normalarni tuzish masalalari I.R.Begishev, K.N.Yevdokimov, T.L.Tropina, U.V.Zinina, A.G.Volevoz, V.B.Vexovlarning ishlarida yoritilgan.

Ikkinchi yo‘nalish kriminologik xususiyatga ega bo‘lib, kiberjinoyatchilarni shaxsi, raqamli jinoyatchilik determinantlari va uning oldini olish mexanizmlari T.M. Lopatina, D.V. Puchkov, A.S. Kamko, A.I. Xaliullin, M.M. Dolgievlarning tadqiqot ishlarida o‘z aksini topgan.

Uchinchi yo‘nalish xalqaro-huquqiy va qiyosiy-huquqiy yo‘nalishga ega bo‘lib, Yevropa Kengashining 2001-yildagi Kiberjinoyatchilik to‘g‘risidagi konvensiyasi (Budapesht konvensiyasi) hamda xalqaro standartlarni implementatsiya qilishning milliy modellarini tahlil qilish D.S. Uoll, M. Gudman, E.J. Eshvort, N. Juravlenko va L. Shvedovalarning ishlarida qayd etilgan[2].

Ushbu tadqiqotlar muammoning doktrinal asosini yaratdi, biroq ularning hech biri O‘zbekiston huquqiy tizimining o‘ziga xos xususiyatlarini, jumladan, O‘zbekiston Respublikasi JKning amaldagi tahriri, AKT va kriptoaktivlar bilan bog‘liq jinoyatlar bo‘yicha huquqni qo‘llash amaliyotining o‘ziga xos xususiyatlarini, shuningdek, raqamli muhitda viktimizatsiyaning ijtimoiy-madaniy omillarini to‘liq hisobga olmaydi. Mavzuning ilmiy jihatdan ishlab chiqilganligi ushbu kamchiliklar ishning tadqiqot vazifasini belgilashni taqozo etmoqda.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya Toshkent davlat yuridik universitetining ilmiy-tadqiqot ishlari rejasiga muvofiq “O‘zbekiston Respublikasi Jinoyat kodeksi va uni qo‘llash amaliyotini takomillashtirish muammolari”, “Globallashuv sharoitida jinoyatchilikka qarshi kurashni takomillashtirish muammolari”, “Sud-huquq sohasini isloh qilish va jinoyat qonunini liberallashtirish sharoitida jazo tizimini isloh qilish muammolari” mavzusidagi ilmiy tadqiqotlarning ustuvor yo‘nalishlari doirasida amalga oshirilgan.

Tadqiqotning maqsadi kiberjinoyatchilik holatining kriminologik tushunchasini shakllantirish va ularning ijtimoiy xavflilik darajasini aniqlash uchun zarur bo‘lgan AKT sohasidagi jinoyatlarning jinoiy-huquqiy mohiyatini ochib berishdan iborat.

Tadqiqotning vazifalari:

[2] Ushbu mualliflarning asarlari dissertatsiyaning foydalanilgan adabiyotlar ro‘yxatida keltirilgan.

kiberjinoyatchilikning umumiy tavsifini tahlil qilish;

kiberjinoyat institutining huquqiy tartibga solinishi genezisini o‘rganish;

kiberjinoyatchilikning obyektiv va subyektiv belgilarini tahlil qilish;

xorijiy mamlakatlarning jinoyat qonunchiligi bo‘yicha kiberjinoyatlar uchun javobgarlikni o‘rganish;

kiberjinoyatlarni kvalifikatsiya qilish va boshqa o‘xshash jinoyat tarkiblaridan farqlash masalalarini o‘rganish;

kiberjinoyatlar uchun javobgarlik sohasida jinoyat qonunchiligini takomillashtirishga qaratilgan amaliy tavsiyalar va takliflarni ishlab chiqish.

Tadqiqotning obyekti sifatida kiberjinoyatlar uchun javobgarlik belgilangan JK normalarini takomilllashtirish bilan bog‘liq jinoyat-huquqiy va kriminologik munosabatlar tizimi hisoblanadi.

Tadqiqotning predmetini kiberjinoyatlar uchun javobgarlikka oid huquqiy munosabatlarni tartibga soluvchi normativ-huquqiy hujjatlar, huquqni qo‘llash amaliyoti, xorijiy mamlakatlar qonunchiligi va amaliyoti hamda yuridik fanda mavjud bo‘lgan konseptual yondashuvlar, ilmiy-nazariy va huquqiy qarashlar hamda kriminologik tushunchalar tashkil etadi.

Tadqiqotning usullari. Tadqiqotni amalga oshirishda tarixiy, tizimli-tuzilmaviy, qiyosiy-huquqiy, mantiqiy, aniq sotsiologik, ilmiy manbalarni kompleks tadqiq etish, induksiya va deduksiya, statistik ma’lumotlar tahlili, ijtimoiy so‘rovlar o‘tkazish, huquqni qo‘llash amaliyotini tahlil qilish, jinoyat ishi materiallarini o’rganish tadqiqot ishining ishonchligi va sifatini ta’minlashga xizmat qiladi.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

kriptoaktivlarning noqonuniy muomalasi bilan bog‘liq qilmishlarni, ya’ni: kriptoaktivlarni g‘ayriqonuniy tarzda olish, sotish yoki ayirboshlashni; kriptoaktivlar sohasida xizmat ko‘rsatuvchi provayderlar faoliyatini tegishli litsenziyasiz amalga oshirishni; anonim kriptoaktivlar bilan operatsiyalar o‘tkazishni; kriptoaktivlarning anonim mayningini yoxud mayning faoliyatini belgilangan tartibni buzgan holda amalga oshirishni jinoyatlarning mustaqil tarkibi sifatida jinoiy javobgarlikka tortish zarurati asoslangan;

kriptoaktivlar muomalasi sohasidagi qonunchilikni buzish bilan bog‘liq qilmishlarni ma’muriy huquqbuzarlikning mustaqil tarkibi sifatida mustahkamlash, nazorat-idora mexanizmlarini kuchaytirishga va kriptoaktivlardan noqonuniy foydalanishning oldini olishga qaratilgan mutanosib ma’muriy javobgarlik choralarini belgilash zarurati asoslangan;

O‘zbekiston Respublikasi Jinoyat Kodeksining 168-moddasi uchinchi qismining “g” bandi bo‘yicha axborot tizimidan, shu jumladan axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etiladigan firibgarlikni malakalashning doktrinal mezonlari asoslab berildi. Moliya-bank tashkilotlari, jamg‘armalar va shu kabi boshqa tashkilotlar nazorati ostidagi mol-mulkni hisoblash texnikasi, aloqa vositalari, planshetlar yoki boshqa shunga o‘xshash texnik qurilmalardan foydalanib, manipulyatsiyalar qilish, jumladan, kompyuter tizimida qayta ishlanadigan, tegishli axborot tashuvchilarda saqlanadigan yoxud axborot uzatish tarmoqlari orqali uzatiladigan axborotni o‘zgartirish, shuningdek, kompyuter tizimiga bila turib yolg‘on axborot kiritish orqali firibgarlik yo‘li bilan o‘zlashtirish

ana shunday jinoyat sirasiga kiritildi. Bunday firibgarlikni axborot tizimiga g‘ayriqonuniy (ruxsatsiz) kirish yoki undan foydalanish orqali sodir etilgan o‘g‘irlikdan farqlash mezoni shakllantirildi: firibgarlikda aldangan yoki ishonchni suiiste’mol qilish ta’siridagi jabrlanuvchi mol-mulk yoki unga bo‘lgan huquqni aybdorga ixtiyoriy ravishda topshiradi va bunda mol-mulk uning egaligidan chiqib ketayotganini belgilaydi. Shuningdek, shaxsning o‘zganing mulkini keyinchalik qo‘lga kiritish maqsadida qalbaki hujjat tayyorlash uchun kompyuter texnologiyalaridan foydalanishi O‘zbekiston Respublikasi JKning 168-moddasi uchinchi qismining “g” bandi bilan kvalifikatsiya qilinishi mumkin emasligi to‘g‘risidagi qoida qo‘shimcha ravishda asoslangan;

kiberjinoyatchilikka qarshi kurashish choralarini takomillashtirish, ushbu sohadagi huquqbuzarliklar uchun javobgarlikni kuchaytirish va ularning oldini olishning tashkiliy-huquqiy mexanizmlarini rivojlantirish zarurati asoslab berildi. Jumladan, axborot resurslarini yaratish va axborot tizimlarining faoliyat yuritishida sun’iy intellekt texnologiyalaridan foydalanishning huquqiy asoslarini mustahkamlash, shuningdek, O‘zbekiston Respublikasi MJtKning 46^{2}-moddasi ikkinchi qismiga tegishli o‘zgartirishlar kiritish orqali sun’iy intellekt texnologiyalarini qo‘llagan holda shaxsga doir ma’lumotlarga noqonuniy ishlov berganlik uchun ma’muriy javobgarlik belgilash zarurati asoslangan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

Jinoyat Kodeksining “Fuqarolarning konstitutsiyaviy huquq va erkinliklariga qarshi jinoyatlar” deb nomlangan VII bobini shaxsni ta’qib qilish (stalking) va kiberzo‘ravonlik uchun javobgarlikni nazarda tutuvchi 141^{4}-modda bilan hamda “Oila, yoshlar va axloqqa qarshi jinoyatlar” deb nomlangan V bobini axborot-kommunikatsiya tarmoqlari orqali voyaga yetmagan shaxsni shahvoniy xarakterdagi harakatlarga jalb qilish (onlayn-gruming) uchun javobgarlikni nazarda tutuvchi 127^{2}-modda bilan to‘ldirish taklifi asoslangan;

Jinoyat Kodeksiga “Kiberjinoyatlar” nomli alohida VI^{1} bo‘lim kiritish taklifi asoslangan;

Jinoyat Kodeksiga “Axborot-kommunikatsiya texnologiyalariga qarshi jinoyatlar” deb nomlangan alohida bob kiritish, uning tarkibiga “278^{1}-modda. Raqamli axborotni egallash”, “278^{2}-modda. Raqamli axborotni berishga majburlash”, “278^{3}-modda. Foydalanish cheklangan elektron axborot resurslarini qonunga xilof ravishda tarqatish”, “278^{4}-modda. Kompyuter axborotini qonunga xilof ravishda yo‘q qilish, blokirovka qilish yoki modifikatsiya qilish” kabi jinoiy harakatlarni kiritish taklifi asoslangan;

Jinoyat Kodeksiga “Axborot-kommunikatsiya texnologiyalari sohasidagi jinoyatlar” deb nomlangan alohida bob kiritish, uning tarkibiga “278^{5}-modda. Axborotlashtirish qoidalarini buzish”, “278^{6}-modda. Kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish”, “278^{7}-modda. Axborot resurslaridan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o‘tkazish maqsadida tayyorlash yoxud o‘tkazish, ulardan foydalanish yoki ularni tarqatish”, “278^{8}-modda. Zararli dasturlarni yaratish, ulardan foydalanish yoki ularni tarqatish”, “278^{9}-modda. Telekommunikatsiyalar tarmog‘idan qonunga xilof ravishda (ruxsatsiz) foydalanish”, “278^{10}-modda. Kripto aktivlar aylanmasi

sohasidagi qonunchilikni buzish", "278[11]-modda. Mayning faoliyatini noqonuniy amalga oshirish", "278[12]-modda. Internet jahon axborot tarmog‘ida umumfoydalanishdagi axborotni tarqatish qoidalarini buzish" kabi jinoiy harakatlarni kiritish taklifi asoslangan;

JKning "Atamalarning huquqiy ma'nosi" bo‘limiga "kiberjinoyatchilik", "kiberjinoyat", "kompyuter", "kompyuter tizimi" atamalarini kiritish taklifi asoslangan;

axborot texnologiyalari sohasidagi jinoyatlarga aloqador jinoiy qilmishlarning ayrim tarkiblarining amaldagi moddalari sanksiyalarini kuchaytirish choralarini ko‘rish taklifi asoslangan;

JKning 48[1]-moddasi 3-qismiga "kiberjinoyat sodir etgan shaxsga nisbatan ozodlikni cheklash jazosi tayinlanganda sud tomonidan mahkumga tegishli kommunikatsiya va texnologiya vositalaridan foydalanishni taqiqlash tarzidagi qo‘shimcha cheklovni yuklash" kabi o'zgartirishlar bilan to'ldirish asoslangan.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalari milliy qonunchilik normalari, xalqaro hujjatlar, bir qator xorijiy davlatlar tajribasi va zamonaviy huquqni qo‘llash amaliyoti asosida shakllantirilgan bo‘lib, 132 ta sud hujjatlari (hukm va qarorlar), 224 ta nazariyotchi va amaliyotchi olimlar, jumladan, surishtiruvchilar, tergovchilar, sudyalar, advokatlar va professor-o‘qituvchilar ishtirokida o‘tkazilgan ekspert sotsiologik tadqiqotlar natijalari, shuningdek, 2025-yil dekabr oyida 155 nafar respondentning tanlanmasi bo‘yicha muallif tomonidan o‘tkazilgan mustaqil ijtimoiy so‘rovnoma natijalarini (uchta mavzuli blokga birlashtirilgan 23 ta savoldan iborat so‘rovnoma: ijtimoiy-demografik tavsif va tajriba; xabardorlik darajasi va viktimizatsiya; amaldagi qonunchilik va istiqboldagi qarshi kurashish choralarini baholash) umumlashtirish, O‘zbekiston Respublikasi Ichki ishlar vazirligi, O‘zbekiston Respublikasi Oliy sudi va O‘zbekiston Respublikasi Davlat xavfsizlik xizmati huzuridagi Davlat kiberxavfsizlik markazining 2019-2024-yillardagi statistik ma'lumotlarini tahlil qilish orqali amaliy jihatdan asoslangan; natijalar vakolatli tuzilmalar tomonidan ma'qullangan va amaliyotga joriy etilgan.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati shundan iboratki, mazkur tadqiqot natijasida ishlab chiqilgan qoidalar jinoyat huquqi nazariyasining rivojlanishiga, kelajakda ilmiy tadqiqot ishlarini olib borishda, yuridik oliy o‘quv yurtlarida jinoyat huquqi fanidan dars o‘tish hamda metodik tavsiyalar tayyorlashda, shuningdek, ushbu tadqiqot ishi natijasi kiberjinoyatchilikka qarshi kurashish bilan bog‘liq muammolarning hal etilishiga xizmat qiladi.

Tadqiqot natijalarining amaliy kiberjinoyatchilikka qarshi kurashish amaliyotini takomillashtirishga qaratilgan bir qator qoida va amaliy tavsiyalar ishlab chiqishda, Jinoyat kodeksini takomillashtirishda, O‘zbekiston Respublikasi Oliy sudi Plenumi qarorlarini takomillashtirishda foydalanish mumkin.

Tadqiqot natijalarining joriy etilishi. Kiberjinoyatchilikka qarshi kurashishning nazariy va amaliy jihatlarini o‘rganish natijalari asosida:

kriptoaktivlarning noqonuniy muomalasi sohasidagi qilmishlarni kriminalizatsiya qilishga qaratilgan takliflardan O‘zbekiston Respublikasi Jinoyat

kodeksi loyihasining 278^8 va 278^9-moddalarini ishlab chiqishda foydalanilgan.

Xususan, quyidagilar inobatga olingan: kriptoaktivlarni qonunga xilof ravishda olish, sotish yoki ayirboshlash, shuningdek, kriptoaktivlar sohasidagi xizmatlar provayderlarining tegishli litsenziyasiz faoliyat yuritishi va anonim kriptoaktivlar bilan operatsiyalarni amalga oshirganlik uchun javobgarlikni nazarda tutuvchi normani kiritish to‘g‘risidagi taklif (278^8-modda); kriptoaktivlarning anonim mayningini va mayning faoliyatini belgilangan tartibni buzgan holda amalga oshirishni kriminalizatsiya qilish to‘g‘risidagi taklif (278^9-modda). Mazkur takliflarning qabul qilinishi kriptoaktivlar muomalasi sohasidagi qonunchilikni buzganlik va noqonuniy mayning faoliyati uchun jinoiy javobgarlikni kuchaytirishga qaratilgan (O‘zbekiston Respublikasi Bosh prokuraturasining 2025-yil 5-iyuldagi 27/2-146-25-sonli va 2025-yil 18-iyundagi /№ 5-108416-25-sonli joriy etish dalolatnomalari);

kriptoaktivlar muomalasi sohasidagi qonunchilikni buzganlik uchun ma’muriy javobgarlik belgilashga oid takliflardan O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksi loyihasining 155^4-moddasi 1 va 2-qismlarini ishlab chiqishda foydalanilgan. Taqdim etilgan tashabbus nazorat-kuzatuv mexanizmlarini kuchaytirishga hamda kriptoaktivlardan noqonuniy foydalanish bilan bog‘liq qilmishlar uchun sanksiyalarni belgilashga qaratilgan (O‘zbekiston Respublikasi Davlat xavfsizlik xizmatining 2025-yil 26-iyundagi 17/01-34-sonli joriy etish dalolatnomasi);

tavsiyalar O‘zbekiston Respublikasi Oliy sudi Plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-sonli Qarorini tayyorlashda hisobga olingan. Xususan, mazkur Qarorning 22-bandiga doir axborot tizimidan, jumladan, axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etiladigan firibgarlikni malakalash, bunday firibgarlikni axborot tizimiga g‘ayriqonuniy (ruxsatsiz) kirish orqali sodir etilgan o‘g‘rilikdan chegaralash bo‘yicha takliflar, shuningdek, shaxsning keyinchalik o‘zganing mulkini qo‘lga kiritish maqsadida qalbaki hujjat tayyorlash uchun kompyuter texnologiyalaridan foydalanishi O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi uchinchi qismi “g” bandi bilan malakalash mumkin emasligi to‘g‘risidagi qoidalar e’tiborga olingan (O‘zbekiston Respublikasi Oliy sudining 2025-yil 28-maydagi 08/225-25-sonli joriy etish dalolatnomasi);

tadqiqot natijalari bo‘yicha tayyorlangan takliflardan O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-sonli Qarorini – kiberjinoyatchilikka qarshi kurashish choralarini takomillashtirish, ushbu sohadagi huquqbuzarliklar uchun javobgarlikni kuchaytirish va kiberjinoyatlarning oldini olishning tashkiliy-huquqiy mexanizmlarini rivojlantirish qismida – hamda O‘zbekiston Respublikasining 2026-yil 21-yanvardagi “Sun’iy intellektni qo‘llashda yuzaga keladigan munosabatlarni tartibga solish munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga qo‘shimcha va o‘zgartirishlar kiritish to‘g‘risida”gi O‘RQ-1115-sonli Qonunini ishlab chiqishda foydalanilgan. Xususan, izlanuvchining takliflari mazkur Qonun 1-moddasining

4-bandini – axborot resurslarini yaratish va axborot tizimlarining faoliyat yuritishida sun'iy intellektdan foydalanishning huquqiy asoslarini mustahkamlash qismida – shuningdek, mazkur Qonunning 2-moddasini – sun'iy intellekt texnologiyalaridan foydalangan holda shaxsga doir ma'lumotlarga qonunga xilof ravishda ishlov berganlik uchun O'zbekiston Respublikasining Ma'muriy javobgarlik to'g'risidagi kodeksining 46^2-moddasi ikkinchi qismiga tegishli o'zgartirishlar kiritish qismida – shakllantirishda inobatga olingan (O'zbekiston Respublikasi Ichki ishlar vazirligi Toshkent shahar ichki ishlar bosh boshqarmasining 2026-yil 28-apreldagi 27/3-1345/4k va 27/3-1345/5k-sonli joriy etish dalolatnomalari).

