TOSHKENT DAVLAT YURIDIK UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI PhD.07/03.06. 2023.Yu.22.04-SONLI ILMIY KENGASH

TOSHKENT DAVLAT YURIDIK UNIVERSITETI

NAEEM ALLAHRAKHA

RAQAMLI IQTISODIYOTDA MOLIYAVIY BARQARORLIK UCHUN TRANSCHEGARAVIY ELEKTRON JINOYATLARNING OLDINI OLISH

12.00.10 – Xalqaro huquq

Yuridik fanlar bo‘yicha falsafa doktori (PhD) dissertatsiyasi AVTOREFERATI

Toshkent – 2024

UDK:33(043.5) (575.1)

Falsafa Doktori (PhD) dissertatsiyasi avtoreferati mundarijasi
Content of the abstract of the dissertation of the Doctor of Philosophy (PhD)
Содержание автореферата диссертации доктора философских наук (PhD)

TOSHKENT DAVLAT YURIDIK UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI PhD.07/03.06. 2023.Yu.22.04-SONLI ILMIY KENGASH

TOSHKENT DAVLAT YURIDIK UNIVERSITETI

NAEEM ALLAHRAKHA

RAQAMLI IQTISODIYOTDA MOLIYAVIY BARQARORLIK UCHUN TRANSCHEGARAVIY ELEKTRON JINOYATLARNING OLDINI OLISH

12.00.10 – Xalqaro huquq

Yuridik fanlar bo‘yicha falsafa doktori (PhD) dissertatsiyasi AVTOREFERATI

Toshkent – 2024

Falsafa doktori (PhD) dissertatsiyasining mavzusi O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasi tomonidan № B2024.2.PhD/Yu1491 raqam bilan ro‘yxatga olingan.

Dissertatsiya ishi Toshkent davlat yuridik universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, ingliz, rus (rezyume)) Ilmiy kengash veb-sahifasida (www.tsul.uz/uz-ilmiy-kengash) va «ZiyoNET» ta’lim axborot tarmog‘ida (www.ziyonet.uz) joylashtirildi.

Ilmiy rahbar:	**Rustambekov Islambek Rustambekovich** yuridik fanlar doktori, professor
Rasmiy opponentlar:	**Umarxanova Dildora Sharipxanovna,** yuridik fanlar doktori (DSc), professor
	Tillaboyev Mirzatilla Alisherovich yuridik fanlar bo‘yicha falsafa doktori (PhD), professor
Yetakchi tashkilot:	**O‘zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi**

Dissertatsiya himoyasi Toshkent davlat yuridik universiteti huzuridagi ilmiy darajalar beruvchi PhD.07/03.06. 2023.Yu.22.04- raqamli Ilmiy kengashning 2024 yil «5» dekabr kuni soat 10:00 dagi majlisida bo‘lib o‘tadi (Manzil: 100047, Toshkent sh., Sayilgoh ko‘chasi, 35. Tel.: (99871) 233-66-36; faks: (99871) 233-37-48; e-mail: info@tsul.uz).

Dissertatsiya bilan Toshkent davlat yuridik universiteti Axborot-resurs markazida tanishish mumkin (1298-son bilan ro‘yxatga olingan) (Manzil: 100047, Toshkent sh., A.Temur ko‘chasi, 13. Telefon: (99871) 233-66-36).

Dissertatsiya avtoreferati 2024-yil 4-noyabr kuni tarqatildi.

(2024-yil 4-noyabrdagi 11-raqamli reestr bayonnomasi).

S.S.Gulyamov
Ilmiy darajalar beruvchi ilmiy kengash raisi, yuridik fanlar doktori, professor

D.N. Maxkamov
Ilmiy darajalar beruvchi ilmiy kengash kotibi, yuridik fanlari doktori, dotsent

Sh.X. Fayziyev
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, yuridik fanlar doktori, professor

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. To‘rtinchi sanoat inqilobi raqamli va jismoniy ishlab chiqarish tizimlari moslashuvchan tarzda birgalikda ishlaydigan davrni belgilaydi. Ushbu inqilob bizni kompyuterlar, turli elektronika va internet bilan tanishtirgan Raqamli inqilob deb ham ataladigan Uchinchi sanoat inqilobiga asoslanadi.[1] U turli sohalarda raqamli texnologiyalar va jarayonlarni o‘zlashtirish orqali an’anaviy va raqamli biznesni birlashtiradi. Ushbu inqilob avvalgi ixtirolarning imkoniyatlarini to‘rtta asosiy ilg‘or texnologiyalar bilan kengaytiradi: ulanish, ma’lumotlar, hisoblash quvvati va qiymat zanjirida qo‘llaniladigan bulutli hisoblash sensorlari. “Bulut”ga asoslangan raqamli platformalar ushbu raqamli siljishning muhim tarkibiy qismidir. Platforma iqtisodiyotining yuksalishi muhim va adolatli daromad olish imkoniyatlarini ta’minlab, raqamli platformalarga o‘tkazilgan ishlarning ko‘payishiga olib keldi.[2]

2023-yilda raqamli transformatsiya bo‘yicha jahon bozori 2,27 trillion dollarga baholandi. 2024-yildagi 2,71 trillion dollardan 2032-yilga kelib 12,35 trillion dollargacha oshib, yillik 20,9 foizga o‘sishi prognoz qilinmoqda. 2023-yilga kelib, dunyo bo‘ylab taxminan 2,64 milliard onlayn xarid qiluvchilar mavjud bo‘lib, bu dunyo aholisining 33% dan ortig‘ini tashkil qiladi (Statista). Raqamlashtirishning o‘sishi banklar, nobank kreditorlar, sug‘urta kompaniyalari, qimmatli qog‘ozlar bozorlari va investitsiya fondlarini o‘z ichiga olgan moliya sektoridagi faollikni ham oshirdi. Ushbu sektor, shuningdek, kliring kontragentlari, to‘lov provayderlari, markaziy banklar, moliyaviy regulyatorlar va nazoratchilarni o‘z ichiga oladi. Moliyaviy tizimlar global raqamli iqtisodiyotning o‘sishini qo‘llab-quvvatlab, tobora ko‘proq raqamlashtirilmoqda. Global transchegaraviy to‘lovlar bozori 2022-yilda 181,9 trillion dollarga baholandi va 2032-yilga kelib 356,5 trillion dollarga yetishi kutilmoqda, 2023-yildan 2032 yilgacha har yilgi o‘sish sur‘ati 7,3 foizni tashkil etadi (Yahoo Finance).

