O‘ZBEKISTON RESPUBLIKASI JAMOAT XAVFSIZLIGI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.32/.30.12.2020.Yu.74.01 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON RESPUBLIKASI JAMOAT XAVFSIZLIGI UNIVERSITETI

ANORBOYEV AMIRIDDIN ULUG‘BEK O‘G‘LI

JAMOAT XAVFSIZLIGIGA TAHDID SOLUVCHI KIBERJINOYATLARNING JINOIY-HUQUQIY JIHATLARI

12.00.08 – Jinoyat huquqi. Jinoyat-ijroiya huquqi

Yuridik fanlar doktori (DSc) dissertatsiyasi AVTOREFERATI

Toshkent – 2025

UO‘K: 343.140.02:004.9

Fan doktori (DSc) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертации доктора наук (DSc)

Contents of the abstract of the dissertation of the Doctor of Science (DSc)

O‘ZBEKISTON RESPUBLIKASI JAMOAT XAVFSIZLIGI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.32/.30.12.2020.Yu.74.01 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON RESPUBLIKASI JAMOAT XAVFSIZLIGI UNIVERSITETI

ANORBOYEV AMIRIDDIN ULUG‘BEK O‘G‘LI

JAMOAT XAVFSIZLIGIGA TAHDID SOLUVCHI KIBERJINOYATLARNING JINOIY-HUQUQIY JIHATLARI

12.00.08 – Jinoyat huquqi. Jinoyat-ijroiya huquqi

Yuridik fanlar doktori (DSc) dissertatsiyasi AVTOREFERATI

Toshkent – 2025

Yuridik fan doktori (DSc) dissertatsiya mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2023.1.DSc/Yu235 raqam bilan ro‘yxatga olingan.

Dissertatsiya O‘zbekiston Respublikasi Jamoat xavfsizligi universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) «ZiyoNET» ta’lim axborot tarmog‘ida (www.ziyonet.uz) joylashtirilgan.

Ilmiy maslahatchi:	**Rustambayev Mirzayusup Xakimovich,** yuridik fanlar doktori, professor
Rasmiy opponentlar:	**Urazaliyev Murod Korayevich** yuridik fanlar doktori, professor
	Turg‘unboyev Elbekjon Odiljonovich yuridik fanlar doktori
	Akrom Ikromovich Toshpo‘latov yuridik fanlar doktori, dotsent
Yetakchi tashkilot:	**O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti**

Dissertatsiya himoyasi O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti huzuridagi Ilmiy darajalar beruvchi DSc.32/30.12.2020.Yu.74.01 raqamli Ilmiy kengashning 2025-yil 12-dekabr kuni soat 11-00.dagi majlisida bo‘lib o‘tadi. (Manzil: 100211, Toshkent viloyati, Zangiota tumani, Chorsu qo‘rg‘oni. Tel.: (+998971) 230-32-71; faks: (99871) 230-32-50, info@mgjxu.uz).

Dissertatsiya bilan O‘zbekiston Respublikasi Jamoat xavfsizligi Axborot-resurs markazida tanishish mumkin (_____raqami bilan ro‘yxatga olingan). (Manzil:100121, Toshkent., Zangiota tumani, Chorsu qo‘rg‘oni. Tel.: (+99871) 230-32-71; faks: (+99871) 230-32-50)

Dissertatsiya avtoreferati 2025-yil 28-noyabr kuni tarqatildi.

(2025-yil 28-noyabr kunidagi 21-raqamli reyestr bayonnomasi)

D.M.Mirazov
Ilmiy darajalar beruvchi Ilmiy kengash raisining o‘rinbosari, yuridik fanlar doktori, professor

J.D.Axmedov
Ilmiy darajalar beruvchi Ilmiy kengash kotibi, yuridik fanlar bo‘yicha falsafa doktori (PhD)

Sh.X.Zulfiqarov
Ilmiy darajalar beruvchi Ilmiy kengash huzuridagi ilmiy seminar raisi, yuridik fanlar doktori, professor

KIRISh (fan doktori (DSc) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Dunyodagi barcha sohalar va tarmoqlarni raqamlashtirish, axborot tizimlari va resurslari, muhim axborot infratuzilmalari, telekommunikatsiya, shu jumladan, butun jahon internet tarmog‘i, shaxsga doir ma’lumotlar bazalari, axborotlashtirish va telekommunikatsiya infratuzilmasi, axborot-kommunikatsiya texnologiyalari, shu jumladan, sun’iy intellekt, kiber-, nono-, bio- va boshqa texnologiyalar hamda texnik vositalarning keyingi rivojiga kiberjinoyatlar katta xavf solmoqda va buning oqibatida jamoat xavfsizligi tahdid ostida qolmoqda. Hozirda, 2023-yilda har 39 soniyada, hozirda esa, **har 14 soniyada bitta kiberhujum** sodir etilib[1], boshqa manbalarda esa, **har soniyada** kiberhujum amalga oshirilib[2], buning oqibatida 2023-yilda dunyodagi 71 foiz tashkilotlar tovlamachilik dasturlari qurboni bo‘lishgan bo‘lsa, hozirda barcha kiberxavfsizlik hodisalarining 80 foiz qismi jinoiy guruhlar bilan bog‘liq[3]. Jahon iqtisodiyotiga yetkazilgan zarar miqdori esa, 2018-yilda 3 trln. dollar, 2019-yilda 3,5 trln. dollar, 2020-yilda 4,2 trln. dollar, 2021-yilda 6 trln. dollar, 2022-yilda 7 trln. dollar, 2023-yilda 8,4 trln. dollar, 2024-yilda 9,5 trln. dollarni tashkil etgan[4] bo‘lsa, 2025-yilda **10,5 trln. dollar**[5], 2026-yilda **20 trln. dollar**, 2027-yilda 22 trln. dollar, 2028-yilda 24 trln. dollar, 2029-yilda 26 trln. dollarni tashkil etishi tahmin qilinmoqda[6]. Ko‘rib o‘tilganidek, kiberjinoyatlarning keltirayotgan zarar miqdori 2026-yilga kelib ikki barobarga ko‘paymoqda va bu esa, zudlik bilan barcha dunyo davlatlari hamjihatlikda xalqaro transchegaraviy jinoyat bo‘lgan kiberjinoyatlarga qarshi birgalikda kurashish va bu sohada keng ko‘lamli islohotlar amalga oshirish zarurligini taqozo etmoqda.

Jahonda kiberjinoyatlar tufayli ro‘y beradigan iqtisodiy inqirozlarning oldini olish va uning salbiy oqibatlarini bartaraf etish, shaxs, jamiyat va davlat manfaatlarini himoya qilish, jamoat xavfsizligi va kiberxavfsizlikni ta’minlash yuzasidan dunyo davlatlari xalqaro hujjatlar asosida ushbu kibertranschegeraviy jinoyatlarga qarshi yalpi kurashish bo‘yicha keng ko‘lamli ishlarni amalga oshirishmoqda, ushbu kiberjinoyatlarga qarshi kurashish uchun ta’lim tizimida keskin islohotlar o‘tkazilib, kiberxavfsizlikka ixtisoslashtirilgan mutaxassislar yetishtirilmoqda, maxsus labaratoriya, oliy ta’lim va ilmiy tadqiqot tashkilotlarini tashkil qilishmoqda, kiberhodisalarni oldindan prognoz va tahlil qilish uchun sun’iy intellekt va avtomatlashtirilgan «*aqlli tizim*»lardan foydalanishmoqda, kiberxavfsizlikni ta’minlash bo‘yicha xayriya, grant va byudjet mablag‘larini ajratishmoqda, transchegaraviy munosabatlarda qonunchilik hujjatlarini takomillashtirish va o‘zaro birxillashtirish orqali ularni tizimlashtirish, texnik va texnologik jarayonlardan tortib, yuridik masalalargacha yagona huquqiy-texnik

[1] https://www.datensicherheit.de/2024-2025-cyber-attack-companies-14-seconds.
[2] https://cybermap.kaspersky.com/ru/stats.
[3] https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts/#sources.
[4] https://newsletter.radensa.ru/archives/4840.
[5] https://www.cenlanow.com/business/press-releases/ein-presswire/674883055/cybercrime-damages-to-cost-the-world-9-5-trillion-usd-in-2024/.
[6] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide#:~:text=The%20global%20cost%20of%20cybercrime,trillion%20U.S.%20dollars%20in%202022.

amaliyotni yo‘lga qo‘yish choralarini ko‘rishmoqda. Shu sababli kibermuhitda, shu jumladan, kibermakonda shaxs, jamiyat va davlat xavfsizligi bilan bir qatorda jamoat xavsizligi va kiberxavsizlikni ta’minlash yuzasidan ilmiy-amaliy yechimlarni topish dolzarb ahamiyat kasb etib bormoqda.

Respublikamizda ham jamoat xavfsizligini ta’minlash bo‘yicha qonunchilik hujjatlari va boshqa hujjatlar bilan zarur islohotlar amalga oshirib borilmoqda. Jumladan, mamlakatimizda xavfsiz kibermuxit, shu jumladan, kibermakonni yaratish maqsadida 2017-2025-yillar davomida 150 ga yaqin qonunchilik hujjatlari qabul qilinib, 500 ga yaqin keng ko‘lamli chora-tadbirlar amalga oshirildi. Biroq raqamli texnologiyalarning keyingi rivoji, jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun javobgarlikning yetarli darajada jinoyat qonunchiligimizda aniq belgilanmaganligi va bu borada hali hamon “*huquqiy bo‘shliqlar*”ning mavjudligi “*latent*” kiberjinoyatlarning vujudga kelib, ularning soni, turi, keltirilgan zarar ko‘lami kundan-kunga oshib ketishiga, huquqni qo‘llash jarayonida “*kollizion holatlar*” ko‘payishiga sabab bo‘lmoqda. Birgina, statistik ma’lumotlarga asosan, O‘zbekiston Respublikasida 2020-yilda 863 ta, 2021-yilda 785 ta, 2022-yilda 7570 ta, 2023-yilda 6 450 ta, 2024-yilda 58 800 ta qilmish axborot texnologiyalaridan foydalanib sodir etilganligi ro‘yxatga olingan bo‘lsa, bu borada kiberjinoyatlar soni 2020-yilga qaraganda 2024-yilda tahminan **68,13** barobarga ko‘tarilgan. Bu esa, o‘z navbatida bu xavfga qarshi tezkor, keng ko‘lamli, kompleks va tizimli kurashish va kiberxavfsizlikni ta’minlash uchun olib borilayotgan islohotlarni yanada kuchaytirish zarurligini ko‘rsatmoqda.

O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil), O‘zbekiston Respublikasining «Axborotlashtirish to‘g‘risida»gi (2003-yil), «Elektron hukumat to‘g‘risida»gi (2015-yil), «Shaxsga doir ma’lumotlar to‘g‘risida»gi (2019-yil), «Kiberxavfsizlik to‘g‘risida»gi (2022-yil), «Telekommunikatsiyalar to‘g‘risida»gi (2024-yil) qonunlari, O‘zbekiston Respublikasi Prezidentining «O‘zbekiston Respublikasi Jamoat xavfsizligi konsepsiyasini tasdiqlash va uni amalga oshirish chora-tadbirlari to‘g‘risida»gi (2021-yil), «O‘zbekiston — 2030» strategiyasi to‘g‘risida”gi (2023-yil), «Korrupsiyaga qarshi kurashish tizimini yanada takomillashtirish bo‘yicha belgilangan ustuvor vazifalar ijrosini samarali tashkil etishga doir chora-tadbirlar to‘g‘risida»gi (2025-yil) farmonlari, «Jinoyat va jinoyat-protsessual qonunchiligi tizimini tubdan takomillashtirish chora-tadbirlari to‘g‘risida»gi (2018-yil), «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi (2023-yil), «Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida» (2024-yil), «Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida»gi (2025-yil) qarorlari, Vazirlar Mahkamasining «Idoralararo elektron hamkorlik tizimi va ma’lumotlarning axborot almashinuvini yanada takomillashtirish chora-tadbirlari to‘g‘risida»gi (2022-yil), «Shaxsga doir ma’lumotlarga ishlov berish sohasidagi ayrim normativ-huquqiy hujjatlarni tasdiqlash to‘g‘risida»gi (2022-yil) qarorlari, Markaziy bank boshqaruvining «To‘lov tizimi operatorlarining va to‘lov tashkilotlarining faoliyatini nazorat qilish

va kuzatuvni amalga oshirish tartibi to‘g‘risidagi nizomni tasdiqlash haqida»gi (15.05.2023-y., ro‘y.: 3434), «To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralarini ko‘rish to‘g‘risidagi nizomni tasdiqlash haqida»gi (21.05.2024-y., ro‘y.: 3513) qarorlari, Davlat xavfsizlik xizmati raisining «O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risidagi nizomni tasdiqlash haqida»gi (22.09.2023-y., ro‘y.: 3458), «O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarini toifalash va ularning yagona reestrini shakllantirish tartibi to‘g‘risidagi vaqtinchalik nizomni tasdiqlash haqida»gi (11.11.2024-y., ro‘y.: 3570), «Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish tartibi to‘g‘risidagi nizomni tasdiqlash haqida»gi (14.11.2024-y., ro‘y.: 3573), «Axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo‘llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi to‘g‘risidagi nizomni tasdiqlash haqida»gi (14.11.2024-y., ro‘y.: 3574) buyruqlari, adliya vazirining «Shaxsga doir ma’lumotlarga ishlov berishning namunaviy tartibini tasdiqlash haqida»gi (15.11.2023-y., ro‘y.: 3478) va sohaga oid boshqa qonunchilik hujjatlarida belgilangan ustuvor vazifalarning amalga oshirilishida ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Dissertatsiya respublika fan va texnologiyalar rivojlanishining I. «Demokratik va huquqiy jamiyatni ma’naviy-axloqiy va madaniy rivojlantirish, innovatsion iqtisodiyotni shakllantirishning ustuvor yo‘nalishi»ga muvofiq bajarilgan.

Dissertatsiya mavzusi bo‘yicha xorijiy ilmiy tadqiqotlar sharhi. Tadqiqot ishi xorijiy davlatlarda qisman o‘rganilgan. Xususan, Germaniyada Fraungofer instituti, Kyoln kiberjinoyatchilikni tadqiq etish instituti, Germaniyaning axborot, telekommunikatsiya va mediahuquq instituti, Norvegiyaning Oslo universiteti Norvegiya komyuterlar va huquq ilmiy-tadqiqot markazi, Buyuk Britaniyaning axborot texnologiyalari xavfsizligi markazi, Shveyratsiyaning kiberxavfsizlik kompusi, Kanadaning kiberjinoyatchilikni tadqiq etish xalqaro markazi va uning «International Centre for Comparative Criminology», «Darknet and Anonymity Research Center», «Cybersecurity Laboratory» kabi o‘nlab laboratoriyalari, Shveysariyaning kiberxavfsizlik kompusi, Italiyaning jinoyatchilik va innovatsiyalar bo‘yicha transjinoyatlarni birgalikda tadqiq etish markazi, Kanadaning kiberjinoyatchilikni tadqiq etish xalqaro markazi, Germaniya, Avstraliya, Irlandiya, Buyuk Britaniya, Rossiya, AQSh, Chexiya, Vengriya, Italiya, Latviya, Litva, Niderlandiya, Polsha, Slovakiya, Ispaniya, Gresiya, Turkiya, Belgiya, Portugaliya, Avstriya, Shvesiya, Finlyandiya, O‘zbekistonda kiberxavfsizlik markazlari va boshqa tashkilotlar, shuningdek, BMT o‘zining UNICRI dasturi orqali kiberjinoyatlarga qarshi kurashish bo‘yicha bevosita tadqiqot o‘tkazishadi.

Garchi yuqoridagi tashkilotlar tomonidan jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarni o‘z faoliyati nuqtai nazaridan qisman o‘rganishayotgan bo‘lsa-da, biroq ular ushbu sohani kompleks shaklda ham huquqiy, ham texnik, ham ilmiy jihatdan baravar o‘rganishmaydi.

Muammoning o‘rganilganlik darajasi. Tadqiqot mavzusi bilan bog‘liq ba’zi masalalar u yoki bu darajada o‘rganilganligini ta’kidlash lozim.

Chunonchi, **milliy olimlardan** A. Joldasov, A. Karaxanyan, A. Norov, A. Nosirov, A. Rasulev, B. Kiselev, B. Matmuratov, B. Ulug‘bekov, B. Turdialiyev D. Topildiyeva, F. Batirov, F. Djurayev, I. Toroxodjayeva, I. Ismailov, K. Zinchenko, L. Ismailova, M. Xaydarova, M. Xolmatov, M. Rustamboyev, N. Kaxxarova, N. Polevoy, N. Salayev, P. Shagilov, R. Kabulov, R. Ro‘ziyev, S.Svetkov, U. Nizamedinxodjayev, U. Rasulev, V. Krilov, V. Xurgin, X. Ochilov, Y. Mastinskiy, Y. Solovev, Sh. Xaydarov, Sh. G‘ulomov, Sh. Shamsidinov va boshqalar;

MDH ga kiruvchi davlatlar olimlaridan A. Borovikova, A. Doxoyan, A. Fedorov, A. Kuznesov, A. Volevodz, A. Zinsova, B. Kondrashov, D. Korotchenkov, D. Kiryuxina, Y. Dozorseva, Y. Yefimova, Y. Osipova, F. Kramer, G. Valiaxmetova, I. Maslova, I. Chekunov, K. Belskiy, L. Vens, L. Popov, L. Sukanov, M. Avakyan, N. Bobrovnikova, N. Zorina, O. Cherkasenko, S. Kochoi, S. Starr, S. Stepashin, T. Tropina, T. Volcheskaya;

boshqa **xorijiy olimlardan** N. Paradis, H.Halperin, K. Kern, V.Wenzel, D. Chamberlain, M. Hatta va boshqalar jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar bo‘yicha qisman tadqiqot olib borishgan[7].

Yuqoridagi olimlar jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarni qisman tadqiq etishgan bo‘lsa-da, biroq ular kompleks shaklda ham huquqiy, ham texnik, ham ilmiy jihatdan baravar uni o‘rganishmagan. O‘zbekistonda shu paytga qadar jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar, ularni aniqlash, ularning oldini olish, ularga qarshi kurashish hamda oqibatlarini bartaraf etishga oid munosabatlar aniq qonunchilik hujjatlari bilan tartibga solib qo‘yilmagan, olimlar bu mavzuni to‘liq keng qamrovli va kompleks shaklda o‘rganishmagan.

Dissertatsiya mavzusining dissertatsiya bajarilayotgan oliy ta’lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya mavzusi O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti ilmiy-tadqiqot ishlari rejasiga muvofiq «O‘zbekiston Respublikasida amalga oshirilayotgan sud-huquq tizimidagi islohotlar asosida qonunchilik normalarini takomillashtirish» mavzusidagi ilmiy loyiha doirasida bajarilgan.

Tadqiqotning maqsadi jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning jinoiy-huquqiy jihatlarini tadqiq etish va jamoat xavfsizligini ta’minlash bo‘yicha ilmiy-amaliy taklif va tavsiyalar ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning umumiy tavsifi va tasnifini o‘rganish;

---

[7] Ushbu va boshqa olimlarning ilmiy ishlari dissertatsiyaning foydalanilgan adabiyotlar ro‘yxatida keltirilgan.

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun javobgarlikni belgilash va takomillashtirishning ijtimoiy zaruriyatini aniqlash;

asosiy, qo‘shimcha va fakultativ bevosita obyekti “jamoat xavfsizligi” bo‘lgan kiberjinoyatlarning jinoiy-huquqiy tahlilini amalga oshirish;

xorijiy davlatlarning jinoyat qonunchiligida va xalqaro hujjatlarda jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning jinoiy-huquqiy jihatlarini tahlil qilish;

O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishda raqamli nazoratning roli va ahamiyatini tadqiq etish;

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun jazo muqarrarligini ta’minlashda ushbu jinoyatning vujudga kelish sabablarini aniqlash va ularga qo‘llanilgan jazolarni ijro etishni tushuntirishdan iborat.

Tadqiqotning obyekti jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning jinoiy-huquqiy jihatlarini huquqiy tartibga solish bilan bog‘liq bo‘lgan jinoiy-huquqiy munosabatlardir.

Tadqiqotning predmeti jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning nazariy-huquqiy va yuridik tahlili, jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning xorijiy va xalqaro jinoiy-huquqiy jihatlari, jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun jazo muqarrarligini ta’minlashda raqamli texnologiyalarning o‘rni va rolini huquqiy tartibga solishga qaratilgan normativ-huquqiy hujjatlar, huquqni qo‘llash amaliyoti bilan bog‘liq muammolardan iborat.

Tadqiqotning usullari. Tadqiqot davomida analiz, sintez, deduksiya, induksiya, qiyosiy-huquqiy tahlil, tarixiylik, anketa so‘rovi, empirik materiallar va statistik ma’lumotlar tahlili, kuzatuv, tizimli yondoshuv, mantiqiylik usullaridan keng foydalanilgan. Anketa so‘rovi natijalari dissertatsiyaga 8-ilova tariqasida taqdim etilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

telekommunikatsiya tarmoqlaridan yoki Internet butunjahon axborot tarmog‘idan foydalangan holda ommaviy tartibsizliklarga va fuqarolarga nisbatan zo‘ravonlik qilishga omma oldida da’vat qilish uchun jinoiy javobgarlik belgilanishi jamoat xavfsizligi ta’minlanishi mustahkamlanishiga xizmat qilishi asoslangan;

O‘zbekiston Respublikasi hududida joylashgan texnik vositalarda hamda ma’lumotlar bazalarida shaxsga doir ma’lumotlarni yig‘ishga, tizimlashtirishga va saqlashga oid talablarga rioya etmaslik uchun jinoiy javobgarlik belgilanishi fuqarolarning shaxsiy ma’lumotlarini himoyalash va ijtimoiy barqarorlik ta’minlanishiga hissa qo‘shishi asoslangan;

kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarini toifalash, ularning kiberxavfsizligini ta’minlash darajasini baholash, kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish, axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo‘llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi belgilanishi kiberxavfsizlik sohasidagi munosabatlarni tizimlashtirishga, kibermakonda shaxs, jamiyat va davlat xavfsizligi ta’minlanishiga xizmat qilishi isbotlangan;

qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib jamoat xavfsizligiga tahdid soluvchi jinoyat sodir etish, shu jumladan kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzish va mayning faoliyatini qonunga xilof ravishda amalga oshirish uchun jinoiy javobgarlikni belgilash kiberxavfsizlikni kuchaytirish, kripto-aktivlar bo‘yicha qonunchilik buzilishiga qarshi qat’iy choralar ko‘rish, axborot tizimlariga ruxsatsiz kirish va ulardan noqonuniy foydalanishning barvaqt profilaktikasiga xizmat qilishi asoslangan;

giyohvandlik vositalarini, ularning analoglarini yoki psixotrop moddalarni, ularni targ‘ib qiluvchi mahsulotni telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida tarqatish, reklama qilish, namoyish etish maqsadida tarqatish, reklama qilish, namoyish etish tayyorlash, olish, saqlash, tashish yoki jo‘natish, shuningdek ularni qonunga xilof ravishda o‘tkazish uchun jinoiy javobgarlikni belgilanishi inson hayoti va sog‘lig‘i muhofazasi kuchaytirilishiga xizmat qilishi asoslantirilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning umumiy tavsifi va tasnifi tushuntirildi;

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun javobgarlikni belgilash va takomillashtirishning ijtimoiy zaruriyati ko‘rsatib berildi;

asosiy, qo‘shimcha va fakultativ bevosita obyekti “jamoat xavfsizligi” bo‘lgan kiberjinoyatlarning jinoiy-huquqiy tahlili amalga oshirildi;

xorijiy davlatlarning jinoyat qonunchiligida jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning jinoiy-huquqiy jihatlari ko‘rsatib berildi;

xalqaro hujjatlarda jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning jinoiy-huquqiy jihatlari ochib berildi;

O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishda raqamli nazoratning roli va ahamiyati tushuntirildi;

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun jazo muqarrarligini ta’minlashda ushbu jinoyatning vujudga kelish sabablarini aniqlash va ularga qo‘llanilgan jazolarni ijro etish tartibi tushuntirildi.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi **125** ta davlat organi va tashkiloti, shuningdek, boshqa tashkilotda ishlovchi **3905 nafar xodim**, shu jumladan, 14 ta mahalliy ijroiya hokimiyati, 28 ta yirik korxona, tashkilot va muassasalar, barcha banklar va boshqa tashkilotlar, **Namangan viloyatidagi** 37 ta davlat organlari va tashkilotlari, **21 ta fuqarolik jamiyati institutlari** o‘rtasida o‘tkazilgan so‘rovlar, o‘rganishlar, xorijiy tajriba va milliy qonun hujjatlarining o‘zaro tahlil qilingani, xulosa, taklif va tavsiyalarning amaliyotda joriy etilgani, olingan natijalarning vakolatli tuzilmalar tomonidan berilgan dalolatnomalar tasdiqlangani orqali izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Dissertatsiya ishining ilmiy ahamiyati shundaki, izlanishlar natijasida bildirilgan xulosa, taklif va tavsiyalar jinoyat huquqining nazariy bilimlarini boyitadi va yangi ilmiy tadqiqotlar olib borishga imkon yaratadi hamda undagi ilmiy-nazariy g‘oya va xulosalar O‘zbekiston Respublikasi jinoyat qonunchiligining huquqiy

mexanizmini takomillashtirish bilan bog‘liq masalalarni yanada chuqurroq o‘rganishda ilmiy ahamiyat kasb etadi.