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 10 ta, jumladan 8 ta xalqaro, 2 ta respublika ilmiy-amaliy anjumanlarida muhokamadan o'tkazilgan.

Tadqiqot natijalarining e'lon qilinganligi. Dissertatsiya mavzusi bo'yicha 20 ta ilmiy ish, jumladan, 6 ta ilmiy maqola xorijiy nashrlarda, 6 ta ilmiy maqola respublika jurnallarida va 8 ta tezis chop etilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, uchta bob, xulosa, foydalanilgan adabiyotlar ro'yxati va ilovalardan iborat. Dissertatsiyaning hajmi 158 betni tashkil etgan.

DISSERTATSIYANING ASOSIY MAZMUNI

Dissertatsiyaning kirish (falsafa doktori (PhD) dissertatsiyaning annotatsiyasi) qismida tadqiqoti mavzusining dolzarbligi va ahamiyati, tadqiqot ishining respublika fan va texnologiyalari rivojlanishining asosiy ustuvor yo'nalishlariga bog'liqligi, tadqiq etilayotgan muammoning o'rganilganlik darajasi, dissertatsiya mavzusining dissertatsiya bajarilayotgan oliy ta'lim muassasasining ilmiy-tadqiqot ishlari bilan bog'liqligi, tadqiqotning maqsad va vazifalari, obyekti va predmeti, usullari, tadqiqotning ilmiy yangiligi va amaliy natijasi, tadqiqot natijalarining ishonchliligi, tadqiqot natijalarining ilmiy va amaliy ahamiyati, ularning joriy qilinishi, tadqiqot natijalarining aprobatsiyasi, natijalarning e'lon qilinganligi, dissertatsiyaning tuzilishi va hajmi yoritib berilgan.

Dissertatsiyaning **"Kiberjinoyatlar uchun javobgarlikning umumiy tavsifi va kiberjinoyatchilikka qarshi kurashishning xorijiy tajribasi"**ga bag'ishlangan birinchi bobida tadqiqotchi tomonidan jinoyat-huquqiy muhofazaning mustaqil hodisasi sifatida kiberjinoyatchilikning ijtimoiy-huquqiy tabiati har tomonlama yoritilgan. Unda O'zbekiston Respublikasida kiberjinoyatlar uchun jinoiy javobgarlik institutining shakllanishi retrospektiv tahlildan o'tkazilgan, shuningdek, dunyoning yetakchi davlatlari jinoyat qonunchiligi batafsil qiyosiy-huquqiy tahlil qilingan.

Mazkur bobda M.X. Rustambayev, N.S. Salayev, X.R. Ochilov, A.K. Rasulov, A.S. Tursunov, T.L. Tropina, T.M. Lopatina, K.N. Yevdokimov, O.A. Zigmunt, U.V. Zinina, A.M. Tarasov, L.P. Shmatkova, A.N. Tretyakov, D.V. Puchkov, G. Yanke, N.I. Juravlenko va L.E. Shvedova, A.J. Ashworth, D.S. Wall, S. Brenner, M. Goodman, R.M. Kowalski kabi olimlarning qarashlari o'rganilib, kompyuter vositalaridan foydalangan holda sodir etiladigan talon-toroj qilmishlarni, kiberjinoyatchilikka qarshi kurashishning jinoyat-huquqiy choralarini va mazkur

toifadagi qilmishlarning kriminologik xususiyatlarini, kiberjinoyatchilikning xalqaro-huquqiy hamda qiyosiy-huquqiy o‘lchovi masalalarini, kompyuter vositalaridan foydalangan holda sodir etiladigan firibgarlik jinoyatlarining xalqaro o‘lchovdagi yuridik konstruksiyasini tadqiq etishda doktrinal tayanch sifatida foydalanildi, shuningdek, kiberjinoyatchilik tabiatining doktrinal va kriminologik jihatlari tahlil qilindi.

Muallif axborot-kommunikatsiya texnologiyalari sohasidagi harakatlar uchun javobgarlikni tartibga soluvchi amaldagi normalarini, xususan, Jinoyat Kodeksining XX[1] bobining 278[1]–278[7]-moddalarini kompleks doktrinal tahlil qilgan. Tadqiqotchi kiberjinoyatlarni tizimli ravishda uch turkumga ajratadi: bevosita kompyuter tizimlariga tajovuzda ifodalangan qilmishlar – “toza kompyuter” (cyber-dependent); raqamli texnologiyalar ta’sirida o‘zgargan an’anaviy jinoyatlar – “instrumental” (cyber-enabled) va raqamli muhit faqat aloqa kanali sifatida xizmat qiladigan “yordamchi” (cyber-assisted) qilmishlar. Muallifning nuqtayi nazariga ko‘ra, “evolyutsion-tahririy” yondashuv o‘z salohiyatini butunlay tugatgan: u havola normalarning ko‘payib ketishiga olib keladi, tarkiblar o‘rtasida raqobatni yuzaga keltiradi va ijtimoiy xavfli qilmishlarning butun bir toifasini jinoyat-huquqiy himoyadan chetda qoldiradi. Tadqiqotchi texnik omil bilan murakkablashtirilgan an’anaviy mulkiy tajovuzlar paradigmasi haqidagi yondashuvga qat’iyan qo‘shilmaydi va kiberjinoyatchilikning o‘ziga xos belgilari ya’ni tajovuz obyektining nomoddiy xususiyati, eksterritoriallik, harakatlarning avtomatlashganligi, subyektning maxsus ko’nikmaga egaligi, 85–95 foiz oralig‘idagi latentlik – Jinoyat kodeksida alohida bo‘limga ajratishni taqozo etadigan sifat jihatidan yangi jinoyat-huquqiy hodisani shakllantirshni isbotlagan. Muallif tomonidan mazkur konsepsiyalarni respublikaning huquqiy tizimi sharoitlariga moslashuvi asoslantirilgan.

Bundan tashqari, muallif tomonidan o‘tkazgan retrospektiv tahlil natijasida respublikada kiberjinoyatlar uchun jinoiy javobgarlik institutining shakllanishini uch bosqichga ajratgan holda davrlashtiradi. Bular: institutsionalgacha bo‘lgan davr (1994–2007-yillar) ya’ni kiberhujumlar Jinoyat kodeksining umumiy moddalari bo‘yicha malakalangan, maxsus jinoiy-huquqiy normalar mavjud bo‘lmagan davr; shakllanish bosqichi (2007–2022-yillar) ya’ni “Axborot texnologiyalari sohasidagi jinoyatlar” deb nomlangan XX[1]-bobning kiritilishi; modernizatsiya bosqichi (2022-yildan hozirgi kunga qadar) ya’ni “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasi Qonunining qabul qilinishi, Kiberjinoyatchilikka qarshi kurashish milliy strategiyasining shakllantirilishi hamda yangi Jinoyat kodeksiga 278[8]–278[9]-moddalarning kiritilishi asoslantirilgan. Bobda kiberjinoyatchilik firibgarlik, ekstremistik, terroristik, qo‘poruvchilik va shaxs daxlsizligiga tajovuz qiluvchi harakatlarni birlashtiradigan o‘ziga xos ontologiyaga ega ekanligi haqidagi qarash asoslantirilgan. Dissertatsiyada Jinoyat kodeksining amaldagi tahririda “kompyuter tizimi” o‘rniga “EHM” kabi terminologik jihatdan eskirgan tushunchalardan foydalanilgani, shuningdek, “botnet”, “DDoS-hujum”, “zararli dasturiy ta’minot”, “o‘ta muhim axborot infratuzilmasi”, “kriptoaktiv”, “dipfeyk”, “ijtimoiy muhandislik” kabi tushunchalarning qonuniy ta’riflari mavjud emasligi tanqidiy baholangan, natijada

muallif kodeksga norma-ta’rif sifatida kiritilishi lozim bo‘lgan yagona terminologik apparatni – “Kiberjinoyatchilikning kategorial lug‘ati” konsepsiyasini taklif etgan.

Tadqiqot doirasida dissertant Rossiya Federatsiyasi (RF JK 28-bobi), Moldova Respublikasi, Buyuk Britaniya (2006-yilgi Firibgarlik to‘g‘risidagi qonun, 1990-yilgi Kompyuterdan qonunga xilof ravishda foydalanish to‘g‘risidagi qonun), Amerika Qo‘shma Shtatlari (1986-yilgi Kompyuter firibgarligi va suiiste’molchiligi to‘g‘risidagi qonun), Germaniya Federativ Respublikasi (GJK 202a, 202b, 202c, 263a, 303a, 303b-moddalari), Avstraliya (2001-yilgi Kiberjinoyatlar to‘g‘risidagi qonun), Qozog‘iston Respublikasi (Qozog‘iston Respublikasi JK 7-bobi), Koreya Respublikasi, Yaponiya, Singapur kabi mamlakatlarning qonunchiligini, shuningdek, Kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasini batafsil qiyosiy-huquqiy tahlil qildi. Tadqiqotchi metodologik cheklovlarga qarshi o‘laroq, “huquqiy filtr” tamoyiliga asoslangan mualliflik implementatsiya modelini ishlab chiqish zarurati asoslantirilgan. Unga ko‘ra, xorijiy tajribani o‘zlashtirishga faqat to‘rtta majmuaviy mezonga – milliy huquqiy an’analarga moslik, konstitutsiyaviy qadriyatlarga muvofiqlik, donor mamlakatdagi empirik samaradorlik va qo‘llash uchun infratuzilmaviy tayyorgarlikning mavjudligi shartlariga rioya qilingan taqdirdagina yo‘l qo‘yiladi. Izlanuvchi yigirmadan ortiq aniq retsepsiyadan iborat normalarni asoslab beradi: dipfeyklardan foydalangan holda sodir etiladigan firibgarlik, kriptoaktivlar bilan bog‘liq harakatlar, “dropperlar” faoliyati, SIM-kartalar bilan bog‘liq manipulyatsiyalar, aloqa xizmatlari provayderlarining korporativ javobgarligi hal etilishi asoslantirilgan.

Dissertatsiyaning **“Kiberjinoyatchilikka qarshi kurashishning jinoyat-huquqiy jihatlari”** deb nomlangan ikkinchi bobida muallif tomonidan kiberjinoyatlarning obyektiv va subyektiv belgilarini chuqur doktrinal tahlil qilgan. Shuningdek, unda turdosh tarkiblarni malakalash va chegaralash masalalari yoritilib, kodeksni tizimli isloh qilish bo‘yicha takliflar majmui ishlab chiqilgan.

Muallif o‘z ishida kiberjinoyatlarning obyektiv tomonini o‘ziga xos doktrinal tahlil qiladi. U hukmron doktrina vakillari – A.I. Rarog, N.A. Lopashenko va S.A. Pashin bilan ilmiy bahsga kirishadi. Mazkur olimlar zararli dasturlarni faqat jinoyat sodir etish vositasi deb ta’riflaganlar. Ularning qarashicha, zararli dasturiy ta’minot o‘zining huquqiy rejimiga ko‘ra, klassik jinoyat-huquqiy ma’nodagi jinoyat quroliga (pichoq, o‘qotar qurol, ochqich bilan qiyoslash mumkin) tenglashtirilgan. Tadqiqotchi bu yondashuvga mutlaqo qo‘shilmaydi va konseptual jihatdan butunlay boshqacha yondashuvni asoslab bergan. Unga ko‘ra, zararli dasturlar o‘ziga xos (“sui generis”) tajovuz predmeti sifatida qaralishi lozim. Ushbu predmet uchta asosiy belgiga ega: maqsadga yo‘naltirilganlik (dastur boshidanoq muayyan bir buzg‘unchi natijaga erishishga dasturlangan bo‘ladi), buzg‘unchilik salohiyati (ko‘lami cheklanmagan zarar yetkazish qobiliyati) va avtonomlik (ishga tushirilgandan so‘ng o‘z yaratuvchisining irodasidan mustaqil harakat qila olishi). Muallifning pozitsiyasi zamonaviy polimorf viruslar, sun’iy intellekt texnologiyalariga asoslangan o‘z-o‘zini o‘rganuvchi zararli modullar va avtonom botnetlar raqamli muhitda kvazi-subyektlik xususiyatiga ega bo‘lgani uchun

“qurol”ning klassik tushunchasiga sig‘masligi bilan quvvatlanadi. Muallif zararli kodning avtonom ishlash xususiyati uni har qanday moddiy quroldan tubdan farqlashini va alohida jinoyat-huquqiy rejimni ya’ni Jinoyat kodeksiga zararli kodni tayyorlash, tarqatish va undan foydalanganlik uchun tabaqalashtirilgan sanksiyalarga ega mustaqil jinoyat tarkiblarini kiritishni talab qilishini dalillar bilan isbotlaydi. Muallif “kompyuter viruslari”, “qurtlar”, “troyan dasturlar”, “josuslik dasturlar (spyware)”, “tovlamachi dasturlar (ransomware)”, “klaviatura josuslari (keyloggers)”, “masofaviy boshqaruv vositalari”, “kriptojeking dasturlar (cryptojackers)” kabi batafsil jinoyat-huquqiy tavsif bergan. Shuningdek, u ommaviy “fishing” va texnologik jarayonlarni boshqarishning avtomatlashtirilgan tizimlariga tajovuz qilganlik uchun javobgarlik belgilash zarurati asoslab bergan.

Tadqiqotchi tomonidan kiberjinoyat subyektining ijtimoiy-demografik, psixologik, motivatsion va xulq-atvoriga oid parametrlarini o‘z ichiga olgan kompleks kriminologik portreti shakllantirilgan. O‘zbekiston Respublikasida kiberjinoyatning odatiy subyekti AKT sohasida maxsus bilimlarga ega, aksariyat hollarda ilgari sudlanmagan, 16 yoshdan 35 yoshgacha bo‘lgan erkak kishi ekanligi asoslantirib berilgan. Muallif kiberjinoyatlar uchun jinoiy javobgarlik yoshini pasaytirish maqsadga muvofiq emas deb hisoblovchi konservativ yondashuv vakillari – A.I. Dolgova, Yu.M. Antonyan va G.A. Avanesovlar bilan ilmiy bahsga kirishadi. Ularning fikricha, voyaga yetmaganlarning “raqamli sohada yetukmasligi” ularni bunday qilmishlar uchun javobgarlikka tortishga to‘sqinlik qiladi. Muallif voyaga yetmaganlarning javobgarligi muammosiga, asosan, amaldagi yosh chegarasi doirasida o’zgartirishlar kiritilishini asoslagan. Izlanuvchi o‘zining 2023-yildan 2025-yilgacha mamlakatda kiberjinoyat sodir etgan shaxslarning 14 yoshdan 16 yosh yoki 23,4 foizini mazkur toifadagi shaxslar tashkil etgani haqidagi empirik ma’lumotlarga tayanib, Jinoyat kodeksining 17-moddasi ikkinchi qismini to‘ldirish orqali kiberjinoyatlarning ayrim turlari uchun jinoiy javobgarlik yoshini 14 yoshdan belgilash zarurligini asoslagan. Raqamli muhitga nisbatan muallifning pozitsiyasi aniq: aynan yuqorida sanab o‘tilgan yosh chegarasi eng yuqori raqamli savodxonlikni namoyon etadi va bu ko‘pincha voyaga yetgan subyektlarning savodxonligidan ham ustun turishi asoslangan. Bu esa umumiy yosh chegarasini saqlab qolishni kriminologik jihatdan ahamiyatsizligini asoslagan.

Mazkur ishda muallif Jinoyat kodeksini tizimli isloh qilishning konseptual modelini ishlab chiqish taklif etilgan. Muallif kodeksga Maxsus qismning mutlaqo yangi tarkibiy unsur sifatida “Kiberjinoyatlar” nomli alohida 6^1-bo‘limni; barcha “sof kompyuter” jinoyat tarkiblarini o‘zida jamlagan “Axborot-kommunikatsiya texnologiyalariga qarshi jinoyatlar” nomli alohida bobni hamda stalking va kiberzo‘ravonlik uchun javobgarlikni belgilovchi normalarni kiritish zarurligini asoslagan.

Tadqiqotchi, kompyuter modifikatsiyasi va kompyuter sabotaji to‘g‘risidagi normalarni mustaqil va bir-biri bilan raqobatlashmaydigan tarkiblar sifatida ko‘ruvchi S.V. Maksimov va G.A. Yesakovning qarashlariga zid o‘laroq o‘z pozitsiyasini asoslagan. Muallifning nuqtayi nazari bevosita huquqni qo‘llash amaliyoti uchun ahamiyatli bo‘lib, kompyuter modifikatsiyasini nazarda tutuvchi modda dispozitsiyasini kengaytirish bilan bir vaqtda Jinoyat kodeksidan kompyuter

sabotaji to‘g‘risidagi normani chiqarib tashlash taklifini asoslagan. Shuningdek, muallif jinoyat-huquqiy himoya darajasida ikki bosqichli autentifikatsiyaga oid majburiy talablarni belgilash, kiberjinoyatlar bo‘yicha ishlarni ko‘ruvchi, majburiy texnik mutaxassislikka ega bo‘lgan ixtisoslashtirilgan sudyalar institutini joriy qilish hamda O‘zbekiston Respublikasi Bosh prokuraturasi huzurida tezkor faoliyatni amalga oshiruvchi mobil kriminalistik guruhlar tuzish taklif qilingan.

Dissertatsiyaning **“Kiberjinoyatchilikning kriminologik tavsifi”** deb nomlangan uchinchi bobida kiberjinoyatlar sodir etilishiga imkon beradigan sabab va shart-sharoitlar tahlil qilingan, kiberjinoiy faoliyat subyektlarining mualliflik tipologiyasi ishlab chiqilgan hamda respublikada kiberjinoyatchilikning ko‘p bosqichli profilaktikasiga doir o‘ziga xos konsepsiya shakllantirilgan.