Moliyaviy tizimlar jadal raqamlashtirilib, global raqamli iqtisodiyotga imkon beradi. Raqamli texnologiyalarning yuksalishi iqtisodiy barqarorlikka tahdid soladigan kiberjinoyatlarni ham oshirdi. Moliyaviy sektordagi kiberjinoyatlar pul daromadlariga qaratilgan noqonuniy faoliyatni o‘z ichiga oladi. Bunga shaxsiy ma’lumotlarni o‘g‘irlash, to‘lov dasturi hujumlari, internet va elektron pochta orqali amalga oshiriladigan firibgarlikning turli shakllari kiradi[3]. Jinoyatchilar to‘lov kartasi ma’lumotlarini o‘g‘irlash (kartalash), ruxsatsiz operatsiyalarni amalga oshirish uchun moliyaviy hisoblarga kirish va tovlamachilik kabi faoliyat bilan shug‘ullanadilar. Masalan, 2023-yil may oyida LockBit tovlamachi dastur guruhi Indoneziyadagi eng yirik banklardan biri bo‘lgan BSIga hujum qildi. Bank 20

[1] Raja Santhi, A., & Muthuswamy, P. (2023). Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. *International Journal of Interactive Design and Manufacturing*, *17*(3), 947–979. https://doi.org/10.1007/s12008-023-01217-8

[2] Javaid, M., Haleem, A., Singh, R. P., & Sinha, A. K. (2024). Digital economy to improve the culture of industry 4.0: A study on features, implementation and challenges. *Green Technologies and Sustainability*, *2*(2), 100083. https://doi.org/10.1016/j.grets.2024.100083

[3] Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). Rising cyber threats pose serious concerns for financial stability. *IMF Blog*. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

million AQSh dollari miqdoridagi to‘lov talabini to‘lashdan bosh tortdi, bu esa hujumchilar tomonidan 1,5 terabaytdan ortiq maxfiy ma’lumotlarni internetga chiqarishiga olib keldi. Bu ochiqlangan ma’lumotlar taxminan 15 million mijoz va xodimlarning shaxsiy va moliyaviy ma’lumotlarini o‘z ichiga olgan.[4]

XVJ ma’lumotlariga ko‘ra, so‘nggi yigirma yil ichida 20 000 dan ortiq kiberhujumlar qayd etilgan bo‘lib, moliyaviy xizmatlarga to‘lovga qarshi hujumlar soni 2021-yildagi 34 foizdan 2023-yilda 64 foizgacha o‘sdi (IMF). Bunga qarshi kurashish uchun bunday kiber hodisalarning aholi ishonchini yo‘qotish yoki muhim xizmatlarni buzish orqali iqtisodiyotni beqarorlashtirishi mumkin bo‘lgan tizimli inqirozlarni keltirib chiqarishining oldini olish uchun mustahkam tartibga soluvchi barqarorlik muhim ahamiyatga ega. Moliyaviy ma’lumotlar xavfsizligini ta’minlashga qaratilgan muhim qoidalarga to‘lov kartalari sanoati ma’lumotlar xavfsizligi standarti (PCI DSS), Evropa Ittifoqining ma’lumotlarni himoya qilish bo‘yicha umumiy reglamenti (GDPR) va to‘lov xizmatlari bo‘yicha 2-direktiva (PSD2) kiradi, bu esa bank sohasida raqobat va xavfsizlikni kuchaytiradi. Bundan tashqari, SWIFT xizmatlaridan foydalanadigan muassasalar SWIFT Mijoz xavfsizligi dasturiga (SWIFT CSP) muvofiq bo‘lishi kerak va ISO/IEC 27001 moliyaviy ma’lumotlar bilan ishlashda xavfsizlik xatarlarini boshqarish uchun asos yaratadi.

O‘zbekistonda moliyaviy barqarorlikni ta’minlashga qaratilgan qator me’yoriy-huquqiy hujjatlar ishlab chiqilgan. 2022-yil 15-aprelda kuchga kirgan “Kiberxavfsizlik to‘g‘risida”gi qonun (O‘RQ-764-son) va 1994-yil 22-sentabrdagi O‘zbekiston Jinoyat kodeksi (2012-XII-son), 2024-yil 21-fevraldagi so‘nggi o‘zgartishlari shular jumlasidandir. Yuqoridagilar kabi, 1994-yil 22-sentyabrda qabul qilingan O‘zbekistonning Ma’muriy javobgarlik to‘g‘risidagi kodeksi (2015-XII-son, 2024-yil 29-fevralda qayta ko‘rib chiqilgan), 2019-yil 2-iyuldagi “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun (O‘RQ-547-son) va 2003-yil 30-avgustdagi “Bank siri to‘g‘risida”gi Qonun (№ 530-II, oxirgi marta 2023-yil 28-noyabrda va 2022-yil 11-aprelda o‘zgartirilgan), muhim nizomlar qatoriga 1996-yil 25-apreldagi “Banklar va bank faoliyati to‘g‘risida”gi (216-I-son, 2024-yil 21-fevralda qayta ko‘rib chiqilgan), 2019-yil 1-noyabrdagi “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonun (O‘RQ-578-son, 2024-yil 7-fevralda o‘zgartirilgan) va 2004-yil 26-avgustdagi “Jinoyat faoliyatidan olingan daromadlarni legallashtirishga qarshi kurashish to‘g‘risida”gi Qonun (660-II-son, oxirgi marta 2023-yil 28-noyabrda yangilangan), “Sug‘urta faoliyati to‘g‘risida”gi Qonun (O‘RQ-730-son, 2021-yil 23-noyabrda kiritilgan), O‘zbekiston Respublikasi Prezidentining 2020-yil 12-maydagi “2020-2025-yillarda O‘zbekiston bank tizimini isloh qilish strategiyasi to‘g‘risida”gi (PF-5992-son qarori, unga o‘zgartish va qo‘shimchalar 2023-yil 12-iyulda kiritildi), O‘zbekiston Markaziy bankining 2020-yil 30-iyundagi “To‘lov tizimlarida axborot xavfsizligini tartibga solish to‘g‘risida”gi 3268-son qarori va 2020-yil 15-fevraldagi 3/13-sonli “Elektron pullarni mamlakatimizda tartibga solish to‘g‘risida”gi qarorlarni shular jumlasiga kiritsa bo‘ladi.

[4] Hasham, S., Joshi, S., & Mikkelsen, D. (2019, October). *Risk Practice: Financial crime and fraud in the age of cybersecurity*. Mc Kinsey & Company.