Tadqiqot natijalarining amaliy ahamiyati norma ijodkorligi faoliyatida, xususan, jinoyat qonunchiligini takomillashtirish jarayonida, huquqni qo‘llash amaliyotini takomillashtirishda hamda oliy yuridik ta’lim muassasalarida «Jinoyat huquqi», «Jinoyat protsessi», «Fuqarolik huquqi», «Kibernetika», «Informatika», «Axborot huquqi», «Kiberxavfsizlik», «Kiberxavfsizlik asoslari», «Axborot xavfsizligi asoslari», «Kiberhuquq», «Raqamli huquq» fanlari o‘quv jarayonida ma’ruza va seminarlar o‘tkazish va tadqiqot olib borishda foydalanish mumkin.

Tadqiqot natijasida ishlab chiqilgan ilmiy xulosa va takliflar asosida O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi qonuni qabul qilingan. Ushbu qonun va ilg‘or xorijiy tajriba asosida O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi, Jinoyat va jinoyat-protsesual kodekslarini takomillashtirish bo‘yicha O‘zbekiston Respublikasining qonunlari, O‘zbekiston Respublikasi Prezidentining farmonlari, qarorlari, Vazirlar Mahkamasining qarorlari, idoraviy normativ-huquqiy hujjatlar va boshqa huquqiy hujjatlar ishlab chiqildi va qabul qilindi.

Tadqiqot natijalarining joriy qilinishi. Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning jinoiy-huquqiy jihatlari mavzusidagi tadqiqot ishi bo‘yicha olingan ilmiy natijalar asosida:

1. O‘zbekiston Respublikasining «O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida» 2021-yil 30-martdagi O‘RQ–679-son Qonuni bilan «telekommunikatsiyalar tarmoqlaridan, Internet jahon axborot tarmog‘idan, shuningdek matnni ko‘paytirishning bosma yoki boshqa usullaridan foydalangan holda ommaviy tartibsizliklarga va fuqarolarga nisbatan zo‘ravonlik qilishga omma oldida da’vat qilish» uchun Jinoyat kodeksining 244-moddasining ikkinchi qismi «b»-bandi bilan jinoiy javobgarlik belgilandi. (O‘zkomnazoratning 05.12.2024-yildagi 01/07-1-son dalolatnomasi);

2. O‘zbekiston Respublikasining «O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida» 2021-yil 29-oktabrdagi O‘RQ–726-son Qonuni bilan axborot texnologiyalaridan foydalangan holda, shu jumladan Internet jahon axborot tarmog‘ida O‘zbekiston Respublikasi fuqarolarining shaxsga doir ma’lumotlariga ishlov berilayotganda jisman O‘zbekiston Respublikasi hududida joylashgan texnik vositalarda hamda Shaxsga doir ma’lumotlar bazalarining davlat reestrida belgilangan tartibda ro‘yxatdan o‘tkazilgan shaxsga doir ma’lumotlar bazalarida shaxsga doir ma’lumotlarni yig‘ishga, tizimlashtirishga va saqlashga oid talablarga rioya etmaslik uchun O‘zbekiston Respublikasi Jinoyat kodeksining 141^2-moddasida jinoiy javobgarlik belgilab qo‘yildi (O‘zkomnazoratning 05.12.2024-yildagi 01/07-1-son dalolatnomasi);

3. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida» 2022-yil 15-apreldagi O‘RQ–764-son Qonuni qabul qilindi hamda O‘zbekiston Respublikasi Prezidentining 2024-yil 19-fevraldagi PQ–75-son qarori ijrosi yuzasidan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati raisining

«O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risidagi nizomni tasdiqlash haqida» 2023-yil 4-sentabrdagi 91-son (22.09.2023-y., ro‘y.: 3458), «O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarini toifalash va ularning yagona reestrini shakllantirish tartibi to‘g‘risidagi vaqtinchalik nizomni tasdiqlash haqida» 2024-yil 24-oktabrdagi 118-son (11.11.2024-y., ro‘y.: 3570), «Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o‘tkazish tartibi to‘g‘risidagi nizomni tasdiqlash haqida» 2024-yil 15 oktyabrdagi 113-son (14.11.2024-y., ro‘y.: 3573), «Axborot tizimlari va resurslarining kiberxavfsizligini ta’minlash uchun qo‘llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi to‘g‘risidagi nizomni tasdiqlash haqida» 2024-yil 15-oktabrdagi 114-son (14.11.2024-y., ro‘y.: 3574) buyruqlari qabul qilindi, shuninhdek, O‘zbekiston Respublikasi Prezidentining «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida» 2023-yil 31-maydagi PQ–167-son qarori bilan O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tartibi va O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlarida kiberxavfsizlikning umumiy talablari tasdiqlab qo‘yildi. (Raqamlashtirish vazirligining 14.05.2024-yildagi 20-8/3142-son va O‘zkomnazoratning 05.12.2024-yildagi 01/07-1-son dalolatnomalari);

4. O‘zbekiston Respublikasining «Xotin-qizlar va bolalar huquqlari, erkinliklari hamda qonuniy manfaatlarini ishonchli himoya qilish tizimi yanada takomillashtirilishi munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida» 2023-yil 11-apreldagi O‘RQ–829-son Qonuni bilan O‘zbekiston Respublikasi Jinoyat kodeksining 141^3-moddasida shaxs tanasining va (yoki) jinsiy a’zolarining yalang‘och holdagi foto- va (yoki) videotasvirini o‘z ichiga olgan axborotni uning roziligisiz tarqatish, shu jumladan ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida tarqatish yoxud bunday axborotni tarqatish bilan qo‘rqitish, O‘zbekiston Respublikasining «O‘zbekiston Respublikasining Jinoyat, Jinoyat-protsessual kodekslariga hamda O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksiga o‘zgartirish va qo‘shimchalar kiritish haqida» 2024-yil 19-yanvardagi O‘RQ–899-son Qonuni bilan Jinoyat kodeksining 165-moddasida tovlamachilik jabrlanuvchining axborot resursini yo‘q qilish, o‘zgartirish, egallab olish yoki to‘sib qo‘yish yoki jabrlanuvchi uchun sir saqlanishi lozim bo‘lgan ma’lumotlarni oshkor qilish, uni sharmanda qiladigan uydirmalar tarqatish bilan qo‘rqitib o‘zgadan mulkni yoki mulkiy huquqni topshirishni, mulkiy manfaatlar berishni yoxud mulkiy yo‘sindagi harakatlar sodir etishni talab qilish yoxud jabrlanuvchini o‘zining mulkini yoki mulkka bo‘lgan huquqini berishga majbur qiladigan sharoitga solib qo‘yish, 278^8-moddasida kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzish, 278^9-moddasida mayning faoliyatini qonunga xilof ravishda amalga oshirish uchun jinoiy javobgarlik belgilanib, Jinoyat kodeksining sakkizinchi bo‘limiga «kripto-aktiv» va «mayning» tushunchalari kiritildi hamda O‘zbekiston Respublikasining

«O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida» 2022-yil 19-oktabrdagi O‘RQ–794-son Qonuni bilan Jinoyat kodeksining 168-moddasining uchinchi qismi g-bandida axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib firibgarlik va 169-modda uchinchi qismining «b» bandida qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib o‘g‘rilik jinoyatini sodir etganlik uchun jinoiy javobgarlik belgilab qo‘yilgan. (O‘zkomnazoratning 05.12.2024-yildagi 01/07-1-son dalolatnomasi);

5. O‘zbekiston Respublikasining «O‘zbekiston Respublikasining Jinoyat, Jinoyat-protsessual kodekslariga hamda O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksiga giyohvandlik vositalarining, ular analoglarining yoki psixotrop moddalarning, shuningdek kuchli ta’sir qiluvchi va zaharli moddalarning qonunga xilof muomalasiga qarshi kurashishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish haqida» 2024-yil 5-oktabrdagi O‘RQ–971-son Qonuni bilan Jinoyat kodeksining 251^1-moddasida giyohvandlik vositalari, ularning analoglari yoki psixotrop moddalar hisoblanmaydigan kuchli ta’sir qiluvchi moddalarni targ‘ib qiluvchi mahsulotni tarqatish, reklama qilish, namoyish etish maqsadida telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida tarqatish, reklama qilish, namoyish etish, 273-moddaning uchinchi qismi «d»-bandida telekommunikatsiya tarmoqlaridan, shuningdek Internet jahon axborot tarmog‘idan foydalanib giyovandlik vositalari, ularning analoglari yoki psixotrop moddalarni o‘tkazish maqsadini ko‘zlab qonunga xilof ravishda tayyorlash, olish, saqlash, tashish yoki jo‘natish, o‘tkazish, Jinoyat kodeksining 274-moddasida giyohvandlik vositalarini, ularning analoglarini yoki psixotrop moddalarni targ‘ib qiluvchi mahsulotni tarqatish, reklama qilish, namoyish etish maqsadida telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida tarqatish, reklama qilish, namoyish etish uchun jinoiy javobgarlik belgilandi. (O‘zkomnazoratning 05.12.2024-yildagi 01/07-1-son dalolatnomasi).

Tadqiqot natijalarining aprobatsiyasi. Tadqiqot natijalari 4 ta xalqaro va 8 ta respublika miqyosida o‘tkazilgan ilmiy-amaliy konferensiya va seminarlarda muhokamadan o‘tgan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 31 ta ilmiy ish, shu jumladan, 2 ta monografiya, 2 ta o‘quv-uslubiy qo‘llanma sifatida lug‘at OAKning dissertatsiya asosiy ilmiy natijalarini chop etish tavsiya etilgan nashrlarda 11 ta maqola (2 tasi xorijiy nashrda), xalqaro va Respublika ilmiy-amaliy konferensiya to‘plamlarida 16 ta maqola chop etilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, 10 ta paragrafni qamrab olgan 4 ta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiyaning hajmi 594 betni, shu jumladan asosiy qismi 233 betni tashkil etgan.

DISSERTATSIYANING ASOSIY MAZMUNI

Dissertatsiyaning kirish (dissertatsiya annotatsiyasi) qismida dissertatsiya mavzusining dolzarbligi, tadqiqotning maqsad va vazifalari hamda obyekt va predmeti asoslangan, O‘zbekiston Respublikasi fan va texnologiyasi taraqqiyotining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, tadqiqotning ilmiy yangiligi va amaliy natijalari bayon qilingan, olingan natijalarning nazariy va amaliy ahamiyati ochib berilgan, tadqiqot natijalarini amaliyotga joriy etish, nashr etilgan ishlar va dissertatsiya tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning «**Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning nazariy-huquqiy tahlili**» birinchi bobi ikkita paragrafdan iborat bo‘lib, unda jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning umumiy tavsifi va tasnifi hamda ushbu turdagi kiberjinoyatlar uchun javobgarlikni belgilash va takomillashtirishning ijtimoiy zaruriyati ochib berilgan.

Ushbu bobda muallif jinoyat qonunchiligi va boshqa qonunchilik hujjatlarida «jamoat xavfsizligi» va «jamiyat xavfsizligi» tushunchalarining o‘zaro farq qilishiga ahamiyat berilmaganligini va ular aslida o‘zaro farq qilishini hamda bundan kelib chiqib, qonunchilik hujjatlariga tegishli o‘zgartirish va qo‘shimchalar kiritish zarurligini, qonunchilik hujjatlarida mavjud normalarning to‘g‘ri emasligi ijtimoiy munosabatlarga jiddiy ta’sir ko‘rsatishini, xalqaro hamkorlikda ham bir qator muammolarni vujudga keltirishni tushuntirib o‘tadi.

Bundan tashqari, muallif jamoat xavfsizligiga tahdid soluvchi jinoyatlar, shu jumladan, jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar, jamoat xavfsizligiga qarshi jinoyatlar va jamoat xavfsizligiga qarshi kiberjinoyatlar o‘zaro farq qilishini, xatto jamiyat xavfsizligiga tahdid soluvchi kiberjinoyatlarga qaraganda ushbu jinoyat zararliroq jinoyat hisoblanadi degan fikrni o‘rtaga tashlab, ularni nazariy-huquqiy jihatdan asoslab beradi.

Shuningdek, muallif Jinoyat kodeksining oltinchi bo‘limidagi «*Jamoat xavfsizligi va tartibiga qarshi jinoyatlar*» deya Jinoyat kodeksining XVII bobidagi «*Jamoat xavfsizligiga qarshi jinoyatlar*» va XX bobidagi «*Jamoat tartibiga qarshi jinoyatlar*» alohida boblarda belgilangan holda, ushbu bo‘limda qo‘shimcha ravishda Jinoyat kodeksining XVIII bobidagi «*Transport harakati va undan foydalanish xavfsizligiga qarshi jinoyatlar*», XIX bobidagi «*Giyovandlik vositalari yoki psixotrop moddalar bilan qonunga xilof ravishda muomala qilishdan iborat jinoyatlar*», XX[1] bobidagi «*Axborot texnologiyalari sohasidagi jinoyatlar*» ham ushbu bo‘limda nazarda tutilganligi, jinoyat obyekti nuqtai nazaridan ular o‘zaro farq qilishini bayon qilib o‘tadi.

Muallif asosiy muammo sifatida *«kiberjinoyat», «kibermuhit», «jamoat xavfsizligiga tahdid soluvchi axborot», «jamoat xavfsizligiga tahdid soluvchi jinoyat», «jamoat xavfsizligiga tahdid soluvchi kiberjinoyat», «kiberxavfsizlik», «jamoat xavfsizligi», «jamiyat xavfsizligi»* kabi tushunchalar qonunda aniq nazarda tutilmaganligini, *«kiberxavfsizlik», «kiberjinoyatchilik», «kiberxavfsizlik obyekti», «kiberxavfsizlik subyekti»* tushunchalari qonunda aniq va to‘g‘ri belgilanmaganligi oqibatida muammolar vujudga kelayotganligini ta’kidaylaydi.

Xususan, muallif «*kiberjinoyat*» tushunchasi Jinoyat kodeksi va maxsus qonun – O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonunida aniq nazarda tutilmaganligi uchun axborot texnologiyalaridan foydalanib, axborot texnologiyalari yordamida sodir etilgan jinoyatlar bilan kiberjinoyatlar o‘zaro farq qilsa-da, amaliyotda bunga e’tibor berilmayotganligini, bunga oid nazariy-huquqiy yondashuvlar noto‘g‘ri shakllanayotganligini, «*jamoat xavfsizligi*» va «*jamiyat xavfsizligi*» tushunchasi amalda bitta tushuncha sifatida qonunchilikda inobatga olinib ketilayotganligini, «*kiberxavfsizlik obyekti*» faqatgina axborot tizimi yoki muhim axborot infratuzilmasi bo‘lgan axborotlashtirish tizimidan iborat emasligini, aslida kiberjinoyatlar axborot-kommunikatsiya texnologiyalari, tizim, vosita, qurilma, tarmoq, uskuna, dastur, aloqa, dasturiy ta’minot, axborot bilan ham sodir etilishi mumkinligini va sodir etilayotganligini, xatto ularning o‘ziga nisbatan ham kiberjinoyat содир этилишини amaliy va nazariy tomondan tushuntirib beradi.

Bundan tashqari muallif, «*kiberjinoyatchilik*» tushunchasini berishda uning axborotni ishlov berishga oid boshqa usullar bilan ham sodir etilishini, axborot tizimigagina bog‘lab, bu tushunchaga ta’rif berish, «*kiberxavfsizlik*» tushunchasi bilan o‘zaro bog‘lamaslik xato hisoblanishini asoslab beradi.

«***Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning umumiy tavsifi va tasnifi***» birinchi paragrafida muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning nazariy-huquqiy mazmun-mohiyatini ochib bergan.

Muallif ushbu paragrafda *«jamoat», «jamiyat», «jinoyat», «kiberjinoyat», «jamoat xavfsizligi», «jamiyat xavfsizligi», «jamoat xavfsizligiga tahdid soluvchi jinoyatlar», «jamiyat xavfsizligiga tahdid soluvchi jinoyatlar», «jamoat xavfsizligiga qarshi jinoyatlar», «jamiyat xavfsizligiga qarshi jinoyatlar», «jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar», «jamiyat xavfsizligiga tahdid soluvchi kiberjinoyatlar», «jamoat xavfsizligiga qarshi kiberjinoyatlar», «jamiyat xavfsizligiga qarshi kiberjinoyatlar», «kibermuhit», «kibermakon», «kibertahdid», «kiberxavfsizlik hodisasi», «kiberxavfsizlik obyekti», «kiberxavfsizlik subyekti»* kabi tushunchalarning mazmun-mohiyatini ochib berib, ularning o‘zaro farq qilishini nazariy-huquqiy jihatdan asoslab bergan.

Shunga ko‘ra, Jinoyat kodeksining oltinchi bo‘limi va undagi boblarning jamoat xavfsizligiga emas, balki jamiyat xavfsizligiga qarshi qaratilgan jinoyatlar, shu jumladan, kiberjinoyat ekanligini, jamoat xavfsizligi jamiyat xavfsizligidan o‘zaro farq qilishini, shaxs, jamiyat va davlat o‘rtasida jamoat xavfsizligiga oid munosabatlar vujudga kelishini muallif tushuntirgan holda, nazariy-huquqiy jihatdan ushbu bo‘lim va undagi boblarni qayta ko‘rib chiqish zarurligini asoslagan.

Muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning klassifikatsiyasini, ularni vertikaliga ko‘ra, umumiy, turdosh, maxsus va bevosita obyekti jamoat xavfsizligi bo‘lgan kiberjinoyatlarga bo‘linishini, bevosita obyekti jamoat xavfsizligi bo‘lgan kiberjinoyatlar o‘z navbatida asosiy, qo‘shimcha va fakultativ bevosita obyekti jamoat xavfsizligi bo‘lgan kiberjinoyatlarga bo‘linishini, ularga amaldagi Jinoyat kodeksining qaysi moddalari taalluqli ekanligini, ushbu kiberjinoyatlarning zaruriy belgilarini sanab, axborot-

kommunikatsiya texnologiyalari axborot texnologiyalari va telekommunikatsiya texnologiyalaridan iboratligini ta’kidlab, qolgan texnologiyalar ularning tarkibiy qismi sanalishini hamda kiberjinoyatlar ulardan foydalangangan holda yoki ularga nisbatan sodir etilishini ilmiy va amaliy jihatdan tushuntirgan.

*«**Jinoyat qonunchiligida jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun javobgarlikni belgilashning ijtimoiy zaruriyati**»* ikkinchi paragrafida muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun javobgarlikni belgilashning 23 ta ijtimoiy zaruriyatini asoslab bergan.

Xususan, kiberjinoyatlarning soni 2020-2025-yillar davomida deyarli **80 barobarga** ko‘payganligi, xatto ushbu jinoyatlar bo‘yicha alohida statistika yuritilayotganligi, sodir qilinayotgan kiberxavfizlik hodisalari uchun amaldagi Jinoyat kodeksimizda yetarlicha jinoiy javobgarlik belgilab qo‘yilmaganligi oqibatida qariyb **90 foiz** kiberjinoyatlar latent shaklida sodir etilib, **11 mingdan ortiq** shaxsga doir ma’lumotlar bazasi, **1500 ga yaqin** axborot tizimlari, **36 mln.ga yaqin** telekommunikatsiyalar xizmatlaridan foydalanuvchilar va ularga aloqador bo‘lgan shaxslarning qonunchilikdagi huquqlari, ma’lumotlari, shaxs, jamiyat va davlat xavfsizligiga tahdid vujudga kelayotganligi, amaldagi qonunchilik hujjatlarida mulkdorlar, foydalanuvchilar va kiberxavfsizlik subyektlarining qonunchilik hujjatlari bo‘yicha olgan majburiyatlarining bajarilmasligi qonunchilikka muvofiq javobgarlikni keltirib chiqarishi belgilangan holda, amaldagi Jinoyat kodeksida bu bo‘yicha yetarlicha javobgarlik belgilanmaganligi, buning oqibatida jamoat xavfsizligiga tahdidlar kuchayib borayotganligi, buning uchun jinoiy-huquqiy tomondan Jinoyat kodeksida jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun yetarlicha jinoiy javobgarlikni belgilash va mavjud qonunchilikni qayta ko‘rib chiqib, uni takomillashtirish zarurligi nazarda tutilgan.

Dissertatsiyaning **«Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning yuridik tavsifi»** ikkinchi bobida muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarni obyektiga qarab, asosiy, qo‘shimcha va fakultativ bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarga ajratilganligini inobatga olib, ularning jinoiy-huquqiy tahlilini ko‘rsatib o‘tadi.

Muallif «jamoat xavfsizligi»ga bevosita yoki bilvosita ta’sir ko‘rsatishiga qarab, asosiy, qo‘shimcha va fakultativ bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlar o‘zaro farq qilishini, ushbu turdagi jinoyatlarning subyektiv tomondan doimo qasddan, kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib axborot-kommunikatsiya texnologiyalari, shu jumladan, telekommunikatsiya infratuzilmalari orqali sodir etilishi va boshqa jinoyatlardan, shuningdek, axborot-kommunikatsiya texnologiyalari yordamida va undan foydalanib sodir etiladigan jinoyatlardan o‘zaro farq qilishini, ushbu turdagi jinoyatlar kiberjinoyatning bir turkumi yoki guruhiga kiruvchi kiberjinoyat ekanligini va o‘zining obyekti bilan boshqa kiberjinoyatlardan o‘zaro farq qilishini tushuntirib o‘tgan.

Shuningdek, muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar kiberjinoyatlarning bir turi sifatida o‘zining keng qamrovligi va ijtimoiy xavfi bo‘yicha boshqa kiberjinoyatlar o‘zaro farq qilishini, bir vaqtning o‘zida yoki

alohida-alohida tartibda shaxs, jamiyat va davlat manfaatlariga xavf tug‘dirishini ta’kidlab o‘tadi.

Tadqiqot davomida muallif sun’iy intellektning tashkilotchi, dalolatchi va yordamchi sifatida jinoyat ishtirokchisi bo‘lishi mumkinligini, biroq bu bo‘yicha uning jinoiy javobgarligi Jinoyat kodeksimizda nazarda tutilmaganligini qayd etadi. Sun’iy intellekt jinoyat ishida tashkilotchi sifatida barcha axborot tizimlari, sun’iy intellektlar o‘zaro integratsiya qilinishi orqali kompleks axborot tizimidan iborat bo‘lgan sun’iy intellekt yaratilgan vaqtida u tashkilotchi sifatida tegishli axborot tizimlari yoki sun’iy intellekt bo‘lgan boshqa tizimlarga noqonuniy kirib yoki ulanib olgan holda, shaxsga nisbatan qasddan turli xil jinoyatlarni sodir etishi, xatto jamiyatda tartibsizliklarni vujudga keltirishi, aholini manipulyatsiya qilishi va boshqa noqonuniy harakatlari oqibatida jamoat xavfsizligiga tahdid solishi mumkinligini ta’kidlaydi. Sun’iy intellekt yordamchi sifatida chat-bot yoki boshqacha ko‘rinishda kiberjinoyatchiga maslahatlar berishi, xatto ko‘rsatmalari bilan, vositalar berishni tashkil qilish yoki to‘siqlarni yo‘qotish bilan ko‘maklashish, shuningdek kiberjinoyat sodir etish quroli, izlari va vositalarini yoxud jinoiy yo‘l bilan qo‘lga kiritilgan narsalarni yashirishga, shuningdek bunday narsalarni olish va o‘tkazish to‘g‘risida oldindan va’da bergan holda, jinoyat ishtirokchisi bo‘lishi mumkinligini bayon qiladi. Sun’iy intellekt manipulyatsiya qilish yoki tovlamachilik qilish yo‘li bilan boshqa jinoyat yoki kiberjinoyat tayyorgarlik ko‘rilishiga yoki jinoyat sodir etilishiga rahbarlik qilgan holda, jinoyat ishtirokchisi bo‘lishi mumkin.

Ijtimoiy tarmoqlarning keng rivoji, uning qulayliklari bir tomondan insoniyatga foyda tegsa, ikkinchi tomondan unga sun’iy intellektning kirib kelishi turli xil shaxslarning har xil jinoyatlar, shu jumladan, kiberjinoyat sodir etilishiga qiziqtirishda sun’iy intellektga vosita rolini bajarmoqda. Sun’iy intellekt qasddan manipulyatsiya, tovlamachilik va boshqa yo‘llar orqali bir vaqtning o‘zida jabrlanuvchi bo‘lgan shaxslarga tegishli jinoyat yoki kiberjinoyat sodir etilishiga qiziqtirishi bilan dalolatchi sifatida jinoyat ishtirokchisiga aylanishi mumkin.