Muallif kiberjinoyatchilik determinatsiyasining o‘ziga xos integral to‘rt omilli modelini taklif qilgan. Ushbu model quyidagilarni o‘zida birlashtiradi: ijtimoiy-iqtisodiy omillar, ya’ni raqamli tengsizlik, IT-mutaxassislar o‘rtasidagi ishsizlik, kriptoiqtisodiyotning yashirin sektori; huquqiy va institutsional omillar, xususan, jinoyat qonunchiligidagi bo‘shliqlar, idoralararo hamkorlikning zaifligi, ixtisoslashtirilgan tergov bo‘linmalarining yo‘qligi; texnologik omillar, jumladan, “Crime-as-a-Service” modeli bo‘yicha zararli dasturiy ta’minotdan foydalanish imkoniyatining ortishi, sun’iy intellekt va “dipfeyk” texnologiyalarining tarqalishi, “DarkNet” segmentida anonimlik; psixologik va viktimologik omillar, ya’ni aholining raqamli savodxonlik darajasi pastligi, “raqamli ishonch sindromi” hamda keksa yoshdagi shaxslarning viktimologik himoyasizligi. Muallif iqtisodiy-deterministik yondashuvni himoya qilib, kiberjinoyatchilikni faqat ijtimoiy-iqtisodiy omillarga bog‘laydigan monokauzal konsepsiyalar tarafdorlari V.V. Luneyev va Ya.I. Gilinskiy, shuningdek, texnokratik konsepsiyaga tayanib, uni asosan raqamli foydalanish imkoniyati darajasi bilan izohlaydigan Peter Grabosky bilan ilmiy munozaraga kirishadi. Muallifning fikricha, iqtisodiy, institutsional va ijtimoiy-madaniy determinantlar teng darajada ta’sir ko‘rsatadigan O‘zbekiston Respublikasida birorta ham monofaktorli model kiberjinoyatchilikning tuzilishi va dinamikasini tushuntirib bera olmsligini asoslagan. Muallif tomonidan o‘tkazilgan mustaqil sotsiologik tadqiqotga (tanlanma hajmi – O‘zbekiston Respublikasining 12 ta hududidan 1 247 nafar respondent, davri – 2024–2025-yillar) ko‘ra, respondentlarning atigi 16,1 foizi kiberjinoyatlar to‘g‘risidagi jinoyat qonunchiligini bilish darajasini qoniqarli deb baholashgan, 21,3 foizi “Kiberxavfsizlik to‘g‘risida”gi Qonun talablaridan xabardor ekanligini, 31,0 foizi kiberfiribgarlar harakatlarini aniqlay olishiga ishonishligini, 43,7 foizi so‘nggi bir yil ichida kiberfiribgarlik harakatlariga duch kelishganligini, 12,4 foizi esa kiberjinoyat qurboniga aylanganligini ma’lum qilishgan. Shu bilan birga, so‘rovda qatnashganlarning 79,3 foizi O‘zbekiston Respublikasi Jinoyat kodeksiga “Kiberjinoyatlar” nomli alohida bo‘lim kiritish zaruratini, 68,9 foizi ayrim kiberjinoyatlar uchun jinoiy javobgarlik yoshini pasaytirish zaruratini, 84,2 foizi esa “dropperlar”ning yagona reyestrini yaratish taklifini qo‘llab-quvvatlashgan. Muallifning ishonch bildirishicha, keltirilgan empirik ma’lumotlar O‘zbekiston Respublikasi kriminologiya faniga qo‘shilgan mustaqil hissa bo‘lib, mamlakatimiz

doktrinasida keng tarqalgan aholining huquqiy ma’rifati bo‘yicha amaldagi chora-tadbirlarning “yetarliligi” to‘g‘risidagi fikrni rad etadi.

To‘plangan ma’lumotlar asosida kiberjinoiy faoliyati subyektlarining kompleks tipologiyasi tushuntirib berilgan bo‘lib, u “xaker-tadqiqotchi” (grey-hat), “xaker-buzg‘unchi” (black-hat), “karder”, “insayder”, “uyushgan kiberjinoiy guruh a’zosi”, “skript-kiddi”, “Crime-as-a-Service operatori” kabi toifalarni o‘z ichiga oladi va ta’lim, xulq-atvor, psixologik hamda retsidiv mezonlari bo‘yicha tabaqalashtirish zarurati asoslagan. Muallif kiberjinoyatchini asosan yolg‘iz ishqiboz siymosida ko‘rsatuvchi “romantizatsiyalashgan” maktab vakillari Paul Taylor va Steven Levy bilan ilmiy polemikaga kirishadi. Ularning qarashlariga ko‘ra, kiberjinoyatchilikka qarshi kurash individual ta’sir choralariga yo‘naltirilishi lozim. Ushbu pozitsiyaga qarshi o‘laroq, muallif 2020-yildan hozirgi kunga qadar davom etayotgan zamonaviy bosqich kiberjinoyatchilikning “demokratlashuvi” va elitar xakerlardan ommaviy skript-kiddilarga o‘tish, yashirin xizmatlarni tijoratlashtirish, “DarkNet” segmentida yillik aylanmasi 1,5 milliard dollardan ortiq bo‘lgan transmilliy raqamli bozorlarning shakllanishi bilan tavsiflanishini ta’kidlagan. Muallifning pozitsiyasi shundan iboratki, “yolg‘iz jinoyatchi”ga qaratilgan an’anaviy kurash modeli o‘z samarasini butkul yo‘qotgan va uning o‘rnini izlanuvchi tomonidan barcha mavjud doktrinal yondashuvlarga qarama-qarshi o‘laroq ishlab chiqilgan konseptsiya – tarmoqli reaksiya modeli egallashi kerakligi taklif etilgan.

Tadqiqotchi tomonidan kiberjinoyatchilikning o‘zaro bog‘liq beshta darajani o‘z ichiga olgan ko‘p bosqichli profilaktika konsepsiyasini asoslagan. Umumdavlat darajasida kiberjinoyatchilikning yagona kriminologik monitoring markazini yaratish, kiberjinoyatlardan jabrlanganlarga yetkazilgan zararni qoplash jamg‘armasini ta’sis etish, “dropperlar”ning yagona milliy reyestrini shakllantirish taklif etilgan. Tarmoq darajasida o‘ta muhim axborot infratuzilmasi subyektlari uchun majburiy kibersug‘urtani joriy etish, “Bug Bounty” institutlarini joriy etish, majburiy korporativ o‘qitish standartlarini joriy qilish taklif etilgan. Ta’lim darajasida o‘rta, o‘rta maxsus va oliy ta’lim tizimiga “raqamli gigiyena” milliy dasturini joriy etish, barcha bosqichdagi o‘quv dasturlariga “Kiberxavfsizlik asoslari” majburiy kursini kiritish taklif etilgan. Vertikal tizimda mahallalar miqyosida manzilli profilaktikaga doir tajriba loyihalarini amalga oshirish (videokuzatuv tizimlari, SOS-tugmalarini o‘rnatish, oilalar va voyaga yetmaganlar bilan manzilli ishlash, fuqarolar yig‘inlarini kiberjinoyatchilikka qarshi kurashishda jalb etish), xalqaro darajada esa Budapesht konvensiyasi hamda G7ning 24/7, Yevropol va Interpol mexanizmlariga qo‘shilish taklif etilgan.

Bundan tashqari, muallif repressiv yondashuv tarafdori E.F. Pobegaylo bilan bahsga kirishib, rivojlangan profilaktika tizimi mavjud bo‘lmagan taqdirda, na sanksiyalarni kuchaytirish, na jinoiy jazolanadigan qilmishlar ro‘yxatini kengaytirish kiberjinoyatchilik darajasini pasaytira olmasligini asoslagan.

Muallif transchegaraviy kiberhujumlar bo‘yicha majburiy yurisdiksiyaga ega bo‘lgan, kiberjinoyatchilikka qarshi kurash muvofiqlashtiruvchi ixtisoslashtirilgan xalqaro institut – “KiberBMT”ni yaratish konsepsiyasini asoslagan. Muallif imperativ yurisdiksiyaga ega ixtisoslashtirilgan institutning mavjud emasligi,

transchegaraviy kiberjinoyatchilikning o‘sishiga sabab bo‘layotgan asosiy institutsional omillardan biri ekanligini asoslantirilgan, birgina 2025-yilda jahon miqyosidagi zarar 10,5 trillion AQSH dollariga yetganligiga ta’rif bergan holda, “KiberBMT”ni ta’sis etish O‘zbekiston Respublikasining xalqaro maydondagi tashabbusi bo‘lishi va uning BMTning Raqamli xavfsizlik bo‘yicha xalqaro tashabbusidagi faol ishtirokchi sifatidagi rolini yanada rivojlantirishi taklif etilgan.

Mazkur dissertatsiya natijalaridan “Toshkent shahar Shayxontohur tumanida kiberjinoyatchilikning oldini olish va unga qarshi kurashishning kriminologik metodikasi”ni ishlab chiqishda foydalanilgan. Shunga ko‘ra, ushbu tadqiqot ishi O‘zbekiston Respublikasi Prezidentining 2026-yil 5-yanvardagi PQ–1-son “Respublika mahallalarida xavfsiz muhit yaratish yo‘nalishida yaxlit manzilli ishlash tizimini joriy etishga qaratilgan qo‘shimcha chora-tadbirlar to‘g‘risida”gi qarori va O‘zbekiston Respublikasi Prezidentining 2026-yil 16-fevraldagi PF-21-son “Mamlakat taraqqiyotining 2023-yilgacha mo‘ljallangan ustuvor yo‘nalishlari doirasida islohotlarni izchil yangi bosqichga olib chiqishning qo‘shimcha chora-tadbirlari to‘g‘risida”gi Farmonida belgilangan ustuvor vazifalarni amalga oshirish mexanizmlarini yaratishga muayyan darajada xizmat qiladi.

XULOSA

“Kiberjinoyatchilikka qarshi kurashning jinoyat-huquqiy va kriminologik jihatlari” mavzusidagi dissertatsiya tadqiqoti natijasida jinoyat qonunchiligi normalarini takomillashtirish va huquqni qo‘llash amaliyotini rivojlantirishga qaratilgan umumiy-nazariy xulosalar, takliflar va tavsiyalar ishlab chiqildi. Xulosalar uchta umumiy sohani qamrab oladi va quyidagilardan iborat:

I. Ilmiy-nazariy xulosalar:

1. O‘zbekistonda kiberjinoyatchilikka samarali qarshi kurashish milliy qonunchilikni takomillashtirishni, kiberxavfsizlikning yagona standartlari asosida xalqaro hamkorlikni kuchaytirishni hamda profilaktika ishlariga ta’lim va jamoat institutlarini jalb etishni taqozo etadi.

2. Tajovuz obyektining nomoddiy tabiati, yuqori darajadagi latentlik va yurisdiksiya hamda ekstraditsiya masalalarini murakkablashtiradigan transmilliy xususiyat kiberjinoyatlarning asosiy belgilaridir. Ularning sodir etilishi yuqori texnologiyalar, anonimlashtirish vositalari va sun’iy intellektdan foydalanish bilan bog‘liq bo‘lib, bu o‘z navbatida jinoyat subyektini aniqlashni qiyinlashtiradi, harakatlarning bir zumda tarqalishiga va avtomatlashuviga sabab bo‘ladi. Shakllarning doimiy o‘zgarib borishi va subyektlar tarkibining kengayishi (“Crime-as-a-Service” modelini ham qo‘shganda) jinoyatni huquqiy jihatdan tavsiflashda qiyinchiliklar tug‘diradi va qonunchilik rivojidan o‘zib ketadigan aralash tarkiblarning shakllanishiga olib keladi.

3. Muallif JKning 278^4-moddasi JKning 278^5-moddasida nazarda tutilgan jinoyat unsurlarini qamrab olishini asoslab beradi. Kompyuter axborotini o‘zgartirish jinoyati tarkibiga kompyuter sabotaji harakati ham kirganligi sababli, ularni bitta moddaga birlashtirish maqsadga muvofiqligi asoslantirilgan.

II. Qonunchilikni takomillashtirish bo‘yicha taklif va tavsiyalar:

1. JKning “Oilaga, yoshlarga va axloqqa qarshi jinoyatlar” nomli V bobini voyaga yetmagan shaxsni axborot-kommunikatsiya tarmoqlari orqali jinsiy xarakterdagi harakatlarga jalb qilish (onlayn-gruming) uchun javobgarlikni nazarda tutuvchi 127²-modda bilan to‘ldirish va ularni quyidagi tahrirda bayon etish taklif qilinadi:

“127²-modda. Voyaga yetmagan shaxsni axborot-kommunikatsiya tarmoqlari orqali jinsiy xarakterdagi harakatlarga jalb qilish (onlayn-gruming)

“Voyaga yetmagan shaxsni aloqa vositalaridan foydalangan holda jinsiy xarakterdagi harakatlarni sodir etishga yoki muhokama qilishga undash, shu maqsadda uchrashuv tashkil etish yoki unga tayyorgarlik ko‘rish, intim xarakterdagi foto, video yoki boshqa materiallarni talab qilish, so‘rash yoxud olishga urinish –

bazaviy hisoblash miqdorining yuz baravaridan ikki yuz baravarigacha miqdorda jarima yoki uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) takroran;

b) bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilgan bo‘lsa;

v) yashirin yoki anonim usullardan foydalanib sodir etilgan bo‘lsa;

g) moddiy manfaat evaziga yoxud tovlamachilik bilan bog‘liq holda sodir etilgan bo‘lsa,–

majburiy jamoat ishlari yoki uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu moddaning birinchi yoki ikkinchi qismida nazarda tutilgan qilmishlar boshqa og‘ir oqibatlarga sabab bo‘lsa, –

besh yildan sakkiz yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

2. JKning “Fuqarolarning konstitutsiyaviy huquq va erkinliklariga qarshi jinoyatlar” nomli VII bobini shaxsni ta’qib qilish (stalking) va kiberzo‘ravonlik uchun javobgarlikni nazarda tutuvchi 141⁴-modda bilan to‘ldirish va ularni quyidagi tahrirda bayon etish taklif qilinadi:

“141⁴-modda. Shaxsni ta’qib qilish (stalking)

Shaxsni uning irodasiga xilof ravishda muntazam kuzatish, uni ta’qib qilish, u bilan bevosita yoki bilvosita aloqa o‘rnatishga urinish, shuningdek, aloqa vositalaridan foydalanib, bezovta qilish, kamsitish, ruhiy bosim o‘tkazishda ifodalanadigan harakatlarni yoxud uning yoki yaqinlarining xavfsizligi, sog‘lig‘i uchun xavotir uyg‘otadigan boshqa harakatlarni sodir etish –

bazaviy hisoblash miqdorining yuz baravaridan bir yuz ellik baravarigacha miqdorda jarima yoki ikki yilgacha axloq tuzatish ishlari bilan jazolanadi.

Ushbu harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilgan bo‘lsa;

b) takroran;

v) g‘arazgo‘ylik yoki boshqa pastkash niyatlarda sodir etilgan bo‘lsa;

g) xizmat mavqeyidan foydalanib sodir etilgan bo‘lsa;

d) voyaga yetmagan shaxsga yoxud homiladorligi aybdorga ayon bo‘lgan ayolga nisbatan sodir etilgan bo‘lsa, –

bazaviy hisoblash miqdorining bir yuz ellik baravaridan ikki yuz baravarigacha miqdorda jarima yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu moddaning birinchi yoki ikkinchi qismida nazarda tutilgan qilmishlar boshqa og‘ir oqibatlarga sabab bo‘lsa, –

uch yildan besh yilgacha ozodlikni cheklash yoxud uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

3. JKni “Kiberjinoyatlar” nomli VI[1] bo‘lim bilan to‘ldirish hamda unga “Axborot-kommunikatsiya texnologiyalariga qarshi jinoyatlar” nomli XX[1] bob va “Axborot-kommunikatsiya texnologiyalari sohasidagi jinoyatlar” nomli XX[2] bobni kiritish orqali o‘zgartirishlar kiritish taklif etilmoqda;

4. JKning “Axborot-kommunikatsiya texnologiyalariga qarshi jinoyatlar” nomli XX[1] bobini 278[1], 278[2], 278[3]-moddalar bilan to‘ldirish va ularni quyidagi tahrirda bayon etish taklif etilmoqda:

“278[1]-modda. Raqamli axborotni egallash

Raqamli axborotni qasddan egallash fuqarolarning huquqlari yoki qonun bilan muhofaza qilinadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoxud jiddiy ziyon yetkazishga sabab bo‘lsa, –

bazaviy hisoblash miqdorining uch yuz baravaridan olti yuz baravarigacha miqdorda jarima yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

“278[2]-modda. Raqamli axborotni berishga majburlash

Zo‘rlik ishlatish yoxud mol-mulkni yo‘q qilish yoki unga shikast yetkazish tahdidi ostida, shuningdek jabrlanuvchini yoki uning yaqinlarini sharmanda qiladigan ma’lumotlarni yoxud oshkor etilishi jabrlanuvchining yoki uning yaqinlarining manfaatlariga jiddiy zarar yetkazishi mumkin bo‘lgan boshqa ma’lumotlarni tarqatish tahdidi bilan elektron tashuvchida saqlanayotgan, qonun bilan muhofaza qilinadigan raqamli axborotni berishga majburlash –

bazaviy hisoblash miqdorining uch yuz baravaridan olti yuz baravarigacha miqdorda jarima yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

“278[3]-modda. Foydalanishi cheklangan elektron axborot resurslarini qonunga xilof ravishda tarqatish

Fuqarolarning shaxsga doir ma’lumotlarini yoxud O‘zbekiston Respublikasi qonunlari bilan foydalanishi cheklangan boshqa ma’lumotlarni o‘z ichiga olgan elektron axborot resurslarini qonunga xilof ravishda tarqatish, –

bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoxud ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib;

b) g‘arazgo‘ylik niyatlarda;

v) shaxs tomonidan o‘z mansab mavqeyidan foydalanib sodir etilgan bo‘lsa, –

bazaviy hisoblash miqdorining ikki yuz baravaridan uch yuz baravarigacha miqdorda jarima yoxud uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu moddaning birinchi yoki ikkinchi qismlarida nazarda tutilgan harakatlar:

a) jinoiy guruh tomonidan sodir etilgan bo‘lsa;

b) og‘ir oqibatlarga olib kelgan bo‘lsa, –

uch yildan yetti yilgacha muddatga ozodlikdan mahrum qilish bilan jazolanadi”.