Mazkur dissertatsiyada taqdim etilgan tadqiqot natijalari O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi “Raqamli mahsulotlar (xizmatlar) iste‘molchilari huquqlarini himoya qilishni kuchaytirish va raqamli texnologiyalar orqali sodir etiladigan huquqbuzarliklarga qarshi kurashish choralari to‘g‘risida”gi PQ-381-son qarori mazmun-mohiyatiga mos keladi. Iqtisodiyot sektori tranzaktsiyalarning sifati va xavfsizligini ta’minlaydigan elektron tijorat platformalari, raqamli xizmatlar va moliyaviy texnologiyalar hisobiga tez sur‘atlar bilan kengaydi. Shu bilan birga, bank kartalarini o‘g‘irlash va firibgarlik holatlarining ko‘payishi aholining raqamli moliyaviy savodxonligi yetarli emasligi, huquqni muhofaza qiluvchi organlarning malakasi yetarli emasligi, tijorat banklari, to‘lov tashkilotlari va to‘lov tizimlari operatorlarida qonunbuzarliklarning oldini olish bo‘yicha zamonaviy tizimlar mavjud emasligini ko‘rsatmoqda.

Tadqiqotning respublika fan va texnologiyalarni rivojlantirishning ustuvor yo‘nalishlariga muvofiqligi. Dissertatsiya tadqiqoti respublika fan va texnologiyalari rivojlanishining I. “Axborotlashgan jamiyat va demokratik davlatni ijtimoiy, huquqiy, iqtisodiy, madaniy, ma’naviy-ma’rifiy rivojlantirishda innovasion g‘oyalar tizimini shakllantirish va ularni amalga oshirish yo‘llari” ustuvor yo‘nalishiga muvofiq bajarilgan.

Muammonining o‘rganilganlik darajasi. Moliyaviy jinoyatlar noqonuniy faoliyatni amalga oshirish uchun texnologiyadan foydalanishni o‘z ichiga oladi. Adabiyotlarni ko‘rib chiqish qismida quyida keltirilganidek, mavjud ilmiy tadqiqotlar va ularning natijalari ko‘rib chiqiladi. Turli yurisdiktsiyalarda ushbu tizimlarning samaradorligini baholash, shuningdek, ularning kibertahdidlarning tez rivojlanayotgan tabiatiga moslashishi juda muhim rol o‘ynaydi (Saeed va boshq., 2023). Transchegaraviy kiberjinoyatlarni tekshirishning huquqiy muammolari haqida tushuncha beradigan Fran (2022) ishi kabi kiber barqarorlikni oshirishda xalqaro hamkorlikning qiyinchiliklari va muvaffaqiyatlari (Fran Casino va boshq., 2022). Huquqiy tizimlarning o‘zaro muvofiqligi va moliyaviy elektron jinoyatlarni ta’qib qilishni va oldini olishni soddalashtirishi mumkin bo‘lgan yagona tartibga solish yondashuvi imkoniyatlariga e‘tibor qaratish lozim (Spapens, Peters & Daele, 2015).

Kiberxavfsizlik texnologiyalarini, shu jumladan blokcheynva sun‘iy intellektni ishlab chiqish va joriy etish bo‘yicha tadqiqotlar ularning elektron jinoyatlarning oldini olishdagi samaradorligi tahlil qilinishi kerak (Ferrag, Maglaras va Benbouzid, 2023).

Muhim manbalar qatoriga texnologiyaning kiber jinoyatlarni amalga oshirish va ularga qarshi kurashishdagi rolini muhokama qilgan (Bellasio va boshq., 2020) hamda texnologiyaning moliyaviy barqarorlikka ta’sirini o‘rgangan (Lu, He, & Yan, 2022) asarlari kiradi. Turli mamlakatlar va xalqaro tashkilotlarning siyosiy tashabbuslari moliyaviy elektron jinoyatlarning oldini olishga qaratilgan (McDowell & Novis, 2001).

Masalan, moliyaviy elektron jinoyatlarni kamaytirishdagi ta’sirini tushunish uchun Pul yuvishga qarshi kurashish bo‘yicha moliyaviy chora-tadbirlar guruhi (FATF)ning pul yuvish va terrorizmni moliyalashtirishga qarshi kurash bo‘yicha tavsiyalari ko‘rib chiqilishi mumkin (Schott, 2006). Bu Xalqaro valyuta jamg‘armasi

(XVJ) va Jahon banki kabi xalqaro moliya institutlarining kiber tahdidlarning global moliyaviy tizimlarga iqtisodiy oqibatlarini tahlil qiluvchi hisobotlarini o‘rganishni o‘z ichiga oladi (Gulyás & Kiss, 2023).

O‘zbekiston Respublikasi olimlarining tegishli adabiyotlar sharhi sifatida Rivojlanayotgan kapital bozorlarining institutsional va huquqiy asoslari: MDH mamlakatlari tajribasi (Said G‘ulomov, I. Rustambekov, Boboqulov I. I., Eshmatova Feruza Farxodovna, Safarov Nurbek Abdivalievich, Tillaboyev Mirzatillo Alisherovich, Umarxonova D. Sh., G‘afurova S. A., Tursunov Husan Mirzaevich, Shukurov Xolbek Nazarovich, D. Sh. Umarxonova, Qodirqulov A.O., V. A. Ortiqova, Mirzairova S. Z., A. A. Qosimova, Sh. Sh. Mirzaev, H. A. Qazoqxonov, Azimov M. M., Qaxarov S. R.

Raqamli moliyaviy jinoyatlarga qarshi kurashda texnologik yutuqlar va xalqaro huquqiy bazalarning keng yoritilishiga qaramay, adabiyotlar bir qancha muhim kamchiliklarni ochib beradi. Huquqiy tizimlarning tez rivojlanayotgan texnologiyalarga moslashuvi, xususan, kiberjinoyatchilikning yangi shakllariga qarshi kurashish uchun amaldagi qonunlar yetarli darajada o‘rganilmaganligi shular jumlasidan hisoblanadi. Bundan tashqari, xalqaro hamkorlikning ahamiyati e‘tirof etilgan bo‘lsa-da, turli yurisdiktsiyalarda bunday hamkorlikning samaradorligi va ularning moliyaviy barqarorlikka ta’siri bo‘yicha batafsil tahlillar mavjud emas. Bundan tashqari, adabiyotda tartibga solishning yagona yondashuvlarini qo‘llash mumkinligi haqida taxminlar bildirilgan bo‘lsa ham, ammo ularning amalga oshirilishi, ayniqsa turli huquqiy tizimlarga ega bo‘lgan global kontekstda yetarlicha muhokama qilinmagan. Ushbu bo‘shliqlar raqamli iqtisodiyotda elektron jinoyatlarga qarshi samarali kurashish uchun texnologik innovatsiyalar, huquqiy moslashuvlar va xalqaro tartibga solish harakatlari o‘rtasidagi dinamik o‘zaro ta’sirni keng qamrovli tadqiq qilish zarurligini ta’kidlaydi.