Shu sababli sun’iy intellekt orqali jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning keng tarqalishining oldini olish uchun axborot tizimlarini o‘zboshimchalik bilan strategik o‘ylamasdan o‘zaro integratsiya qilish, ularning raqamli izlarini loglash, ularni saqlash, hisobini avtomatik yuritishning texnik imkoniyatini sun’iy intellektga hech qachon to‘liq bermaslik, uning raqamli nazoratini amalga oshirish zarurligini muallif ta’kidlab o‘tadi.

«***Asosiy bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarning jinoiy-huquqiy tahlili***» paragrafida muallif asosiy bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarning yuridik tahlilini bayon qilib, jinoiy-huquqiy tahlilini dissertatsiya ilovalarida ko‘rsatgan.

Muallif ushbu paragrafda jamoat xavfsizligiga qarshi qaratilgan, ya’ni bevosita jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning jinoiy-huquqiy tahlilini amalga oshirgan.

«***Qo‘shimcha bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarning jinoiy-huquqiy tahlili***» ikkinchi paragrafida muallif qo‘shimcha bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarning

yuridik tahlilini bayon qilib, jinoiy-huquqiy tahlilini dissertatsiya ilovalarida ko‘rsatgan.

Muallif ushbu paragrafda jamoat xavfsizligiga tahdid soluvchi axborot texnologiyalari yoki raqamli texnologiyalar sohasiga kiruvchi kiberjinoyatlarning jinoiy-huquqiy tahlilini amalga oshirgan.

«***Fakultativ bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarning jinoiy-huquqiy tahlili***» uchinchi paragrafida muallif fakultativ bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlarning yuridik tahlilini bayon qilib, jinoiy-huquqiy tahlilini dissertatsiya ilovalarida ko‘rsatgan. Muallif ushbu paragrafda asosiy va qo‘shimcha obyekti bilan bir qatorda fakultativ ta’siri bo‘lgan boshqa kiberjinoyatlarning jinoiy-huquqiy tahlilini amalga oshirgan.

Dissertatsiyaning **«Jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning xorijiy va xalqaro jinoiy-huquqiy jihatlari»** uchinchi bobida muallif 150 dan ortiq xorijiy davlatlarda va 50 dan ortiq xalqaro hujjatlarda jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning jinoiy-huquqiy jihatlarini ko‘rsatib o‘tgan.

Muallif ushbu bobda kiberjinoyatlar deganda faqatgina texnik tomondan axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar tushunmaslik kerakligini ilmiy, amaliy, huquqiy, texnik jihatdan xorijiy tajriba asosida tushuntirib bergan. Shuningdek, muallif axborot tizimiga noqonuniy kirish, tarmoqqa noqonuniy ulanib olish, axborot tizimiga noqonuniy yoki qonuniy kirgan holda, noqonuniy harakatlarni amalga oshirish, tarmoqqa noqonuniy ulanib yoki tarmoqdan qonuniy foydalanayotgan vaqtida noqonuniy harakatlar qilish, kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib, qonunchilik bilan tarqatilishi taqiqlangan yoki cheklangan yohud maxfiy axborot toifasiga kiritilgan axborotni noqonuniy tarqatish harakatlari ham kiberjinoyat bo‘lishini, tarmoqdan va axborot tizimidan ruxsat bilan foydalangan taqdirda ham noqonuniy harakatlar qilish kiberhuquqbuzarlikni keltirib chiqarishi mumkinligini, axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki foydalanishdan tashqari axborotni uzatish, tarqatish, egasizlantirish kabi harakatlar bilan ham kiberjinoyat sodir etilishi mumkinligi va buning uchun ham xorijiy davlatlarda va xalqaro qonunchilikda yetarlicha javobgarlik belgilab qo‘yilganligi ko‘rsatilgan.

*«**Xorijiy davlatlarning jinoyat qonunchiligida jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning jinoiy-huquqiy jihatlari**»* paragrafida muallif xorijiy davlatlarning jinoyat qonunchiligini tadqiq etgan. Xususan, Buyuk Britaniya, Fransiya, Germaniya, Albaniya, Gresiya, AQSh, Ispaniya, Italiya, Belgiya, Niderlendiya, Singapur, Xitoy, Hindiston, Malayziya, Indoneziya, Rossiya, Qozog‘iston, Qirg‘iziston, Tojikiston, Ozorboyjon, Armaniston, Gruziya, Sloveniya, Latviya, Finlandiya, Norvegiya, BAA, Saudiya Arabistoni, Kanada va boshqa xorijiy davlatlarning jinoyat qonunchiligida jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun alohida jinoiy javobgarlik borligini, bu turdagi jinoyatlar ularning jinoyat qonunchiligida alohida bo‘lim, bob yoki moddalarda aks ettirilganligini tushuntirib o‘tgan.

«***Xalqaro hujjatlarda jamoat xavfsizligiga tahdid soluvchi ayrim kiberjinoyatlarning jinoiy-huquqiy jihatlari***» ikkinchi paragrafida muallif xalqaro hujjatlarda jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun dunyo davlatlarida alohida jinoiy javobgarlik bo‘lishi zarurligi va uni amalga oshirish mexanizmi qanday bo‘lishi darkorligi ko‘rsatilgan. Muallif 12 ta xalqaro hujjatlardan 4 tasiga O‘zbekiston qo‘shilganligini, kiberjinoyatlar xalqaro transchegaraviy jinoyat bo‘lganligi sababli dunyo davlatlari bilan O‘zbekiston o‘zaro hamkorlikdan manfaat ko‘rishi mumkinligini tahlil qilib, qolgan 8 ta xalqaro hujjatlarga qo‘shimcha shartlar bilan O‘zbekiston Respublikasi qo‘shilishi zaruriyatini tushuntirib bergan.

Dissertatsiyaning **«Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun jazo muqarrarligini ta’minlashda raqamli texnologiyalarning o‘rni va roli»** to‘rtinchi bobida muallif O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishda raqamli nazoratning roli va ahamiyati hamda jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun jazo muqarrarligini ta’minlashda ushbu jinoyatning vujudga kelish sabablarini aniqlash va ularga qo‘llanilgan jazolarni ijro etish tartibi haqida so‘z yuritgan. Ushbu bobda muallif nafaqat kiberjinoyatlar, balki jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar bo‘yicha vakolatli idoralar tomonidan amalga oshirayotgan islohotlar yetarlicha o‘zini oqlamayotganligini, vakolatli idoralar raqamli texnologiyalardan unumli foydalanmayotganligini, huquqiy targ‘ibot tizimli va samarali yo‘lga qo‘yilmaganligini, «yashil», «sariq» va «qizil» toifalarga ajratilgan mahallalardagi kriminogen vaziyat bo‘yicha yo‘lga qo‘yilgan mavjud tartib-taomillar kiberjinoyatlarga qarshi kurashishda yetarlicha naf keltirmasligini, fuqarolik jamiyati institutlari, mahalliy davlat vakillik organlari, mahalliy ijroiya hokimiyati organlari, sud, nazorat va huquqni muhofaza qiluvchi organlar faoliyatini to‘liq qayta ko‘rib chiqish va bugungi kun talablariga moslashtirish, tezkor-qidiruv organning kiberxodimi, kiberprokuror, kibersudya va boshqa kiberxavfsizlikni ta’minlashga mas’ul shaxslarning aniq vazifalar taqsimotini belgilash, jinoyat qonunchiligimizni qayta ko‘rib chiqish, anglosakson qonunchiligi qoidalaridan yetarlicha foydalanish zarurligini ko‘rsatib bergan.

*«**O‘zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishda raqamli nazoratning roli va ahamiyati**»* paragrafida muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar raqamlashtirish orqali yaratilgan infratuzilmalar yoki ular bilan bog‘liq bo‘lgan axborotga nisbatan amalga oshirilayotganligi xususida to‘xtalib o‘tadi. Mazkur turdagi jinoyatlar uchun amalga oshirilayotgan islohotlar o‘zini yetarlicha oqlamayotganligini, an’anaviy usullardan voz kechib, axborot-kommunikatsiya texnologiyalari, shu jumladan, raqamli texnologiyalardan unumli foydalanish zaruriyatini, raqamli nazorat deya atalayotgan «Ping» ma’lumotga asoslangan, «Raqamli nazorat» kompleks axborot tizimi orqali jamoat xavfsizligini to‘liq ta’minlash imkoniyati mavjud emasligini, balki u orqali jamoat xavfsizligiga tahdidlar vujudga kelishi mumkinligini tushuntirib o‘tadi.

Muallif vujudga kelgan og‘ir vaziyatni faqatgina «**Jamoat xavfsizligining raqamli monitoringi**» kompleks axborot tizimi va uning tarkibiy qismi sanalgan «**Log menejment**», «**Raqamli jamoatchilik**», «**CYBER**», «**Bolalar xavfsizligi**»,

«**Kelajak**», «**Aqlli ta’lim**», «**CYBERSTAT**», «**CYBERPREVEN**», «**CYBERPROB**» kompleks axborot tizimlarini to‘liq yo‘lga qo‘yish, fuqarolarning shaxsga doir ma’lumotlariga ishlov berishning alohida shartlariga rioya qilishga mas’ul bo‘lgan messenjer va ijtimoiy tarmoq mulkdorlari va operatorlarining faoliyati hamda foydalanuvchilarning barcha axborotini to‘liq nazorat qilish imkonsizligi sababli foydalanuvchilarning eng muhim axborotlarining raqamli ma’lumotlari xavfsizligini ta’minlash orqali qisman, biroq hozirgiga qaraganda samaraliroq natijalarga erishish mumkinligini tushuntirib bergan. Ushbu axborot tizimlari ichida «**Jamoat xavfsizligining raqamli monitoringi**» kompleks axborot tizimiga sun’iy intellektni jory qilish mumkin emas, qolgan axborot tizimlari esa, sun’iy intellekt texnologiyalarini yo‘lga qo‘yish mumkin, bundan yopiq axborot bilan ishlovchi tizimlarning tarkibiy qismi mustasno. Yuqorida ta’kidlangan axborot tizimlarining har biri o‘zaro integratsiya qilinishi mumkin hamda raqamli izlari loglash yo‘li bilan saqlanadi va avtomatik hisobi yuritib boriladi. Bundan tashqari, boshqa zarur axborot tizimlari ularga integratsiya qilinishi darkor. Misol uchun, “Qalqon” axborot tizimi orqali “xavfsiz shahar” loyihasi va boshqa loyihalar hamda tashabbuslar bilan yurtimizda o‘rnatilgan videomakamera yozuvi orqali qidiruvdagi shaxslarni sun’iy intellekt yoki avtomatlashtirilgan tizimlar orqali aniqlash mumkin. Biroq ushbu tizimda sun’iy intellektning mavjud emasligi, “aqlli linza”, “aqlli ko‘zoynak” kabi texnologiyalarning qo‘llanilmayotganligi, qolaversa, mahalla inspektoriga kelib tushayotgan xabarda aynan qidiruvdagi shaxs uning hududiga kelganligi alohida avtomatik xabar berishi yo‘lga qo‘yilmaganligi, xabarlar avtomatik tahlil qilinmayotganligi va xabardor etish tizimida kamchiliklar borligi sababli mazkur tizimni takomillashtirib, axborotni «**Raqamli jamoatchilik**» axborot tizimiga ham yo‘naltirib berish yo‘lga qo‘yilishi maqsadga muvofiq.

«***Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun jazo muqarrarligini ta’minlashda ushbu jinoyatning vujudga kelish sabablarini aniqlash va ularga qo‘llanilgan jazolarni ijro etish***» ikkinchi paragrafida muallif jamoat xavfsizligiga tahdid soluvchi qilmishlarning oldini olish, ularni aniqlash, kiberjinoyatchini fosh etish, uni ushlash, kiberjinoyatlarning oqibatlarini bartaraf etishda raqamli texnologiyalarning o‘rnini hamda jazoni ijro etish tartibini tushuntirib beradi. Ushbu paragrafda muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarni ijro etishda ushbu jinoyatlarning vujudga kelish sabablariga e’tibor qaratish zarurligini alohida ta’kidlab o‘tadi. Muallif kiberjinoyat uchun qo‘llanilgan jazoning ijrosini ta’minlashda taqdimnoma, xususiy ajrim yuborishda surishtiruvchi, tergovchi, prokuror va sudya har bir kiberjinoyatning vujudga kelish sababini albatta o‘rganishi darkorligini ta’kidlab, amaliyotda Namangan viloyati misolida o‘rganilganida ushbu subyektlar tomonidan yuborilgan taqdimnoma va xususiy ajrimlar vakolatli organlarning bayonnomalari va foto-hisobotlari bilan ijrosini noto‘g‘ri ta’minlanayotganligi, vujudga kelgan kiberjinoyatning oqibatlari amalda bartaraf etilishi bo‘yicha biron bir ijobiy ishlar amalga oshirilmayotganligini ta’kidlab o‘tadi. Muallif agarda jazo to‘liq ijro etilishini va shu kabi qilmishlar boshqa takrorlanmasligini xohlasalar albatta taqdimnoma va xususiy ajrimda kiberjinoyatning vujudga kelish sabablarini unda qayd etib,

uning oqibatlarini vakolatli organlar tomoridan bartaraf etilishi tartibini tushuntirib o‘tadi. Bundan tashqari, muallif jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar jazo muqarrarligini ta’minlash va kiberjinoyatlarning kamayishiga erishish uchun kiberjinoyatchilarga qo‘llanilayotgan jazoni to‘liq qayta ko‘rib chiqish zarurligini, zararni undirishga ko‘proq e’tibor qaratib, imtiyozli normalarni ko‘proq belgilash orqali bu turdagi jinoyatlar bilan kurashish mumkinligini bayon qiladi.

XULOSA

Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarni huquqiy tartibga solishni kompleks tadqiq etish davomida milliy, xalqaro, xorijiy tajriba tahlil qilinib, olimlarning doktrinal qarashlari ko‘rib chiqilib, quyidagi konseptual xulosalar qilindi va tegishli qonunchilik hujjatlarini yanada takomillashtirish yuzasidan ilmiy-amaliy taklif hamda tavsiyalar ishlab chiqildi:

I. Ilmiy-nazariy xulosalar

1. «*Jamoat*» va «*jamiyat*», shuningdek, «*jamoat xavfsizligi*» va «*jamiyat xavfsizligi*» tushunchalari o‘zaro farq qilganligi va amaldagi qonunchiligimizda ushbu tushunchalarning o‘zaro bir mazmunda noto‘g‘ri qo‘llanilayotganligi sababli ularni dissertatsiya 6- va 20-ilovasiga muvofiq tahrirda qo‘llash maqsadga muvofiqdir. Xususan, «**jamoat xavfsizligi** – tarixiy taraqqiyotning muayyan bosqichida, aniq bir hududda, maqsad va o‘y fikrlari o‘zaro o‘xshash yoki bir xil bo‘lgan jismoniy shaxslar, yuridik shaxslar yoki davlatdan iborat subyektlar ixtiyoriylik va tenglik tamoyillari asosida aniq bir maqsad sari birlashishi natijasida vaqtinchalik tuzilgan ijtimoiy tuzilmaning ichki va tashqi xavfdan himoyalanganlik holati» bo‘lsa, «**jamiyat xavfsizligi** – hududiy joylashuvidan qat’i nazar, fikrlar xilma-xilligi asosida tarixan shakllangan, aniq va bir xil maqsadga ega bo‘lmagan, doimiy asosda faoliyat yurituvchi ijtimoiy, iqtisodiy, siyosiy tizimlarni va (yoki) katta miqyosdagi odamlar guruhi, ya’ni millat, xalq, davlatni qamrab oluvchi, davlat tomonidan tan olingan, muayyan toifa, sinf, yo‘nalish, soha, tuzum, hokimiyat yoki ta’limot atrofida birlashgan insonlar guruhidan iborat ijtimoiy tuzilmaning ichki va tashqi xavfdan himoyalanganlik holati» sanaladi; Bunda, jamoat xavfsizligiga bo‘layotgan tahdid individual, jamoaviy va milliy (institutsional) xavf darajasi bilan milliy xavfsizlik bilan jamoat xavfsizligi o‘zaro bog‘liq bo‘ladi va jamoat xavfsizligi ishtirokchilari jismoniy va yuridik shaxslar hamda davlat sanaladi va ular aralash yoki bir turdagi subyektlardan iborat shaklda tuzilgan bo‘lishi mumkin.

2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunda «kiberxavfsizlik obyekti» sifatida axborot tizimlari hamda muhim axborot infratuzilmalari mavjud bo‘lgan axborotlashtirish tizimlari nazarda tutilgan. Biroq, «kiberxavfsizlik obyekti»ga axborot, aloqa, axborot resursi, tarmoq, tizim, vosita, qurilma, uskuna, dastur, dasturiy ta’minot ham kirishi mumkinligi inobatga olinmagan hamda «kiberxavfsizlik» tushunchasining ta’rifi juda keng bayon etilgan, uning ta’rifini berishda «kiberjinoyatchilik» va «kiberxavfsizlik obyekti» tushunchalari ushbu tushuncha bilan bevosita bog‘liqligi, «kiberjinoyatchilik»

tushunchasiga ta’rif berishda qonun chiqaruvchi mazkur Qonunda nazarda tutilgan boshqa usullarda ham kiberjinoyat sodir etilishi mumkinligi e’tiborga olinmagan. Oqibatda O‘zbekiston Respublikasida kiberjinoyatchilik va kiberxavfssizlik sohalariga oid qonunchilik alohida rivojlanmoqda, zarur tadbirlar amalga oshirilmoqda. Qonunchilik yetarlicha to‘g‘ri tizimlashtirilmaganligi natijasida amaliyot noto‘g‘ri yo‘nalishga qarab shakllanmoqda va ushbu holatga chek qo‘yish juda zarur sanaladi. Shu sababli dissertatsiyada nazarda tutilgan asoslardan kelib chiqib, «kiberjinoyat», «kiberjinoyatchilik», «kibermuhit», «kibermakon», «kiberxavfsizlik», «kiberxavfsizlik obyekti»ga quyidagicha ta’riflar ishlab chiqildi:

«**kiberjinoyat** – Jinoyat kodeksi bilan taqiqlangan, axborot-kommunikatsiya texnologiyalari orqali kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib sodir etiladigan va buning uchun Jinoyat kodeksida jazo qo‘llash tahdidi bo‘lgan aybli ijtimoiy xavfli qilmish (harakat yoki harakatsizlik);

kiberjinoyatchilik – kiberjinoyatlar yig‘indisi bo‘lib, u kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib axborotni egallash, uni o‘zgartirish, yo‘q qilish, uzatish, tarqatish, ishlov berish, egasizlantirish, foydalanish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida axborot-kommunikatsiya texnologiyalari orqali amalga oshiriladigan jinoyatlar majmui;

kibermuhit – axborot-kommunikatsiya texnologiyalari orqali axborot-kommunikatsiya tizimi, shu jumladan, axborot tizimi hamda aloqa, axborotlashtirish, telekommunikatsiya, sun’iy intellekt, bio-, nono-, kibertexnologiyalar infratuzilmasi va boshqa texnik vositalarda yoki ular orasida yaratilgan kibermakon, shart-sharoitlar, hodisalar va holatlarni o‘z ichiga oluvchi hamda virtual olam haqida axborot beruvchi muhit;

kibermakon – axborot-kommunikatsiya texnologiyalari orqali axborot-kommunikatsiya tizimi, shu jumladan, axborot tizimi hamda aloqa, axborotlashtirish, telekommunikatsiya, sun’iy intellekt, bio-, nono-, kibertexnologiyalar infratuzilmasi va boshqa texnik vositalarda yoki ular orasida yaratilgan kibermuhitdagi aniq o‘rin, joy, nuqta va hudud;

kiberxavfsizlik — kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib kiberxavfsizlik obyektlari hamda ularga bog‘langan shaxs, jamiyat, davlat va jamoat manfaatlarining tashqi va ichki tahdidlardan muhofaza qilishga qaratilgan huquqiy, tashkiliy va texnik chora-tadbirlar majmui orqali ta’minlanadigan xavfsizlik holati;

kiberxavfsizlik obyekti – axborot-kommunikatsiya texnologiyalari, shu jumladan, axborot, raqamli, sun’iy intellekt, telekommunikatsiya, bio-, nono-, kibertexnologiyalar, shu bilan birga, ularga bog‘liq bo‘lgan vositalar, qurilmalar, uskunalar va boshqa texnik vositalar, axborot-kommunikatsiya tizimi, shu jumladan, axborot tizimi yoki ulardagi axborotning kibertahdid va kiberxavfsizlik hodisasidan himoya qilinishi hamda kiberxavfsizligi ta’minlanuvchi ulardagi mavjud resurslar, infratuzilmalar, tizimlar, muhim axborot infratuzilmasi obyektlari bo‘lgan kiberhimoyaga olingan yoki olinmaganligidan qat’iy nazar kiberhimoya qilinishi zarur bo‘lgan obyekt;»;

3. Amaldagi qonunchilikda «*jamoat*» va «*jamiyat*», «*jamoat xavfsizligi*» va «*jamiyat xavfsizligi*», «*jamiyat xavfsizligiga tahdid soluvchi jinoyat*» va «*jamiyat xavfsizligiga tahdid soluvchi kiberjinoyat*», «*jamoat xavfsizligiga tahdid soluvchi jinoyat*» va «*jamoat xavfsizligiga tahdid soluvchi kiberjinoyat*», «*jamoat xavfsizligiga tahdid soluvchi axborot*» tushunchalarining ta'riflari nazarda tutilmaganligi hamda jamiyat va jamoat xavfsizligini ta'minlovchi alohida sohaviy maxsus qonunlar mavjud emasligi va bu boradagi munosabatlarni tartibga solib qo‘yish jinoyat qonunchiligimizdagi qonuniylik prinsipining to‘liq amalda namoyon bo‘lishiga sabab bo‘ladi. Shu sababli O‘zbekiston Respublikasining «Jamiyat xavfsizligi to‘g‘risida»gi va «Jamoat xavfsizligi to‘g‘risida»gi qonunlar qabul qilinib, tegishincha ushbu tushunchalarning ta'riflari ushbu qonunlarda nazarda tutilib, ularga kiruvchi jinoyatlar guruhi belgilab qo‘yilishi darkor. Bunda, fikrimizcha,

«jamoat xavfsizligiga tahdid soluvchi axborot – tarixiy taraqqiyotning muayyan bosqichida, aniq bir hududda, maqsad va o‘y fikrlari o‘zaro o‘xshash yoki bir xil bo‘lgan jismoniy shaxslar, yuridik shaxslar yoki davlatdan iborat subyektlar ixtiyoriylik va tenglik tamoyillari asosida aniq bir maqsad sari birlashishi natijasida vaqtinchalik tuzilgan ijtimoiy tuzilmaning ichki va tashqi xavfdan himoyalanganlik holatiga kibertahdid soluvchi yoki kiberxavfsizlik hodisasi vujudga keltiruvchi Jinoyat kodeksi bilan taqiqlangan, axborot-kommunikatsiya texnologiyalari orqali kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib sodir etiladigan va buning uchun Jinoyat kodeksida jazo qo‘llash tahdidi bo‘lgan aybli ijtimoiy xavfli qilmish (harakat yoki harakatsizlik)larni keltirib chiqaruvchi destruktiv axborotning bir turi;

jamoat xavfsizligiga tahdid soluvchi jinoyatlar – tarixiy taraqqiyotning muayyan bosqichida, aniq bir hududda, maqsad va o‘y fikrlari o‘zaro o‘xshash yoki bir xil bo‘lgan jismoniy shaxslar, yuridik shaxslar yoki davlatdan iborat subyektlar ixtiyoriylik va tenglik tamoyillari asosida aniq bir maqsad sari birlashishi natijasida vaqtinchalik tuzilgan ijtimoiy tuzilmaning ichki va tashqi xavfdan himoyalanganlik holatiga tahdid soluvchi Jinoyat kodeksi bilan taqiqlangan va jazo qo‘llash tahdidi bo‘lgan aybli ijtimoiy xavfli qilmish (harakat yoki harakatsizlik)lar;

jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar – tarixiy taraqqiyotning muayyan bosqichida, aniq bir hududda, maqsad va o‘y fikrlari o‘zaro o‘xshash yoki bir xil bo‘lgan jismoniy shaxslar, yuridik shaxslar yoki davlatdan iborat subyektlar ixtiyoriylik va tenglik tamoyillari asosida aniq bir maqsad sari birlashishi natijasida vaqtinchalik tuzilgan ijtimoiy tuzilmaning ichki va tashqi xavfdan himoyalanganlik holatiga kibertahdid soluvchi yoki kiberxavfsizlik hodisasi vujudga keltiruvchi Jinoyat kodeksi bilan taqiqlangan, axborot-kommunikatsiya texnologiyalari orqali kibermuhitda, shu jumladan, kibermakonda yoki undan foydalanib sodir etiladigan va buning uchun Jinoyat kodeksida jazo qo‘llash tahdidi bo‘lgan aybli ijtimoiy xavfli qilmish (harakat yoki harakatsizlik)lar», – deb bayon etilishi maqsadga muvofiq;

4. Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar, shu jumladan boshqa kiberjinoyatlar dissertatsiya 2-ilovasida nazarda tutilgan o‘ziga xos xususiyatlarga

ega hamda ularning obyekti, sodir etish usuli yoki vositasi, subyekti, subyektiv tomoniga qarab tasniflash mumkin va dissertatsiyada biz ularni obyektiga va bevosita obyektiga qarab tasnifladik. Xususan, ushbu turdagi kiberjinoyatlarni bevosita obyektiga ko‘ra, asosiy, qo‘shimcha va fakultativ obyekti «*jamoat xavfsizligi*» bo‘lgan kiberjinoyatlarga bo‘ldik hamda jinoyat qonunchiligimizdagi qonuniylik prinsipi va kiberjinoyatlarning hozirgi holatidan kelib chiqib, ularning jinoiy-huquqiy tahlilini dissertatsiya asosiy qismi va uning 7-, 10-, 12- va 14-ilovalarida to‘liqroq ko‘rsatdik;

5. Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning zaruriy belgilarini asosiy va maxsus belgilarga ajratib, qo‘riqlanadigan ijtimoiy munosabat, ijtimoiy xavfli qilmish, javobgarlik yoshi, aqli rasolik, **ayb asosiy zaruriy belgi**, kibermuhit, shu jumladan, kibermakon, axborot, aloqa, shu jumladan, radiochastota, telekommunikatsiya, pochta aloqasi, axborot-kommunikatsiya texnologiyalarini **maxsus zaruriy belgilarga** kiradi, deb guruhladik, tergov va sud amaliyotini o‘rganib jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarning qurollari va vositalariga dissertatsiyaning 22-ilovasidagi axborot-kommunikatsiya texnologiyasi infratuzilmalari kirishi aniqlandi va ularning ro‘yxati tuzib chiqildi hamda ***axborot-kommunikatsiya texnologiyalari*** *– axborotni yaratish, uzatish, ishlash va boshqarish bilan bog‘liq texnologiyalar”* bo‘lib, u axborot texnologiyalari va telekommunikatsiya texnologiyalaridan iborat ekanligi, raqamli, bulutli, bio, nono, kiber, sun’iy intellekt, blokcheyn va axborot yoki (va) aloqa mavjud bo‘lgan boshqa texnologiyalar ushbu texnologiyalarning tarkibiy qismi sanalishi tushuntirildi;

6. Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar obyekti murakkab obyekt bo‘lib, jamoat xavfsizligiga bo‘layotgan kibertahdid va xavf-xatarlarga qarab, o‘zgarib boradi va ushbu obyektlarga dissertatsiya 23-ilovasidagi kiberxavfsizlik obyektlari kiradi. Bunda, qasd jamoat xavfsizligiga bevosita yoki bilvosita qaratilganiga qarab, asosiy, qo‘shimcha va fakultativ bevosita obyekti «jamoat xavfsizligi» bo‘lgan kiberjinoyatlar o‘zaro farq qiladi. Biroq, barchasida kibertahdid yoki kiberhujum jamoat xavfsizligiga tahdid solishi mumkin.