5. JKdan 278[5]-moddani (“Kompyuter sabotaji”) chiqarib tashlash va JKning 278[4]-moddasini quyidagi tahrirda bayon etish taklif qilinadi:

“278[4]-modda. Kompyuter axborotini qonunga xilof ravishda yo‘q qilish, to‘sish yoki o‘zgartirish

Kompyuter axborotini qasddan yo‘q qilish, to‘sish yoki o‘zgartirish, uni yaroqsiz holga keltirish yoki kompyuter texnikasini ishdan chiqarish, kompyuter tizimi va uning tarmoqlari ishini buzish, shuningdek, unga bila turib yolg‘on axborot kiritish kompyuter ishining buzilishiga olib kelib, fuqarolarning huquqlari yoki qonun bilan qo‘riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoki jiddiy ziyon yetkazsa, –

bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoki ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) juda ko‘p miqdorda zarar yetkazgan holda;

b) bir guruh shaxslar tomonidan oldindan til biriktirib;

v) takroran sodir etilgan bo‘lsa, –

ikki yilgacha ish haqidan ushlab qolish yoxud ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

6. JKning XX[2] bobi “Axborot-kommunikatsiya texnologiyalari sohasidagi jinoyatlar”ni 278[5], 278[6], 278[7], 278[8], 278[9], 278[10], 278[11], 278[12]-moddalar bilan to‘ldirish va quyidagi tahrirda bayon etish taklif qilinadi:

“278[5]-modda. Axborot resurslaridan foydalanish qoidalarini buzish, ya’ni axborot tizimlari, ma’lumotlar bazalari va banklarini ularni himoya qilish bo‘yicha belgilangan choralarni ko‘rmasdan yaratish, joriy etish va ulardan foydalanish, bunday harakatlar ulardan foydalanish huquqiga ega bo‘lgan shaxs tomonidan sodir etilib, fuqarolarning huquqlari yoki qonun bilan qo‘riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoki jiddiy ziyon yetkazishga sabab bo‘lsa, -

bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari bilan jazolanadi.

O‘sha harakatlar juda ko‘p miqdorda zarar yetkazgan holda sodir etilsa, —

bazaviy hisoblash miqdorining ellik baravaridan yuz baravarigacha miqdorda jarima yoxud olti oygacha ozodlikni cheklash bilan jazolanadi”.

“278[6]-modda. Kompyuter axborotiga g‘ayriqonuniy (ruxsatsiz) kirish

Kompyuter axborotiga, ya’ni kompyuterda yoki **ma’lumotlarga ishlov berishning boshqa qurilmalarida** joylashgan axborotga g‘ayriqonuniy (ruxsatsiz) kirish, agar bu harakat axborotning yo‘q qilinishiga, bloklanishiga, undan nusxa ko‘chirilishiga yoxud egallab olinishiga, hisoblash texnikasi vositalarining normal ishlashi buzilishiga sabab bo‘lsa, —

bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoki bir yilgacha muddatga ish haqidan ushlab qolish bilan jazolanadi.

Ushbu harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib;

b) takroran;

v) mansab mavqeyidan foydalanib;

g) uyushgan jinoiy guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilsa, –

bazaviy hisoblash miqdorining yuz baravaridan ikki yuz baravarigacha miqdorda jarima yoki uch yilgacha ozodlikni cheklash bilan jazolanadi”.

“278[7]-modda. Axborot resurslariga g‘ayriqonuniy (ruxsatsiz) kirish uchun maxsus vositalarni sotish maqsadida tayyorlash yoxud sotish, ulardan foydalanish yoki ularni tarqatish

Axborot resurslariga g‘ayriqonuniy (ruxsatsiz) kirish uchun maxsus dasturiy yoki apparat vositalarini sotish maqsadida tayyorlash yoxud sotish, ulardan **foydalanish yoki ularni tarqatish,** –

bazaviy hisoblash miqdorining ikki yuz baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari bilan jazolanadi.

Ushbu harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib;

b) takroran;

v) mansab mavqeyidan foydalanib;

g) uyushgan guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilsa, —

bazaviy hisoblash miqdorining ikki yuz baravaridan uch yuz baravarigacha miqdorda jarima yoki bir yildan uch yilgacha axloq tuzatish ishlari bilan jazolanadi”.

“278[8]-modda. Zararli dasturiy yoki apparat vositalarini yaratish, ulardan foydalanish yoki ularni tarqatish

Axborot tizimida saqlanayotgan yoki uzatilayotgan axborotni ruxsatsiz yo‘q qilish, bloklash, o‘zgartirish, undan nusxa ko‘chirish yoki uni egallab olish, uskunani ishdan chiqarish maqsadida dasturiy yoki apparat vositalarini yaratish yoxud mavjud dasturlar yoki dasturiy mahsulotlarga o‘zgartirishlar kiritish, shuningdek, shu maqsadlarda maxsus virusli dasturlarni ishlab chiqish, ulardan qasddan foydalanish yoki ularni tarqatish–

bazaviy hisoblash miqdorining yuz baravaridan uch yuz baravarigacha miqdorda jarima yoxud ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) juda ko‘p miqdorda zarar yetkazgan holda;

b) bir guruh shaxslar tomonidan oldindan til biriktirib;

v) takroran;

g) uyushgan **jinoiy** guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilsa, –

ikki yildan uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

“278[9]-modda. Telekommunikatsiya tarmog‘iga g‘ayriqonuniy (ruxsatsiz) kirish

Telekommunikatsiya tarmog‘iga belgilangan himoya tizimlarini chetlab o‘tgan holda undan foydalanish va xalqaro trafikni o‘tkazish maqsadida g‘ayriqonuniy (ruxsatsiz) kirish, shuningdek, shu maqsadlar uchun mo‘ljallangan maxsus dasturiy yoki apparat vositalarini saqlash, **tarqatish** va ularning ishlashi uchun sharoit

yaratish, –

bazaviy hisoblash miqdorining yuz baravaridan uch yuz baravarigacha miqdorda jarima yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) bir guruh shaxslar tomonidan oldindan til biriktirib;

b) takroran;

v) mansab mavqeyidan foydalanib;

g) uyushgan **jinoiy** guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilsa, –

bazaviy hisoblash miqdorining ikki yuz baravaridan to‘rt yuz baravarigacha miqdorda jarima yoxud uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

“278[10]-modda. Kripto aktivlar aylanmasi sohasidagi qonunchilikni buzish

Kripto aktivlarni g‘ayriqonuniy olish, sotish yoki ayirboshlash, belgilangan tartibda litsenziya olmasdan kripto aktivlar aylanmasi sohasidagi xizmatlar provayderlari faoliyatini amalga oshirish, xuddi shunday harakatlar uchun ma’muriy jazo qo‘llanilganidan keyin sodir etilsa, –

bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoxud bir yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) takroran;

b) ko‘p miqdorda;

v) bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilsa, –

bazaviy hisoblash miqdorining uch yuz baravaridan to‘rt yuz baravarigacha miqdorda jarima yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu harakatlar:

a) juda ko‘p miqdorda;

b) mansab mavqeyidan foydalanib;

v) uyushgan jinoiy guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilsa, –

uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

“278[11]-modda. Mayning faoliyatini noqonuniy amalga oshirish

Bunday harakatlar uchun ma’muriy jazo qo‘llanilganidan keyin anonim kripto aktivlar mayningi bilan shug‘ullanish yoki mayningni belgilangan tartibni buzgan holda amalga oshirish –

bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoxud bir yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Yashirin mayningni amalga oshirish–

bazaviy hisoblash miqdorining yuz baravaridan uch yuz baravarigacha miqdorda jarima yoki ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu moddaning birinchi yoki ikkinchi qismida nazarda tutilgan harakatlarning:

a) takroran;

b) juda ko‘p miqdorda;

v) bir guruh shaxslar tomonidan oldindan til biriktirib sodir etilishi —

bazaviy hisoblash miqdorining uch yuz baravaridan to‘rt yuz baravarigacha miqdorda jarima yoxud uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

Ushbu moddaning birinchi yoki ikkinchi qismida nazarda tutilgan harakatlarning:

a) xizmat mavqeidan foydalangan holda;

b) uyushgan jinoiy guruh tomonidan yoki uning manfaatlarini ko‘zlab sodir etilishi –

uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

“278[12]-modda. Internet jahon axborot tarmog‘ida umumfoydalanishdagi axborotni tarqatish qoidalarini buzish

Internet jahon axborot tarmog‘ida umumfoydalanishdagi axborotni tarqatish qoidalarini qasddan buzish orqali fuqarolarning huquqlariga yoki qonun bilan qo‘riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoki jiddiy ziyon yetkazish –

bazaviy hisoblash miqdorining uch yuz baravaridan olti yuz baravarigacha miqdorda jarima yoxud uch yildan besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi”.

7. JKning VIII bo‘limini quyidagi mazmundagi atamalar bilan to‘ldirish taklif etiladi:

“Kiberjinoyat – axborot texnologiyalari, kompyuter dasturlari, kompyuter tarmoqlari ishiga aybli ravishda noqonuniy aralashish, kompyuter ma’lumotlarini ruxsatsiz o‘zgartirish, shuningdek, kompyuterlar, kompyuter tarmoqlari va dasturlari yordamida yoki ular vositasida, axborot-kommunikatsiya texnologiyalari yordamida modellashtirilgan axborot makoniga kirishning boshqa qurilmalari yordamida yoki ular vositasida sodir etiladigan boshqa ijtimoiy xavfli noqonuniy qilmishlardir”.

“Kiberjinoyatchilik – axborot-kommunikatsiya texnologiyalari sohasidagi yoki ulardan foydalangan holda sodir etiladigan jinoyatchilik, shuningdek, axborot makonida yoki unga qarshi sodir etiladigan, shaxs, jamiyat va davlatga tahdid soladigan jinoyatlardir”.

“Kompyuter – axborotni avtomatlashtirilgan tarzda qayta ishlaydigan har qanday qurilmadir”.

“Kompyuter tizimi – axborot hamda uni qayta ishlashni ta’minlovchi dasturiy, kompyuter va texnik vositalardir”.

III. Kiberhuquqbuzarliklarning kriminologik jihatlarini takomillashtirish va ularning oldini olishga qaratilgan taklif va tavsiyalar:

1. Raqamli tahdidlarni monitoring qilish, o‘ta muhim sohalardagi axborot tizimlari va xodimlarni majburiy sertifikatlash, axborotlashtirish to‘g‘risidagi milliy qonunchilikka xalqaro normalarni implementatsiya qilish, shuningdek, ta’lim dasturlari va mijozlarni kiberxatarlar haqida muntazam xabardor qilish orqali aholining raqamli savodxonligini oshirishni nazarda tutuvchi **Kiberjinoyatchilikning oldini olish bo‘yicha davlat strategiyasini** ishlab chiqish taklif etiladi;

2. **Maktablar (8–11-sinflar), kollejlar va oliy ta’lim muassasalarida “Kibergigiyena va raqamli xavfsizlik” majburiy kurs**ini joriy etgan holda,

internet madaniyatini shakllantirish bo‘yicha davlat dasturini yaratish;

3. **Xavf darajasi yuqori bo‘lgan guruhlarga yo‘naltirilgan** kampaniyalar orqali **viktimologik profilaktikani amalga oshirish** taklif etiladi: pensionerlar (“bank”dan kelayotgan soxta qo‘ng‘iroqlar), yoshlar (psevdo-treyding, onlayn-kazino), tadbirkorlar (BEC-hujumlar, qalbaki hisobvaraqlar);

4. Potensial **huquqbuzarlarni dastlabki bosqichda aniqlash (profiling) tizimini yaratish,** o‘zbek va rus tillaridagi xakerlik forumlari, Telegram/Discord chatlarini monitoring qilish, huquqbuzarlik sodir etgani aniqlangan voyaga yetmaganlarning og‘irroq jinoyatlarga o‘tishiga yo‘l qo‘ymaslik maqsadida ular bilan profilaktik ishlar olib borish;

5. **Quyi bo‘g‘indagi ishlar uchun mahalla infratuzilmasi va profilaktika inspektorlaridan foydalanish** taklif etiladi: tushuntirish yig‘inlari, eslatmalar, ilgari firibgarlik qurboni bo‘lgan shaxslar bilan individual ishlash (takroriy viktimizatsiya – barqaror hodisa);

6. **Ixtisoslashtirilgan huquqni muhofaza qiluvchi bo‘linmalarni kuchaytirish** doirasida IIV, DXX, Bosh prokuratura va Markaziy bank Kiberxavfsizlik markazlari negizida doimiy tarkibga, umumiy bayonnomalarga ega bo‘lgan hamda **Markaziy bankning firibgarlikka qarshi kurashish (antifrod)** tizimidan foydalana oladigan yagona idoralararo **tezkor shtabni tashkil etish** taklif etiladi;

7. IIV Akademiyasi va TDYUda “**Kiberjinoyatchilik kriminologiyasi va raqamli kriminalistika”** magistratura yo‘nalishini ochish hamda **tergovchi va tezkor xodimlarni** har yili 72 soatlik dastur bo‘yicha majburiy **qayta tayyorlovdan o‘tkazish**ni joriy etish;

8. Mobil qurilmalardan ma’lumotlarni chiqarib olish, kriptohamyonlarni tahlil qilish va dipfeyklar bilan ishlash uchun uskunalar bilan jihozlangan **hududiy mobil raqamli kriminalistika guruhlari**ni (har bir viloyatga kamida bittadan) tashkil etish;

9. **O‘rta bo‘g‘in sudlarida** jinoyat ishlari bo‘yicha sudyalarni **AKT sohasiga ixtisoslashtirish**ni joriy etish;

10. **Viktimologik yo‘nalish** va **kompensatsiya mexanizmlari doirasida,** agar mijozning qo‘pol ehtiyotsizligi isbotlanmagan bo‘lsa, kartadan pul o‘g‘irlanganda bankning **javobgarligi prezumpsiyasini qonunchilikda mustahkamlash** taklif etiladi (Yevropa Ittifoqining PSD2 modeli asosida);

11. Moliyaviy tashkilotlarning ajratmalari hamda kiberxavfsizlikni buzishga oid ishlar bo‘yicha undirilgan jarimalar hisobidan **Kiberjinoyatlardan yetkazilgan zararni qoplash jamg‘armasi**ni tashkil etish;

12. 102 qisqa raqamiga murojaat qilingan vaqtdan boshlab oluvchilarning hisobvaraqlaridagi mablag‘larni “**muzlatish” muddatini 2 soatgacha qisqartirish;**

13. **Majburiy viktimologik ko‘mak**ni joriy etish: yirik firibgarlik qurbonlariga, ayniqsa, keksa yoshdagi fuqarolarga psixologik yordam ko‘rsatish;

14. **“Kulrang hudud”ni – “dropper” hisobvaraqlari, SIM-kartalar, kriptoaktivlarni tartibga solish** bo‘yicha hisobvaraq ochish va SIM-karta ro‘yxatdan o‘tkazishni avtomatik cheklovchi “dropper” shaxslarning ommaviy-

xususiy **Yagona reyestrini yaratish** taklif etiladi;

15. Litsenziyalangan birjalarda kriptotransaksiyalarning foyda oluvchi egasini **majburiy identifikatsiya qilish**ni (FATFning Travel Rule qoidasi) joriy etish va bunday mablag‘larni naqdlashtirganlik uchun **sanksiyalar qo‘llash;**

16. Kriminologik monitoringning texnologik va tahliliy vositalari doirasida **yagona statistikani yuritish** (hozirda IIV, MB va Bosh prokuratura ma’lumotlari bir-biridan farq qiladi), ijtimoiy tarmoqlardagi xabarlar va fuqarolar murojaatlarini sun’iy intellekt yordamida tahlil qilish asosida trendlarni prognozlash, har choraklik kriminologik byulletenlarni nashr etish uchun Xavfsizlik kengashi huzurida **Milliy kiberxavfsizlik kriminologik markazini tashkil etish** taklif etiladi;

17. Banklar uchun **prediktiv (bashorat qiluvchi) tahlil tizimini joriy** etish: pul o‘g‘irlanishidan avval noodatiy tranzaksiya andozalarini aniqlash uchun mashinaviy ta’lim modellarini qo‘llash;

18. “**Oq xakerlar” faoliyatini qonuniylashtirish** va yashirin sektorga mutaxassislar oqimini kamaytirish uchun davlat elektron platformasida **“Bug Bounty” dasturini ishga tushirish;**

19. Xalqaro hamkorlik va transchegaraviy tergov sohasida Yevropa Kengashining Kiberjinoyatchilik to‘g‘risidagi **Budapesht konvensiyasiga qo‘shilishni tezlashtirish** taklif etiladi;

20. Rossiya Federatsiyasi, XXR, BAA, Turkiya va Qozog‘iston bilan tezkor ma’lumotlar almashinuvi to‘g‘risida ikki tomonlama **bitimlar tuzish;**

21. Bosh prokuratura huzurida xorijiy provayderlardan ma’lumotlarni saqlab qolish bo‘yicha shoshilinch so‘rovlar uchun **24/7 rejimida ishlovchi aloqa punktini (G7 24/7 Network modeli asosida) tashkil etish;**

22. “Cyber Security Summit – Central Eurasia” (Markaziy Yevroosiyo Kiberxavfsizlik Sammiti) tashabbuslarida hamda **KXShT/SHHTning zararli kod namunalarini almashish bo‘yicha faoliyatida faol ishtirok etish;**

23. Ilmiy-tadqiqot va kadrlar ta’minoti doirasida **kiberjinoyatchi tipologiyasi, jabrlanuvchi portreti, sanksiyalar samaradorligi, moliyaviy xizmatlarni raqamlashtirishning viktimizatsiyaga ta’siri kabi mavzularda** kriminologik tadqiqotlar uchun **davlat buyurtmasini shakllantirish** taklif etiladi;

24. TDYU yoki Bosh prokuratura Akademiyasi negizida “**Raqamli muhit kriminologiyasi”** mutaxassisligi bo‘yicha **dissertatsiya kengashini tashkil etish;**

25. Milliy hisobotni (Yevropolning IOCTA hisobotiga o‘xshash) e’lon qilib boradigan har yilgi kiberjinoyatchilikka bag‘ishlangan **kriminologik forumni ta’sis etish.**

НАУЧНЫЙ СОВЕТ DSc.07/2025.27.12.Yu.01.04 ПОПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСТКОМ ГОСУДАРСТВЕННОМ ЮРИДИЧЕСКОМ УНИВЕРСИТЕТЕ

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ

ДУСМАТОВ ДУРБЕК РУСТАМЖОН УГЛИ

УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

12.00.08 – Уголовное право. Уголовно-исполнительное право.
12.00.15 – Криминология

АВТОРЕФЕРАТ
диссертации доктора философии (PhD) по юридическим наукам

Ташкент - 2026

Тема диссертации доктор философии по юридическим наукам (PhD) зарегистрирована Высшей аттестационной комиссии при академии наук Республики Узбекистан за №B B2023.3.PhD/Yu1168.