Dissertatsiya tadqiqotining dissertatsiya bajarilayotgan oliy ta’lim muassasasining ilmiy-tadqiqot rejalari bilan bog‘liqligi. Elektron moliyaviy jinoyatlarga qarshi kurashni tartibga solish strategiyalariga bag‘ishlangan dissertatsiya tadqiqoti Toshkent davlat yuridik universitetining huquqiy asoslarni rivojlantirish va raqamli davrda moliyaviy barqarorlikni ta’minlashga bag‘ishlangan tadqiqot rejalari bilan uzviy bog‘liqdir.

Tadqiqot maqsadi moliyaviy jinoyatlarga qarshi kurashning tartibga solish strategiyalarini aniqlash va raqamli iqtisodiyot uchun barqarorlikni mustahkamlashga qaratilgan ilmiy asoslantitilgan taklif va tavsiyalar ishlab chiqishdan iborat.

Tadqiqot vazifalari:

raqamli aloqa, raqamli iqtisodiyot va transmilliy kiber tahdidlarning o‘sishini tahlil qilish;

elektron jinoyatlarning moliyaviy tizim barqarorligi va raqamli iqtisodiyot rivojlanishiga ta’sirini o‘rganish;

tartibga solish tamoyillari va yondashuvlarini belgilash;

global institutsional tartibga solish standartlari mohiyatini oydinlashtirish;

raqamli iqtisodiyotda kiberxavflarni boshqarishdagi qiyinchiliklarni aniqlash;

transchegaraviy elektron jinoyatlar monitoringi, tergov va ta’qibga e‘tibor qaratish;

sud jarayoni va tergovning jahon standartlarini tushuntiring;

milliy qoidalar va javobli choralarni uyg‘unlashtirish;

davlat, xususiy va fuqarolik sektorlaridagi sheriklikning rolini tasniflash;

kiberjinoyat ta’sirini sug‘urtalash va qoplash;

qonunchilik bazasi va huquqni qo‘llash amaliyotini takomillashtirish bo‘yicha taklif va tavsiyalar ishlab chiqishdan iborat.

Tadqiqot obyekti raqamli iqtisodiyotning barqarorligini oshirish maqsadida xalqaro me‘yoriy-huquqiy bazani va uning elektron moliyaviy jinoyatlarga qarshi kurashdagi samaradorligini aniqlash va tahlil qilishdan iborat.

Tadqiqot predmetini tez o‘zgaruvchan raqamli moliyaviy landshaft sharoitida mavjud chora-tadbirlarni aniqlash va tahlil qilish, bo‘shliqlarni aniqlash va joriy strategiyalarning samaradorligini baholash tashkil etadi.

Tadqiqot usullari. Tadqiqot olib borishda qiyosiy-huquqiy tadqiqot, tarixiy, ilmiy manbalarni kompleks tadqiq etish, mantiqiy tahlil etish, umumlashtirish, tizimli yondashuv, empirik tadqiqotlar hamda muammoli vaziyatlar (case law) tahlili kabi usullardan foydalanildi.

Tadqiqotning ilmiy yangiligi quyidagilarni o‘z ichiga oladi.

O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksiga mobil qurilmalarning xalqaro identifikatsiya kodini yoki abonent qurilmasini identifikatsiya qilish modulini qonunga xilof ravishda o‘zgartirganlik, kriptoaktivlar muomalasi sohasidagi qonun hujjatlarini buzganlik va konchilik faoliyatini noqonuniy amalga oshirganlik uchun ma’muriy javobgarlikni qo`llashga oid takliflar asoslantirilgan;

“Internet global axborot tarmog‘iga to‘siqlarsiz kirish uchun zarur shart-sharoitlarni yaratish, milliy internet makonida kiberxavfsizlikni ta’minlash va fuqarolarning internetdan foydalanish savodxonligini oshirishga oid normalarni qonunchilikda belgilash zarurati asoslantirilgan;

vakolatli davlat organi o‘z vakolatlari doirasida muhim axborot infratuzilmasi kiberxavfsizligini ta’minlash sohasidagi xalqaro tadbirlarda ishtirok etishi va xalqaro shartnomalarga muvofiq kiberxavfsizlik tahdidlari va hodisalari to‘g‘risida ma’lumot almashishiga oid norma kiritilshi asoslantirilgan;

“elektron (raqamli) dalillar” tushunchasini, elektron dalillarni aniqlash, to‘plash, tekshirish, tekshirish, baholash, qayd etish, saqlash tartiblarini, shuningdek ishtirokchilarning huquq va majburiyatlarini belgilash zaruriyatiga oid takliflari, ushbu jarayonlarda axborot texnologiyalaridan foydalangan holda sodir etilgan jinoyatlar bo‘yicha majburiy videoyozuvdan foydalangan holda, guvohlar ishtirokisiz kibermakonda tintuv va tekshirishlar o‘tkazish tartibini belgilash, shuningdek, axborotda raqamli barmoq izlarini saqlashda ma’lumotlarni saqlash bo‘yicha aniq talablarni (axborot turlarini) belgilash to‘g‘risidagi takliflar ilmiy jihatdan asoslantirilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

elektron moliyaviy jinoyatlarga qarshi kurashish va raqamli iqtisodiyotning barqarorligini oshirish bo‘yicha xalqaro tartibga solish strategiyalari uchun yo‘l xaritasini taqdim etish asoslantirilgan;

mijozlarni zarur tekshirishni kuchaytirish va shaxsiy ma’lumotlar o‘g‘irlanishining oldini olish maqsadida robotlar va xavfsiz raqamli identifikatsiya yechimini joriy etish orqali real vaqt rejimida tranzaktsiyalarni monitoring qilish, axborot almashish va hisobot berish talablarini joriy etish uchun boshqa mamlakatlarning tegishli organlari bilan hamkorlik mexanizmlarini yaratish maqsadga muvofiqligi asoslab berilgan;