7. Kibermuhitda, shu jumladan, kibermakonda amalga oshirilishi kutilayotgan shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar yoki ularning majmui **kibertahdid** bo‘lsa, **kiberhujum** ushbu tahdidning amalga oshirilishiga oid xarakat sanalishi nazarda tutilib, kibertahdid, kiberhujum, kiberxavfsizlik hodisasi, kiberhuquqbuzarlik, kiberjinoyat o‘zaro farq qilishi dissertatsiyada ko‘rsatib berildi va ularning tushunchalarining ta’riflari ishlab chiqildi;

8. Jinoyat kodeksining oltinchi bo‘limidagi boblar ushbu bo‘lim nomi va mazmuniga mos emasligi, obyekti turlicha ekanligi, «*jamiyat*» va «*jamoat*», «*jamiyat xavfsizligi*», «*jamoat xavfsizligi*» tushunchalarining o‘zaro farqi borligi sababli qonuniylikni ta’minlash maqsadida Jinoyat kodeksining oltinchi bo‘limining nomini quyidagicha bayon etish taklif qilinadi:

«Oltinchi bo‘lim. Jamiyat xavfsizligi va tartibiga tahdid soluvchi jinoyatlar».

9. Jinoyat kodeksining oltinchi bo‘limida taklif sifatida Jinoyat kodeksining XVII bobidagi «*Jamoat xavfsizligiga qarshi jinoyatlar*», XVIII bobidagi «*Transport harakati va undan foydalanish xavfsizligiga qarshi jinoyatlar*», XIX bobidagi «*Giyovandlik vositalari yoki psixotrop moddalar bilan qonunga xilof ravishda muomala qilishdan iborat jinoyatlar*», XX bobidagi «*Jamoat tartibiga qarshi jinoyatlar*»ni ular avvalo jamoat, balki jamiyat xavfsizligiga tahdid soluvchi jinoyatlarning asosiy, qo‘shimcha, fakultativ bevosita obyekti jamiyat xavfsizligini ta’minlovchi ijtimoiy munosabatlar ekanligidan kelib chiqib, qayta ko‘rib chiqish va XX[1] bobidagi «*Axborot texnologiyalari sohasidagi jinoyatlar*» bir vaqtning o‘zida asosiy bevosita obyekti axborot texnologiyalari sohasi ekanligidan kelib chiqib, axborot texnologiyalari o‘z navbatida faqatgina jamoat yoki jamiyat xavfsizligiga oid tushuncha emas, balki **shaxs va davlatga bog‘liq bo‘lgan tushuncha ekanligidan kelib chiqib**, alohida oltinchi kichik bo‘lim sifatida quyidagicha shakllantirilishi taklif qilinadi:

«**Oltinchi kichik bo‘lim. Axborot-kommunikatsiya texnologiyalari sohasiga oid jinoyatlar**»;

10. Kiberjinoyat faqatgina texnik vositalarning boshqa bir texnik vositalarga zarar keltirishi yoki ularga noqonuniy kirib olish orqali axborotni egallash, o‘zlashtirish va yaroqsiz holatga keltirish orqali sodir etiladigan qilmish emas, balki u shaxs, jamiyat va davlat manfaatlariga axborot orqali ham tahdid qiladigan jinoyat sanaladi. Shuningdek, axborot texnologiyalari yordamida sodir etiladigan jinoyatlar, axborot texnologiyalaridan foydalanib sodir etiladigan jinoyatlar va kiberjinoyatlar o‘zaro farq qiladi. Shu sababli kiberjinoyatlar bilan axborot texnologiyalari bog‘liq bo‘lgan boshqa jinoyatlarni aralashtirib yubormaslik zarur hamda qonunchilikdagi xatoliklar bartaraf etilmog‘i darkor. Bunda, an’anaviy usullarda jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar bilan yetarlicha kurashib bo‘lmaydi va nafaqat jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar, balki axborot-kommunikatsiya texnologiyalari bilan sodir etilayotgan barcha kiberjinoyatlar bo‘yicha texnologik yechimlar ishlab chiqilishi darkor hamda jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarga qarshi kurashishning eng samarali usuli bu sun’iy intellekt, «aqlli tizimlar»ga asoslangan raqamli nazorat va monitoringni to‘liq yo‘lga qo‘yish, raqamli texnologiyalardan unumli foydalanish maqsadga muvofiq;

11. O‘zbekiston Respublikasining kiberxavfsizlik konsepsiyasi, qisqa, o‘rta va uzoq muddatga mo‘ljallangan milliy kiberxavfsizlik strategiyasi, ularni amalga oshirish rejasi (yo‘l-xarita) hamda ular asosida O‘zbekiston Respublikasining kiberjinoyatchilikka qarshi kurashish konsepsiyasi, qisqa, o‘rta va uzoq muddatga mo‘ljallangan kiberjinoyatchilikka qarshi kurashish strategiyasini qabul qilish zarur. 42-ilovaga muvofiq konsepsiya loyihasi tayyorlandi. Ta’kidlash kerakki bunda, yuqoridagi hujjatlar asosida jamoat xavfsizligiga tahdid soluvchi munosabatlar keng qamrovga ega ekanligi va ushbu munosabatlarni yetarlicha to‘liq tartibga solib qo‘yish uchun Axborot kodeksi, Axborot-kommunikatsiya texnologiyalari kodeksi, «Onlayn-platformalar va veb-sayt foydalanuvilarining huquqlarini himoya qilish to‘g‘risida», «Kiberbulling to‘g‘risida»gi, «Kiberagressiya to‘g‘risida»gi yoki «Kiberbullingga qarshi kurashish

to‘g‘risida»gi, «Sun’iy intellekt to‘g‘risida»gi, «Jamoat xavfsizligi to‘g‘risida»gi «Jamiyat xavfsizligi to‘g‘risida»gi Qonun qabul qilinishi maqsadga muvofiq. Shuningdek, xalqaro maydonda sodir bo‘layotgan kiberjinoyatlar bo‘yicha yuridik shaxslarning jinoiy javobgarligini belgilash maqsadga muvofiq hamda xalqaro maydonda nafaqat jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar, balki barcha kiberjinoyatlar uchun ham dunyo davlatlari bir-biriga o‘xshash yoki bir xil jinoiy javobgarlikni belgilashi, sud-tergov amaliyotini birxillashtirishi, axborot-kommunikatsiya texnologiyalaridan foydalanib sodir etilgan ma’muriy huquqbuzarliklar va jinoyat ishlari yuzasidan anglo-sakson qonunchiligini tadbiq etish, romana-german qonunchiligiga qaraganda ko‘proq samara beradi, shu sababli ushbu ishlarda bu oilaga oid qonunchilikni qo‘llash orqali kiberjinoyatchilikka qarshi kurashish va bu borada kiberjinoyat uchun jazo muqararligini ta’minlash uchun aralash milliy qonunchilikni ishlab chiqib, amaliyotga tadbiq etish maqsadga muvofiq;

12. Axborot tizimi, axborot texnologiyalari, telekommunikatsiya yoki internet tarmog‘ida yoki undan foydalanib va boshqa usullarda jinoyat sodir etganlikka oid Jinoyat kodeksiga kiritilayotgan har xil o‘zgartirish va qo‘shimchalarga oid turlicha amaliyotdan voz kechib, bir xil huquqiy va texnik jihatdan amaliyot to‘g‘ri bo‘lishi uchun ularning o‘rniga «*axborot-kommunikatsiya texnologiyalaridan foydalanib*» so‘zlarini almashtirish maqsadga muvofiq. Zero, kiberjinoyatlar Jinoyat kodeksimizda nazarda tutilgan holatlardan tashqari boshqa usullar bilan ham sodir etilishi mumkin, shu sababli ularni bir xil bayon etish uchun mazkur taklifni amaliyotga kiritish joizdir.

II. O‘zbekiston Respublikasining qonunchilik hujjatlarini takomillashtirish bilan bog‘liq bo‘lgan taklif va tavsiyalar:

O‘zbekiston Respublikasining qonunchilik hujjatlarini takomillashtirish bilan bog‘liq bo‘lgan taklif va tavsiyalar quyidagilardan iborat:

1. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida» 2022-yil 15-apreldagi O‘RQ–764-son Qonunining 3-moddasidagi «**kibermakon**», «**kiberxavfsizlik hodisasi**», «**kibertahdid**», «**kiberxavfsizlik obyekti**», «**kiberxavfsizlik subyekti**» tushunchalari **yuqorida biz tomonimizdan ta’kidlangan tushunchalarning ta’rifi bilan almashtirilishi** hamda **ushbu Qonunga qo‘shimcha ravishda «kiberjinoyat» va «kibermuhit» tushunchalarini** dissertatsiyaning 21-ilovasiga muvofiq ishlab chiqilgan O‘zbekiston Respublikasining qonuni loyihasida nazarda tutilgan tahrirda kiritish taklif qilinadi.

Shuningdek, «kiberjinoyat», «kibermuhit», «kibermakon», «jamoat xavfsizligiga tahdid soluvchi axborot» va «jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar» uchun jinoiy javobgarlikni belgilashning ijtimoiy zaruriyatidan kelib chiqib, bu tushunchalarning ta’rifini biz tomonimizdan ta’riflangani kabi Jinoyat kodeksining VIII bo‘limi yoki yangi tahrirda qabul qilinadigan Jinoyat kodeksida ham aks ettirish maqsadga muvofiq.

2. Jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar uchun munosib javobgarlikni belgilash maqsadida mavjud resurs va ilg‘or xorijiy tajriba asosida

Jinoyat kodeksiga dissertatsiyaning 21-ilovasiga muvofiq axborot va kiberxavfsizlikni yanada kuchaytirishga qaratilgan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish darkor;

3. Dastlabki bosqichda BMT Bosh Assambleyasining 2024-yil 24-dekabrdagi 79/243-son rezolyusiyasi bilan tasdiqlangan Kiberjinoyatchilikka qarshi konvensiyasi, keyingi bosqichlarda Yevropa Kengashining «Kiberjinoyatchilik to‘g‘risida» 2001-yil 23-noyabrdagi Konvensiya (Budapesht konvensiyasi) va uning 2 ta qo‘shimcha bayonnomalari va boshqa xalqaro hujjatlarga qo‘shimcha shartlar bilan a’zo bo‘lish va shu orqali xalqaro transchegeraviy munosabatlarda xorijiy davlatlar bilan yaqindan hamkorlik qilish hamda milliy qonunchilik bilan xorijiy va xalqaro jinoyat qonunchiligini o‘zaro birxillashtirish va yaqinlashtirish maqsadga muvofiq.

4. O‘zbekiston Respublikasi o‘zining dunyo davlatlari tomonidan qabul qilinadigan BMTning «Kiberxavfsizlik to‘g‘risida»gi Konvensiyasini ishlab chiqishi va uni BMT qabul qilishi uchun zarur tartib-taomillarni amalga oshirishi maqsadga muvofiq;

5. Kibersug‘urta tizimi yo‘lga qo‘yilib, bunga oid qonunchilik to‘liq amaliyotga joriy qilinishi va kiberhuquqbuzarliklar, shu jumladan, kiberjinoyatlar natijasida yetkazilgan zararni hisoblash metodikasi, kiberjinoyatlar uchun sanksiyalarni belgilash tartibini qabul qilish kerak;

6. Kibermudofaa tizimi yo‘lga qo‘yilib, bunga oid qonunchilik to‘liq amaliyotga joriy qilinishi, kiberinqirozlarni sun’iy ravishda vujudga keltirish, unga qarshi kurashish va oqibatlarini bartaraf etish bo‘yicha yagona va yakdil tizim yo‘lga qo‘yilishi hamda kiberinqirozlarga nisbatan bardoshlilik indekslari va mezonlari ishlab chiqilishi va amaliyotga tatbiq etilishi, vazirlik va idoralarning o‘xshash va takroriy vazifalari va funksiyalarini xatlovdan o‘tkazib, ularni birxillashtirish va tizimlashtirish darkor;

7. Shaxsga doir ma’lumotlar bazasi va bulutli texnologiyalarga oid majburiy maxsus yuridik va texnik talablarni belgilash, shaxs, jamiyat va davlatga doir ma’lumotlar bazasidan tashqari ularga doir raqamli ma’lumotlarning muhofazasini ham ta’minlash va ularga oid qonunchilik to‘liq ishlab hamda kibermuxitda, shu jumladan, kibermakonda raqamli nazoratni o‘rnatish tartib-taomillarini, shu jumladan, davlat organlari va tashkilotlarining, shuningdek, xususiy sektor vakillarining aniq vazifa va majburiyatlari amaldagi qonunchilikda aniq belgilanishi darkor;

8. Raqamli nazoratdagi infratuzilmalarga nisbatan kiberhujumlar qachon, qaerda va kim tomonidan amalga oshirilayotganligini bilish, kiberjinoyatchilarni fosh etish uchun qurilmalarning MAC-adressiga oid tartibot belgilanishi va dissertatsiya 16-ilovasiga muvofiq tahrirda ishlab chiqilgan Vazirlar Mahkamasining alohida qarori qabul qilinib, ijroga qaratilishi darkor;

9. Dissertatsiyaning 17-ilovasiga muvofiq O‘zbekiston Respublikasida raqamli nazoratni amalga oshirish tartibi to‘g‘risidagi nizom va ularning tarkibiy qismi bo‘lgan nizom, reglament va boshqa hujjatlar asosida raqamli nazoratni o‘rnatishning bitta usuli sifatida ishlab chiqilgan O‘zbekiston Respublikasi Prezidentining qarori loyihasining ilovalari qabul qilinishi zarur va u O‘zbekiston

Respublikasining raqamli transformatsiyasi ustidan raqamli nazorat ta’minlanishiga xizmat qiladi;

10. Kiberxavfsizlik subyektlari tomonidan qonunchilik bo‘yicha olgan majburiyatlarini bajarmasligi bo‘yicha Ma’muriy javobgarlik to‘g‘risidagi kodeks va Jinoyat kodeksida alohida javobgarlik chorasi belgilanishi shart;

11. Bolalarning shaxsiy akkaunt va profilini ochish huquqi vujudga kelishining aniq yoshi, ota-onalar, qonuniy vakillarning o‘z ehtiyotsizligi oqibatida jinoiy javobgarlikka tortish yoshiga yetmagan bolalari tomonidan sodir etilayotgan kiberjinoyatlar uchun ularga aniq ma’muriy va jinoiy javobgarlik belgilash kerak.

12. O‘zbekiston Respublikasining «Axborotlashtirish to‘g‘risida»gi Qonunida «sun’iy intellekt», «sun’iy intellekt texnologiyalari», «axborot texnologiyasi» tushunchasining o‘rniga «axborot-kommunikatsiya texnologiyalari», «axborot tizimi» tushunchasining o‘rniga «axborot-kommunikatsiya tizimi» tushunchasining ta’rifini berish va ushbu Qonunga o‘zgartish va qo‘shimchalar kiritish zarur.

III. Kiberjinoyatchilik sohasida qonunchilik hujjatlarini qo‘llash amaliyotini takomillashtirish bilan bog‘liq bo‘lgan taklif va tavsiyalar:

Kiberjinoyatchilik sohasida qonunchilik hujjatlarini qo‘llash amaliyotini takomillashtirish bilan bog‘liq bo‘lgan taklif va tavsiyalar quyidagilardir:

1. O‘zbekiston Respublikasining qonunchilik hujjatlarini takomillashtirish bilan bog‘liq bo‘lgan taklif va tavsiyalarda nazarda tutilgan Jinoyat kodeksiga kiritilgan o‘zgartish va qo‘shimchalardan iborat mazkur moddalardan tashqari boshqa moddalardagi qilmishlar ham axborot-kommunikatsiya texnologiyalari sohasidagi jinoyatlar yoki kiberjinoyatlar bo‘lishi mumkin, biroq mavjud ijtimoiy munosabatlarning rivoji va ijtimoiy zaruriyati tufayli ularning axborot-kommunikatsiya texnologiyalari yoki tizimi yohud telekommunikatsiya tarmog‘i va vositasi orqali sodir etilishi holatini og‘irlashtiruvchi belgisi sifatida qabul qilish va JKning 56-moddasiga kiritilayotgan qo‘shimchadan unumli foydalanish maqsadga muvofiq.

2. Kiberjinoyatlar, shu jumladan, jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlar bo‘yicha sud amaliyoti turlicha bo‘lmoqda va uni birxillashtirish zarur va buning uchun ushbu yo‘nalishda alohida maxsus O‘zbekiston Respublikasi Oliy sudi Plenumining qarorini qabul qilish darkor.

3. O‘zbekiston Respublikasi Oliy sudi Plenumi axborot-kommunikatsiya texnologiyalari sohasi va kiberjinoyatlarga oid qarorida O‘zbekiston Respublikasining «Axborotlashtirish to‘g‘risida»gi, «Kiberxavfsizlik to‘g‘risida»gi qonunlarida va Telekommunikatsiya xizmatlarini ko‘rsatish qoidalarida operator, provayder, shuningdek, foydalanuvchining axborot xavfsizligi va kiberxavfsizlik bo‘yicha alohida majburiyati borligini va ushbu majburiyatning buzishi oqibatida bu turdagi jinoyatlar vujudga kelishiga sudlar e’tiborni qaratishi kerakligi bo‘yicha alohida tushuntirish berishi zarur va shu orqali mavjud amaliyotdagi bo‘shliq mavjud qonunchilik bilan to‘g‘ri yo‘naltirilgan holda, to‘ldirilishi mumkin.

4. Aloqa, axborotlashtirish, elektron hukumat, elektron raqamli imzo, sun’iy intellekt, raqamli texnologiyalar, raqamlashtirish, telekommunikatsiya va boshqa sohalarga oid nazorat tadbirlarini o‘tkazish tartibini belgilash kerak;

5. Raqamli nazoratni amalga oshirish tartib-taomillari ishlab chiqilib, amaliyotga tatbiq etilishi, aniq qonunchilik hujjatlari bilan majburiy qoidalar belgilanishi, davlat va xususiy sektor o‘rtasidagi o‘zaro hamkorlik to‘liq va to‘g‘ri o‘rnatilishi, majburiy interatsiya qilinadigan axborot tizimlariga qo‘yilgan talablarni belgilash va shundan foydalanib, zarur barcha axborot tizimlarini to‘liq integratsiya qilish, integratsiyalashuv jarayoni yakunlanguniga mavjud axborot tizimlarining yangi versiyalarini ishga tushirish, qo‘shimcha modul va funksiyalarni qo‘shishdan tashqari yangi axborot tizimlarini yaratish va joriy qilishga maratoriy e’lon qilish kerak, shundan keyin yagona raqamli platforma orqali kiberxavfsizlikni ta’minlash bo‘yicha zarur choralar ko‘rish darkor;

6. Respublika raqamli texnologiyalar ekspertiza markazini tashkil etish va uni axborot-kommunikatsiya texnologiyalari sohasida o‘tkazilayotgan ekspertiza turlarini amalga oshiruvchi yagona davlat ekspertiza muassasasini belgilash hamda sud-kompyuter texnikaviy ekspertizasining o‘rniga dalillarning olinishi, saqlanishi, to‘planishi, foydalanuvi, ishlov berilishida qonun buzilishi bo‘lmaganligi, dalillarning ishonchliligi va olingan manbalarning aniq va to‘g‘ri ekanligini ta’minlovchi **sud-kiber ekspertiza**, shuningdek, telekommunikatsiya tarmog‘i, telekommunikatsiya infratuzilmasi, axborot tizimi va kompyuter axboroti, dastur va dasturiy ta’minot, kriptografik hamda aloqa qamrovi va sifati ekspertiza turlari amaliyotga joriy qilinishi darkor;

7. «Kiberxavfsizlik», «Kiberxavfsizlik asoslari», «Kiberhuquq» kabi fanlar va kiberxavfsizlikka oid o‘quv dasturlari va qo‘llanmalarni ishlab chiqib, ularni boshlang‘ich, o‘rta, o‘rta-maxsus va oliy ta’limda majburiy va uzluksiz o‘qitilishini yo‘lga qo‘yish, yuridik va texnik fanlar bo‘yicha yagona kiberxavfsizlik bo‘yicha mutaxassis yetishtiruvchi oliy ta’lim tashkilotini tashkil etish va eng muhimi, oliy ta’limda kadrlar tayyorlash uchun mavjud standart va klassifikator qayta ko‘rib chiqilishi, o‘quv dasturlari har bir kiberjinoyat uchun qonunchilikda belgilangan javobgarlikka qarab, ushbu qilmishni fosh etish va jazo muqarrarligini ta’minlash uchun qanday yuridik va texnik xarakatlar kompleks tartibda amalga oshirilishi zarurligidan kelib chiqib amaliyotga joriy etilishi zarur;

8. Kibermuxitda, shu jumladan, kibermakonda raqamli nazoratni o‘rnatish uchun «**Jamoat xavfsizligining raqamli monitoringi**» kompleks axborot tizimini to‘liq ishga tushirish va unga barcha davlat organlari va tashkilotlari, mulkchilik shaklidan qat’iy nazar barcha kiberxavfsizlik subyektlarining axborot tizimlari ulanishi, ularning maxfiylik siyosatiga rioya etgan holda ular ustidan raqamli nazoratni amalga oshirish kerak;

9. Xalqaro va milliy kibermaydonda bo‘layotgan kiburxurujlar bo‘yicha xalqaro hamkorlik, murojaatlar bilan ishlash, kiberxurujlar bo‘yicha tezkor xabar berish, javoblar olish va qayta aloqa mavjud bo‘lgan 24/7 rejimda ishlovchi ishonch telefoni, aloqa markazlari faoliyatini yo‘lga qo‘yish hamda O‘zbekiston Respublikasidagi barcha axborot infratuzilmalarini xatlovdan o‘tkazish va muhim axborot infratuzilmalarining reestrini shakllantirish, ularning reestrini muntazam yuritib borilishini ta’minlash kerak;

10. Raqamli nazorat **«Jamoat xavfsizligining raqamli monitoringi» kompleks axborot tizimi** orqali axborot-kommunikatsiya infratuzilmasi

toifalangan holda, amalga oshirilishi maqsadga muvofiq hamda respublikadagi barcha axborot tizimlari, ma’lumotlar bazalari va banklari, telekommunikatsiya tarmoqlari va ularning tarkibiy qismlari o‘zaro integratsiya qilinib, raqamli nazorat o‘rnatilganidan keyin **ushbu tizimdagi tegishli axborot tizimining** sun’iy intellekti orqali jinoyatchilik va kriminogen vaziyatdan kelib chiqib, kelgusida qachon va qayerda jinoyatlar sodir etilishi mumkinligi bo‘yicha bashorat qilish, prognoz qilish tizimi yo‘lga qo‘yilishi darkor va u orqali mavjud resurslarni qachon va qaerga olib borish va shu orqali kiberjinoyatchilikni fosh etishning samarali texnik yechimi va tizimini yo‘lga qo‘yish mumkin.