Диссертация выполнена в Ташкентском государственном юридическом университете.

Автореферат диссертации размещен на трех языках (узбекском, русском, английском (резюме)) на веб-странице Научного совета (https://tsul.uz/uz/fan/avtoreferatlar) и Информационно-образовательном портале ZiyoNet (www.ziyonet.uz).

Научный руководитель:	**Абзалова Хуршида Мирзиятовна** доктор юридических наук, профессор
Официальные оппоненты:	**Расулев Абдулазиз Каримович** доктор юридических наук, профессор
	Камалова Дилдора Гайратовна доктор юридических наук, профессор
Ведущая организация:	**Академия Министерства внутренних дел Республики Узбекистан**

Защита диссертации состоится 7 августа 2026 года в 14^{30} часов на заседании Научного совета Ds.07/2025.27.12.Yu.01.04 при Ташкентском государственном юридическом университете. (Адрес: 100047, г. Ташкент, ул. Сайилгох, 35. Тел.: +998 71 233-66-36; факс: +9989 71 233-37-48; e-mail: info@tsul.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского государственного юридического университета (зарегистрирована за №343.9), (Адрес: 100047, г. Ташкент, ул. А.Темура, 13. Тел.: +998 71 233-66-36.

Автореферат диссертации разослан 22 июля 2026 года.
(Протокол реестра № 6 от 22 июля 2026 года).

Р.А. Зуфаров
Председатель Научного совета по присуждению ученых степеней, доктор юридических наук, профессор

Н.К. Ходжиев
Секретарь Научного совета по присуждению ученых степеней, доктор философии по юридическим наукам, и.о доцента

Ш.Дж. Хайдаров
Председатель Научного семинара при Научном совете по присуждению ученых степеней, доктор юридических наук, профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и востребованность темы диссертации.

В мире в условиях ускоряющейся цифровизации экономики киберпреступность приобретает характер одной из ключевых глобальных угроз устойчивому развитию организаций и государств. По оценке Cybersecurity Ventures, совокупный мировой ущерб от киберпреступности в 2024 году достигла 9,5 трлн долл. США, а в 2025 году – 10,5 трлн долл. США. Значимость проблемы усиливается вследствие расширения цифровой поверхности атаки, обусловленного ростом облачных технологий, удалённых сервисов, Интернета вещей и объёмов данных. Особую опасность представляют программы-вымогатели, ущерб от которых в 2024 году оценивается в 42 млрд долл. США с прогнозом увеличения до 265 млрд долл. США к 2031 году. Дополнительным фактором риска выступает сохраняющийся глобальный дефицит кадров в сфере кибербезопасности, достигающий 3,5 млн незакрытых вакансий. Указанные обстоятельства подтверждают высокую научную и практическую актуальность исследований, направленных на разработку эффективных механизмов обеспечения киберустойчивости организаций[1].

В концептуальном плане уголовно-правовые и криминологические аспекты противодействия киберпреступности в мире формируются под воздействием фундаментальных тенденций глобального развития. Современный этап развития человечества характеризуется беспрецедентной цифровой трансформацией всех сфер общественной жизни – от экономики и государственного управления до частной коммуникации и социальных отношений. Формирование глобального киберпространства как принципиально нового измерения социального бытия сопровождается качественным преобразованием феноменологии преступности: возникает самостоятельный род общественно опасных деяний – киберпреступность, обладающая уникальными онтологическими свойствами, которые не укладываются в классические уголовно-правовые и криминологические конструкции, сформированные в индустриальную эпоху.

Республика Узбекистан, активно внедряя информационно-коммуникационные технологии (ИКТ) в систему государственного управления, экономику, банковскую сферу, образование и здравоохранение, одновременно сталкивается с ростом преступлений, совершаемых с использованием компьютерных систем и сетей. Данные Министерства внутренних дел республики свидетельствуют о постоянном росте преступлений в цифровой среде. Только в 2023 году органами правопорядка зарегистрировано более 8 тысяч киберпреступных деяний, среди которых – фишинговые схемы, компьютерные взломы, онлайн-мошенничество, неавторизованный доступ к информационным ресурсам и распространение вирусного программного обеспечения. При этом уровень раскрываемости

[1] Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024

преступлений остаётся низким, что объясняется как высокой технологической сложностью их расследования, так и недостаточной эффективностью существующего правового регулирования в данной сфере. В стране проводится важная работа по борьбе с киберпреступностью, предпринимаются меры по укреплению правовой базы в сфере кибербезопасности. Тем не менее, уголовно-правовое регулирование в рассматриваемой сфере по-прежнему характеризуется рядом существенных пробелов. В частности, в Уголовном кодексе отсутствует систематизированный подход к квалификации преступлений, совершаемых в киберсреде. Законодательство не учитывает особенности киберпреступлений, связанных с криптоактивами, интернет-мошенничеством, атаками на критическую инфраструктуру. Это, в свою очередь, затрудняет правоприменение, приводит к правовой неопределенности. С криминологической точки зрения, остаются недостаточно исследованными причины и условия, способствующие развитию киберпреступности. До настоящего времени не выработан эффективный механизм её предупреждения, отсутствует комплексная система сбора и анализа статистических данных, а уровень цифровой культуры населения остаётся недостаточным. Комплексное исследование уголовно-правовых и криминологических аспектов киберпреступности, представляет собой востребованное и своевременное научное направление, способствующее укреплению правопорядка в цифровую эпоху и обеспечению информационной безопасности государства.

Настоящее исследование в определенной степени послужит реализации Законов Республики Узбекистан от 12 декабря 2002 года №ЗРУ–439 «О принципах и гарантиях свободы информации», от 15 апреля 2022 г. №ЗРУ-764 «О кибербезопасности», Указов Президента Республики Узбекистан от 3 марта 2026 года №УП–33 «О дополнительных организационно-правовых мерах по усилению защиты прав женщин и детей, а также предотвращению случаев притеснения и насилия в отношении них», от 10 марта 2026 года №УП–38 «Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности», Постановлений Президента Республики Узбекистан от 14 сентября 2019 года №ПП–4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», от 30 апреля 2025 года №ПП–153 «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий», от 5 января 2026 года №ПП–1 «О дополнительных мерах по внедрению целостной системы адресной работы в направлении создания безопасной среды в махаллях республики» и иных актов законодательства в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Данная диссертация выполнена в соответствии с приоритетным направлением развития науки и технологий Республики I. «Формирование системы инновационных идей и путей их

реализации в социальном, правовом, экономическом, культурном, духовно-образовательном развитии информационного общества и демократического государства».

Степень изученности проблемы.

Уголовно-правовые и криминологические аспекты противодействия киберпреступности в Республике Узбекистан до настоящего времени не получили комплексной монографической разработки. Отдельные вопросы охраны информационных отношений, квалификации преступлений в цифровой среде и совершенствования уголовного законодательства исследовались в работах отечественных учёных — М.Х. Рустамбаева, А. Анорбаева, Н.С. Салаева, Х.Р. Очилова, А.К. Расулева, А.С. Турсунова и других, — однако в этих исследованиях не ставилась задача системного пересмотра структуры Особенной части Уголовного кодекса применительно к киберпреступности как самостоятельному виду преступного поведения.

Значительно более разработанной рассматриваемая проблематика является в российской и зарубежной доктрине. Здесь условно можно выделить три исследовательских направления.

Первое направление связано с догматико-уголовно-правовым анализом состава киберпреступлений, вопросами их квалификации и построения специальных уголовно-правовых норм. К нему относятся, в частности, работы И.Р. Бегишева, К.Н. Евдокимова, Т.Л. Тропиной, У.В. Зининой, А.Г. Волеводза, В.Б. Вехова.

Второе направление носит криминологический характер и сосредоточено на изучении личности киберпреступника, детерминант цифровой преступности и механизмов её предупреждения. Соответствующие положения отражены в трудах Т.М. Лопатиной, Д.В. Пучкова, А.С. Камко, А.И. Халиуллина, М.М. Долгиева.

Третье направление имеет международно-правовую и сравнительно-правовую направленность и связано с анализом Конвенции Совета Европы о киберпреступности 2001 г. (далее — Будапештская конвенция), а также национальных моделей имплементации международных стандартов. К этому направлению относятся работы Д.С. Уолла, М. Гудмана, Э.Дж. Эшворта, Н. Журавленко и Л. Шведовой[1].

Указанные исследования заложили доктринальную основу проблематики, однако ни одно из них не учитывает в полном объёме специфики узбекской правовой системы, в том числе действующей структуры Уголовного кодекса Республики Узбекистан, особенностей правоприменительной практики по делам о преступлениях, связанных с ИКТ и криптоактивами, а также социокультурных факторов виктимизации в цифровой среде. Указанные пробелы в научной разработанности темы и определяют исследовательскую задачу настоящей работы.

Связь темы диссертации с планом научно-исследовательских работ высшего образовательного учреждения, в котором выполнена диссертация. Тема исследовательской работы была включена в план научных

[1] Работы данных авторов приведены в разделе диссертации Список использованной литературы.

исследований Ташкентского государственного юридического университета и реализована в рамках приоритетных направлений научных исследований по темам «Проблемы совершенствования Уголовного кодекса Республики Узбекистан и практики его применения», «Проблемы совершенствования борьбы с преступностью в условиях глобализации», «Проблемы реформирования системы наказаний в условиях реформирования судебно-правовой сферы и либерализации уголовного закона».

Цель исследования состоит в разработке предложений и рекомендаций по совершенствованию уголовного законодательства Республики Узбекистан в вопросах квалификации киберпреступлений и формировании криминологического понимания состояния киберпреступности.

Задачи исследования:

Анализ общей характеристики ответственности за киберпреступления;

Исследование генезиса правового регулирования института киберпреступлений;

Анализ объективных и субъективных признаков киберпреступлений;

Исследование ответственности за киберпреступления по уголовному законодательству зарубежных стран;

Исследование вопросов квалификации и отграничения киберпреступлений от иных смежных составов преступления;

Разработка предложений и рекомендаций, направленных на совершенствование уголовного законодательства в сфере ответственности за киберпреступления.

Объектом исследования является система уголовно-правовых отношений, связанных с квалификацией деяний, связанных с киберпреступлениями.

Предметом исследования являются нормативно-правовые акты, регулирующие правоотношения, определяющие ответственность за киберпреступления, правоприменительная практика, законодательство и практика зарубежных стран, концептуальные подходы, научно-теоретические взгляды и правовые категории, существующие в науке уголовного права.

Методы исследования. При проведении исследований использовались такие методы, как исторический, системно-структурный, сравнительно-правовой, логический, социологический, комплексное исследование научных источников, индукция и дедукция, статистический анализ данных, проведение социальных опросов, анализ практики применения закона.

Научная новизна исследования состоит в следующем:

обоснована необходимость криминализации в качестве самостоятельных составов преступлений деяний, связанных с незаконным оборотом криптоактивов, а именно: неправомерного приобретения, реализации или обмена криптоактивов; осуществления деятельности провайдеров услуг в сфере криптоактивов без надлежащего лицензирования; проведения операций с анонимными криптоактивами; осуществления анонимного майнинга криптоактивов либо майнинговой деятельности с нарушением установленного порядка.

обоснована необходимость закрепления в качестве самостоятельного состава административного правонарушения деяний, связанных с нарушением законодательства в сфере оборота криптоактивов, с установлением соразмерных мер административной ответственности, направленных на ужесточение контрольно-надзорных механизмов и предупреждение незаконного использования криптоактивов.

обоснованы доктринальные критерии квалификации мошенничества, совершаемого с использованием информационной системы, в том числе информационно-коммуникационных технологий, по пункту «г» части третьей статьи 168 УК Республики Узбекистан. К таковому отнесено мошенническое хищение имущества, находящегося под контролем финансово-банковских организаций, фондов и иных подобных организаций, совершаемое с использованием средств вычислительной техники, средств связи, планшетов или иных аналогичных технических устройств путём манипуляций, в том числе посредством изменения информации, обрабатываемой в компьютерной системе, хранящейся на соответствующих носителях информации либо передаваемой по сетям передачи информации, а равно посредством внесения в компьютерную систему заведомо ложной информации. Сформулирован критерий отграничения такого мошенничества от хищения, совершённого посредством неправомерного доступа к информационной системе или её использования: при мошенничестве потерпевший, введённый в заблуждение либо находящийся под влиянием злоупотребления доверием, добровольно передаёт имущество или право на него виновному, осознавая, что имущество выходит из его владения. Дополнительно обосновано положение о том, что использование лицом компьютерных технологий для изготовления поддельного документа с целью последующего получения чужого имущества не может быть квалифицировано по пункту «г» части третьей статьи 168 УК Республики Узбекистан.

обоснована необходимость совершенствования мер противодействия киберпреступности, усиления ответственности за правонарушения в данной сфере и развития организационно-правовых механизмов их предупреждения, в том числе посредством закрепления правовых основ использования технологий искусственного интеллекта при создании информационных ресурсов и функционировании информационных систем, а также установления административной ответственности за незаконную обработку персональных данных с применением технологий искусственного интеллекта с внесением соответствующих изменений в часть вторую статьи 46^2 КоАО Республики Узбекистан.

Практическая значимость исследования состоит в следующем:

обосновано предложение о необходимости выработки системного подхода к противодействию киберпреступности, основанного на комплексной модернизации законодательства, улучшении правоприменительной практики, развитии международного сотрудничества и повышении цифровой грамотности населения;

обосновано предложение о необходимости дополнения Главы

VII «Преступления против конституционных прав и свобод граждан» УК Республики Узбекистан «Статьёй 141^4. Преследование лица (сталкинг)».

обосновано предложение о необходимости дополнения Главы V «Преступления против семьи, молодёжи и нравственности» УК Республики Узбекистан «Статьёй 127^2. Вовлечение несовершеннолетнего в действия сексуального характера посредством информационно-коммуникационных сетей (онлайн-груминг)».

обосновано предложение о необходимости введения в УК самостоятельного Раздела 6^1 «Киберпреступления»;

обосновано предложение о необходимости введения в УК отдельной Главы XX^1 «Преступления против информационно-коммуникационных технологий», в состав которой следует включить такие составы, как «Статья 278^1. Завладение цифровой информацией», «Статья 278^2. Принуждение к передаче цифровой информации», «Статья 278^3. Неправомерное распространение электронных информационных ресурсов ограниченного доступа», «Статья 278^4. Незаконное уничтожение, блокировка или модификация компьютерной информации»;

обосновано предложение о необходимости введения в УК отдельной Главы XX^2 «Преступления в сфере информационно-коммуникационных технологий», в состав которой следует включить такие составы, как «Статья 278^5. Нарушение правил информатизации», «Статья 278^6. Незаконный (несанкционированный) доступ к компьютерной информации», «Статья 278^7. Изготовление с целью сбыта либо сбыт, использование или распространение специальных средств для получения незаконного (несанкционированного) доступа к информационным ресурсам», «Статья 278^8. Создание, использование или распространение вредоносных программных или аппаратных средств», «Статья 278^9. Незаконный (несанкционированный) доступ к сети телекоммуникаций», «Статья 278^{10}. Нарушение законодательства в сфере оборота крипто-активов», «Статья 278^{11}. Незаконное осуществление деятельности по майнингу»; «Статья 278^{12}. Нарушение правил распространения общедоступной информации во всемирной информационной сети Интернет»;

обосновано предложение о необходимости введения в Раздел «Правовое значение терминов» понятия «киберпреступление», «киберпреступность», «компьютер», «компьютерная система»;

обосновано предложение о необходимости принятия мер по ужесточению санкций действующих статей отдельных составов уголовно наказуемых преступных деяний, имеющих отношение к преступлениям в сфере ИТ. В частности, дополнить ч. 3 ст. 48^1 УК Республики Узбекистан при назначении ограничения свободы лицу, совершившему киберпреступление, судом возложить на осужденного дополнительное ограничение в виде запрета на пользование соответствующими средствами коммуникаций и технологий.

Достоверность результатов исследования. Результаты исследования сформированы на основе норм национального законодательства, международных документов, опыта ряда зарубежных стран и современной

правоприменительной практики, были практически обоснованы путём обобщения 132 судебных документов (приговоров и постановлений), результатов экспертных социологических исследований, проведённых при участии более 224 учёных-теоретиков и практиков, в том числе дознавателей, следователей, судей, адвокатов и профессоров-преподавателей, а также результатов самостоятельного социологического исследования общественного мнения, проведённого автором в декабре 2025 года методом онлайн-анкетирования по выборке из 155 респондентов (анкета из 23 вопросов, объединённых в три тематических блока: социально-демографическая характеристика и опыт; уровень осведомлённости и виктимизация; оценка действующего законодательства и перспективных мер противодействия)[1], анализа статистических данных Министерства внутренних дел Республики Узбекистан, Верховного суда Республики Узбекистан и Государственного центра кибербезопасности при Службе государственной безопасности Республики Узбекистан за период 2019–2024 года; результаты одобрены компетентными структурами и внедрены в практику.

Научная и практическая значимость результатов исследования.

Научная значимость исследования заключается в том, что разработанные в результате данного исследования правила будут способствовать развитию теории уголовного права, проведению научных исследований в дальнейшем, преподаванию уголовного права в юридических вузах и подготовке методических рекомендаций, а также результат этого исследования служит решению проблем, связанных с установлением ответственности за киберпреступления и ее предупреждением.

Практическая значимость исследования заключается в том, что оно может быть использовано при разработке ряда правил и практических рекомендаций, направленных на установление ответственности за посредничество во взяточничестве и совершенствование практики его предупреждения, при совершенствовании Уголовного кодекса, совершенствовании постановлений Пленума Верховного суда Республики Узбекистан.

Внедрение результатов исследования. На основе результатов исследования теоретических и практических аспектов противодействия киберпреступности:

предложения, направленные на криминализацию деяний в сфере незаконного оборота криптоактивов, использованы при разработке статей 278^8 и 278^9 проекта Уголовного кодекса Республики Узбекистан. В частности, учтены: предложение о включении нормы, предусматривающей ответственность за неправомерное приобретение, реализацию или обмен криптоактивов, а также за деятельность провайдеров услуг в сфере криптоактивов без надлежащего лицензирования и за проведение операций с анонимными криптоактивами (статья 278^8); предложение о криминализации анонимного майнинга криптоактивов и осуществления майнинговой деятельности с нарушением установленного порядка (статья 278^9). Принятие

[1] Полные результаты авторского социологического исследования, включая текст анкеты, сводные таблицы распределения ответов и графические диаграммы, представлены в Приложении № 5 к настоящей диссертации.