moliyaviy ma’lumotlar va bank ma’lumotlarini “Moliyaviy ma’lumotlar” toifasiga kiritish uchun kuchaytirilgan himoya talab etilishi, ruxsatsiz uchinchi shaxslar tomonidan bank ma’lumotlarini qayta ishlashni aniq taqiqlanishini ta`minlash maqsadida moliyaviy ma’lumotlar va bank ma’lumotlariga ruxsatsiz kirish, noto‘g‘ri foydalanish yoki noqonuniy tarqatish uchun jiddiy jarimalarni joriy etish asoslantirilgan;

virtual aktivlar bilan operatsiyalarni jo‘natuvchi va oluvchi to‘g‘risida tegishli ma’lumotlarni almashish uchun kripto-aktivlar bilan operatsiyalarni amalga oshirishda mijozlar to‘g‘risidagi ma’lumotlarni to‘plash va uzatishni talab qilish bo‘yicha qoidani kiritish ilmiy jihatdan asoslantirilgan;

sug‘urta kompaniyalaridan hayot va umumiy sug‘urta sektorlari bo‘ylab ishonchli kiberxavfsizlik choralarini va raqamli operatsiyalari va elektron tranzaktsiyalari uchun ma’lumotlarni himoya qilishni nazorat qilishni talab qiladigan qoidalarni joriy etish asoslantirilgan.

Tadqiqot natijalarining ishonchliligi xalqaro huquq qoidalari va taniqli mualliflarning ilmiy maqolalaridagi ma‘lumotlarga asoslanganligi sababli sezilarli darajada yaxshilandi, tadqiqot xulosalari aniq belgilangan printsiplarga va dinamik raqamli moliyaviy tahdidlarni o‘rganishda izchil va takror tekshirilgan ma’lumotlarga asoslandi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot raqamli iqtisodiyotda kiberjinoyatlarni boshqarishning nazariy va amaliy jihatlariga katta hissa qo‘shadi.

Nazariy jihatdan, u xalqaro me‘yoriy-huquqiy bazalardagi kamchiliklarni aniqlash va yaxlit ko‘p yurisdiksiyali boshqaruv yondashuvi zarurligini ta’kidlab, ilmiy (akademik) doktrinani kengaytiradi.

Amaliy jihatdan u siyosatchilar va amaliyotchilarga kiberjinoyatlarga qarshi kurashish bo‘yicha samarali siyosiy va texnologik chora-tadbirlarni amalga oshirish bo‘yicha amaliy tushunchalarni taqdim etadi.

Tadqiqot natijalarining joriy qilinishi. Tadqiqot natijalaridan quyidagilarda foydalanilgan:

mobil qurilmalarning xalqaro identifikatsiya kodini yoki abonent qurilmasini identifikatsiya qilish modulini qonunga xilof ravishda o‘zgartirganlik, kriptoaktivlar muomalasi sohasidagi qonun hujjatlarini buzganlik va konchilik faoliyatini noqonuniy amalga oshirganlik uchun ma’muriy javobgarlik to‘g‘risidagi takliflar O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksining 155-moddasi 3-qismi va 155-moddasining “a” bandlarini shakllantirishda foydalanilgan (O‘zbekiston Respublikasi Oliy Majlis Qonunchilik palatasining 2024y-yil 20-martdagi dalolatnomasi). Bu taklif kriptoaktivlar muomalasi sohasidagi qonun

hujjatlarini buzganlik va konchilik faoliyatini noqonuniy amalga oshirishga samarali ta`sir chorasi bo`lishga xizmat qilgan;

Internet global axborot tarmog‘iga to‘siqlarsiz kirish uchun zarur shart-sharoitlarni yaratish, milliy internet makonida kiberxavfsizlikni ta’minlash va fuqarolarning internetdan foydalanish savodxonligini oshirish bo‘yicha ilmiy asoslangan taklifi. O‘zbekiston Respublikasi Prezidentining 2023-yil 11-sentabrdagi “O‘zbekiston – 2030” strategiyasi to‘g‘risida”gi PF-158-son Farmoni bilan tasdiqlangan “O‘zbekiston – 2030” strategiyasi ishlab chiqilishida foydalanilgan (O‘zbekiston Respublikasi Adliya vazirligining 2024-yil 5-avgustdagi dalolatnomasi). Bu taklif milliy internet makonida kiberxavfsizlikni ta’minlash va fuqarolarning internetdan foydalanish savodxonligini oshirishga xizmat qilgan;

vakolatli davlat organi o‘z vakolatlari doirasida muhim axborot infratuzilmasi kiberxavfsizligini ta’minlash sohasidagi xalqaro tadbirlarda ishtirok etishi va xalqaro shartnomalarga muvofiq kiberxavfsizlik tahdidlari va hodisalari to‘g‘risida ma’lumot almashishi bilan bog`liq takliflar O‘zbekiston Respublikasi Prezidentining 2023 yil 11-sentabrdagi «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi № PQ-167-son Qarori bilan tasdiqlangan O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tartibi to‘g‘risidagi Nizomning 8-bandini ishlab chiqishda foydalanilgan (O‘zbekiston Respublikasi Adliya vazirligining 2024-yil 5-avgustdagi dalolatnomasi). Bu taklif axborot infratuzilmasi kiberxavfsizligini ta’minlash sohasidagi xalqaro tadbirlarda ishtirok etishi va xalqaro shartnomalarga muvofiq kiberxavfsizlik tahdidlari va hodisalari to‘g‘risida ma’lumot almashishini yanada soddalashtirishga xizmat qilgan;

“elektron (raqamli) dalillar” tushunchasini, elektron dalillarni aniqlash, to‘plash, tekshirish, tekshirish, baholash, qayd etish, saqlash tartiblarini, shuningdek ishtirokchilarning huquq va majburiyatlarini belgilash zaruriyatiga oid takliflari, ushbu jarayonlarda axborot texnologiyalaridan foydalangan holda sodir etilgan jinoyatlar bo‘yicha majburiy videoyozuvdan foydalangan holda, guvohlar ishtirokisiz kibermakonda tintuv va tekshirishlar o‘tkazish tartibini belgilash, shuningdek, axborotda raqamli barmoq izlarini saqlashda ma’lumotlarni saqlash bo‘yicha aniq talablarni (axborot turlarini) belgilash to‘g‘risidagi takliflar O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi “Raqamli mahsulotlar (xizmatlar) iste‘molchilari huquqlarini himoya qilish va raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashishni kuchaytirish choralari to‘g‘risida”gi PQ-381-son qarori bilan tasdiqlangan “Raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashish va raqamli mahsulotlar (xizmatlar) iste‘molchilari huquqlarini himoya qilish tizimini takomillashtirish bo‘yicha” YO‘L XARITASIning 8-bandini ishlab chiqishda foydalanilgan (O‘zbekiston Respublikasi Adliya vazirligining 2024-yil 5-avgustdagi dalolatnomasi) Bu taklif elektron dalillarni aniqlash, to‘plash, tekshirish, tekshirish,

baholash, qayd etish, saqlash tartiblarini, shuningdek ishtirokchilarning huquq va majburiyatlarini belgilash, kibermakonda tintuv va tekshirishlar o‘tkazish tartibini belgilash, shuningdek, axborotda raqamli barmoq izlarini saqlashda ma’lumotlarni saqlash bo‘yicha aniq talablarni (axborot turlarini) belgilashga xizmat qilgan.