11. Axborot xavfsizligi yoki kiberxavfsizlik talablarini foydalanuvchiga buzgan taqdirda telekommunikatsiya tarmoqlari orqali avtomatik sun’iy intellekt va vakolatli organlar tomonidan foydalanuvchiga bepul sms-xabarnoma yuborib, unda uning huquqbuzarligi va uni to‘xtatishi zarurligi bo‘yicha eslatma taqdim etish, yuborilgan sms-xabarnomani olgan bo‘lsa-da, o‘z qilmishini davom ettirgan shaxslarga nisbatan og‘irroq jazo qo‘llash va o‘z qilmishini davom ettirishdan ixtiyoriy qaytgan shaxslarni javobgarlikdan ozod etish, yuborilgan sms-xabarnoma va uni haqiqatan ham huquqbuzar olganligi faktni tasdiqlovchi ma’lumotlarni dalil sifatida qabul qilish tartibi yo‘lga qo‘yilishi shart.

12. Xalqaro maydonda O‘zbekiston Respublikasining kiberxavfsizlik bo‘yicha nufuzini oshirish maqsadida kiberxavfsizlikni ta’minlash reytingi, IT-audit yo‘lga qo‘yilib, xalqaro jinoyat huquqida kiberjinoyatlarga oid yagona namunadagi terminologiya tanlanishi hamda model qonunlar qabul qilinishi hamda jamoat xavfsizligini ta’minlovchi axborot-kommunikatsiya texnologiyalariga oid dunyo standartlarga javob beruvchi milliy texnik vosita, tarmoq, qurilma, tizim, dastur va dasturiy ta’minot ishlab chiqarilishi yoki tayyorlanishi va amaliyotga to‘liq joriy etilishi zarur;

13. Moliya va bank sohasida raqamli operatsiyalarning barqarorligini ta’minlash, veb-sayt va axborot tizimlarining 41-ilovaga muvofiq raqamli izlarning saqlanishi yo‘lga qo‘yilib, uning hisobini yuritish tartiвлариni belgilash hamda jamoat xavfsizligi va kiberxavfsizlik to‘liq va yetarlicha ta’minlanishi uchun axborot-kommunikatsiya tizimlarining barchasini to‘liq integratsiya qilish maqsadga muvofiq emas, balki ularni toifalash orqali o‘zaro integratsiyasini va uning raqamli nazoratini amalga oshirish maqsadga muvofiq.

Mazkur xulosalarimiz tadqiqot ishida asoslantirilgan bo‘lib, ushbu takliflarning qabul qilinishi jamoat xavfsizligiga tahdid soluvchi kiberjinoyatlarga qarshi kurashish bo‘yicha yagona nazariy, ilmiy, amaliy, huquqiy, texnik, tashkiliy tomondan yagona amaliyot vujudga kelishiga, qonunchilik hujjatlari takomillashishiga, shaxs, jamiyat va davlat manfaatlari, shu jumladan, jamoat xavfsizligi va kiberxavfsizlik ta’minlanishiga, bu boradagi islohotlar yangi bosqichga ko‘tarilishiga xizmat qiladi.

НАУЧНЫЙ СОВЕТ № DSc.32/30.12.2020.Yu.74.01 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ УНИВЕРСИТЕТЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

УНИВЕРСИТЕТ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

АНОРБОЕВ АМИРИДДИН УЛУҒБЕК ЎҒЛИ

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ КИБЕРПРЕСТУПЛЕНИЙ, УГРОЖАЮЩИХ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

12.00.08 – Уголовное право. Уголовно-исполнительное право

Автореферат
диссертации доктора юридических наук (DSc)

Ташкент – 2025

Тема диссертации доктора юридических наук (DSc) зарегистрирована в Высшей аттестационной комиссии (ВАК) при Министерстве высшего образования, науки и инноваций Республики Узбекистан за номером B2023.1. DSc/Yu235.

Диссертация выполнена в Университете общественной безопасности Республики Узбекистан.

Автореферат диссертации размещен на трех языках (узбекском, русском, английском (резюме)) на сайте информационно-образовательного портала «ZiyoNET» (www.ziyonet.uz).

Научный консультант:	**Рустамбаев Мирзаюсуп Хакимович,** доктор юридических наук, профессор
Официальные оппоненты:	**Уразалиев Мурод Кораевич** доктор юридических наук, профессор
	Турғунбоев Элбекжон Одилжонович доктор юридических наук
	Акром Икромович Тошпўлатов доктор юридических наук, доцент
Ведущая организация:	**Институт криминологических исследований Республики Узбекистан**

Защита диссертации состоится «12» декабря 2025 года в 11-00 часов на заседании Научного совета № DSc.32/30.12.2020.Yu.74.01 по присуждению ученых степеней при Университете общественной безопасности Республики Узбекистан. (Адрес: 100211, Ташкентская обл., Зангиотинский район, поселок Чорсу. Тел.: (99871) 230-32-71; факс: (99871) 230-32-50; info@mgjxu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Университета общественной безопасности Республики Узбекистан (зарегистрирован за № _____). (Адрес: 100121, Ташкентская обл., Зангиотинский район, поселок Чорсу. Тел.: (99871) 230-32-71; факс: (99871) 230-32-50)

Автореферат диссертации разослан «28» ноября 2025 года.

(Реестр протокола рассылки № 21 от «28» ноября 2025 года)

Д.М.Миразов
Заместитель председателя Научного совета по присуждению ученых степеней, доктор юридических наук, профессор

Ж.Д.Ахмедов
Научный секретарь Научного совета по присуждению ученых степеней, доктор философии по юридическим наукам (PhD)

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

ВВЕДЕНИЕ (аннотация диссертации доктора наук (DSc))

Актуальность и необходимость темы диссертации. В мире цифровизация всех сфер и отраслей, информационные системы и ресурсы, критически важная информационная инфраструктура, телекоммуникации, включая глобальную сеть Интернет, базы персональных данных, информационно-телекоммуникационная инфраструктура, информационно-коммуникационные технологии, в том числе искусственный интеллект, кибер-, нано-, био- и другие технологии и технические средства – всё это подвержено серьёзной угрозе со стороны киберпреступлений, что ставит под угрозу общественную безопасность. В 2023 году одна кибератака происходила каждые 39 секунд, а в настоящее время – уже каждые 14 секунд[1]. Согласно другим источникам, кибератаки совершаются каждую секунду[2]. В результате этого, в 2023 году 71% организаций по всему миру стали жертвами программ-вымогателей. В настоящее время 80% всех инцидентов в сфере кибербезопасности связаны с деятельностью преступных группировок[3]. Ущерб, нанесённый мировой экономике, составил 3 трлн долларов в 2018 году, 3,5 трлн долларов в 2019 году, 4,2 трлн долларов в 2020 году, 6 трлн долларов в 2021 году, 7 трлн долларов в 2022 году, 8,4 трлн долларов в 2023 году и 9,5 трлн долларов в 2024 году[4]. Ожидается, что в 2025 году эта цифра достигнет **10,5 трлн долларов**[5], в 2026 году – **20 трлн долларов**, в 2027 году – 22 трлн долларов, в 2028 году – 24 трлн долларов, а в 2029 году – 26 трлн долларов[6]. Удвоение ущерба к 2026 году подчёркивает настоятельную необходимость немедленного и скоординированного реагирования со стороны всех государств мира путём совместной борьбы с киберпреступностью как международным трансграничным преступлением и проведения широкомасштабных реформ в этой области.

Во мире в целях предотвращения экономических кризисов, возникающих вследствие киберпреступлений, и устранения их негативных последствий, защиты интересов личности, общества и государства, обеспечения общественной безопасности и кибербезопасности государства осуществляют широкомасштабные меры по всесторонней борьбе с указанными кибертрансграничными преступлениями на основе международных документов. Для противодействия данным киберпреступлениям в системе образования проводятся кардинальные реформы, подготавливаются специалисты, специализирующиеся в области кибербезопасности, создаются специальные лаборатории, высшие

---

[1] https://www.datensicherheit.de/2024-2025-cyber-attack-companies-14-seconds.
[2] https://cybermap.kaspersky.com/ru/stats.
[3] https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts/#sources.
[4] https://newsletter.radensa.ru/archives/4840.
[5] https://www.cenlanow.com/business/press-releases/ein-presswire/674883055/cybercrime-damages-to-cost-the-world-9-5-trillion-usd-in-2024/.
[6] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide#:~:text=The%20global%20cost%20of%20cybercrime,trillion%20U.S.%20dollars%20in%202022.

образовательные и научно-исследовательские учреждения, используются искусственный интеллект и автоматизированные «интеллектуальные системы» для прогнозирования и анализа киберинцидентов, выделяются благотворительные, грантовые и бюджетные средства на обеспечение кибербезопасности, принимаются меры по совершенствованию и унификации законодательства в сфере трансграничных отношений, посредством чего осуществляется их систематизация, а также выстраивается единая правовая и техническая практика – от технических и технологических процессов до юридических вопросов. Всё это, в свою очередь, приобретает актуальное значение для нахождения научно-теоретического и практического решения задач обеспечения общественной безопасности.

В нашей Республике посредством нормотворчества и цифровизации осуществляются масштабные реформы по обеспечению общественной безопасности, кибербезопасности и верховенства закона. В частности, с целью создания безопасной киберсреды, включая киберпространство, в 2017–2025 годах было принято около 150 законодательных актов и реализовано около 500 масштабных мероприятий. Однако дальнейшее развитие цифровых технологий, а также то обстоятельство, что в уголовном законодательстве нашей страны ответственность за киберпреступления, угрожающих общественной безопасности, не определена в достаточной степени и в этой сфере до сих пор сохраняются «правовые пробелы», приводит к возникновению «латентных» киберпреступлений, число, виды и масштабы причиненного ущерба которых с каждым днем возрастают, а также к увеличению количества «коллизионных ситуаций» в процессе правоприменения. Так, только в Республике Узбекистан было зарегистрировано совершение деяний с использованием информационных технологий: в 2020 году – 863, в 2021 году – 785, в 2022 году – 7 570, в 2023 году – 6 450, в 2024 году – 58 800. Таким образом, количество киберпреступлений в 2024 году по сравнению с 2020 годом возросло примерно в 68,13 раза. В связи с этим, возрастающая угроза киберпреступлений общественной безопасности обусловливает необходимость достаточного правового регулирования данной сферы.

Настоящее диссертационное исследование в определённой степени служит выполнению приоритетных задач, предусмотренных нормативно-правовыми актами Республики Узбекистан, включая, Уголовный кодекс (1994 г.), Законы «Об информатизации» (2003 г.), «Об электронном правительстве» (2015 г.), «О персональных данных» (2019 г.), «О кибербезопасности» (2022 г.), «О телекоммуникациях» (2024 г.); Указы Президента Республики Узбекистан «Об утверждении Концепции общественной безопасности Республики Узбекистан и мерах по её реализации» (2021 г.), «О Стратегии «Узбекистан – 2030» (2023 г.), «О мерах по эффективной организации выполнения приоритетных задач по дальнейшему совершенствованию системы борьбы с коррупцией» (2025 г.), «О мерах по коренному совершенствованию системы уголовного и уголовно-процессуального законодательства» (2018 г.), «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов

критической информационной инфраструктуры Республики Узбекистан» (2023 г.), «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года» (2024 г.), «О мерах по дальнейшему усилению деятельности по борьбе с преступлениями, совершаемыми с использованием информационных технологий» (2025 г.); постановления Кабинета Министров «О мерах по дальнейшему совершенствованию межведомственного электронного взаимодействия и обмена информацией» (2022 г.), «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» (2022 г.); положения Центрального банка «Об утверждении Положения о порядке осуществления контроля и наблюдения за деятельностью операторов платежных систем и платежных организаций» (15.05.2023 г., рег. №3434), «Об утверждении Положения о мерах по обеспечению информационной безопасности и кибербезопасности платежных систем операторов платежных систем и поставщиков платежных услуг и профилактики правонарушений, совершаемых посредством цифровых технологий» (21.05.2024 г., рег. №3513); приказы председателя Службы государственной безопасности «Об утверждении Положения о порядке оценки уровня обеспечения кибербезопасности объектов важной информационной инфраструктуры и кибербезопасности Республики Узбекистан» (22.09.2023 г., рег. №3458), «Об утверждении Временного положения о категорировании важных объектов информационной инфраструктуры Республики Узбекистан и формировании их единого реестра» (11.11.2024 г., рег. №3570), «Об утверждении Положения о порядке проведения экспертизы на соответствие требованиям кибербезопасности» (14.11.2024 г., рег. №3573), «Об утверждении Положения о порядке сертификации аппаратных, аппаратно-программных и программных средств, применяемых для обеспечения кибербезопасности информационных систем и ресурсов» (14.11.2024 г., рег. №3574); приказ министра юстиции «Об утверждении типового порядка обработки персональных данных» (15.11.2023 г., рег. №3478), а также другими действующими нормативно-правовыми актами в данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий Республики. Диссертация выполнена в соответствии с приоритетным направлением развития науки и технологий в Республике Узбекистан I «Духовно-нравственное и культурное развитие демократического правового общества, формирование инновационной экономики».

Обзор зарубежных научных исследований по теме диссертации. Уголовно-правовые аспекты киберпреступлений, угрожающих общественной безопасности, частично изучаются высшими учебными заведениями и научно-исследовательскими учреждениями зарубежных государств. В частности, в Германии такими исследованиями занимаются Институт Фраунгофера, Кёльнский институт по изучению киберпреступности, Германский институт информационного, телекоммуникационного и медиа-права; в Норвегии – Научно-исследовательский центр «Компьютеры и право» при Университете Осло, в Великобритании – Центр безопасности

информационных технологий, в Швейцарии – Кампус кибербезопасности, в Канаде – Международный центр по изучению киберпреступности и его многочисленные лаборатории, такие как «International Centre for Comparative Criminology», «Darknet and Anonymity Research Center», «Cybersecurity Laboratory»; в Италии – Центр совместных исследований транснациональной преступности, криминологии и инноваций; а также аналогичные центры кибербезопасности в Германии, Австралии, Ирландии, Великобритании, России, США, Чехии, Венгрии, Италии, Латвии, Литве, Нидерландах, Польше, Словакии, Испании, Греции, Турции, Бельгии, Португалии, Австрии, Швеции, Финляндии и Узбекистане. Кроме того, Организация Объединённых Наций через свою программу UNICRI непосредственно проводит исследования, направленные на борьбу с киберпреступлениями. Хотя вышеуказанные организации частично изучают киберпреступления, угрожающие общественной безопасности с точки зрения своей деятельности, однако они не исследуют данную сферу в комплексе – одновременно с правовой, технической и научной сторон.

Степень изученности проблемы. Следует отметить, что отдельные вопросы, связанные с темой исследования, в той или иной степени уже изучались. В частности, среди отечественных учёных данную проблематику частично исследовали А. Джолдасов, А. Караханян, А. Норов, А. Носиров, А. Расулев, Б. Киселёв, Б. Матмуратов, Б. Улугбеков, Б. Турдиялиев, Д. Топильдиева, Ф. Батиров, Ф. Джураев, И. Торохаджаева, И. Исмаилов, К. Зинченко, Л. Исмаилова, М. Хайдарова, М. Холматов, М. Рустамбоев, Н. Каххарова, Н. Полевой, Н. Салаев, П. Шагилов, Р. Кабулов, Р. Рузиев, С. Светков, У. Низамединходжаев, У. Расулев, В. Крылов, В. Хургин, Х. Очилов, Я. Мастинский, Я. Соловьёв, Ш. Хайдаров, Ш. Гулямов, Ш. Шамсидинов, а также учёные государств – участников СНГ: А. Боровикова, А. Дохоян, А. Фёдоров, А. Кузнецов, А. Волеводз, А. Зинсова, Б. Кондрашов, Д. Коротченков, Д. Кирюхина, Е. Дозорцева, Е. Ефимова, Е. Осипова, Ф. Крамер, Г. Валияхметова, И. Маслова, И. Чекунов, К. Бельский, Л. Венс, Л. Попов, Л. Суканов, М. Авакян, Н. Бобровникова, Н. Зорина, О. Черкасенко, С. Кочой, С. Старр, С. Степашин, Т. Тропина, Т. Вольчецкая, а также другие зарубежные учёные – N. Paradi, X. Xalperin, K. Kern, V. Vensel, D. Chemberlen, M. Xatta и др., которые проводили частичные исследования, посвящённые киберпреступлениям, угрожающих общественной безопасности[7]. Хотя вышеуказанные учёные частично исследовали киберпреступления, угрожающие общественной безопасности, однако они не изучали данную проблему комплексно – одновременно с правовой, технической и научной точек зрения. В Узбекистане до настоящего времени отношения, связанные с киберпреступлениями, представляющими угрозу общественной безопасности, их выявлением, предупреждением, противодействием им, а также устранением их последствий, не были урегулированы конкретными

[7] Научные труды этих и других ученых представлены в списке использованной литературы диссертации.

законодательными актами, а учёные не изучали данную тему в полном комплексном и всестороннем масштабе.

Связь темы диссертации с планами научно-исследовательских работ высшего образовательного учреждения, в котором выполняется диссертация. Тема диссертационного исследования выполнена в рамках научного проекта «Совершенствование норм законодательства на основе реформ, осуществляемых в судебно-правовой системе Республики Узбекистан», предусмотренного планом научно-исследовательских работ Университета общественной безопасности Республики Узбекистан.

Целью исследования является изучение уголовно-правовых аспектов киберпреступлений, угрожающих общественной безопасности, а также разработка научно-практических предложений и рекомендаций по обеспечению кибербезопасности.

Задачи исследования:

изучение общей характеристики и классификации киберпреступлений, угрожающих общественной безопасности;

определение социальной необходимости установления, и совершенствования ответственности за киберпреступления, угрожающие общественной безопасности;

осуществление уголовно-правового анализа киберпреступлений, основным, дополнительным и факультативным непосредственным объектом которых является «общественная безопасность»;

анализ уголовно-правовых аспектов отдельных киберпреступлений, угрожающих общественной безопасности, в уголовном законодательстве зарубежных государств и в международных актах;

исследование роли и значения цифрового контроля в борьбе с киберпреступностью в Республике Узбекистан;

определение причин совершения данных преступлений и разъяснение исполнения назначенных наказаний с целью обеспечения неотвратимости наказания за киберпреступления, угрожающие общественной безопасности.

Объектом исследования являются уголовно-правовые отношения, связанные с правовым регулированием уголовно-правовых аспектов киберпреступлений, угрожающих общественной безопасности.

Предметом исследования являются теоретико-правовой и юридический анализ киберпреступлений, угрожающих общественной безопасности, зарубежные и международные уголовно-правовые аспекты отдельных киберпреступлений, угрожающих общественной безопасности, нормативно-правовые акты, направленные на правовое регулирование роли и значения цифровых технологий в обеспечении неотвратимости наказания за киберпреступления, угрожающие общественной безопасности, а также проблемы, связанные с правоприменительной практикой в данной сфере.

Методы исследования: в ходе исследования широко использовались методы анализа, синтеза, дедукции, индукции, сравнительно-правового анализа, исторического подхода, анкетирования, анализа эмпирических материалов и статистических данных, наблюдения, системного подхода

и логического метода. Результаты анкетного опроса представлены в диссертации в качестве приложения №8.

Научная новизна исследования заключается в следующем:

обосновано, что установление уголовной ответственности за публичные призывы к массовым беспорядкам и насилию в отношении граждан с использованием телекоммуникационных сетей или сети Интернет способствует укреплению обеспечения общественной безопасности;

обосновано, что установление уголовной ответственности за несоблюдение требований, касающихся сбора, систематизации и хранения персональных данных на технических средствах и в базах данных, расположенных на территории Республики Узбекистан, способствует защите персональных данных граждан и укреплению социальной стабильности;

обосновано, что установление порядка категорирования объектов кибербезопасности и критической информационной инфраструктуры, оценки уровня обеспечения их кибербезопасности, проведения экспертизы на соответствие требованиям кибербезопасности, а также сертификации аппаратных, программно-аппаратных и программных средств, применяемых для обеспечения кибербезопасности информационных систем и ресурсов, способствует систематизации отношений в сфере кибербезопасности и обеспечению безопасности личности, общества и государства в киберпространстве;

обосновано, что установление уголовной ответственности за совершение преступлений, представляющих угрозу общественной безопасности, посредством незаконного (несанкционированного) доступа к информационным системам или их использования, в том числе за нарушение законодательства в сфере обращения криптоактивов и за осуществление майнинговой деятельности с нарушением закона, способствует укреплению кибербезопасности, принятию жёстких мер в отношении нарушений в сфере криптоактивов, а также своевременной профилактике несанкционированного доступа к информационным системам и их незаконного использования;

обосновано, что установление уголовной ответственности за изготовление, приобретение, хранение, перевозку, пересылку, а также за распространение, рекламу или демонстрацию в телекоммуникационных сетях либо в сети Интернет наркотических средств, их аналогов, психотропных веществ или продукции, пропагандирующей их, в целях их незаконного сбыта, способствует укреплению защиты жизни и здоровья человека.

Практические результаты исследования заключаются в следующем:

разъяснены общая характеристика и классификация киберпреступлений, угрожающих общественной безопасности;

показана социальная необходимость установления и совершенствования ответственности за киберпреступления, угрожающие общественной безопасности;

осуществлён уголовно-правовой анализ киберпреступлений, основным, дополнительным и факультативным непосредственным объектом которых является «общественная безопасность»;

выявлены уголовно-правовые аспекты отдельных киберпреступлений, представляющих угрозу общественной безопасности, в уголовном законодательстве зарубежных государств;

раскрыты уголовно-правовые аспекты отдельных киберпреступлений, угрожающих общественной безопасности, в международных правовых актах;

разъяснены роль и значение цифрового контроля в борьбе с киберпреступностью в Республике Узбекистан;

определены причины совершения данных преступлений и разъяснён порядок исполнения наказаний, применяемых за киберпреступления, угрожающие общественной безопасности, с целью обеспечения неотвратимости наказания.

Достоверность результатов исследования. Достоверность результатов исследования объясняется тем, что они основаны на опросах и изучениях, проведённых среди 125 государственных органов и организаций, а также **3905 сотрудников** других учреждений, в том числе 14 местных исполнительных органов власти, 28 крупных предприятий, организаций и учреждений, всех банков и иных структур; среди 37 государственных органов и организаций **Намаганской области** и 21 института гражданского общества; на взаимном анализе зарубежного опыта и национальных нормативно-правовых актов; на внедрении выводов, предложений и рекомендаций в практику, а также подтверждении полученных результатов соответствующими документами, выданными уполномоченными структурами.

Научное и практическое значение результатов исследования. Научная значимость диссертационной работы заключается в том, что выдвинутые в результате исследования выводы, предложения и рекомендации обогащают теоретические знания в области уголовного права и создают возможности для проведения новых научных исследований. Научно-теоретические идеи и выводы, изложенные в работе, имеют научную ценность для более глубокого изучения вопросов, связанных с совершенствованием уголовного законодательства Республики Узбекистан.

Практическая значимость результатов исследования заключается в возможности их использования в нормотворческой деятельности, в частности, в процессе совершенствования уголовного законодательства, в совершенствовании правоприменительной практики, а также при чтении лекций и семинарских занятий в высших юридических учебных заведениях по таким дисциплинам, как «Уголовное право», «Уголовный процесс», «Гражданское право», «Кибернетика», «Информатика», «Информационное право», «Кибербезопасность», «Основы кибербезопасности», «Основы информационной безопасности», «Киберправо», «Цифровое право».

На основе научных выводов и предложений, разработанных в результате исследования, был принят Закон Республики Узбекистан «О кибербезопасности». На основе данного Закона и передового зарубежного

опыта были разработаны и приняты законы Республики Узбекистан о совершенствовании Кодекса Республики Узбекистан об административной ответственности, Уголовного и Уголовно-процессуального кодексов, а также указы и постановления Президента Республики Узбекистан, постановления Кабинета Министров, ведомственные нормативно-правовые акты и другие правовые документы.

Внедрение результатов исследования. На основе научных результатов, полученных по теме исследования уголовно-правовое аспекта киберпреступлений, угрожающих общественной безопасности:

1. В соответствии с Законом Республики Узбекистан «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан» от 30 марта 2021 года № ЗРУ–679 установлена ответственность по пункту «б» части второй статьи 244 Уголовного кодекса за публичные призывы к массовым беспорядкам и насилию в отношении граждан с использованием телекоммуникационных сетей, сети Интернет, а также с помощью печатных или иных способов воспроизведения текста (Акт Узкомназорат от 05.12.2024 г. № 01/07-1);

2. В соответствии с Законом Республики Узбекистан от 29 октября 2021 года № ЗРУ–726 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан» в статье 141^2 Уголовного кодекса Республики Узбекистан установлена уголовная ответственность за несоблюдение требований, касающихся сбора, систематизации и хранения персональных данных граждан Республики Узбекистан при их обработке с использованием информационных технологий, в том числе в сети Интернет, без использования технических средств, физически размещённых на территории Республики Узбекистан, а также без регистрации баз персональных данных в Государственном реестре персональных данных в установленном порядке; (Акт Узкомназората от 05.12.2024 г. № 01/07-1);

3. Принят Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ–764 «О кибербезопасности» и на его основе:

постановлением Президента Республики Узбекистан от 31 мая 2023 года № ПП–167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» утверждены порядок обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан и общие требования к кибербезопасности в объектах критической информационной инфраструктуры Республики Узбекистан (Акт Узкомнадзора от 05.12.2024 года № 01/07-1);

во исполнение Постановления Президента Республики Узбекистан от 19 февраля 2024 года № ПП–75 были приняты следующие нормативные акты председателем Службы государственной безопасности Республики Узбекистан: приказы от 4 сентября 2023 года № 91 (рег. № 3458 от 22.09.2023 г.) «Об утверждении Положения о порядке оценки уровня обеспечения кибербезопасности объектов важной информационной инфраструктуры и кибербезопасности Республики Узбекистан», от 24 октября 2024 года № 118 (рег. № 3570 от 11.11.2024 г.)