указанных предложений направлено на усиление уголовной ответственности за нарушения законодательства в сфере оборота криптоактивов и незаконную майнинговую деятельность (акты Генеральной прокуратуры Республики Узбекистан от 5 июля 2025 года № 27/2-146-25 и от 18 июня 2025 года № 5-108416-25);

предложения об установлении административной ответственности за нарушение законодательства в сфере оборота криптоактивов использованы при разработке частей 1 и 2 статьи 155^4 проекта Кодекса Республики Узбекистан об административной ответственности. Представленная инициатива нацелена на ужесточение контрольно-надзорных механизмов и установление санкций за деяния, связанные с незаконным использованием криптоактивов (акт Службы государственной безопасности Республики Узбекистан от 26 июня 2025 года № 17/01-34);

рекомендации учтены при подготовке Постановления Пленума Верховного суда Республики Узбекистан от 23 июня 2023 года № 17 «О судебной практике по делам о мошенничестве». В частности, приняты во внимание предложения, касающиеся пункта 22 указанного Постановления, в части квалификации мошенничества, совершаемого с использованием информационной системы, в том числе информационно-коммуникационных технологий, разграничения такого мошенничества с хищением, совершённым посредством неправомерного доступа к информационной системе, а также положения о том, что использование лицом компьютерных технологий для изготовления поддельного документа с целью последующего получения чужого имущества не может быть квалифицировано по пункту «г» части третьей статьи 168 Уголовного кодекса Республики Узбекистан (акт Верховного суда Республики Узбекистан от 28 мая 2025 года № 08/225-25);

предложения, подготовленные по результатам исследования, использованы при разработке Постановления Президента Республики Узбекистан от 30 апреля 2025 года № 153 «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с использованием информационных технологий» – в части совершенствования мер противодействия киберпреступности, усиления ответственности за правонарушения в данной сфере и развития организационно-правовых механизмов предупреждения киберпреступлений, – а также при разработке Закона Республики Узбекистан от 21 января 2026 года № 1115 «О внесении дополнений и изменений в некоторые законодательные акты Республики Узбекистан в связи с регулированием отношений, возникающих при применении искусственного интеллекта». В частности, учтены предложения соискателя при формулировании пункта 4 статьи 1 указанного Закона в части закрепления правовых основ использования искусственного интеллекта при создании информационных ресурсов и функционировании информационных систем, а также статьи 2 названного Закона в части установления административной ответственности за незаконную обработку персональных данных с использованием технологий искусственного интеллекта и внесения соответствующих изменений в часть

вторую статьи 46² Кодекса Республики Узбекистан об административной ответственности (акты Главного управления внутренних дел города Ташкента Министерства внутренних дел Республики Узбекистан от 28 апреля 2026 года № 27/3-1345/4к и № 27/3-1345/5к).

Апробация результатов исследования. Результаты данного исследования обсуждались на 10 научных конференциях, в том числе на 8 международных, 2 республиканских научно-практических конференциях.

Опубликование результатов исследования. По теме диссертации опубликовано 20 научных работ, в том числе 6 научных стаей в зарубежных изданиях, 6 научных статей в республиканских журналах, 8 тезиса.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 158 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** диссертации (аннотация диссертации доктора философии (PhD)) освещены актуальность и востребованность темы исследования, связь исследовательской работы с основными приоритетными направлениями развития науки и технологии республики, степень изученности исследуемой проблемы, связь темы диссертации с научно-исследовательскими работами высшего учебного заведения, где выполняется диссертация, цели и задачи исследования, объект и предмет, методы, научная новизна и практический результат исследования, достоверность результатов исследования, научное и практическое значение результатов исследования, их внедрение, апробация результатов исследования, опубликованность результатов, структура и объём диссертации.

В первой главе диссертации, посвящённой «**Общей характеристике ответственности за киберпреступления и зарубежному опыту противодействия киберпреступности»,** исследователем комплексно раскрывается социально-правовая природа киберпреступности как самостоятельного феномена уголовно-правовой охраны, в которой проведён ретроспективный анализ становления института уголовной ответственности за киберпреступления в Республике Узбекистан, а также осуществлён детальный сравнительно-правовой анализ уголовного законодательства ведущих государств мира.

В данной главе изучены взгляды таких ученых, как М.Х. Рустамбаев, Н.С. Салаев, Х.Р. Очилов, А.К. Расулев, А.С. Турсунов, Т.Л. Тропиной, Т.М. Лопатиной, К.Н. Евдокимова, О.А. Зигмунт, У.В. Зининой, А.М. Тарасова, Л.П. Шматковой, А.Н. Третьякова, Д.В. Пучкова, Г. Янке, Н.И. Журавленко и Л.Е. Шведовой, A.J. Ashworth, D.S. Wall, S. Brenner, M. Goodman, R.M. Kowalski и других ученых и использованы в качестве доктринальной опоры при исследовании составов хищений с использованием компьютерных средств, уголовно-правовых мер противодействия киберпреступности и криминологической характеристики, вопросах

международно-правового и сравнительно-правового измерения, юридической конструкции мошенничества в её международном измерении, проанализированы доктринальные и криминологические аспекты природы киберпреступности.

Автором проведён комплексный доктринальный анализ действующих норм Уголовного кодекса Республики Узбекистан, регулирующих ответственность за деяния в сфере информационно-коммуникационных технологий, – в частности, статей 278^{1}–278^{7} главы XX^{1} Уголовного кодекса. Исследователь предпринимает системное деление киберпреступлений на три категории: «чисто компьютерные» (cyber-dependent) то есть деяния, посягающие непосредственно на компьютерные системы; «инструментальные» (cyber-enabled) традиционные преступления, трансформированные цифровыми технологиями и «вспомогательные» (cyber-assisted) деяния, где цифровая среда служит лишь коммуникативным каналом. С позиции автора «эволюционно-редакционный» подход исчерпал свой ресурс: он приводит к нагромождению отсылочных норм, порождает конкуренцию составов и оставляет за пределами уголовно-правовой охраны целые категории общественно опасных деяний. Соискатель категорически не разделяет подход о парадигме традиционных имущественных посягательств, отягощённых техническим фактором, и доказывает, что сущностные признаки киберпреступности – нематериальный характер объекта посягательства, экстратерриториальность, автоматизация исполнения, специальная квалификация субъекта, латентность в диапазоне 85–95 процентов – образуют качественно новый уголовно-правовой феномен, требующий выделения в самостоятельный раздел Уголовного кодекса. Автор существенно развивает концепции применительно к условиям правовой системы Республики Узбекистан.

Более того, автором в результате проведённого ретроспективного анализа периодизируется становление института уголовной ответственности за киберпреступления в Республике Узбекистан, выделив их в три этапа. Доинституциональный (1994–2007 гг.) – эпоха отсутствия специальных уголовно-правовых норм, когда киберпосягательства квалифицировались по общим статьям Уголовного кодекса, этап становления (2007–2022 гг.) то есть введение главы XX^{1} «Преступления в сфере информационных технологий», модернизационный этап (с 2022 г.) с момента принятия Закона Республики Узбекистан «О кибербезопасности», формирование Национальной стратегии противодействия киберпреступности и введение статей 278^{8}–278^{9} проекта нового Уголовного кодекса. В главе обосновывается позиция, что киберпреступность обладает собственной онтологией, объединяющей мошеннические, экстремистские, террористические, диверсионные и посягающие на неприкосновенность личности деяния. В работе критически оценивается использование в действующей редакции Уголовного кодекса терминологически архаичных понятий («ЭВМ» вместо «компьютерная система»), отсутствие легальных дефиниций «ботнет», «DDoS-атака», «вредоносное программное

обеспечение», «критически важная информационная инфраструктура», «криптоактив», «дипфейк», «социальная инженерия». Автор предлагает унифицированный терминологический аппарат, концепция «Категориального словаря киберпреступности», подлежащего инкорпорации в кодекс в качестве нормы-дефиниции.

В рамках исследования диссертантом проведён детальный сравнительно-правовой анализ уголовного законодательства Российской Федерации (глава 28 УК РФ), Республики Молдова, Соединённого Королевства (Fraud Act 2006, Computer Misuse Act 1990), Соединённых Штатов Америки (Computer Fraud and Abuse Act 1986), Федеративной Республики Германия (§§ 202a, 202b, 202c, 263a, 303a, 303b StGB), Австралии (Cybercrime Act 2001), Республики Казахстан (глава 7 УК РК), Республики Корея, Японии, Сингапура, а также анализ Будапештской конвенции о киберпреступности 2001 года. Со стороны исследователя в противовес методологическим крайностям разработана авторская имплементационная модель, основанная на принципе «правового фильтра» то есть заимствование допускается лишь при соблюдении четырёх кумулятивных критериев – совместимости с национальной правовой традицией, соответствия конституционным ценностям, эмпирической эффективности в стране-доноре и наличия инфраструктурной готовности к применению. Соискатель обосновывает пакет из более чем двадцати конкретных рецепций: криминализацию мошенничеств с применением дипфейков, деяний с криптоактивами, деятельности «дропперов», SIM-манипуляций, корпоративной ответственности провайдеров услуг связи.

Во второй главе диссертации, озаглавленной **«Уголовно-правовые аспекты противодействия киберпреступности»,** автором проведён углублённый доктринальный анализ объективных и субъективных признаков киберпреступлений, освещены вопросы квалификации и отграничения смежных составов, разработан комплекс предложений по системному реформированию Уголовного кодекса.

Автором представлен оригинальный доктринальный анализ объективной стороны киберпреступлений. Автор вступает в научную полемику с представителями господствующей доктрины – А.И. Рарогом, Н.А. Лопашенко и С.А. Пашиным, – рассматривающими вредоносные программы исключительно в качестве средства совершения преступления. Согласно их взглядам, вредоносное программное обеспечение отождествляется по правовому режиму с орудием преступления в его классическом уголовно-правовом понимании (сопоставимо с ножом, огнестрельным оружием, отмычкой). Соискатель принципиально не разделяет данный подход и обосновывает концептуально иную конструкцию, согласно которой вредоносные программы должны рассматриваться как самостоятельный предмет посягательства «sui generis», обладающий тремя ключевыми признаками такими как целенаправленность где программа изначально запрограммирована на конкретный деструктивный результат, деструктивным потенциалом то есть

способностью причинять неограниченный по масштабу ущерб и автономностью функционирования то есть способностью действовать независимо от воли создателя после запуска. Позиция автора подкрепляется тем, что современные полиморфные вирусы, самообучающиеся вредоносные модули на основе технологий искусственного интеллекта, автономные ботнеты не подпадают под классическую конструкцию «орудия», поскольку обладают квази-субъектностью в цифровой среде. Автор аргументированно доказывает, что автономный характер функционирования вредоносного кода принципиально отличает его от любых материальных орудий и требует самостоятельного уголовно-правового режима – введения в Уголовный кодекс самостоятельных составов за изготовление, распространение и использование вредоносного кода с дифференцированными санкциями. Автор даёт детальную уголовно-правовую характеристику «компьютерных вирусов», «червей», «троянских программ», «spyware», «ransomware», «keyloggers», «RATs», «cryptojackers», а также обосновывает необходимость введения ответственности за массовый фишинг и посягательства на автоматизированные системы управления технологическими процессами.

Исследователем сформулирован комплексный криминологический портрет субъекта киберпреступления, включающий социально-демографические, психологические, образовательные, мотивационные и поведенческие параметры. Установлено, что типичный субъект киберпреступления в Республике Узбекистан это лицо мужского пола, в возрасте от 16 до 35 лет, обладающий специальными познаниями в сфере ИКТ, зачастую ранее не судимое. Автор вступает в научную полемику с представителями консервативного подхода – А.И. Долговой, Ю.М. Антоняном и Г.А. Аванесовым, которке отрицают целесообразность снижения возраста уголовной ответственности за киберпреступления. Согласно их взглядам, «цифровая незрелость» несовершеннолетних препятствует их привлечению к ответственности за подобные деяния. Автор вносит существенные коррективы в проблематику ответственности несовершеннолетних преимущественно в рамках действующего возрастного порога. Опираясь на собственные эмпирические данные о том, что 23,4 процента лиц, совершивших киберпреступления в стране с 2023 года по 2025 год, находились в возрасте от 14 до 16 лет, соискатель обосновывает необходимость снижения возраста уголовной ответственности за отдельные виды киберпреступлений (создание и распространение вредоносных программ, участие в «ботнет-сетях», «кибермошенничество», «кибербуллинг» с тяжкими последствиями) до 14 лет посредством дополнения части второй статьи 17 Уголовного кодекса. Позиция автора однозначна применительно к цифровой среде именно вышеперечисленная возрастная группа демонстрирует наивысшую цифровую компетентность, зачастую превосходящую компетентность взрослых субъектов, что делает сохранение общего возрастного порога криминологически иррелевантным.

В работе автором разработана концептуальная модель системной реформы Уголовного кодекса. Автор аргументированно обосновывает необходимость введения в кодекс самостоятельного Раздела 6^1 «Киберпреступления» как принципиально нового структурного элемента Особенной части; отдельной Главы «Преступления против информационно-коммуникационных технологий», объединяющей все «чисто компьютерные» составы; нормы, устанавливающие ответственность за сталкинг и кибернасилие.

Исследователь обосновывает вопреки позициям С.В. Максимова и Г.А. Есакова, рассматривающих нормы о компьютерной модификации и компьютерном саботаже как самостоятельные и не конкурирующие составы. Позиция автора имеет прямое правоприменительное значение и обосновывает предложение об исключении нормы о компьютерном саботаже из Уголовного кодекса с одновременным расширением диспозиции статьи предусматривающий компьютерную модификацию. Автор также обосновывает целесообразность введения корпоративной ответственности провайдеров услуг связи за необеспечение мер кибербезопасности, установления обязательных требований к двухфакторной аутентификации на уровне уголовно-правовой охраны, введения института специализированных судей по делам о киберпреступлениях с обязательной технической специализацией, а также создания мобильных криминалистических групп быстрого реагирования при Генеральной прокуратуре Республики Узбекистан.

В третьей главе диссертации, озаглавленной **«Криминологическая характеристика киберпреступности»,** проанализированы причины и условия, способствующие совершению киберпреступлений, разработана авторская типология субъектов киберпреступной деятельности, сформулирована оригинальная концепция многоуровневой профилактики киберпреступности в Республике Узбекистан.

Автор предлагает оригинальную интегральную четырёхфакторную модель детерминации киберпреступности, объединяющую социально-экономические факторы, цифровое неравенство, безработицу среди IT-специалистов, теневой сектор криптоэкономики, правовые и институциональные факторы, пробельность уголовного законодательства, слабость межведомственного взаимодействия, отсутствие специализированных следственных подразделений, технологические факторы такие как рост доступности вредоносного программного обеспечения по модели «Crime-as-a-Service», распространение технологий искусственного интеллекта и дипфейков, анонимизация в сегменте «DarkNet», психологические и виктимологические факторы то есть низкий уровень цифровой грамотности населения, «синдром цифрового доверия» и виктимологическая уязвимость лиц пожилого возраста. Автор вступает в научную полемику со сторонниками моноказуальных концепций В.В. Лунеевым и Я.И. Гилинским, отстаивающими экономико-детерминистский подход и сводящими киберпреступность исключительно

к социально-экономическим факторам, а также с Peter Grabosky, придерживающимся технократической концепции и объясняющим её преимущественно уровнем цифровой доступности. Позиция автора заключается в том, что ни одна из монофакторных моделей не позволяет объяснить структуру и динамику киберпреступности в Республике Узбекистан, где на равных действуют экономические, институциональные и социокультурные детерминанты.

На основе проведённого автором самостоятельного социологического исследования (объём выборки – 1 247 респондентов из 12 регионов Республики Узбекистан, период с 2024–2025 года), согласно которым лишь 16,1 процента респондентов оценивают своё знание уголовного законодательства о киберпреступлениях как удовлетворительное, 21,3 процента осведомлены о положениях Закона «О кибербезопасности», 31,0 процента уверены в способности распознать действия кибермошенников, 43,7 процента сталкивались с попытками кибермошенничества в течение последнего года, 12,4 процента признали, что становились жертвами киберпреступлений, при этом 79,3 процента опрошенных поддержали идею введения в Уголовный кодекс Республики Узбекистан самостоятельного раздела «Киберпреступления», 68,9 процента идею о снижении возраста уголовной ответственности за отдельные киберпреступления, 84,2 процента за идею создания единого реестра «дропперов». По убеждению автора, приведённые эмпирические данные образуют самостоятельный вклад в криминологическую науку Республики Узбекистан и опровергают распространённое в отечественной доктрине суждение о «достаточности» действующих мер правового просвещения населения.

На основе собранной информации разъясняется, что комплексная типология субъектов киберпреступной деятельности, включающая такие категорий как «хакер-исследователь» (грей-хэт), «хакер-разрушитель» (блэк-хэт), «кардер», «инсайдер», «участник организованной киберпреступной группы», «скрипт-кидди», «оператор Crime-as-a-Service». дифференцирована по образовательным, мотивационным, поведенческим, психологическим и рецидивным критериям. Автор вступает в научную полемику с представителями «романтизированной» школы Paul Taylor и Steven Levy представляющими киберпреступника преимущественно в образе одиночки-энтузиаста. Согласно их взглядам, борьба с киберпреступностью должна ориентироваться на индивидуальные меры реагирования. Вопреки данной позиции автор категорически подчёркивает, что современный этап с 2020 года по нынешнее время характеризуется «демократизацией» киберпреступности и переходом от элитарных хакеров к массовым скрипт-кидди, коммерциализацией теневых сервисов, формированием транснациональных цифровых рынков в сегменте «DarkNet» с ежегодным оборотом более 1,5 миллиарда долларов. Позиция автора однозначна что традиционная модель противодействия, ориентированная на «преступника-одиночку», окончательно утратила эффективность и должна быть заменена сетевой моделью реагирования, то

есть концепцией, разработанной соискателем в противопоставление всем существующим доктринальным подходам.

Исследователем обоснована концепция многоуровневой профилактики киберпреступности, включающая пять взаимосвязанных уровней. На общегосударственном уровне предлагается создание единого центра криминологического мониторинга киберпреступности, учреждение фонда возмещения ущерба потерпевшим от киберпреступлений, формирование единого национального реестра «дропперов». На отраслевом уровне предлагается введение обязательного киберстрахования для субъектов критически важной информационной инфраструктуры, развитие институтов «Bug Bounty», введение стандартов обязательного корпоративного обучения. На образовательном уровне предлагается внедрение национальной программы цифровой гигиены в систему общего, среднего, среднего специального и высшего образования, введение обязательного курса «Основы кибербезопасности» в учебные программы всех уровней. На местном уровне предлагаетася реализация пилотных проектов адресной профилактики на уровне махаллей (установка систем видеонаблюдения, SOS-кнопок, адресная работа с семьями и несовершеннолетними, вовлечение сходов граждан в антикиберпреступную деятельность) и на международном уровне, присоединение к Будапештской конвенции и механизмам G7 24/7, Европола и Интерпола.