Tadqiqot natijalarining aprobatsiyasi universitet va milliy hamda xalqaro anjumanlardagi ma’ruza va taqdimotlarda o‘z aksini topgan.

Tadqiqot natijalarining e`lon qilinganligi. Dissertatsiya mavzusi bo‘yicha tadqiqot natijalari 2 ta milliy va 5 ta xalqaro anjumanlarda e‘lon qilingan. Bundan tashqari, tadqiqot natijalari 2 ta monografiya, 1 ta milliy jurnal va 19 ta xalqaro jurnallarda (shu jumladan 4 tasi Scopus bazasida) chop etilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, uchta bob, xulosa va foydalangan adabiyotlar ro‘yxatidan iborat. Dissertatsiyaning hajmi 153 betni tashkil etadi.

DISSERTASINING ASOSIY MAZMUNI

Dissertatsiyaning kirish qismida (doktorlik dissertatsiyasi annotatsiyasi) tadqiqot mavzusining dolzarbligi va zarurligi, tadqiqotning fan va texnika rivojlanishining asosiy ustuvor yo‘nalishlariga mosligi, muammoning o‘rganilganlik darajasi, ilmiy tadqiqot mavzusining dolzarbligi ko‘rsatilgan. ilmiy-tadqiqot muassasasiga dissertatsiya, maqsad va vazifalar. tadqiqotning ob‘ekti va predmeti, usullari, ilmiy yangiligi va amaliy natijalari, tadqiqot natijalarining ishonchliligi, ilmiy va amaliy ahamiyati, ularni joriy etish, tadqiqot natijalarini aprobatsiya qilish, natijalarni nashr etish, dissertatsiyaning hajmi va tuzilishi haqida ma’lumotlar keltirilgan.

Dissertatsiyaning “**Raqamli iqtisodiyotda transchegaraviy elektron jinoyat xavfini kontseptsiyalash va optimal tartibga solish**” deb nomlangan birinchi bobida transchegaraviy elektron jinoyatlarning tabiati va ko‘lami, ularning potensial oqibatlari, shuningdek ularga qarshi samarali kurashish uchun zarur bo‘lgan me‘yoriy-huquqiy bazaga bag‘ishlangan. Xalqaro dasturlar va nodavlat subyektlarning milliy siyosatga ta’sirini tan oladigan transmilliy siyosatni rivojlantirish nazariyasiga asoslanib, ushbu bobda raqamli asrda iqtisodiy, ijtimoiy-madaniy va siyosiy transmilliyizm o‘rtasidagi munosabatlar o‘rganiladi.

Raqamli iqtisodiyotning texnologik taraqqiyot va global ulanish tufayli jadal o‘sishi korxonalar va jismoniy shaxslarning chegaralar orqali tranzaktsiyalarni amalga oshirish usullarini o‘zgartirdi. Biroq, bu evolyutsiya, shuningdek, moliyaviy tizimlar, iste‘molchilar huquqlarini himoya qilish va iqtisodiy barqarorlik uchun jiddiy xavf tug‘diruvchi transmilliy kibertahdidlarning yangi turini keltirib chiqardi. Shaxsga doir ma’lumotlarni o‘g‘irlash, fishing, tovlamachi dastur hujumlari va xakerlik kabi transchegaraviy elektron jinoyatlar raqamli infratuzilmalardagi zaifliklardan foydalanadi, milliy chegaralar va yurisdiktsiyalardan tashqariga chiqadi.

Raqamli iqtisodiyot: raqamli texnologiyalar va elektron kommunikatsiyalardan, jumladan, elektron tijorat, raqamli marketing va moliyaviy

texnologiyalardan foydalanishga asoslangan iqtisodiy va tijorat faoliyatining keng spektri.

Transchegaraviy elektron jinoyatlar: Milliy chegaralar orqali jinoyatlar sodir etish yoki ularni osonlashtirish uchun internet va tarmoqqa ulangan kompyuterlardan foydalanadigan noqonuniy harakatlar, masalan, shaxsiy ma'lumotlarni o'g'irlash, sanoat josusligi va kredit kartalaridagi firibgarlik.

Transmilliy siyosatni rivojlantirish: g'oyalar, ma'lumotlar, odamlar va resurslarning transchegaraviy oqimi, an'anaviy milliy chegaralardan oshib, inson va ijtimoiy rivojlanish bilan bog'liq siyosatni shakllantirish.

Chegarasiz dunyo nazariyasi: integratsiyalashgan global iqtisodiyotda milliy chegaralarning ahamiyatini pasaytirish, xalqaro chegaralar orqali resurslar, kapital, mehnat va texnologiyaning cheklanmagan oqimini osonlashtirish.

Tavakkalga asoslangan va moslashuvchan tartibga solish yondashuvlari: turli mamlakatlarning turli imkoniyatlari va noyob moliyaviy landshaftlarini hisobga olgan holda global standartlarni ilgari surish bilan birga mahalliy voqelikka tartibga solish.

Dissertatsiyaning "**Raqamli iqtisodiyotda transchegaraviy elektron jinoyat xavfini kontseptsiyalash va optimal tartibga solish"** nomli birinchi bobida turli manbalardan, jumladan Buyuk Britaniya Bosh Politsiya xodimlari assotsiatsiyasi (ACPO), OECD va Jahon banki kabi tashkilotlarning hisobotlari, shuningdek, raqamli iqtisodiyot, kiberjinoyatchilik va xalqaro hamkorlik asoslari bo'yicha akademik adabiyotlardan olingan. Unda transchegaraviy elektron jinoyatlar keltirib chiqaradigan huquqiy va tartibga solish muammolari, ushbu tahdidlarni qo'llab-quvvatlash va ularga qarshi kurashishda paydo bo'layotgan texnologiyalarning roli hamda global standartlar va qonunlarni uyg'unlashtirish zaruriyati ko'rib chiqiladi.