«Об утверждении Временного положения о категорировании важных объектов информационной инфраструктуры Республики Узбекистан и формировании их единого реестра», от 15 октября 2024 года № 113 (рег. № 3573 от 14.11.2024 г.) «Об утверждении Положения о порядке проведения экспертизы на соответствие требованиям кибербезопасности», от 15 октября 2024 года № 114 (рег. № 3574 от 14.11.2024 г.) «Об утверждении Положения о порядке сертификации аппаратных, аппаратно-программных и программных средств, применяемых для обеспечения кибербезопасности информационных систем и ресурсов»; (Акт Минцифры от 14.05.2024 г. № 20-8/3142 года и Акт Узкомназората от 05.12.2024 г. № 01/07-1);

4. В соответствии с Законом Республики Узбекистан № ЗРУ–829 от 11 апреля 2023 года «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с дальнейшим совершенствованием системы надёжной защиты прав, свобод и законных интересов женщин и детей» в статье 141^3 Уголовного кодекса Республики Узбекистан установлена уголовная ответственность за распространение информации, содержащей фото- и (или) видеоматериалы обнажённого тела и (или) половых органов лица без его согласия, в том числе через средства массовой информации, телекоммуникационные сети или сеть Интернет, а также за угрозу распространения такой информации. Законом Республики Узбекистан от 19 января 2024 года № ЗРУ–899 «О внесении изменений и дополнений в Уголовный, Уголовно-процессуальный кодексы Республики Узбекистан, а также Кодекс Республики Узбекистан об административной ответственности» в статье 165 УК вымогательство определяется как требование передачи чужого имущества или права на имущество, предоставления имущественных интересов либо совершения действий имущественного характера под угрозой уничтожения, изменения, захвата или блокировки информационного ресурса потерпевшего, либо разглашения сведений, которые должны храниться в тайне для потерпевшего, распространения позорящих его измышлений, либо постановка потерпевшего в условия, вынуждающие его передать своё имущество или право на имущество. В статье 278^8 установлена уголовная ответственность за нарушение законодательства в сфере оборота крипто-активов, а в статье 278^9 – за незаконное осуществление деятельности по майнингу. Также в восьмую главу УК были введены понятия «крипто-актив» и «майнинг» и в соответствии с Законом Республики Узбекистан от 19 октября 2022 года № ЗРУ–794 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан» в пункте «г» части третьей статьи 168 Уголовного кодекса установлена уголовная ответственность за мошенничество, совершённое с использованием информационной системы, в том числе информационных технологий, а в пункте «б» части третьей статьи 169 – за кражу, совершённую посредством незаконного (несанкционированного) доступа к информационной системе или с её использованием (Акт Узкомназората от 05.12.2024 г. № 01/07-1);

5. В соответствии с Законом Республики Узбекистан от 5 октября 2024 года № ЗРУ–971 «О внесении изменений и дополнений в Уголовный,

Уголовно-процессуальный кодексы Республики Узбекистан и Кодекс Республики Узбекистан об административной ответственности, направленных на противодействие незаконному обороту наркотических средств, их аналогов или психотропных веществ, а также сильнодействующих и ядовитых веществ» в статью 251[1] УК установлена уголовная ответственность за распространение, рекламу или демонстрацию продукции, пропагандирующей сильнодействующие вещества, не являющиеся наркотическими средствами, их аналогами или психотропными веществами, посредством телекоммуникационных сетей или глобальной информационной сети Интернет, а также за размещение такой продукции с целью её распространения, рекламы или демонстрации; в пункте «д» части третьей статьи 273 УК предусмотрена уголовная ответственность за незаконное изготовление, приобретение, хранение, перевозку, пересылку или сбыт наркотических средств, их аналогов или психотропных веществ с использованием телекоммуникационных сетей, в том числе сети Интернет, с целью их распространения; в статье 274 УК установлена уголовная ответственность за распространение, рекламу или демонстрацию продукции, пропагандирующей наркотические средства, их аналоги или психотропные вещества, с использованием телекоммуникационных сетей или сети Интернет с целью её распространения, рекламы или демонстрации (Акт Узкомназората от 05.12.2024 г. № 01/07-1).

Апробация результатов исследования. Результаты исследования были обсуждены на 4 международных и 8 республиканских научно-практических конференциях и семинарах.

Публикация результатов исследования. По теме исследования опубликована всего 31 научная работа, в том числе: 2 монографии, 2 учебно-методических пособия (в форме словарей), а также 11 статей в изданиях, рекомендованных Высшей аттестационной комиссией для публикации основных научных результатов диссертации (2 из них – в зарубежных изданиях), и 16 статей – в сборниках международных и республиканских научно-практических конференций.

Структура и объём диссертации. Диссертация состоит из введения, 4 глав, охватывающих 10 параграфов, заключения, списка использованных источников и приложений. Общий объём диссертации составляет 594 страниц, из которых основная часть – 233 страницы.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

В введении (аннотации диссертации) обоснована актуальность темы диссертации, обозначены цели и задачи, а также объект и предмет исследования, указано соответствие приоритетным направлениям науки и технологий Республики Узбекистан, проведен обзор зарубежных научных исследований по теме диссертации, степени изученности проблемы, изложены научная новизна и практические результаты исследования, раскрыты теоретическая и практическая значимость полученных

результатов, приведены данные о внедрении в практику результатов исследования, опубликованных работах и структуре диссертации.

Первая глава диссертации под названием «**Теоретико-правовой анализ киберпреступлений, угрожающих общественной безопасности**» состоит из двух параграфов, в которых раскрыты общая характеристика и классификация киберпреступлений, представляющих угрозу общественной безопасности, а также социальная необходимость установления и совершенствования ответственности за данный вид киберпреступлений.

В данном главе автор отмечает, что в уголовном законодательстве и других нормативно-правовых актах не уделено должного внимания разграничению понятий «общественная безопасность» и «безопасность общества», хотя на самом деле между ними существует разница. Исходя из этого, автор указывает на необходимость внесения соответствующих изменений и дополнений в законодательные акты, поскольку наличие некорректных норм в законодательстве может существенно повлиять на общественные отношения и вызвать ряд проблем в сфере международного сотрудничества.

Кроме того, автор выдвигает и теоретико-правовым образом обосновывает мнение о том, что преступления, угрожающие общественной безопасности, включая киберпреступления, угрожающие общественной безопасности, отличаются от преступлений против общественной безопасности и киберпреступлений против общественной безопасности, и что данные преступления являются более опасными, чем киберпреступления, угрожающие общественной безопасности.

Также, автор отмечает, что в разделе шестом Уголовного кодекса под названием «*Преступления против общественной безопасности и общественного порядка*» главы XVII «*Преступления против общественной безопасности*» и XX «*Преступления против общественного порядка*» предусмотрены отдельно, при этом в данный раздел дополнительно включены также глава XVIII «*Преступления против безопасности движения и эксплуатации транспорта*», глава XIX «*Преступления, составляющие незаконный оборот наркотических средств или психотропных веществ*», и глава XXI «*Преступления против общественного порядка*». Автор указывает, что с точки зрения объекта преступления данные составы отличаются друг от друга.

Автор подчёркивает, что основной проблемой является отсутствие в законе чётких определений таких понятий, как «киберпреступление», «киберсреда», «информация, угрожающая общественной безопасности», «преступление, угрожающее общественной безопасности», «киберпреступление, угрожающее общественной безопасности», «кибербезопасность», «общественная безопасность», «безопасность общества», а также то, что понятия «кибербезопасность», «киберпреступность», «объект кибербезопасности» и «субъект кибербезопасности» не определены в законе чётко и корректно, что приводит к возникновению ряда проблем.

В частности, автор объясняет, что поскольку понятие «киберпреступление» не предусмотрено прямо ни в Уголовном кодексе, ни в специальном законе — Законе Республики Узбекистан «О кибербезопасности», на практике не уделяется должного внимания различию между преступлениями, совершаемыми с использованием информационных технологий, и, собственно, киберпреступлениями, несмотря на то что они отличаются друг от друга. В результате этого формируются неверные теоретико-правовые подходы. Автор также указывает, что в законодательстве понятия «общественная безопасность» и «безопасность общества» фактически рассматриваются как одно и то же, тогда как они различаются. Кроме того, подчёркивается, что «объект кибербезопасности» не ограничивается только информационной системой или системой информатизации, являющейся частью критической информационной инфраструктуры, поскольку киберпреступления могут совершаться и совершаются с использованием информационно-коммуникационных технологий, систем, средств, устройств, сетей, оборудования, программ, связи, программного обеспечения и информации, и даже могут быть направлены против них самих, что автор подробно объясняет как с практической, так и с теоретической точки зрения.

Кроме того, автор обосновывает, что придавать понятию «киберпреступность» определение, связывая его исключительно с информационной системой, и не соотносить это понятие с «кибербезопасностью» ошибка, поскольку такие преступления совершаются также с использованием иных методов обработки информации.

В первом параграфе «***Общая характеристика и классификация киберпреступлений, угрожающих общественной безопасности***» автор раскрыл теоретико-правовое содержание и сущность киберпреступлений, угрожающих общественной безопасности. В данном параграфе автор раскрыл содержание и сущность таких понятий, как *«общественность», «общество», «преступление», «киберпреступление», «общественная безопасность», «безопасность общества», «преступления, угражающие общественной безопасности», «преступления, угражающие безопасности общества», «преступления против общественной безопасности», «преступления против безопасности общества», «киберпреступления, угражающие общественной безопасности», «киберпреступления, угражающие безопасности общества», «киберпреступления против общественной безопасности», «киберпреступления против безопасности общества», «киберсреда», «киберпространство», «киберугроза», «инцидент кибербезопасности», «объект кибербезопасности», «субъект кибербезопасности»*, и теоретико-правово обосновал их различие и взаимосвязь. Соответственно, автор, разъяснив, что преступления, предусмотренные разделом шестым Уголовного кодекса и его главами, направлены не против общественной безопасности, а против безопасности общества, в том числе киберпреступления, а также то, что общественная безопасность отличается от безопасности общества и что между личностью, обществом и государством возникают отношения, связанные с обеспечением

общественной безопасности, теоретико-правово обосновал необходимость пересмотра данного раздела и его глав. Автор реализовал классификацию киберпреступлений, посягающих на общественную безопасность, разделив их по вертикали на киберпреступления с общим, родовым, видовым и непосредственным объектом – общественную безопасностью. Киберпреступления с непосредственным объектом – общественную безопасностью, в свою очередь, подразделяются на киберпреступления с основным, дополнительным и факультативным непосредственным объектом - общественную безопасностью. Автор с научной и практической точки зрения разъяснил классификацию киберпреступлений, угрожающих общественной безопасности, их деление по вертикали на киберпреступления с общим, родовым, специальным объектом и киберпреступления, непосредственным объектом которых является общественная безопасность. Было разъяснено, что киберпреступления, непосредственным объектом которых является общественная безопасность, в свою очередь, подразделяются на киберпреступления, где общественная безопасность выступает в качестве основного, дополнительного и факультативного непосредственного объекта. Автор перечислил обязательные признаки данных киберпреступлений и указал, какие статьи действующего Уголовного кодекса к ним относятся. Кроме того, было подчёркнуто, что информационно-коммуникационные технологии состоят из информационных технологий и телекоммуникационных технологий, а остальные технологии считаются их составной частью, а также то, что киберпреступления совершаются с использованием данных технологий либо в отношении них.

Во втором параграфе, озаглавленном «***Социальная необходимость установления в уголовном законодательстве ответственности за киберпреступления, угрожающие общественной безопасности***», автор обосновал **23** социальные необходимости установления ответственности за такие киберпреступления.

В частности, что число киберпреступлений за период 2020-2025 годов увеличилось **почти в 80 раз**, и по данным преступлениям даже ведётся отдельная статистика. Вследствие того, что в действующем Уголовном кодексе не установлено достаточной уголовной ответственности за совершаемые инциденты в сфере кибербезопасности, **около 90% киберпреступлений носят латентный характер**. В результате этого возникает угроза законным правам, данным и безопасности личности, общества и государства для более чем **11 тысяч баз персональных данных**, около **1500 информационных систем**, а также около **36 миллионов пользователей** телекоммуникационных услуг и связанных с ними лиц. Несмотря на то, что в действующих законодательных актах установлено, что невыполнение собственниками, пользователями и субъектами кибербезопасности своих обязательств, принятых в соответствии с законодательством, влечёт за собой ответственность, в действующем Уголовном кодексе за это **не предусмотрено достаточной ответственности**. Вследствие этого угрозы общественной безопасности продолжают

усиливаться. В связи с этим подчёркивается **необходимость установления** с уголовно-правовой точки зрения достаточной **уголовной ответственности в Уголовном кодексе** за киберпреступления, угрожающие общественной безопасности, а также пересмотра и совершенствования существующего законодательства.

Во второй главе «**Юридическая характеристика киберпреступлений, угрожающих общественной безопасности**» диссертации, автор, принимая во внимание, что киберпреступления, угрожающие общественной безопасности, в зависимости от объекта делятся на киберпреступления, где «**общественная безопасность**» является **основным, дополнительным и факультативным непосредственным объектом**, представляет их уголовно-правовой анализ.

Автор разъясняет, что киберпреступления, где «общественная безопасность» выступает основным, дополнительным и факультативным непосредственным объектом, различаются между собой в зависимости от прямого или косвенного воздействия на «общественную безопасность». Также он поясняет, что преступления данного вида с субъективной стороны всегда совершаются умышленно, в киберсреде, в том числе в киберпространстве, либо с его использованием посредством информационно-коммуникационных технологий, включая телекоммуникационные инфраструктуры, и этим они отличаются от других преступлений, а также от преступлений, совершаемых с использованием информационно-коммуникационных технологий. Автор подчёркивает, что данный вид преступлений является киберпреступлением, входящим в отдельную категорию или группу киберпреступности, и отличается от других киберпреступлений своим объектом.

Кроме того, автор подчёркивает, что киберпреступления, представляющие угрозу общественной безопасности, как один из видов киберпреступлений, отличаются от других киберпреступлений по своему широкому охвату и степени общественной опасности, а также тем, что они создают угрозу интересам личности, общества и государства как одновременно, так и по отдельности.

В ходе исследования автор отмечает, что искусственный интеллект может выступать участником преступления в качестве организатора, посредника или пособника, однако уголовная ответственность за это в нашем Уголовном кодексе не предусмотрена. Автор отмечает, что искусственный интеллект, выступая организатором при совершении преступления, – в случае создания искусственного интеллекта, представляющего собой комплексную информационную систему, сформированную посредством взаимной интеграции всех информационных систем и искусственных интеллектов, может, незаконно проникнув в соответствующие информационные системы либо подключившись к другим системам на базе ИИ, умышленно совершать различные преступления в отношении лиц, вызывать нарушение общественного порядка, манипулировать населением и совершать иные противоправные действия, что может представлять угрозу общественной безопасности. Автор указывает, что искусственный интеллект

в качестве пособника может выступать участником преступления, предоставляя киберпреступнику советы в форме чат-бота или в иной форме, а также содействуя совершению преступления путём предоставления инструкций, организации средств или устранения препятствий, а также участвуя в сокрытии орудий, следов и средств совершения киберпреступления либо предметов, полученных преступным путём, а также заранее обещая их получение или передачу. Искусственный интеллект может выступать участником преступления, осуществляя манипуляции или мошенничество и при этом руководя подготовкой к совершению иного преступления или киберпреступления либо непосредственно его совершением.

Широкое развитие социальных сетей и их удобство, с одной стороны, приносят пользу человечеству, с другой стороны, проникновение в них искусственного интеллекта играет роль средства, посредством которого различные лица проявляют интерес к совершению различных преступлений, включая киберпреступления. Искусственный интеллект может выступать участником преступления в роли посредника, целенаправленно побуждая посредством манипуляций, мошенничества и иных способов к совершению преступления или киберпреступления в отношении лиц, одновременно являющихся потерпевшими. Поэтому автор подчёркивает необходимость предотвращения широкого распространения киберпреступлений, угрожающих общественной безопасности посредством искусственного интеллекта, а также необходимость не допускать самовольной и стратегически необдуманной интеграции информационных систем между собой; не предоставлять искусственному интеллекту полного технического доступа к возможностям логирования, хранения цифровых следов и их автоматического учёта, и обеспечить надлежащий цифровой контроль за ним.

В первом параграфе «***Уголовно-правовому анализу киберпреступлений, непосредственным объектом которых является общественная безопасность***», автор излагает юридический анализ киберпреступлений, непосредственным объектом которых выступает общественная безопасность, и представляет результаты уголовно-правового анализа в приложениях к диссертации. Автор этого параграфа провел уголовно-правовой анализ киберпреступлений, направленных против безопасности общества, то есть киберпреступлений, непосредственно угрожающих безопасности общества.

Во втором параграфе «***Уголовно-правовому анализу киберпреступлений, дополнительным непосредственным объектом которых является общественная безопасность***», автор излагает юридический анализ киберпреступлений, дополнительным непосредственным объектом которых выступает общественная безопасность, и представляет результаты уголовно-правового анализа в приложениях к диссертации. Автор в данном параграфе провел уголовно-правовой анализ киберпреступлений, угрожающих общественной безопасности, относящихся к сфере информационных технологий или цифровых технологий.

В третьем параграфе «***Уголовно-правовому анализу киберпреступлений, непосредственным объектом которых факультативно является общественная безопасность***», автор излагает юридический анализ киберпреступлений, факультативным непосредственным объектом которых выступает общественная безопасность, и представляет результаты уголовно-правового анализа в приложениях к диссертации. Автор в данном параграфе провел уголовно-правовой анализ иных киберпреступлений, которые, как известно, с основным и дополнительным объектом оказывают факультативное воздействие.

В третьей главе «**Международно-правовой и зарубежный уголовно-правовой анализ киберпреступлений, угрожающих общественной безопасности**» диссертации, автор раскрывает уголовно-правовые аспекты таких киберпреступлений, охарактеризованных более чем в 150 зарубежных государствах и в свыше 50 международных документах. В данной главе автор на основе научного, практического, правового, технического зарубежного опыта разъясняет, что под киберпреступлениями не следует понимать преступления, совершаемые с использованием программного обеспечения и технических средств в киберпространстве с целью овладения информацией, ее изменения, уничтожения или вывода из строя информационных систем и ресурсов. Также автор указывает, что незаконный доступ к информационной системе, незаконное подключение к сети, совершение незаконных действий при незаконном или законном доступе к информационной системе, совершение незаконных действий при незаконном подключении к сети или законном использовании сети, незаконное распространение информации, запрещенной или ограниченной законом для распространения в киберсреде, в том числе в киберпространстве или с ее использованием, или отнесенной к категории конфиденциальной информации, также являются киберпреступлениями, что даже при разрешённом использовании сети и информационной системы совершение незаконных действий может привести к киберпреступлениям, помимо приобретения, изменения, уничтожения или использования информации, киберпреступления могут быть совершены такими действиями, как передача, распространение, обезличивание информации, и за это в зарубежных странах и международном законодательстве установлена достаточная ответственность.

В первом параграфе «***Уголовно-правовые аспекты некоторых киберпреступлений, угрожающих общественной безопасности, в уголовном законодательстве зарубежных стран***», автор исследует уголовное законодательство иностранных государств. Автор отмечает, что в уголовных законах таких стран, как Великобритания, Франция, Германия, Албания, Греция, США, Испания, Италия, Бельгия, Нидерланды, Сингапур, Китай, Индия, Малайзия, Индонезия, Россия, Казахстан, Кыргызстан, Таджикистан, Азербайджан, Армения, Грузия, Словения, Латвия, Финляндия, Норвегия, ОАЭ, Саудовская Аравия, Канада и других, предусмотрена специальная уголовная ответственность за киберпреступления, угрожающие общественной безопасности. Он

подчёркивает, что данные преступления закреплены в их уголовном законодательстве отдельными разделами, главами или статьями.

Во втором параграфе «***Уголовно-правовые аспекты некоторых киберпреступлений, угрожающих общественной безопасности, в международных документах***» автор указывает на необходимость установления в мировых государствах отдельной уголовной ответственности за киберпреступления, угрожающие общественной безопасности, а также на то каким должен быть механизм её реализации. Автор, проанализировав тот факт, что Узбекистан присоединился к 4 из 12 международных документов, пояснил, что, поскольку киберпреступления являются международными трансграничными преступлениями, Узбекистан может извлечь выгоду из сотрудничества с другими странами, и обосновал необходимость присоединения Республики Узбекистан к оставшимся 8 международным документам с дополнительными условиями.

В четвёртой главе «**Роль цифрового контроля в выявлении уголовно-правовых аспектов киберпреступлений, угрожающих общественной безопасности**» диссертации, автор рассматривает необходимость и порядок внедрения цифрового контроля в Республике Узбекистан. Также он освещает методы и технические подходы к предотвращению киберпреступлений, угрожающих общественной безопасности, с использованием цифровых технологий. В данной главе автор отмечает, что реформы, проводимые уполномоченными органами в сфере противодействия киберпреступности, угрожающей не только информационной, но и общественной безопасности, недостаточно обоснованы, что указанные органы неэффективно используют цифровые технологии, а правовая пропаганда не организована системно и результативно. Кроме того, подчёркивается, что существующие нормы, регулирующие криминогенную обстановку в районах, отнесённых к категориям «зелёных», «жёлтых» и «красных», не приносят должных результатов в борьбе с киберпреступностью. В связи с этим автор указывает на необходимость глубокого пересмотра и приведения в соответствие с современными требованиями деятельности институтов гражданского общества, местных представительных органов государственной власти, органов исполнительной власти, судебных, надзорных и правоохранительных органов, а также на установление чёткого распределения обязанностей между киберпреступником, киберпрокурором, киберсудьёй и другими лицами, ответственными за обеспечение кибербезопасности и оперативно-розыскной деятельности. Наряду с этим обращается внимание на необходимость пересмотра уголовного законодательства и более адекватного использования положений англосаксонской правовой системы.

В первом параграфе «***Роль и значение цифрового контроля в борьбе с киберпреступностью в Республике Узбекистан***» автор отмечает, что киберпреступления, угрожающие общественной безопасности, совершаются в отношении инфраструктуры, созданной в результате процессов цифровизации, либо в отношении информации, связанной с этой инфраструктурой. При этом подчёркивается, что проводимые реформы

в данной сфере недостаточно обоснованы, поскольку в них наблюдается отказ от традиционных методов противодействия при одновременном неэффективном использовании информационно-коммуникационных и, в частности, цифровых технологий.

Автор указывает на необходимость более эффективного применения так называемого «пинга» цифрового контроля, который основан на обработке информации в сложной информационной системе. Отмечается, что при помощи цифрового контроля невозможно полностью обеспечить общественную безопасность, напротив, через подобные системы могут возникать новые угрозы для неё. Сложившуюся критическую ситуацию автор описывает как функционирование комплексной информационной системы «**Jamoat xavfsizligining raqamli monitoringi**», включающей в себя такие составные элементы, как «**Log menejment**», «**Raqamli jamoatchilik**», «**CYBER**», «**Bolalar xavfsizligi**», «**Kelajak**», «**Aqlli ta'lim**», «**CYBERSTAT**», «**CYBERPREVEN**» и «**CYBERPROB**». По мнению автора, полное внедрение данных информационных систем, даже если оно осуществляется частично, способно обеспечить более высокий уровень эффективности по сравнению с текущим состоянием. Особое внимание уделяется обеспечению безопасности цифровой информации, в частности – защите, наиболее значимых пользовательских данных. При этом автор подчёркивает, что деятельность владельцев и операторов мессенджеров и социальных сетей, ответственных за соблюдение особых условий обработки персональных данных граждан, а также объективная невозможность полного контроля над всей пользовательской информацией, создают дополнительные сложности в обеспечении цифровой и общественной безопасности. Среди указанных информационных систем внедрение искусственного интеллекта в комплексную информационную систему «Цифровой мониторинг общественной безопасности» невозможно, тогда как в остальные информационные системы применение технологий искусственного интеллекта допускается, за исключением составных частей систем, работающих с закрытой информацией. Каждая из вышеуказанных информационных систем может быть интегрирована между собой, при этом её цифровые следы сохраняются посредством логирования и ведётся их автоматический учёт.