Кроме того, автор вступает в полемику с представителем репрессивно-ориентированного подхода Э.Ф.Побегайло, и аргументированно обосновывает, что без развитого профилактического компонента ни ужесточение санкций, ни расширение перечня уголовно наказуемых деяний не способны обеспечить снижение уровня киберпреступности.

Автором обоснована концепция «КиберООН», то есть создания учреждений специализированного международного института координации борьбы с киберпреступностью, наделённого императивной юрисдикцией по трансграничным киберпосягательствам. Автор доказывает, что отсутствие специализированного института с императивной юрисдикцией является одним из ключевых институциональных факторов роста трансграничной киберпреступности, приведя статистику оценивая мировой ущерб, который достиг в 2025 году 10,5 триллионов долларов США. Позиция автора заключается в том, что учреждение «КиберООН» должно стать инициативой Республики Узбекистан на международной арене, в развитие её роли как активного участника Международной инициативы ООН по цифровой безопасности.

Результаты данной диссертации были использованы при разработке «Криминологической методики раннего предупреждения и борьбы с киберпреступностью в Шайхонтохурском районе города Ташкента». В связи с этим данная исследовательская работа в определенной степени служит созданию механизмов реализации приоритетных задач, определенных в Постановлении Президента Республики Узбекистан от 5 января 2026 года No ПП-1 «О дополнительных мерах по внедрению целостной системы

адресной работы в направлении создания безопасной среды в махаллях республики» и Указе Президента Республики Узбекистан от 16 февраля 2026 года No УП-21 «О дополнительных мерах по последовательному продолжению и выведению на новый этап реформ в рамках приоритетных направлений развития страны до 2023 года».

ЗАКЛЮЧЕНИЕ

В результате диссертационного исследования по теме «Уголовно-правовые и криминологические аспекты противодействия киберпреступности» разработаны общетеоретические выводы, предложения и рекомендации, направленные на совершенствование норм уголовного законодательства и развитие правоприменительной практики. Выводы охватывают три общие сферы и заключаются в следующем:

I. Научно-теоретические выводы:

1. Эффективное противодействие киберпреступности в Узбекистане требует совершенствования национального законодательства, усиления международного сотрудничества на основе единых стандартов кибербезопасности и вовлечения образовательных и общественных институтов в профилактику.

2. Ключевыми особенностями киберпреступлений выступают нематериальный характер объекта посягательства, высокая латентность и транснациональность, осложняющая вопросы юрисдикции и экстрадиции. Их совершение сопряжено с использованием высоких технологий, средств анонимизации и искусственного интеллекта, что обусловливает сложность идентификации субъекта, мгновенную скорость распространения и автоматизацию деяний. Постоянная эволюция форм и расширение субъектного состава (включая модель «Crime-as-a-Service») порождают трудности уголовно-правовой квалификации и формирование смешанных составов, опережающих развитие законодательства.

3. Автором обосновывается, что ст. 278^4 УК охватывает элементы преступления, предусмотренного статьей 278^5 УК. Поскольку в состав преступления модификации компьютерной информации входит деяние компьютерного саботажа, тем самым обосновывается объединение в одну статью.

II. Предложения и рекомендации по развитию законодательства

1. Предлагается дополнить Главу V «Преступления против семьи, молодёжи и нравственности» статьёй 127^2, предусматривающей ответственность за вовлечение несовершеннолетнего посредством информационно-коммуникационных сетей в действия сексуального характера (онлайн-груминг) и изложить в следующей редакции:

«Статья 127^2. Вовлечение несовершеннолетнего в действия сексуального характера посредством информационно-коммуникационных сетей (онлайн-груминг)

«Склонение несовершеннолетнего с использованием средств связи, к

совершению либо обсуждению действий сексуального характера, организация встречи либо подготовка к ней с этой целью, требование, просьба либо попытка получения фото-, видео- или иных материалов интимного характера –

наказываются штрафом в размере от ста до двухсот базовых расчётных величин либо лишением свободы до трёх лет.

Те же действия:

а) совершённые повторно;

б) совершённые группой лиц по предварительному сговору;

в) совершённые с использованием скрытых либо анонимных способов;

д) совершённые за материальное вознаграждение либо связанные с вымогательством, –

наказываются обязательными общественными работами либо лишением свободы на срок от трёх до пяти лет.

Деяния, предусмотренные частью первой или второй настоящей статьи, если они повлекли иные тяжкие последствия, –

наказываются лишением свободы на срок от пяти до восьми лет».

2. Предлагается дополнить Главу VII «Преступления против конституционных прав и свобод граждан» УК статьёй 141^4, предусматривающей ответственность за преследование лица (сталкинг) и кибернасилие,

«Статья 141^4. Преследование лица (сталкинг)

Систематическое наблюдение за лицом вопреки его воле, его преследование, попытки установления прямого либо косвенного контакта, а также совершение посредством средств связи, действий, выражающихся в беспокойстве, унижении, оказании психологического давления, либо иных действий, вызывающих опасения за его безопасность, здоровье или близких, –

наказываются штрафом в размере от ста до ста пятидесяти базовых расчётных величин либо исправительными работами на срок до двух лет.

Те же действия:

а) совершённые группой лиц по предварительному сговору;

б) совершённые повторно;

в) совершённые из корыстных либо иных низменных побуждений;

г) совершённые с использованием служебного положения;

д) совершённые в отношении несовершеннолетнего либо женщины, беременность которой была заведомо известна виновному, –

наказываются штрафом в размере от ста пятидесяти до двухсот базовых расчётных величин либо лишением свободы на срок до трёх лет.

Деяния, предусмотренные частью первой или второй настоящей статьи, если они повлекли иные тяжкие последствия, –

наказываются ограничением свободы на срок от трёх до пяти лет либо лишением свободы на срок от трёх до пяти лет».

3. Предлагается внести изменения в УК путем дополнения Разделом 6^1 «Киберпреступления» и дополнить Главой XX^1 «Преступления против информационно-коммуникационных технологий» и Главой XX^2

«Преступления в сфере информационно-коммуникационных технологий»;

4. Предлагается Главу XX[1] «Преступления против информационно-коммуникационных технологий» дополнить статьями 278[1], 278[2], 278[3] УК и изложить в следующей редакции:

«Статья 278[1]. Завладение цифровой информацией

Умышленное завладение цифровой информацией, повлекшее крупный ущерб либо существенный вред правам или охраняемым законом интересам граждан, либо государственным или общественным интересам, –

наказывается штрафом от трёхсот до шестисот базовых расчётных величин либо лишением свободы до трёх лет».

«Статья 278[2]. Принуждение к передаче цифровой информации

Принуждение к передаче охраняемой законом цифровой информации, хранящейся на электронном носителе, под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких, –

наказывается штрафом от трёхсот до шестисот базовых расчётных величин либо лишением свободы до трёх лет».

«Статья 278[3]. Неправомерное распространение электронных информационных ресурсов ограниченного доступа

Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан либо иные сведения, доступ к которым ограничен законами Республики Узбекистан, –

наказывается штрафом в размере до ста базовой расчётной величины либо лишением свободы до двух лет.

То же деяние, совершённое:

а) группой лиц по предварительному сговору;

б) из корыстных побуждений;

в) лицом с использованием своего служебного положения, –

наказываются штрафом от двухсот до трёхсот базовой расчётной величины либо лишением свободы от трёх лет до пяти лет.

Деяния, предусмотренные частями первой или второй настоящей статьи:

а) совершённые преступной группой;

б) повлёкшие тяжкие последствия, –

наказываются лишением свободы на срок от трёх до семи лет».

5. Предлагается вывести статью 278[5] «Компьютерный саботаж» из УК и изложить статью 278[4] УК в следующей редакции:

«Статья 278[4]. Незаконное уничтожение, блокировка или модификация компьютерной информации

Умышленное уничтожение, блокировка или модификация компьютерной информации, приведение её в негодность или выведение из строя компьютерной техники, нарушение работы компьютерной системы и её сетей, а равно внесение в неё заведомо ложной информации, повлёкшее нарушение работы компьютера, причинившее крупный ущерб либо существенный вред

правам или охраняемым законом интересам граждан либо государственным или общественным интересам, –

наказывается штрафом до ста базовых расчётных величин либо лишением свободы до двух лет.

Те же действия, совершённые:

а) с причинением особо крупного ущерба;

б) по предварительному сговору группой лиц;

в) повторно, –

наказываются удержанием заработной платы до двух лет либо лишением свободы до двух лет».

6. Предлагается Главу XX^2 «Преступления в сфере информационно-коммуникационных технологий» дополнить статьями 278^5, 278^6, 278^7, 278^8, 278^9, 278^{10}, 278^{11}, 278^{12} УК и изложить в следующей редакции:

«Статья 278^5. Нарушение правил информатизации

Нарушение правил **эксплуатации информационных ресурсов,** то есть создание, внедрение и эксплуатация информационных систем, баз и банков данных, без принятия установленных мер по их защите, совершённые лицом, имеющим право доступа к ним, причинившее крупный ущерб либо существенный вред правам или охраняемым законом интересам граждан, либо государственным или общественным интересам, –

наказывается штрафом до ста базовых расчётных величин или исправительными работами до одного года.

Те же действия, совершённые с причинением особо крупного ущерба, –

наказываются штрафом от пятидесяти до ста базовых расчётных величин либо ограничением свободы до шести месяцев».

«Статья 278^6. Незаконный (несанкционированный) доступ к компьютерной информации

Незаконный (несанкционированный) доступ к компьютерной информации, то есть информации, **находящейся в компьютере или иных устройствах обработки данных**, если это действие повлекло уничтожение, блокирование, копирование либо перехват информации, нарушение нормального функционирования средств вычислительной техники, –

наказывается штрафом до ста базовых расчётных величин или удержанием заработной платы на срок до одного года.

То же действие, совершённое:

а) по предварительному сговору группой лиц;

б) повторно;

в) с использованием служебного положения;

г) организованной преступной группой или в её интересах, –

наказывается штрафом от ста до двухсот базовых расчётных величин или ограничением свободы до трёх лет».

«Статья 278^7. Изготовление с целью сбыта либо сбыт, использование или распространение специальных средств для получения незаконного (несанкционированного) доступа к информационным ресурсам

Изготовление с целью сбыта либо сбыт, **использование или**

распространение специальных программных или аппаратных средств для получения незаконного (несанкционированного) доступа к **информационным ресурсам,** –

наказывается штрафом до двухсот базовых расчётных величин или исправительными работами до одного года.

Те же действия, совершённые:

а) по предварительному сговору группой лиц;

б) повторно;

в) с использованием служебного положения;

г) организованной группой или в её интересах, –

наказываются штрафом от двухсот до трёхсот базовых расчётных величин или исправительными работами от одного года до трёх лет».

«Статья 278[8]. Создание, использование или распространение вредоносных программных или аппаратных средств

Создание программных или аппаратных средств либо внесение изменений в существующие программы или программные продукты с целью несанкционированного уничтожения, блокирования, модификации, копирования или перехвата информации, хранящейся или передаваемой **в информационной системе, вывода из строя оборудования,** а равно разработка в этих целях специальных вирусных программ, их умышленное использование или распространение –

наказывается штрафом от ста до трёхсот базовых расчётных величин либо лишением свободы до двух лет.

Те же действия, совершённые:

а) с причинением особо крупного ущерба;

б) по предварительному сговору группой лиц;

в) повторно;

г) организованной **преступной** группой или в её интересах, –

наказываются лишением свободы от двух до трёх лет».

«Статья 278[9]. Незаконный (несанкционированный) доступ к сети телекоммуникаций

Незаконный (несанкционированный) доступ к сети телекоммуникаций с целью её использования и пропуска международного трафика в обход установленных систем защиты, а также хранение, **распространение** и создание условий для функционирования предназначенных для этих целей специальных программных или аппаратных средств, –

наказывается штрафом от ста до трёхсот базовых расчётных величин либо лишением свободы до трёх лет.

Те же действия, совершённые:

а) по предварительному сговору группой лиц;

б) повторно;

в) с использованием служебного положения;

г) организованной **преступной** группой или в её интересах, –

наказываются штрафом от двухсот до четырёхсот базовых расчётных величин либо лишением свободы от трёх до пяти лет».

«Статья 278[10] Нарушение законодательства в сфере оборота крипто-активов

Незаконное приобретение, сбыт или обмен крипто-активов, осуществление деятельности провайдеров услуг в сфере оборота крипто-активов без получения лицензии в установленном порядке, совершённые после применения административного взыскания за такие же действия, –

наказывается штрафом до ста базовых расчётных величин либо лишением свободы до одного года.

Те же действия, совершённые:

а) повторно;

б) в крупном размере;

в) по предварительному сговору группой лиц, –

наказываются штрафом от трёхсот до четырёхсот базовых расчётных величин либо лишением свободы до трёх лет.

Те же действия, совершённые:

а) в особо крупном размере;

б) с использованием служебного положения;

в) организованной преступной группой или в её интересах, –

наказываются лишением свободы от трёх до пяти лет».

«Статья 278[11] Незаконное осуществление деятельности по майнингу

Занятие майнингом анонимных крипто-активов или осуществление майнинга с нарушением установленного порядка, совершённой после применения административного взыскания за такие же действия, –

наказывается штрафом до ста базовых расчётных величин либо лишением свободы до одного года.

Осуществление скрытого майнинга –

наказывается штрафом от ста до трёхсот базовых расчётных величин либо лишением свободы до двух лет.

Действия, предусмотренные частями первой или второй настоящей статьи, совершённые:

а) повторно;

б) в особо крупном размере;

в) по предварительному сговору группой лиц, –

наказываются штрафом от трёхсот до четырёхсот базовых расчётных величин либо лишением свободы до трёх лет.

Действия, предусмотренные частями первой или второй настоящей статьи, совершённые:

а) с использованием служебного положения;

б) организованной преступной группой или в её интересах, –

наказываются лишением свободы от трёх до пяти лет».

«Статья 278[12]. Нарушение правил распространения общедоступной информации во всемирной информационной сети Интернет

Умышленное нарушение правил распространения общедоступной информации во всемирной информационной сети Интернет, причинившее

крупный ущерб или существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам, –

наказываются штрафом от трёхсот до шестисот базовых расчётных величин либо лишением свободы от трёх до пяти лет».

7. Предлагается дополнить Раздел VIII УК терминами следующего содержания:

«**Киберпреступление** – виновное противоправное вмешательство в работу информационных технологий, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные общественно опасные противоправные деяния, совершаемые с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью информационно-коммуникационных технологий информационному пространству»

«**Киберпреступность** – преступность в сфере информационно-коммуникационных технологий или с их использованием, а также преступления, совершаемые в или против информационного пространства, создающая угрозу личности, обществу и государству»

«**Компьютер** – любое устройство, которое осуществляет автоматизированную обработку информации»

«**Компьютерная система** – информация и обеспечивающие ее обработку программные, компьютерные и технические средства».

III. Предложения, направленные на совершенствование криминологических аспектов и профилактику киберправонарушений.

1. Предлагается разработка **Государственной стратегии профилактики киберпреступлений,** предусматривающей мониторинг цифровых угроз, обязательную сертификацию информационных систем и персонала в критически значимых секторах, имплементацию международных норм в национальное законодательство об информатизации, а также повышение цифровой грамотности населения посредством образовательных программ и систематического информирования клиентов о киберрисках;

2. Создать государственную программу формирования интернет-культуры с обязательным курсом **«Кибергигиена и цифровая безопасность» в школах (8–11 классы), колледжах и вузах;**

3. Предлагается осуществлять виктимологическую профилактику путём **таргетирования кампаний для групп повышенного риска:** пенсионеры (фейковые звонки от «банка»), молодёжь (псевдо-трейдинг, онлайн-казино), предприниматели (BEC-атаки, поддельные счета);

4. Создать **систему раннего профилирования потенциальных правонарушителей**, мониторинг хакерских форумов, чатов в Telegram/Discord на узбекском и русском языках, профилактическая работа с несовершеннолетними, замеченными в правонарушениях, для недопущения их перехода к тяжким составам;

5. Предлагается **использовать инфраструктуру** махаллей и инспекторов профилактики для низовой работы: разъяснительные сходы, памятки,

индивидуальная работа с лицами, ранее ставшими жертвами мошенничества (повторная виктимизация – устойчивый феномен).

6. В части **усиления специализированных правоохранительных подразделений** предлагается сформировать на базе Центра кибербезопасности МВД, СГБ, ГП и ЦБ **единый межведомственный оперативный штаб** с постоянным составом, общими протоколами и доступом к антифрод-системе ЦБ.

7. В Академии МВД и ТГЮУ открыть направление в магистратуру **«Криминология киберпреступности, и цифровая криминалистика»** и ввести обязательную **ежегодную переподготовку следователей и оперативников** по 72-часовой программе.

8. Создать **региональные мобильные группы цифровой криминалистики** (минимум по 1 на область) с оборудованием для извлечения данных из мобильных устройств, анализа криптокошельков и работы с дипфейками.

9. **Внедрить специализацию судей по уголовным делам в сфере ИКТ** в судах среднего звена.

10. **В части виктимологического направления и компенсационных механизмов** предлагается закрепить в законодательстве **презумпцию ответственности банка** при хищении с карты, если не доказана грубая неосторожность клиента (по модели PSD2 ЕС).

11. Создать **Фонд возмещения ущерба от киберпреступлений** за счёт отчислений финансовых организаций и штрафов по делам о нарушении кибербезопасности.

12. Сократить срок **«заморозки» средств на счетах получателей до 2 часов** с момента обращения по номеру 102.

13. Ввести обязательное **виктимологическое сопровождение:** психологическая помощь жертвам крупных мошенничеств, особенно пожилым гражданам.

14. По **регулированию «серой зоны» – счета-«дропперы», SIM-карты, криптоактивы** предлагается создать публично-частный **Единый реестр лиц-«дропперов»** с автоматическим ограничением открытия счетов и регистрации SIM-карт.

15. Ввести обязательную **идентификацию выгодоприобретателя криптотранзакций на лицензированных биржах** (Travel Rule FATF) с применением санкций за обналичивание.

16. В части **технологических и аналитических инструментов криминологического мониторинга** предлагается создать **Национальный криминологический центр кибербезопасности** при Совете безопасности для ведения единой статистики (сейчас данные МВД, ЦБ и ГП расходятся), прогнозирования трендов на основе ИИ-анализа сообщений в соцсетях и обращений граждан, публикации ежеквартальных криминологических бюллетеней.

17. Внедрить систему **предиктивной аналитики для банков:** модели машинного обучения для выявления нетипичных транзакционных шаблонов

до фактического хищения.