Dissertatsiyaning "**Transchegaraviy elektron jinoyatlarning xalqaro huquqiy qoidalari**" deb nomlangan ikkinchi bobida xalqaro huquqiy tartibga solishning murakkab sohasi va transchegaraviy elektron jinoyatlar keltirib chiqaradigan muammolar muhokama qilinadi. Bu raqamli asrda yurisdiktsiya, tergov, ta'qib qilish va qonuniy jarayonni saqlashning muhim jihatlarini o'rganadi. Ushbu bobda kibermakonning chegarasiz tabiatidan kelib chiqadigan murakkabliklarni bartaraf etish uchun turli huquqiy bazalar, xalqaro shartnomalar va ilmiy ishlarga asoslanadi.

Yurisdiktsiya: davlat yoki sudning o'z hududi yoki predmeti doirasidagi ishlarni boshqarish va hal qilish uchun qonuniy vakolati.

Komplementarlik: Xalqaro jinoyat sudining (XJS) xalqaro jinoyatlarni ta'qib etishda milliy sud tizimlarini to'ldiruvchi rolini belgilovchi printsip (Rim statuti).

Tegishli jarayon: sud protsessida adolat, xolislik va shaxs huquqlarini himoya qilishni ta'minlaydigan asosiy huquqiy tamoyil.

Kiberjinoyatlar bo'yicha Budapesht konventsiyasi: milliy qonunlarni uyg'unlashtirish, hamkorlikni mustahkamlash va kiberjinoyatchilikka qarshi kurashish uchun huquqiy asos yaratishga qaratilgan innovatsion xalqaro shartnoma.

Ekstraditsiya: ayblanuvchi yoki mahkum shaxsni sud jarayoni yoki jazo uchun bir yurisdiksiyadan boshqasiga o'tkazish.

“**Tizimli barqarorlik uchun boshqaruv asoslari**” deb nomlangan uchinchi bobida turli huquqiy nazariyalar va tamoyillarga, jumladan, davlat suvereniteti kontseptsiyasiga (Jan Bodin, Tomas Xobbs), bir-birini to‘ldirish doktrinasiga (Rim statutiga) va qonuniy jarayon tamoyillariga (Magna Karta, Edvard III nizomi) asoslanadi. Shuningdek, u kiberjinoyat yurisdiktsiyasi (Brenner, 2004; Clough, 2010) va internetning chegarasiz tabiati (Goldsmith & Wu, 2006) keltirib chiqaradigan muammolarga oid ilmiy ishlarga asoslanadi. Bu bobda Kiberjinoyatchilik to‘g‘risidagi Budapesht konventsiyasi (Yevropa Kengashi, 2001-yil), Birlashgan Millatlar Tashkilotining Transmilliy uyushgan jinoyatchilikka qarshi konventsiyasi (UNTOC) kabi xalqaro shartnoma va konventsiyalarga va Arab Davlatlari Ligasining Axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurash to‘g‘risidagi konventsiyasi kabi mintaqaviy kelishuvlarga havola qilingan. (2010).

Onlayn to‘lovlar, ma’lumotlar maxfiyligi va kiberjinoyat yurisdiktsiyasini tartibga solish murakkab va ko‘p qirrali masala bo‘lib, xavfsizlik, innovatsiyalar va individual huquqlarning raqobatdosh manfaatlarini hal qilish uchun muvozanatli yondashuvni talab qiladi. Ushbu bobda xalqaro hamkorlik zarurligi, yagona qonunchilik bazasini yaratish hamda ma’lumotlar xavfsizligini ta’minlash bo‘yicha mustahkam chora-tadbirlar, shaffoflik va shaxsiy ma’lumotlar ustidan foydalanuvchi nazorati ustuvorligiga urg‘u berilgan.

Shuningdek, bobda kiberjinoyatlarga qarshi kurashda mamlakatlar duch keladigan muammolar, masalan, resurslarning cheklanganligi, yurisdiksiyaning murakkabligi, kadrlar tayyorlashning kamchiliklari va eskirgan qonunchilik asoslari yoritilgan. Unda qonunchilik sohasidagi islohotlar, jumladan, huquqni muhofaza qilish organlarining xalqaro hamkorligini mustahkamlash, ixtisoslashtirilgan kadrlar tayyorlashga sarmoya kiritish, texnologik taraqqiyotga hamnafas bo‘lish uchun qonunchilik bazasini uyg‘unlashtirish muhimligi ta’kidlanadi. Bundan tashqari, bob sud jarayonlarida adolat va xolislikni kafolatlovchi asosiy huquqiy tamoyil bo‘lgan qonuniy jarayonni ta’minlash muhimligini yana bir bor tasdiqlaydi. Huquqni muhofaza qilish va sud jarayonlarida texnologiyalardan tobora ko‘proq foydalanish bilan bog‘liq muammolarni tan oladi, bu esa shaxsiy daxlsizlik huquqlari va tegishli tartib-qoidalarning hurmat qilinishini ta’minlash uchun aniq huquqiy asoslar va protokollarni talab qiladi.

Kiberxavfsizlik sohasida “**Tizimli barqarorlik uchun boshqaruv asoslari**” deb nomlangan uchinchi bobida dissertant kiberxavfsizlikni kuchaytirish va kibertahdidlar keltirib chiqaradigan muammolarni hal qilish uchun hukumatlar, xalqaro tashkilotlar va xususiy sektor tomonidan o‘rnatilgan turli siyosatlar, strategiyalar va asoslarni o‘rganadi. Ushbu bob uchta asosiy jihatni o‘rganadi: milliy qoidalar va javob choralarini uyg‘unlashtirish, davlat, xususiy va fuqarolik sektorlari bo‘ylab hamkorlikni rivojlantirish hamda kiberjinoyatlar oqibatlarini yumshatishda sug‘urta va kompensatsiyaning roli.

Kiberxavfsizlik: tizimlar, tarmoqlar, dasturlar, qurilmalar va ma’lumotlarni kiberhujumlardan himoya qilish uchun texnologiyalar, jarayonlar va boshqaruv vositalarini qo‘llash (O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni).

Maxfiylik, yaxlitlik, mavjudlik, haqiqiylik va rad etmaslik: kiberxavfsizlikning beshta asosiy tamoyillari (matnda eslatib o‘tilgan).