Кроме того, к ним должны быть интегрированы и другие необходимые информационные системы. Например, посредством информационной системы «Қалқон» возможно выявление разыскиваемых лиц с использованием искусственного интеллекта или автоматизированных систем на основе видеозаписей, полученных через установленные в стране видеокамеры в рамках проекта «Безопасный город» и других проектов и инициатив. Однако в данной системе отсутствует искусственный интеллект, не применяются такие технологии, как «умная линза» или «умные очки», кроме того, не предусмотрено автоматическое уведомление участкового инспектора о прибытии разыскиваемого лица на его территорию, сообщения не подвергаются автоматическому анализу, а в системе оповещения имеются недостатки. В связи с этим целесообразно

усовершенствовать данную систему и обеспечить направление информации также в информационную систему «Цифровое сообщество».

Во втором параграфе «***Выявление причин возникновения киберпреступлений, угрожающих общественной безопасности и исполнения, применённых к ним наказаний***» автор объясняет роль цифровых технологий в предупреждении деяний, угрожающих общественной безопасности, их выявлении, разоблачении киберпреступника, его задержании, а также в устранении последствий киберпреступлений. В данном параграфе автор особо подчёркивает необходимость уделять внимание причинам возникновения киберпреступлений, угрожающих общественной безопасности, при их совершении. Автор подчёркивает, что при обеспечении исполнения наказания за киберпреступление, при направлении представления или частного определения, дознаватель, следователь, прокурор и судья обязаны изучить причины возникновения каждого киберпреступления. При этом, как отмечает автор, на примере практики Наманганской области установлено, что представления и частные определения, направляемые указанными субъектами, исполняются ненадлежащим образом – протоколами и фотоотчётами уполномоченных органов, а также не предпринимаются какие-либо положительные меры по фактическому устранению последствий совершённого киберпреступления.

Автор разъясняет, что если желают обеспечить полное исполнение наказания и недопущение повторения подобных деяний, то в представлении и частном определении необходимо обязательно указать причины возникновения киберпреступления, а также изложить порядок устранения его последствий уполномоченными органами. Кроме того, автор отмечает, что для обеспечения неотвратимости наказания за киберпреступления, угрожающих общественной безопасности, и для снижения их количества необходимо полностью пересмотреть применяемые к киберпреступникам меры наказания, уделить больше внимания возмещению ущерба, и посредством установления большего числа льготных норм, возможно, эффективно бороться с данным видом преступлений.

ЗАКЛЮЧЕНИЕ

В ходе комплексного исследования правового регулирования киберпреступлений, угрожающих общественной безопасности, был проанализирован национальный, международный, зарубежный опыт, рассмотрены доктринальные взгляды ученых, сделаны следующие концептуальные выводы и разработаны научно-практические предложения и рекомендации по дальнейшему совершенствованию соответствующих законодательных актов:

I. Научно-теоретические выводы

1. В связи с тем, что понятия «общественность» и «общество», а также «общественная безопасность» и «социальная безопасность» различаются между собой, а в действующем законодательстве данные

понятия ошибочно применяются в одном и том же значении, целесообразно использовать их в редакции, приведённой в приложениях 6 и 20 диссертации. В частности, «**общественная безопасность**» – это состояние защищённости временно созданной социальной структуры от внутренних и внешних угроз, возникающее на определённом этапе исторического развития, на конкретной территории, в результате объединения субъектов, состоящих из физических лиц, юридических лиц или государства, чьи цели и взгляды схожи или идентичны и которые объединяются на принципах добровольности и равенства ради достижения определённой цели, а также, «**безопасность общества**» – это состояние защищённости социальной структуры, состоящей из группы людей, объединённых вокруг сферы, режима, власти или доктрины, функционирующей на постоянной основе, независимо от территориального расположения, исторически сложившейся на основе многообразия мнений и не имеющей чётко выраженной и единой цели. К таким структурам относятся социальные, экономические и политические системы и (или) крупномасштабные группы людей – нация, народ, государство, признанные государством категории, классы, направления. Социальная безопасность выражает состояние защищённости этих систем и групп от внутренних и внешних угроз. Угроза общественной безопасности соотносится с национальной безопасностью на трёх уровнях: индивидуальном, коллективном и национальном (институциональном). Участниками общественной безопасности являются физические лица, юридические лица и государство. Эти субъекты могут формировать как однотипные, так и смешанные группы.

2. В Законе Республики Узбекистан «О кибербезопасности» в качестве «объекта кибербезопасности» предусмотрены информационные системы, а также информационные системы, в которых существуют важные информационные инфраструктуры. Однако не учтено, что к «объекту кибербезопасности» также могут относиться информация, связь, информационные ресурсы, сети, системы, средства, устройства, оборудование, программы и программное обеспечение. Кроме того, понятие «кибербезопасность» изложено слишком широко, при его определении не учтена прямая взаимосвязь с понятиями «киберпреступность» и «объект кибербезопасности». При определении понятия «киберпреступность» законодатель не принял во внимание возможность совершения киберпреступлений иными способами, предусмотренными настоящим Законом. В результате законодательство Республики Узбекистан в сфере киберпреступности и кибербезопасности развивается раздельно, и принимаются соответствующие меры. Из-за недостаточной систематизации законодательства в практике формируются ошибочные направления, и данное положение требует безотлагательного устранения. Исходя из положений, изложенных в диссертации, были предложены следующие определения: «киберпреступление», «киберпреступность», «киберсреда», «киберпространство», «кибербезопасность» и «объект кибербезопасности»:

«**киберпреступление** – виновное общественно опасное деяние (действие или бездействие), запрещённое Уголовным кодексом, совершённое

в киберсреде, включая киберпространство, либо с использованием информационно-коммуникационных технологий, за которое Уголовный кодекс предусматривает применение наказания;

киберпреступность – совокупность киберпреступлений, совершённых в киберсреде, включая киберпространство, либо с его использованием с целью завладения, изменения, уничтожения, передачи, распространения, обработки, обезвреживания или использования информации, а также выведения из строя информационных систем и ресурсов, посредством информационно-коммуникационных технологий;

киберсреда – среда, включающая киберпространство, условия, события и состояния, созданные в информационно-коммуникационных системах с использованием информационно-коммуникационных технологий, включая информационные системы, средства связи, телекоммуникации, технологии информатизации, искусственный интеллект, био-, нано- и кибертехнологии, а также другие технические средства, и предоставляющая информацию о виртуальном мире;

киберпространство – конкретное место, точка или территория в киберсреде, созданной с использованием информационно-коммуникационных технологий, включая информационные системы, средства связи, телекоммуникации, технологии информатизации, искусственный интеллект, био-, нано- и кибертехнологии, а также другие технические средства или их комбинации;

кибербезопасность – состояние безопасности, обеспечиваемое совокупностью правовых, организационных и технических мер, направленных на защиту объектов кибербезопасности, а также связанных с ними интересов физических лиц, общества, государства и общественных институтов от внешних и внутренних угроз в киберсреде, включая киберпространство, либо при его использовании;

объект кибербезопасности – объект, который подлежит киберзащите независимо от того, находится он под защитой или нет, включая информационно-коммуникационные технологии, а также информационные, цифровые, искусственный интеллект, телекоммуникационные, био-, нано- и кибертехнологии; связанные с ними средства, устройства, оборудование и другие технические средства; информационно-коммуникационные системы, включая информационные системы; а также ресурсы, инфраструктуры, системы и объекты критической информационной инфраструктуры, информация в которых подлежит защите от киберугроз и обеспечения кибербезопасности».

3. В действующем законодательстве отсутствуют определения таких понятий, как «общество» и «сообщество», «общественная безопасность» и «безопасность общества», «преступление, угрожающее безопасности общества» и «киберпреступление, угрожающее безопасности общества», «преступление, угрожающее общественной безопасности» и «киберпреступление, угрожающее общественной безопасности», «информация, угрожающая общественной безопасности». Также отсутствуют специальные отраслевые законы, обеспечивающие безопасность

общества и сообществ. Установление правового регулирования в этой области будет способствовать полному проявлению принципа законности в нашем уголовном законодательстве. По этой причине необходимо принять законы Республики Узбекистан «О безопасности общества» и «О безопасности сообществ», в которых должны быть предусмотрены определения соответствующих понятий, а также установлены группы преступлений, к ним относящиеся. При этом, по нашему мнению:

«информация, угрожающая общественной безопасности, – тип деструктивной информации, которая посредством информационно-коммуникационных технологий в киберсреде, включая киберпространство, либо при его использовании вызывает совершение общественно опасного деяния (действия или бездействия), запрещённого Уголовным кодексом и влекущего уголовную ответственность, а также создаёт киберугрозу или киберсобытие. Такая информация направлена на социальные структуры, временно созданные на основе принципов добровольности и равенства субъектов – физических лиц, юридических лиц или государства, объединённых общей целью и сходными интересами на определённом этапе исторического развития и в конкретной территории, и ставит под угрозу их внутреннюю и внешнюю защищённость;

преступления, угрожающие общественной безопасности, – общественно опасные деяния (действия или бездействия), запрещённые Уголовным кодексом и влекущие применение уголовной ответственности, которые представляют угрозу внутренней и внешней защищённости временно созданных социальных структур. Эти структуры формируются на основе принципов добровольности и равенства субъектов – физических лиц, юридических лиц или государства, объединённых общей целью и сходными интересами на определённом этапе исторического развития и в конкретной территории;

киберпреступления, угрожающие общественной безопасности, — общественно опасные деяния (действия или бездействия), запрещённые Уголовным кодексом и влекущие уголовную ответственность, которые посредством информационно-коммуникационных технологий в киберсреде, включая киберпространство, либо при его использовании создают киберугрозу или киберсобытие и представляют угрозу внутренней и внешней защищённости временно созданных социальных структур. Эти структуры формируются на основе принципов добровольности и равенства субъектов – физических лиц, юридических лиц или государства, объединённых общей целью и сходными интересами на определённом этапе исторического развития и в конкретной территории».

4. Киберпреступления, угрожающие общественной безопасности, включая другие киберпреступления, обладают специфическими особенностями, указанными в приложении 2 диссертации, и могут быть классифицированы в зависимости от их объекта, способа или средства совершения, субъекта и субъективной стороны. В диссертации мы классифицировали их по объекту и непосредственному объекту. В частности, такие киберпреступления были разделены на киберпреступления с основным,

дополнительным и факультативным объектом – «общественная безопасность». Исходя из принципа законности в нашем уголовном законодательстве и текущего состояния киберпреступлений, их уголовно-правовой анализ был подробно представлен в основной части диссертации и в приложениях 7, 10, 12 и 14.

5. Необходимые признаки киберпреступлений, угрожающих общественной безопасности, были разделены на основные и специальные признаки. К основным необходимым признакам отнесены охраняемые социальные отношения, общественно опасное деяние, возраст привлечения к ответственности, психическая вменяемость и вина. К специальным необходимым признакам – киберсреда, включая киберпространство, информация, связь (в том числе радиочастотная, телекоммуникационная, почтовая), а также информационно-коммуникационные технологии. В данном случае после всестороннего изучения следственной и судебной практики, а также на основе открытых источников, в диссертации в приложении 22 установлено, что к средствам и орудиям киберпреступлений, угрожающих общественной безопасности, относятся инфраструктуры информационно-коммуникационных технологий, и составлен их перечень и **информационно-коммуникационные технологии** (технологии, связанные с созданием, передачей, обработкой и управлением информацией[8], которые включают в себя информационные и телекоммуникационные технологии). Цифровые, облачные, биотехнологии, нанотехнологии, кибертехнологии, технологии искусственного интеллекта, блокчейн, а также информационные и (или) коммуникационные и иные технологии считаются составной частью указанных технологий.

6. Объект киберпреступлений, угрожающих общественной безопасности, является сложным и меняется в зависимости от существующих киберугроз и рисков для общественной безопасности. К этим объектам относятся объекты кибербезопасности, указанные в Приложении 23 к диссертации. При этом, в зависимости от того, направлен ли умысел на общественную безопасность прямо или косвенно, различаются киберпреступления с основным, дополнительным и факультативным непосредственным объектом «общественная безопасность». Однако, во всех случаях киберугроза или кибератака может угрожать общественной безопасности.

7. Если в киберсреде, включая киберпространство, возникают условия и факторы, представляющие угрозу интересам физических лиц, общества и государства, или их совокупность, такая ситуация рассматривается как **киберугроза**, а действия, направленные на реализацию этой угрозы, считаются **кибератакой**. В диссертации показаны различия между

[8] Вазирлар Маҳкамасининг 2014 йил 23 апрелдаги 102-сон қарори билан тасдиқланган “Давлат ва хўжалик бошқаруви, маҳаллий давлат ҳокимияти органлари фаолиятида ахборот-коммуникация технологияларини жорий этиш ва ривожлантиришнинг ҳолатини ўрганишни амалга ошириш тартиби тўғрисида”ги Низом // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

киберугрозой, кибератакой, киберсобытием, киберправонарушением и киберпреступлением, а также разработаны определения этих понятий.

8. Поскольку главы шестого раздела Уголовного кодекса не соответствуют названию и содержанию данного раздела, их объекты различны, а также имеется разница между понятиями *«общество» и «община», «безопасность общества» и «общественная безопасность»*, в целях обеспечения законности предлагается изложить название шестого раздела Уголовного кодекса следующим образом:

«**Раздел VI. Преступления, угрожающие безопасности и порядку общества**».

9. В качестве предложения в шестом разделе Уголовного кодекса Республики Узбекистан рекомендуется пересмотреть главу XVII – «Преступления против общественной безопасности», главу XVIII – «Преступления против безопасности движения и эксплуатации транспорта», главу XIX – «Преступления, связанные с незаконным оборотом наркотических средств или психотропных веществ», главу XX – «Преступления против общественного порядка» с учётом того, что основным, дополнительным или факультативным непосредственным объектом этих преступлений являются общественные отношения, обеспечивающие безопасность не только общества, но и социума в целом (социальную безопасность).

Кроме того, глава XX[1] – «Преступления в сфере информационных технологий» должна быть пересмотрена с точки зрения того, что её основной непосредственный объект – это сфера информационных технологий, которая по своей сути связана не только с безопасностью общества или общественного порядка, но также и с интересами личности и государства.

В связи с этим предлагается выделить данную категорию преступлений в самостоятельный подраздел шестого раздела Уголовного кодекса под следующим наименованием:

«**Шестой подраздел. Преступления в сфере информационно-коммуникационных технологий**».

10. Киберпреступление – это не только деяние, совершаемое посредством причинения вреда одному техническому средству другому техническому средству или незаконного доступа к нему с целью получения, присвоения либо приведения информации в непригодное состояние, но и преступление, представляющее угрозу интересам личности, общества и государства посредством информации. Кроме того, преступления, совершаемые с использованием информационных технологий, преступления, совершаемые при помощи информационных технологий, и киберпреступления различаются между собой. В связи с этим необходимо не смешивать киберпреступления с другими преступлениями, связанными с информационными технологиями, а также устранить ошибки, имеющиеся в законодательстве. При этом традиционными методами невозможно в полной мере бороться с киберпреступлениями, представляющими угрозу общественной безопасности. Необходимо разрабатывать технологические решения не только по киберпреступлениям, угрожающим общественной

безопасности, но и по всем киберпреступлениям, совершаемым с использованием информационно-коммуникационных технологий. Наиболее эффективным способом противодействия киберпреступлениям, представляющим угрозу общественной безопасности, является внедрение цифрового контроля и мониторинга, основанных на искусственном интеллекте и «умных системах», а также рациональное использование цифровых технологий.

11. Необходимо принять Концепцию кибербезопасности Республики Узбекистан, национальную стратегию кибербезопасности на краткосрочный, среднесрочный и долгосрочный периоды, план (дорожную карту) их реализации, а на их основе – Концепцию противодействия киберпреступности в Республике Узбекистан, а также стратегию противодействия киберпреступности на краткосрочный, среднесрочный и долгосрочный периоды. При этом в соответствии, поскольку отношения, угрожающие общественной безопасности, имеют широкий охват, для их достаточного и полного регулирования целесообразно принять следующие законы: Кодекс об информации, Кодекс об информационно-коммуникационных технологиях, законы «О защите прав пользователей онлайн-платформ и веб-сайтов», «О кибербуллинге», «О киберагрессии» или «О противодействии кибербуллингу», «Об искусственном интеллекте», а также законы «О безопасности сообществ» и «О безопасности общества». А также, на международной арене целесообразно установить уголовную ответственность юридических лиц за киберпреступления, а также обеспечить, чтобы страны мира устанавливали одинаковую или сходную уголовную ответственность не только за киберпреступления, угрожающие общественной безопасности, но и за все виды киберпреступлений, что позволит унифицировать судебно-следственную практику. Применение англосаксонской системы законодательства при рассмотрении дел об административных правонарушениях и преступлениях, совершённых с использованием информационно-коммуникационных технологий, показывает более высокую эффективность по сравнению с романо-германской правовой системой. Поэтому целесообразно разработать и внедрить в практику смешанную национальную модель законодательства, основанную на элементах англосаксонской правовой семьи, для более эффективной борьбы с киберпреступностью и обеспечения неотвратимости наказания за киберпреступления.

12. Для обеспечения единообразной и правильной с правовой и технической точки зрения практики вместо различных формулировок, используемых при внесении в Уголовный кодекс изменений и дополнений, касающихся совершения преступлений в информационных системах, с использованием информационных технологий, в телекоммуникационной или интернет-сети либо иными способами, целесообразно заменить их словами «*с использованием информационно-коммуникационных технологий*». Поскольку киберпреступления могут совершаться и иными способами, помимо предусмотренных в нашем Уголовном кодексе, представляется

обоснованным внедрение данного предложения для их единообразного изложения.

II. Предложения и рекомендации, связанные с совершенствованием законодательных актов Республики Узбекистан

На основании научно-теоретических выводов необходимо усовершенствовать следующие законодательные акты:

1. Предлагается заменить в статье 3 Закона Республики Узбекистан № от 15 апреля 2022 года ЗРУ–764 «О кибербезопасности» определения понятий «киберпространство», «инцидент кибербезопасности», «киберугроза», «объект кибербезопасности» и «субъект кибербезопасности» на определения указанных понятий, приведённые выше, а также дополнить данный Закон понятиями «киберпреступление» и «киберсреда» в редакции, предусмотренной в проекте Закона Республики Узбекистан, разработанном в соответствии с приложением 21 диссертации.

Кроме того, исходя из социальной необходимости установления уголовной ответственности за «киберпреступление», «киберсреду», «киберпространство», «информацию, угрожающую общественной безопасности» и «киберпреступления, угрожающиеобщественной безопасности», целесообразно отразить определения данных понятий в Уголовном кодексе – в разделе VIII либо в новой редакции Уголовного кодекса, в той формулировке, в которой они были определены нами.

2. В целях установления надлежащей ответственности за киберпреступления, угрожающие общественной безопасности, на основе имеющихся ресурсов и передового зарубежного опыта необходимо внести изменения и дополнения в некоторые законодательные акты Республики Узбекистан, направленные на дальнейшее усиление информационной и кибербезопасности в соответствии с приложением 21 диссертации к Уголовному кодексу

3. На первоначальном этапе целесообразно присоединиться к Конвенции Организации Объединённых Наций по борьбе с киберпреступностью, утверждённой резолюцией Генеральной Ассамблеи ООН № 79/243 от 24 декабря 2024 года, а на последующих этапах – к Конвенции Совета Европы «О киберпреступности» от 23 ноября 2001 года (Будапештская конвенция), двум дополнительным протоколам к ней и другим международным документам с учётом дополнительных условий. Это позволит обеспечить более тесное сотрудничество с иностранными государствами в сфере международных трансграничных отношений, а также унификацию и сближение национального законодательства с зарубежным и международным уголовным правом.

4. Целесообразно, чтобы Республика Узбекистан разработала собственную Конвенцию ООН «О кибербезопасности», принимаемую мировыми государствами, и осуществила необходимые процедуры для её принятия ООН.

5. Следует внедрить систему киберстрахования и полностью ввести в практику соответствующее законодательство, а также разработать

методику расчёта ущерба, причинённого киберправонарушениями, включая киберпреступления, и утвердить порядок установления санкций за совершение киберпреступлений;

6. Необходимо внедрить систему киберзащиты и полностью реализовать соответствующее законодательство на практике, создать единый и согласованный механизм искусственного создания киберкризисов, борьбы с ними и нейтрализации их последствий, а также разработать и внедрить индексы и критерии устойчивости к киберкризисам. Следует провести инвентаризацию схожих и повторяющихся задач и функций министерств и ведомств с целью их унификации и систематизации.

7. Необходимо установить обязательные специальные юридические и технические требования к базам данных персональных данных и облачным технологиям, обеспечить защиту цифровой информации, относящейся не только к персональным, общественным и государственным данным, полностью разработать соответствующее законодательство, а также закрепить в действующем законодательстве процедуры цифрового контроля в киберсреде, включая киберпространство, с чётким определением задач и обязанностей государственных органов, организаций и представителей частного сектора.

8. Необходимо определить порядок фиксации информации о том, когда, где и кем совершаются кибератаки на инфраструктуры цифрового контроля, а также о MAC-адресах устройств для выявления киберпреступников, и принять отдельное постановление Кабинета Министров в редакции, разработанной в соответствии с приложением 16 диссертации, с последующим его исполнением.

9. Необходимо принять приложения к проекту указа Президента Республики Узбекистан, разработанного в соответствии с приложением 17 диссертации как единый механизм установления цифрового контроля на основе Положения о порядке осуществления цифрового контроля в Республике Узбекистан и входящих в его состав положений, регламентов и других документов. Это будет способствовать обеспечению цифрового контроля над процессом цифровой трансформации в Республике Узбекистан.

10. За неисполнение субъектами кибербезопасности своих обязанностей, установленных законодательством, необходимо предусмотреть отдельные меры ответственности в Кодексе об административной ответственности и в Уголовном кодексе.

11. Необходимо установить точный возраст, с которого возникает право детей на открытие личных аккаунтов и профилей, а также предусмотреть конкретную административную и уголовную ответственность родителей или законных представителей за киберпреступления, совершённые их несовершеннолетними детьми в результате их собственной неосторожности, если дети ещё не достигли возраста уголовной ответственности.

12. В Законе Республики Узбекистан «Об информатизации» необходимо заменить понятия «искусственный интеллект», «технологии искусственного интеллекта», «информационные технологии» на понятие «информационно-коммуникационные технологии», а также заменить понятие

«информационная система» на «информационно-коммуникационная система», а также внести соответствующие изменения и дополнения в данный Закон.

III. Предложения и рекомендации, связанные с совершенствованием практики применения законодательства в сфере киберпреступности:

1. Помимо указанных статей Уголовного кодекса, включающих изменения и дополнения, предусмотренные в предложениях и рекомендациях по совершенствованию законодательства Республики Узбекистан, другие деяния также могут квалифицироваться как преступления в сфере информационно-коммуникационных технологий или киберпреступления. Однако в связи с развитием существующих общественных отношений и социальной необходимостью целесообразно рассматривать совершение таких деяний с использованием информационно-коммуникационных технологий, систем или телекоммуникационных сетей и средств как отягчающее обстоятельство, а также эффективно использовать дополнение к статье 56 УК.

2. Судебная практика по киберпреступлениям, в том числе по киберпреступлениям, угрожающим общественной безопасности, носит разнородный характер, и требуется её унификация. Для этого необходимо принять специальное отдельное постановление Пленума Верховного Суда Республики Узбекистан по данному направлению.

3. Пленум Верховного Суда Республики Узбекистан должен дать отдельное разъяснение, что в законах Республики Узбекистан «Об информатизации» и «О кибербезопасности», а также в Правилах оказания телекоммуникационных услуг, установлены отдельные обязательства операторов, провайдеров и пользователей в области информационной безопасности и кибербезопасности. Суд должен обращать внимание на то, что нарушение этих обязательств может приводить к совершению указанных видов преступлений, и таким образом устранять пробелы в действующей практике с учётом действующего законодательства.

4. Необходимо установить порядок проведения контрольных мероприятий в сферах связи, информатизации, электронного правительства, электронной цифровой подписи, искусственного интеллекта, цифровых технологий, цифровизации, телекоммуникаций и других смежных областях.

5. Необходимо разработать и внедрить процедуры осуществления цифрового контроля, установить обязательные правила с опорой на конкретные законодательные акты, полностью и корректно наладить взаимодействие между государственным и частным секторами, определить требования к информационным системам, с которыми требуется обязательная интеграция, и на их основе полностью интегрировать все необходимые информационные системы. До завершения процесса интеграции необходимо объявить мораторий на запуск новых версий существующих информационных систем, добавление дополнительных модулей и функций, а также создание и внедрение новых информационных

систем. После этого следует принять необходимые меры по обеспечению кибербезопасности через единую цифровую платформу.

6. Необходимо создать Республиканский центр экспертизы цифровых технологий и определить его как единственное государственное экспертное учреждение, осуществляющее виды экспертиз в области информационно-коммуникационных технологий. Вместо судебной компьютерно-технической экспертизы следует внедрить судебную киберэкспертизу, которая обеспечивает законность получения, хранения, сбора, использования и обработки доказательств, их достоверность и точность источников, а также ввести в практику виды экспертиз, включающие оценку телекоммуникационной сети, телекоммуникационной инфраструктуры, информационных систем, компьютерной информации, программного обеспечения, криптографических средств и охвата и качества связи.