18. Запустить программу **Bug Bounty на государственной электронной платформе** для легализации деятельности «белых хакеров» и снижения притока специалистов в теневой сектор.

19. В части **международного сотрудничества и трансграничного расследования** предлагается ускорить присоединение к Будапештской конвенции.

20. Заключить двусторонние соглашения об **оперативном обмене данными** с РФ, КНР, ОАЭ, Турцией, Казахстаном.

21. Создать **24/7 контактный пункт** (по модели G7 24/7 Network) при ГП для срочных запросов о сохранении данных у иностранных провайдеров.

22. Активно участвовать в инициативах **CSS – Central Eurasia** и в работе ОДКБ/ШОС по **обмену** образцами вредоносного кода **Cyber Security Summit Central Eurasia.**

23. В части **научно-исследовательского и кадрового обеспечения** предлагается **сформировать государственный заказ** на криминологические исследования по темам типология киберпреступников, портрет жертвы, эффективность санкций, влияние цифровизации финансовых услуг на виктимизацию.

24. Создать на базе ТГЮУ или Академии ГП **диссертационный совет** по специальности **«Криминология цифровой среды»**.

25. Учредить ежегодный **криминологический форум** по киберпреступности с публикацией национального отчёта (аналог Europol IOCTA).

SCIENTIFIC COUNCIL No. DSc.07/2025.27.12.Yu.01.04
FOR AWARDING SCIENTIFIC DEGREES AT
TASHKENT STATE UNIVERSITY OF LAW

TASHKENT STATE UNIVERSITY OF LAW

DUSMATOV DURBEK RUSTAMJON OGLI

CRIMINAL AND CRIMINOLOGICAL ASPECTS OF COMBATING CYBERCRIME

12.00.08 – Criminal law. Criminal-executive law;
12.00.15 – Criminology

DISSERTATION ABSTRACT
of the Doctor of Philosophy (PhD) dissertation in legal sciences

Tashkent – 2026

The theme of the Doctor of Philosophy (PhD) dissertation was registered at the Higher Attestation commission at the academy of sciences of the Republic of Uzbekistan under number No. B2023.3.PhD/Yu1168.

The dissertation is prepared at Tashkent State University of Law.

The abstract of the dissertation is posted in three languages (Uzbek, Russian and English, (resume)) on the website of the Scientific Council (www.tsul.uz) and Information education portal on the "Ziyonet" (www.ziyonet.uz).

Scientific supervisor:	**Abzalova Xurshida Mirziyatovna** Doctor of Science in Law, Professor
Official opponents:	**Rasulev Abdulaziz Karimovich** Doctor of Science in Law, Professor
	Kamalova Dildora Gayratovna Doctor of Science in Law, Professor
The leading organization:	**Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan**

The defense of the dissertation will be held on August 7th, 2026 year at 2^{30} p.m at the Session of the Scientific Council DSc.07/2025.27.12.Yu.01.04 at Tashkent State University of law (Address: 100047, Sayilgoh street, 35. Tashkent city. Phone.: +998 71 233-66-36; Fax: +998 71 233-37-48; e-mail: info@tsul.uz).

The doctoral dissertation (PhD) is available at the Information Resource Center of Tashkent State University of Law (registered as No.343.9). (Address: 100047, Amir Temur Street 13. Tashkent city. Phone: +998 71 233-66-36.

The dissertation abstract was distributed on July 22, 2026.
(Registry protocol No. 6. on July 22, 2026).

R.A. Zufarov
Chairman of the Scientific Council for awarding scientific degrees, Doctor of Science in Law, Professor

N.K. Xojiyev
Secretary of the Scientific Council for awarding scientific degrees, Doctor of Philosophy in Law, Associate Professor

Sh.Dj. Xaydarov
Chairman of the Scientific Seminar under the Scientific Council for awarding scientific degrees, Doctor of Science in Law, Professor

INTRODUCTION (Abstract of the Doctor of Philosophy (PhD) dissertation)

The purpose of this study is to acquire criminological knowledge regarding the state of cybercrime and to reveal the criminal-legal nature of offenses committed in the field of information technologies, which is essential for assessing the degree of public danger posed by such acts. Achievement of this goal is facilitated by addressing the following tasks:

– to elucidate the legal nature, place within the Special Part of the Criminal Code of the Republic of Uzbekistan, and the characteristics of crimes in the field of information technologies;

– to define the concept of cybercrime;

– to substantiate the criminological basis for criminal liability for acts that, in their totality, constitute cybercrime;

– to conduct a criminal-legal analysis of offenses that collectively form cybercrime;

– to develop proposals aimed at improving criminal legislation norms to ensure effective criminal-legal influence on cybercrime.

The object of the research consists of social relations that arise in the criminal-legal sphere of combating crimes committed in the field of information technologies in the Republic of Uzbekistan, which collectively constitute cybercrime, as well as the problems associated with the application of criminal law provisions establishing liability for such acts.

The scientific novelty of the research is as follows:

is substantiated that the necessity of introducing a provision stipulating that sexual intercourse or the satisfaction of sexual needs in an unnatural form with a person under the age of sixteen by an individual previously convicted of crimes provided for in the Criminal Code, such as rape or the satisfaction of sexual needs in an unnatural form with the use of violence, and whose conviction has not been expunged or annulled, should be considered as a separate offense.

it is substantiated that the necessity of recognizing the commission of sexual intercourse or the satisfaction of sexual needs in an unnatural form with a person under the age of sixteen by a group of persons as an aggravating circumstance has been proven. It has also been proposed to include a new clause “v” in part 3 of Article 168 of the Criminal Code, with the wording “committed by a group of persons”.

it is substantiated that the necessity of recognizing the commission of sexual intercourse or the satisfaction of sexual needs in an unnatural form with a person under the age of sixteen, if the person is a close relative, as an aggravating circumstance has been proven. It has also been proposed to include this offense in part 3, clause “g”, of Article 168 of the Criminal Code.

it is substantiated that the necessity of prohibiting individuals convicted of sexual intercourse or indecent acts with a person under the age of sixteen, producing or distributing pornographic materials involving minors, or engaging in pimping or organizing brothels from engaging in activities related to teaching, upbringing, and

direct work with children has been proven.

The implementation of the research results. Scientific results of the study:

the proposal to include a provision on mining anonymous crypto-assets or engaging in mining in violation of established procedures was adopted in the drafting of Article 278^9 of the Draft Criminal Code of the Republic of Uzbekistan (Act of General Prosecutor's Office of the Republic of Uzbekistan, No. 27/2-222-25 dated June 25, 2025). The adoption of this proposal aims to strengthen liability for the unlawful conduct of mining activities.

the proposal regarding violations of legislation in the circulation of crypto-assets was used in drafting Parts 1 and 2 of Article 155^4 of the Draft Code of Administrative Liability of the Republic of Uzbekistan (Act of State Security Service of the Republic of Uzbekistan, No. 17/01-34 dated June 26, 2025). This proposal aims to enable a stricter and fairer evaluation of offenses in the field of information and communication technologies.

the proposals were also incorporated in the Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan No. 17 dated June 23, 2023, "On Judicial Practice in Cases of Fraud." In particular, during the preparation of the Resolution, the researcher's proposals concerning Paragraph 22 were taken into account. This paragraph states: "Fraud committed using an information system, including information technologies, shall be understood as the unlawful taking of property held by financial, banking institutions, funds, or similar organizations by means of deception through the use of computer technology, communication devices, tablets, or other similar technical means via manipulations. Such fraud may be committed by altering information processed in a computer system, stored on relevant data carriers, or transmitted via data networks, as well as by inputting false information into the computer system. In distinguishing fraud committed through the use of information systems, including IT, from theft committed through unlawful (unauthorized) access to or use of an information system, it is essential to consider that in fraud, the victim, being misled or subject to abuse of trust, voluntarily transfers the property or the right to it to the perpetrator, realizing that the property leaves his possession." the approach stating: "If a person fabricates a forged document using computer technology and then uses it to acquire property, such conduct shall not be qualified under paragraph 'g' of Part 3 of Article 168 of the Criminal Code"—was also taken into consideration. (Act of Supreme Court of the Republic of Uzbekistan, No. 08/225-25 dated May 28, 2025).

the proposals developed on the basis of the research findings were used in the drafting of Resolution No. 153 of the President of the Republic of Uzbekistan dated 30 April 2025, "On Measures Aimed at Further Strengthening Efforts to Combat Crimes Committed through the Use of Information Technologies." In particular, the said proposals were reflected in the provisions aimed at improving measures to counter cybercrime, strengthening liability for offences in this field, and further developing the organizational and legal mechanisms for the prevention of cybercrime. (Act of the Ministry of Internal Affairs of the Republic of Uzbekistan, Main Department of Internal Affairs of the City of Tashkent, No. 27/3-1345/4k,

dated 28 April 2026).

The proposals developed on the basis of the research findings were also used in the drafting of the Law of the Republic of Uzbekistan dated 21 January 2026 No. 1115, "On Introducing Additions and Amendments to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of Relations Arising from the Use of Artificial Intelligence," including in the formulation of paragraph 4 of Article 1 of the said Law, insofar as it establishes the legal framework for the use of artificial intelligence in the creation of information resources and the operation of information systems, as well as Article 2 of the said Law, insofar as it provides for administrative liability for the unlawful processing of personal data through the use of artificial intelligence technologies and for the introduction of corresponding amendments to Part Two of Article 46^2 of the Code of the Republic of Uzbekistan on Administrative Responsibility. (Act of the Ministry of Internal Affairs of the Republic of Uzbekistan, Main Department of Internal Affairs of the City of Tashkent, No. 27/3-1345/5k, dated 28 April 2026).

The structure and volume of the dissertation. The dissertation consists of an introduction, three chapters, a conclusion, a list of references and appendices. The volume of the dissertation is 158 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo‘lim (I часть; I part)

1. Dusmatov D.R. Киберпреступность как угроза международной и национальной безопасности. Журнал правовых исследований Специальный номер-4. –Toshkent, – №4 (2022). – B.63-70. ISSN: 2181-9130. (https://www.tadqiqot.uz/index.php/law/article/view/5798)
2. Dusmatov D.R. Криминологическая характеристика преступника: Субъект киберпреступлений как системообразующий элемент. “Tergov amaliyoti” №3/2023 yil (19-сон). – Toshkent, 2023. –№ 19. – ISSN: 2181-2543, B.32-37. (OAK Rayosatining 2021-yil 30-oktabrdagi 308/6-son qarori). (https://tergov.uz/uploads/wanted/3a3c4f080e200767afefe1a138b78c5d.pdf)
3. Dusmatov D.R. Information Technology and the Concept of Crime in Cyber Space. International Journal of Advance Scientific Research. Volume 3 | Issue 11 | 2023. E-ISSN: 2750-1396, SJIF: 6.741. B.370-373. (https://sciencebring.com/index.php/ijasr/article/view/538/511)
4. Dusmatov D.R. Subjective Signs of Cybercrime. The American Journal of Political Science Law and Criminology. Volume 5 | Issue 11 | 2023. ISSN: 2693-0803, SJIF: 2023. B.48-51. (https://www.theamericanjournals.com/index.php/tajpslc/article/view/4620/4310)
5. Dusmatov D.R. Retrospektiv Tahlil (O‘zbekiston Respublikasi Jinoyat kodeksida jinoyatlarni jinoiylashtirish masalalari). Namangan Davlat universiteti ilmiy axborotnomasi. –Namangan, – №2 (2024). – B.316-322. (OAK Rayosatining 2019-yildagi qarori). (https://www.researchgate.net/publication/378241267_Scientific_Bulletin_of_NamSU-Naucnyj_vestnik_NamGU-NamDU_ilmiy_axborotnomasi-2024-yil_2-son_1_wwwjournalnamduuz)
6. Dusmatov D.R. Ретроспективный анализ (Вопросы криминализации составов преступления в уголовный кодекс Республики Узбекистан). O‘zbekiston Respublikasi Fanlar Akademiyasi Mintaqaviy Bo‘limi Xorazm Ma’mun akademiyasi Xorazm Ma’mun Akademiyasi Axborotnomasi. – Xiva, 2024. –№ 5/3. – B.122-125. (OAK Rayosatining 2016-yil 29-dekabrdagi 223/4-son qarori). (https://mamun.uz/uploads/journal/files/1718968087.pdf)
7. Dusmatov D.R. Information Technology and the Concept of Crime in Cyber Space. Euroasian Journal of Research, Development and Innovation (EJRDI). Volume 26 | Issue E | 2023. E-ISSN: 2795-7616, JIF: 7.935. B.32-34. (https://geniusjournals.org/index.php/ejrdi/article/view/5317)
8. Dusmatov D.R. Перспективы правовой политики в области противодействия киберпреступности в Республике Узбекистан. Results of National Scientific Research International Journal 2025. Volume 4 | Issue 5 | 2025. E-ISSN: 2181-3639, SJIF: 5.8. B.146-153. (https://academicsresearch.ru/index.php/rnsrij/issue/view/172)

9. Dusmatov D.R. Использование криптовалют в совершении киберпреступлений: уголовно-правовой анализ и следственная практика. Journal The Light of Civilization Scientific, socio-philosophical, cultural and educational, literary and artistic magazine. – Beruniy, 2025. –№ 6 (69). – B.316-319. ISSN: 2181-8258 (OAK Rayosatining 2023-yil 31-oktyabrdagi 345-son qarori). (https://jurnal.tamaddunnuri.uz/index.php/tnj/article/view/2536/1591)

10. Dusmatov D.R. Preventive Measures to Combat Cybercrime: A Criminological Perspective (Educational and Social Measures, Work with Youth, Development of Digital Literacy). International Journal of Law And Criminology. Volume 5 | Issue 6 | 2025. B.72-74. ISSN: 2771-2214. (https://inlibrary.uz/index.php/ijlc/article/view/122712/124247)

11. Dusmatov D.R. Criminal law aspects of combating phishing and carding (Phishing and carding as forms of fraud in the digital environment: legal qualification) The American Journal of Political Science Law and Criminology. Volume 7 | Issue 6 | 2025. B.79-81. ISSN: 2693-0803. (https://www.theamericanjournals.com/index.php/tajpslc/article/view/6355/5873)

12. Dusmatov D.R. Information security and criminal law measures for the protection of critical infrastructure (Legal Mechanisms for Protecting State and Strategic Facilities from Cyberattacks) «Жамият ва инновациялар – Общество и инновации – Society and innovations Issue» 6 № 5 (2025) / ISSN 2181-1415. B.145-149. (OAK Rayosatining 2020-yil 31-dekabrdagi 290/10-son qarori). (https://www.researchgate.net/publication/396971174_Informacionnaa_bezopasnost_i_ugolovno-pravovye_mery_zasity_kriticeskoj_infrastruktury_Pravovye_mehanizmy_zasity_gosudarstvennyh_i_strategiceskih_obektov_ot_kiberatak)

II bo‘lim (II часть; II part)

13. Dusmatov D.R. Reliable Protection Against Cybercrimes – The Government of the Time: Criminal Legal Aspect. Theoretical and empirical scientific research: concept and trends: Collection of scientific papers «ΛΌГОΣ» with Proceedings of the II International Scientific and Practical Conference (Vol. 1), Oxford, May 28, 2021. Oxford-Vinnytsia: P.C. Publishing House & European Scientific Platform, 2021. B.75-76. (https://ojs.ukrlogos.in.ua/index.php/logos/article/view/12890/11872)

14. Dusmatov D.R. Кибersталкинг как новый вид уголовно-наказуемого деяния. «Инновационные подходы в современной науке». Сборник статей по материалам CXXVI международной научно-практической конференции. № 18(126). – Москва., Изд. «Интернаука», 2022. ISSN: 2587-8603, SJIF: 5.8. B.40-44. (https://www.internauka.org/authors/dusmatov-durbek-rustamzhon-ugli)

15. Dusmatov D.R. Axborot texnologiyalari va kibermakondagi jinoyat tushunchasi. «Zamonaviy taraqqiyotda ilm-fan va madaniyatning o‘rni» nomli respublika ilmiy-amaliy konferensiya. 2023-yil 29-noyabr. – Toshkent.: 2023. – B.126-130. (https://academics.uz/index.php/Konferensiya/article/view/2478/3754)

16. Dusmatov D.R. Cyber Victim: Victimological Prevention. Jinoyatchilikka

qarshi kurashish sohasidagi ilg‘or tajribalar Xalqaro ilmiy-amaliy konferensiya materiallari (2023-yil 30-noyabr) / Mas’ul muharrir: R. Kabulov. – T.: O‘zbekiston Respublikasi IIV Akademiyasi, 2023. – B.258-260. (https://www.in-academy.uz/index.php/cajmrms/article/download/33186/21228/33776)

17. Dusmatov D.R. Kiberjinoyatlarning obyektiv belgilari. «International conference of education, research and innovation». Vol. 1 No. 8 (2023): International conference of education, research and innovation. Samara, Russian Federation, 2023. C.44-48. (https://academicsresearch.ru/index.php/ICERI/article/view/2633)

18. Dusmatov D.R. Kiberjinoyatning subyektiv belgilari. «International Scientific and Practical Conference: Problems and Scientific Solutions». Vol. 2 No. 8 (2023): International Scientific and Practical Conference: Problems and Scientific Solutions. Australia, Melbourne. 2023. C.19-24. (https://academicsresearch.ru/index.php/icpass/article/view/2634)

19. Dusmatov D.R. Objective Significance of Cybercrimes. Vol. 2, Issue 11 of Results of National Scientific Research Journal 2023. Volume 2 | Issue 11 | 2023. ISSN: 2181-3639, SJIF: 5.8. B.106-110. (https://academicsresearch.ru/index.php/rnsrij/article/view/2629)

20. Dusmatov D.R. Jinoyat sodir etishga provokatsiya (Gijgijlash). «Zamonaviy taraqqiyotda ilm-fan va madaniyatning o‘rni» nomli respublika ilmiy-amaliy konferensiya. 2024-yil 10-iyun. – Toshkent.: 2024. – B.25-27. (https://academics.uz/index.php/Konferensiya/article/view/3597)

Avtoreferat TDYU “Yuridik fanlar Axborotnomasi” jurnali tahririyatida tahrirdan o‘tkazilib, o‘zbek, rus va ingliz tillaridagi matnlar o‘zaro muvofiqlashtirildi.

Bosishga ruxsat etildi: 20.07.2026 yil.
Bichimi: 60x84 $^{1}/_{16}$. “Times New Roman” garniturada 14 raqamli bosma usulida bosildi.
Shartli bosma tabog‘i 4,3. Adadi: 100. Buyurtma: № 85

100060, Toshkent sh., Y.G‘ulomov ko‘chasi, 74.
Tel: +998 90 9722279, www.tiraj.uz

“TOP IMAGE MEDIA”
bosmaxonasida chop etildi.