7. Необходимо разработать учебные дисциплины и методические материалы по кибербезопасности, такие как «Кибербезопасность», «Основы кибербезопасности», «Киберправо», и обеспечить их обязательное и непрерывное преподавание в начальном, среднем, средне-специальном и высшем образовании. Следует создать единое высшее учебное заведение, готовящее специалистов по кибербезопасности как по юридическим, так и по техническим направлениям. При этом крайне важно пересмотреть существующие стандарты и классификаторы подготовки кадров в системе высшего образования, а учебные программы должны быть разработаны с учётом каждого вида киберпреступлений, обеспечивать выявление этих преступлений и гарантировать неотвратимость наказания через комплекс юридических и технических действий, реализуемых на практике.

8. Для установления цифрового контроля в киберсреде, включая киберпространство, необходимо полностью ввести в действие комплексную информационную систему «Цифровой мониторинг общественной безопасности» и подключить к ней информационные системы всех государственных органов и организаций, а также всех субъектов кибербезопасности независимо от формы собственности, и осуществлять цифровой контроль над ними с соблюдением их политики конфиденциальности;

9. Необходимо наладить международное и национальное сотрудничество по кибератакам, организовать обработку обращений, оперативное уведомление о кибератаках, получение ответов и обратной связи через «горячую линию» и контакт-центры, работающие в режиме 24/7. Также следует провести инвентаризацию всех информационных инфраструктур в Республике Узбекистан, сформировать реестр критической информационной инфраструктуры и обеспечить его регулярное ведение.

10. Цифровой контроль целесообразно осуществлять через комплексную информационную систему «**Jamoat xavfsizligining raqamli monitoringi**», при этом классифицируя информационно-коммуникационную инфраструктуру. Все информационные системы, базы данных и банки, телекоммуникационные сети и их составные части в республике должны быть интегрированы между собой. После внедрения цифрового контроля

с помощью искусственного интеллекта соответствующей информационной системы необходимо создать систему прогнозирования и предсказания, которая позволит оценивать, когда и где в будущем могут совершаться преступления исходя из криминогенной обстановки, и на основе этого эффективно распределять имеющиеся ресурсы для раскрытия киберпреступлений, внедряя технические решения и системы для их обнаружения.

11. В случае нарушения пользователем требований информационной безопасности или кибербезопасности через телекоммуникационные сети необходимо автоматически с помощью искусственного интеллекта и уполномоченных органов отправлять пользователю бесплатное SMS-уведомление, в котором предоставляется напоминание о нарушении и необходимости его прекратить. Для лиц, которые, получив уведомление, продолжают свои действия, должно применяться более строгое наказание, а лица, добровольно прекратившие свои действия, освобождаются от ответственности. Следует также установить порядок, по которому отправленное SMS-уведомление и подтверждающие факты его получения нарушителем могут быть приняты в качестве доказательств.

12. С целью повышения международного авторитета Республики Узбекистан в области кибербезопасности необходимо внедрить рейтинг обеспечения кибербезопасности, провести IT-аудит, выбрать единообразную терминологию по киберпреступлениям в международном уголовном праве, принять модельные законы, а также разработать или подготовить национальные технические средства, сети, устройства, системы, программы и программное обеспечение, соответствующие мировым стандартам в области информационно-коммуникационных технологий, обеспечивающих общественную безопасность, и полностью внедрить их в практику.

13. Для обеспечения устойчивости цифровых операций в финансовой и банковской сферах целесообразно внедрить хранение цифровых следов веб-сайтов и информационных систем, определить порядок их учёта. Полная интеграция всех информационно-коммуникационных систем с целью обеспечения общественной безопасности и кибербезопасности не является целесообразной; более эффективным является их классификация и организация взаимной интеграции с последующим цифровым контролем.

Данные выводы обоснованы в исследовательской работе, и принятие этих предложений будет способствовать формированию единых теоретических, научных, практических, правовых, технических и организационных подходов к противодействию киберпреступлениям, угрожающим общественной безопасности, совершенствованию законодательных актов, защите интересов личности, общества и государства, в том числе обеспечению общественной безопасности и кибербезопасности, а также выведет реформы в этой сфере на новый уровень.

SCIENTIFIC COUNCIL AWARDING OF THE SCIENTIFIC DEGREES DSc. 32/30. 12. 2020. Yu. 74. 01 UNDER THE UNIVERSITY OF PUBLIC SECURITY OF THE REPUBLIC OF UZBEKISTAN

UNIVERSITY OF PUBLIC SECURITY OF THE REPUBLIC OF UZBEKISTAN

ANORBOEV AMIRIDDIN ULUGBEK UGLI

CRIMINAL-LEGAL ASPECTS OF CYBERCRIMES THREATENING PUBLIC SECURITY

12.00.08 – Criminal law. Criminal-enforcement law

ABSTRACT
Doctoral dissertation (DSc) in Law

Tashkent – 2025

The topic of the Doctor of Legal Sciences (DSc) dissertation has been registered with the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan, under the number B2023.1.DSc/Yu235.

The dissertation is prepared at the University of Public Security of the Republic of Uzbekistan.

The abstract of the dissertation is posted in three languages (Uzbek, English, Russian (summary)) onthe website of the University of Public Safety of the Republic of Uzbekistan (www.mgjxu.uz) and Information educationalportal «ZiyoNET» (www.ziyonet.uz).

Scientific Consultant:	**Rustambayev Mirzayusup Khakimovich,** Doctor of Law, professor
Official opponents:	**Urazaliyev Murod Korayevich** Doctor of Law, professor
	Turgunboyev Elbekjon Odiljonovich Doctor of Law
	Akrom Ikromovich Toshpolatov Doctor of Law, Associate Professor
Leading organization:	**Criminalistics Research Institute of the Republic of Uzbekistan**

The defense of the dissertation will take place on “12” December 2025 year at 11-00 the meeting of the Scientific Council DSc.32/30.12.2020.Yu.74.01 at the University of Public Security of the Republic of Uzbekistan. (Address: 100211, Tashkent region, Zangiota district, Chorsu kurgan. Tel.: (99871) 230-32-71; fax: (99871) 230-32-50; info@mgjxu.uz)

The dissertation can be reviewed at the Information Resource Center of the University of Public Security of the Republic of Uzbekistan (registered under № _____). (Address: 100121, Tashkent region, Zangiota district, Chorsu settlement. Tel.: (99871) 230-32-71; fax: (99871) 230-32-50).

The abstract of the dissertation was distributed on « 28 » November 2025.

(Register of the distribution protocol № 21 of « 28 » November 2025)

D.M.Mirazov
Deputy Chairman of the Scientific Council for awarding scientific degrees, doctor of Science in Law, professor

J.D.Akhmedov
Secretary of the Scientific Council for awarding scientific degrees, doctor of Philosophy in Law (PhD)

Sh.Zulfikarov
Chairman of the Scientific Seminar under the Scientific Council for awarding scientific degrees, doctor of Science in Law, professor

INTRODUCTION (annotation of the doctoral dissertation (DSc))

The aim of the research is to study the criminal-legal aspects of cybercrimes that pose a threat to public safety, as well as to develop scientific and practical proposals and recommendations for ensuring cybersecurity.

The object of the research is the criminal-legal relations associated with the legal regulation of the criminal-legal aspects of cybercrimes that pose a threat to public safety.

Scientific novelty of the research consists of the following:

It has been substantiated that the establishment of criminal liability for public calls for mass riots and violence against citizens using telecommunication networks or the Internet contributes to strengthening the protection of public security;

It has been substantiated that the establishment of criminal liability for non-compliance with the requirements related to the collection, systematization, and storage of personal data on technical means and in databases located within the territory of the Republic of Uzbekistan contributes to the protection of citizens' personal data and the strengthening of social stability;

It has been substantiated that the establishment of procedures for the categorization of cybersecurity and critical information infrastructure objects, the assessment of the level of their cybersecurity, the conduct of examinations for compliance with cybersecurity requirements, as well as the certification of hardware, hardware-software, and software tools used to ensure the cybersecurity of information systems and resources, contributes to the systematization of relations in the field of cybersecurity and to ensuring the security of the individual, society, and the state in cyberspace;

It has been substantiated that the establishment of criminal liability for committing crimes that pose a threat to public security through unlawful (unauthorized) access to or use of information systems, including for violations of legislation in the field of crypto-asset circulation and for conducting mining activities in violation of the law, contributes to strengthening cybersecurity, taking strict measures against violations in the field of crypto assets, and ensuring the timely prevention of unauthorized access to and illegal use of information systems;

It has been substantiated that the establishment of criminal liability for the manufacture, acquisition, storage, transportation, shipment, as well as for the distribution, advertisement, or demonstration in telecommunication networks or on the Internet of narcotic drugs, their analogues, psychotropic substances, or products promoting them, for the purpose of their illegal distribution, contributes to strengthening the protection of human life and health.

Implementation of the research results. Based on the scientific results obtained during the research work on the topic "Criminal-legal aspects of cybercrimes that pose a threat to public safety":

1) in accordance with the Law of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan" № LRU–679 dated March 30, 2021 criminal liability is also

introduced under item “b” of Part 2 of Article 244 of the Criminal Code for public calls for mass riots and violence against citizens using telecommunications networks, the Internet, as well as by printed or other means of text reproduction. (Uzkomnazorat Act dated 05.12.2024 J № 01/07-1);

2) In accordance with the Law of the Republic of Uzbekistan dated October 29, 2021, № LRU–726 “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan”, Article 141^2 of the Criminal Code of the Republic of Uzbekistan establishes criminal liability for failure to comply with the requirements regarding the collection, systematization, and storage of personal data of citizens of the Republic of Uzbekistan when processing such data using information technologies, including on the Internet, without using technical means physically located on the territory of the Republic of Uzbekistan, as well as without registering personal data databases in the State Register of Personal Data in the prescribed manner; (Uzkomnazorat Act dated 05.12.2024 № 01/07-1);

3) the Law of the Republic of Uzbekistan “On Cybersecurity” № LRU–764 dated April 15, 2022, was adopted and on its basis:

by the Resolution of the President of the Republic of Uzbekistan dated May 31, 2023, № PD–167 “On Additional Measures to Improve the System of Ensuring Cybersecurity of Critical Information Infrastructure Objects of the Republic of Uzbekistan,” the procedure for ensuring cybersecurity of critical information infrastructure objects of the Republic of Uzbekistan and the general requirements for cybersecurity in the critical information infrastructure objects of the Republic of Uzbekistan were approved;

in accordance with the implementation of the Resolution of the President of the Republic of Uzbekistan dated February 19, 2024, № PD–75 the following regulatory acts were adopted by the Chairman of the State Security Service of the Republic of Uzbekistan:

Order № 91 dated September 4, 2023 (Reg. № 3458 dated September 22, 2023) “On Approval of the Regulation on the Procedure for Assessing the Level of Cybersecurity of Important Information Infrastructure Objects and Cybersecurity of the Republic of Uzbekistan”;

Order № 118 dated October 24, 2024 (Reg. № 3570 dated November 11, 2024) “On Approval of the Temporary Regulation on the Categorization of Important Information Infrastructure Objects of the Republic of Uzbekistan and Formation of Their Unified Registry”;

Order № 113 dated October 15, 2024 (Reg. № 3573 dated November 14, 2024) “On Approval of the Regulation on the Procedure for Conducting Expertise for Compliance with Cybersecurity Requirements”;

Order № 114 dated October 15, 2024 (Reg. № 3574 dated November 14, 2024) “On Approval of the Regulation on the Procedure for Certification of Hardware, Software-Hardware, and Software Tools Used to Ensure Cybersecurity of Information Systems and Resources”. (Act of the Ministry of Digital Technologies dated 14.05.2024 J., № 20-8/3142, and Act of Uzkomnazorat dated 05.12.2024 J., № 01/07-1);

4) in accordance with the Law of the Republic of Uzbekistan № LRU–829 dated April 11, 2023, “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Further Improvement of the System for the Reliable Protection of the Rights, Freedoms, and Legitimate Interests of Women and Children” In Article 141^3 of the Criminal Code of the Republic of Uzbekistan, criminal liability is established for the dissemination of information containing photo and/or video materials of a naked body and/or the genital organs of a person without their consent, including through mass media, telecommunication networks, or the Internet, as well as for threats to disseminate such information, in accordance with Law of the Republic of Uzbekistan № LRU–899 of January 19, 2024, “On Introducing Amendments and Additions to the Criminal and Criminal Procedure Codes, as well as the Code on Administrative Liability of the Republic of Uzbekistan”, Article 165 of the Criminal Code was amended to define extortion as demanding the transfer of another person's property, property rights, property interests, or actions of a proprietary nature by threatening to destroy, alter, seize, or block the victim's information resource, or to disclose information that should be kept secret for the victim, or to disseminate defamatory fabrications about them, or by putting the victim in a situation that forces them to give up their property or property rights. Article 278^8 introduced criminal liability for violating legislation in the sphere of crypto-asset circulation, while Article 278^9 established criminal liability for the illegal conduct of mining activities. Furthermore, the concepts of “crypto-asset” and “mining” were added to the eighth chapter of the Criminal Code. In accordance with the Law of the Republic of Uzbekistan № LRU–794 dated October 19, 2022 “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan,” criminal liability has been established:

under subparagraph (g) of part three of Article 168 of the Criminal Code — for fraud committed using an information system, including information technologies;

under subparagraph (b) of part three of Article 169 — for theft committed through illegal (unauthorized) access to an information system or using such a system. (Act of Uzkomnazorat dated 05.12.2024 J., № 01/07-1);

5) In accordance with the Law of the Republic of Uzbekistan № LRU–971 dated October 5, 2024 “On Amendments and Additions to the Criminal Code, the Criminal Procedure Code, and the Code of Administrative Responsibility of the Republic of Uzbekistan aimed at combating the illicit trafficking of narcotic drugs, their analogues or psychotropic substances, as well as potent and toxic substances”:

Article 251^1 of the Criminal Code establishes criminal liability for the dissemination, advertising, or demonstration of products promoting potent substances that are not narcotic drugs, their analogues, or psychotropic substances via telecommunication networks or the global information network Internet, as well as for placing such products with the purpose of their dissemination, advertising, or demonstration;

Subparagraph “d” of Part Three of Article 273 provides for criminal liability for the illegal manufacture, acquisition, storage, transportation, shipment, or sale of narcotic drugs, their analogues, or psychotropic substances using telecommunication networks, including the Internet, with the intent of their dissemination;

Article 274 of the Criminal Code establishes criminal liability for the dissemination, advertising, or demonstration of products promoting narcotic drugs, their analogues, or psychotropic substances using telecommunication networks or the Internet, for the purpose of dissemination, advertising, or demonstration. (Act of Uzkomnazorat dated 05.12.2024 J., № 01/07-1).

The structure and scope of the research. The dissertation consists of an introduction, four chapters containing nine paragraphs, a conclusion, a list of references, and appendices. The volume of the dissertation is 594 pages, including the main part – 233 pages.

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

I бўлим (Часть I; Part I)

1. А. Анорбоев. Жамоат хавфсизлигига таҳдид солувчи кибержиноятларнинг жиноий-ҳуқуқий жиҳатлари. Монография. А. Анорбоев. – Т.: “Dimal” нашриёти, 2025 й. – 530 б.
2. А. Анорбоев. Жамоат хавфсизлигига таҳдид солувчи кибержиноятларга қарши курашиш истиқболлари. Монография. – Т.: Жамоат хавфсизлиги университети таҳририяти, 2025 й. – 527 б.
3. А. Анорбоев. Кибержиноятлар хавфини бартараф этиш йўллари. “Одил судлов” журнали. №5/2020. ISSN 2181-8991. 80 б.
4. А.Анорбоев. Телекоммуникация тармоқларидан қонунга хилоф равишда фойдаланиш: жиноят-ҳуқуқий ва криминологик тавсиф. – Т.: “Huquq va burch” журнали, №11/2021. 64 б.
5. А.Анорбоев. Киберхавфсизликни таъминлаш истиқболлари. – Т.: “Одил судлов” журнали, – Т.: 2022 й ., 2-сон, 110 б.
6. А.Анорбоев. Bulutli texnologiyalardan foydalanish kiberxavfning oldini oladi(mi?). – Т.: “Huquq va burch” журнали, №3/2022. 64 б.
7. А. Анорбоев. Raqamli ko‘nikmalarni tizimli shakllantirish orqali kiberxavfni bartaraf etishning istiqboli. Oriental Renaissance: Innovative, educational, natural and social sciences VOLUME 2 | ISSUE 2, ISSN 2181-1784, Scientific Journal Impact Factor SJIF 2022: 5.947, Advanced Sciences Index Factor ASI Factor = 1.7, 2022 йил февраль, – 790-796 б.
8. А. Анорбоев. Киберхуружларнинг булутли технологиялардан унумли фойдаланишга кўрсатаётган салбий таъсири ва унинг олдини олиш чоралари. –Т.: Фундаментал тадқиқотлар илмий-амалий журнали, 2023 йил январь, 1-сон, 151-160 б.
9. А. Анорбоев. “Darknet” nima? tushuncha va mohiyat. “Huquq va burch” журнали, –Т.: №3/2023, 64-б.
10. А. Анорбоев. Кибержиноятнинг ҳуқуқий тавсифи. – Т.: “Одил судлов” журнал, 6/2023. ISSN 2181-8991, 52 б.
11. А.Анорбоев. Рақамли технологиялар соҳасида Ўзбекистон Республикаси Президентининг ҳужжатлари асосида эришилган ютуқлар ва уларга рахна солаётган кибертаҳдид. Жамият ва инновациялар – Общество и инновации – Society and innovations Journal home page: https://inscience.uz/index.php/socinov/index, 2181-1415/© 2023 in Science LLC. DOI: https://doi.org/10.47689/2181-1415-vol4-iss5-pp42-51. This is an open access article under the Attribution 4.0 International (CC BY 4.0) license (https://creativecommons.org/licenses/by/4.0/deed.ru.), Жамият ва инновациялар – Общество и инновации – Society and innovations. Issue – 4 № 5 (2023) / ISSN 2181-1415, 43-51-б.

12. А.Анорбоев. Шахсга доир маълумотларга оид қонунчиликни бузиш юзасидан жавобгарликни амалга ошириш механизмини аниқлаштириш ва соддалаштириш. Замонавий тадқиқотлар ахборотномаси, ISSN: 2181-4554. Volume II, Issue-8, (August) 2024, Journal homepage: https://inashr.uz/index.php/bocs, 23-28 б.

13. А.Анорбоев. AKT sohasiga mas'ul tashkilotlarga kelayotgan murojaatlarni sifatli ko'rib chiqish omillari. – T.: "Huquq va burch" журнали –T.: №8/2024, 64-б.

II бўлим (Часть II; Part II)

1. А. Анорбоев. Ахборот тизими ва телекоммуникация тармоғига қонунга хилоф (рухсатсиз) киришни кўзлаб нормал ишлашига тўсқинлик қилиш жиноятининг жиноий-ҳуқуқий ва криминологик тавсифи. Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborotkommunikatsiya texnologiyalarining ahamiyati, Respublika ilmiy-texnik anjumani Toshkent, 10-11-mart, 2022 – yil ma'ruzalar to'plami 1-qism, 618 б.

2. А. Анорбоев. Ахборот-коммуникация технологиялари орқали экстремизм жиноятини содир этганлик учун жавобгарликни белгилаш масалалари. Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborotkommunikatsiya texnologiyalarining ahamiyati, Respublika ilmiy-texnik anjumani Toshkent, 10-11-mart, 2022 – yil ma'ruzalar to'plami 1-qism, 618 б.

3. А. Анорбоев. Киберҳуружларнинг дастурий маҳсулот муаллифларига келтираётган зарарининг олдини олишнинг ҳуқуқий асосларини такомиллаштириш. Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №24 (том 2) (март, 2022). – 1490 б.

4. А. Анорбоев. Кибержиноятнинг келиб чиқиш тарихи ва бугунги куни. Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №24 (том 2) (март, 2022). – 1490 б.

5. А. Анорбоев. Киберҳуружларнинг дастурий маҳсулот муаллифларига келтираётган зарарининг олдини олишнинг ҳуқуқий асосларини такомиллаштириш. Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №24 (том 4) (март, 2022). – 1065 б.

6. А. Анорбоев. Кибержиноятнинг келиб чиқиш тарихи ва бугунги куни. Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №24 (том 4) (март, 2022). – 1065 б.

7. А. Анорбоев. Ўзбекистон Республикаси иқтисодиётига кибержиноятларнинг хавф-хатари. "Adliya sohasida raqamlashtirishni rivojlantirishning zamonaviy tendensiyalari" xalqaro konferensiya materiallari (2021-yil 14-dekabr), – 151-161 б.

8. А. Анорбоев. Киберэкстремизм жиноятининг жиноий-ҳуқуқий жиҳатлари. “Adliya sohasida raqamlashtirishni rivojlantirishning zamonaviy tendensiyalari” xalqaro konferensiya materiallari (2021-yil 14-dekabr), – 92-106 б.

9. А. Анорбоев. Кибержиноятларнинг мамлакат иқтисодиётига таҳдиди. “Adliya sohasida raqamlashtirishni rivojlantirishning zamonaviy tendensiyalari” xalqaro konferensiya materiallari (2021-yil 14-dekabr), – 92-106 б.

10. А. Анорбоев. Кибержиноятларнинг келиб чиқиш тарихи ва бугунги кундаги ривожи. “Adliya sohasida raqamlashtirishni rivojlantirishning zamonaviy tendensiyalari” xalqaro konferensiya materiallari (2021-yil 14-dekabr), – 92-106 б.

11. А. Анорбоев. Риски киберпреступности для экономики Республики Узбекистан. “Adliya sohasida raqamlashtirishni rivojlantirishning zamonaviy tendensiyalari”: xalqaro ilmiy-amaliy konferensiya materiallari to‘plami (14-dekabr 2021-yil, Toshkent) Mas’ul muharrir. Sh. Mirzayev. – “in Science” nashriyoti, Toshkent 2022. – 274 b.

12. А. Анорбоев. История возникновения киберпреступности и ее развитие. “Adliya sohasida raqamlashtirishni rivojlantirishning zamonaviy tendensiyalari”: xalqaro ilmiy-amaliy konferensiya materiallari to‘plami (14-dekabr 2021-yil, Toshkent) Mas’ul muharrir. Sh. Mirzayev. – “in Science” nashriyoti, Toshkent 2022. – 274 b.

13. А. Анорбоев. Замонавий жамиятда ахборот хавфсизлигини таъминлашда давлат органларининг ўрни. “Рақамли технологиялар соҳасидаги ҳуқуқбузарликларга қарши курашиш ҳамда ахборот хавфсизлигини таъминлашнинг ташкилий-ҳуқуқий масалалари”: xalqaro ilmiy-amaliy konferensiya materiallari to‘plami. – T.: “in Science” nashriyoti. 2022. – 343-363 b.

14. А. Анорбоев. Булутли технологиялар хизматини кўрсатиш шартномасига оид муаммолар ва уларнинг ечимлари. “Суд ва ҳуқуқни муҳофаза қилувчи органлар фаолиятида рақамлаштириш 224”: xalqaro ilmiy-amaliy konferensiya materiallari to‘plami. – T.: “in Science” nashriyoti, 2022. – 274 b.

15. А. Анорбоев. Ахборот-коммуникация технологияларидан зарарли мақсадларда фойдаланишнинг салбий оқибатлари ва ахборот хавфсизлигини таъминлаш истиқболлари. “Рақамли технологиялар соҳасидаги ҳуқуқбузарликларга қарши курашиш ҳамда ахборот хавфсизлигини таъминлашнинг ташкилий-ҳуқуқий масалалари”: xalqaro ilmiy-amaliy konferensiya materiallari to‘plami. – T.: “in Science” nashriyoti, – 343-363 b.

16. А. Анорбоев. Рақамли изларни логлаш, сақлаш ва ҳисобини юритиш – киберкоррупция ва кибержиноятларни фош этиш ва киберҳимояни таъминлаш усулидир. – Т.: “Ustozlar uchun” журнали. 2025 й., 77 сон, 1 тўплам. – Б. 119.

17. А. Анорбоев. С.А. Анорбоева. Киберхавфсизлик ва кибержиноятларга алоқадор изоҳли луғат. (4 та тилда). – Т.: “Dimal” нашриёти, 2025-й. – 220 б.

18. М. Рустамбаев, А. Анорбоев, С. Анорбоева. Кибертерминология. (5 та тилда изоҳли луғат). Изоҳли луғат. – Т.: Жамоат хавфсизлиги университети таҳририяти, 2025 й., – 205 б.

«O‘zbekiston Respublikasi Jamoat xavfsizligi
universitetining Axborotnomasi»
jurnali tahririyatida tahrirdan o‘tkazildi

№ 10-3279

Bosishga ruxsat etildi: 28.11.2025.
Bichimi: 60x84 1/16 «Times New Roman»
garniturada raqamli bosma usulda bosildi.
Shartli bosma tabog‘i 4,5. Adadi 100. Buyurtma: № 195
Tel: (99) 832 99 79; (77) 300 99 09
Guvohnoma reestr № 10-3279
«IMPRESS MEDIA» MChJ bosmaxonasida chop etildi.
Manzil: Toshkent sh., Yakkasaroy tumani, Qushbegi ko‘chasi, 6-uy.