Milliy kiberxavfsizlik strategiyasi: boshqaruv, xatarlarni boshqarish, tayyorlik, chidamlilik, muhim infratuzilmani himoya qilish, imkoniyatlarni oshirish, qonunchilik asoslari va xalqaro hamkorlikni ta’kidlagan holda mamlakatning kiberxavfsizligini oshirishga qaratilgan kompleks yondashuv (Milliy kiberxavfsizlik strategiyasining ilg‘or amaliyoti).

Boshqaruv tuzilmalari: kiberxavfsizlikni kuchaytirish va kibertahdidlarga qarshi kurashish uchun yaratilgan siyosat, strategiya va asoslar.

Ushbu bob tizimli kiberbardoshlilik uchun boshqaruv tizimini o‘rganishda bir nechta asosiy nazariy asoslar va adabiyotlarga tayanadi. U keng qamrovli milliy yondashuvni tavsiflovchi Milliy kiberxavfsizlik strategiyasining ilg‘or amaliyotiga, shuningdek, Xalqaro elektraloqa ittifoqining Milliy kiberxavfsizlik strategiyasini ishlab chiqish bo‘yicha qo‘llanmasiga havola qilinadi. UNCAC tomonidan tayyorlangan Birlashgan Millatlar tashkilotining UNCAC va xususiy sektor fuqarolik jamiyati qo‘llanmasi fuqarolik jamiyatining xususiy sektorni korrupsiyaga qarshi harakatlarga jalb qilishdagi rolini ta’kidlaydi. Kiberxavfsizlikda samarali boshqaruv bo‘yicha qo‘llanma xavfsizlik sektorini boshqarish tamoyillarini kibermakonda qo‘llashga urg‘u beradi. Buyuk Britaniya hukumatining Fuqarolik jamiyati strategiyasi fuqarolik jamiyati tashkilotlari bilan hamkorlik qilish modelini taqdim etadi. Microsoftning oq qog‘ozi Prinsipialmilliy kiberstrategiyalarni himoya qiladi.

Ushbu bob raqamli dunyoni himoya qilish hukumatlar, xalqaro tashkilotlar va sanoatning turli sohalardagi muvofiqlashtirilgan yondashuvini talab qiladi, degan xulosaga keladi. Unda kiberxavfsizlik tamoyillari, boshqaruv asoslari, risklarni boshqarish, tayyorlik, chidamlilik va qonunchilik asoslari muhimligini ta’kidlaydi. Shuningdek, bobda xalqaro tashkilotlarning global hamkorlikni rivojlantirish, texnik yordam ko‘rsatish va kiberxavfsizlik barqarorligini oshirish siyosatini ishlab chiqishdagi roli ta’kidlangan.

Ushbu bobda elektron jinoyatlarga qarshi kurashda davlat, xususiy va fuqarolik sektorlari o‘rtasidagi hamkorlikning ahamiyati, shuningdek, kibersug‘urtaning kiberjinoyatlarning moliyaviy oqibatlarini yumshatishdagi roli ta’kidlangan. Bob rivojlanayotgan mamlakatlarda turli xil milliy standartlar, huquqiy an‘analar, yurisdiksiyamurakkabligi va resurs to‘siqlari bilan bog‘liq qiyinchiliklarni e‘tirof etadi. Shuningdek, u ijtimoiy media, kriptovalyuta va narsalar interneti (IoT) kabi sohalardagi tez texnologik siljishlar tufayli kengayib borayotgan qonunchilik bo‘shliqlarini bartaraf etish zarurligini tan oladi.

XULOSA

Raqamli inqilob jahon miqyosida iqtisodiyot va jamiyatlarni o‘zgartirib, misli ko‘rilmagan aloqa, samaradorlik va innovatsiyalar davrini boshlab berdi. Ushbu tezkor raqamlashtirish bizning bir-biriga bog‘langan dunyomizning zaif tomonlaridan foydalanadigan murakkab transmilliy kibertahdidlarga ham eshiklarni ochdi. Raqamli texnologiyalar muhim infratuzilma bo‘ylab tarqalmoqda,

kiberxavflar alohida hodisalardan milliy xavfsizlik, iqtisodiy barqarorlik va jamoat xavfsizligi uchun dahshatli oqibatlarga olib keladigan tizimli tahdidlarga aylandi.

I. Ilmiy-nazariy tavsiyalar:

1.1 Raqamli iqtisodiyot bu, birinchi navbatda, raqamli ulanishga asoslangan iqtisodiy tizim bo‘lib, Internet, mobil tarmoqlar va boshqa aloqa kanallari kabi raqamli texnologiyalar orqali ma’lumotlarga kirish va almashish qobiliyatini anglatadi. Manuel Castells tomonidan taklif qilingan tarmoq jamiyati nazariyasi zamonaviy jamiyatlar raqamli aloqa texnologiyalari yordamida osonlashtirilgan tarmoqlar atrofida tuzilganligini ta’kidlaydi. 2022-yil oxiriga kelib internetdan foydalanuvchilarning global kirish darajasi 63,5 foizga yetdi, turli hisobotlarga ko‘ra, dunyo bo‘ylab 5 milliarddan ortiq odam internetdan foydalanadi, bu esa global yalpi ichki mahsulotning 4,5 foizdan 15,5 foizigacha bo‘lgan baholarni tashkil etadi. Transmilliy kibertahdidlar milliy chegaralardan oshib ketadigan va dunyoning istalgan nuqtasidan kelib chiqishi mumkin bo‘lgan zararli kiberfaoliyatdir. 2022-yilgi SonicWall Cyber Threat Report hisobotida 2021-yilda dunyo miqyosida to‘lov dasturi hujumlari 105 foizga oshgani aniqlandi, Strategik va xalqaro tadqiqotlar markazi (CSIS) 2020-yilda kiberjinoyatlarning global qiymati 945 milliard dollarga yetganini taxmin qildi.

1.2 O‘zbekistonning Respublikasining “Kiberxavfsizlik to‘g‘risida’gi qonunida; bu axborotni tortib olish, uni o‘zgartirish, axborot tizimlari va resurslarini yo‘q qilish yoki buzish uchun dasturiy ta’minot va apparat vositalaridan foydalangan holda kiberfazoda sodir etilganhuquqbuzarliklar majmui. Elektron jinoyat (elektron jinoyat) identifikatorni o‘g‘irlash, sanoat josusligi, kredit kartalari bilan firibgarlik, fishing, to‘lovdan foydalanishni anglatadi. Buyuk Britaniyaning Ichki ishlar vazirligi va Og‘ir va uyushgan jinoyatchilik agentligi (SOCA) boshchiligidagi Kiber tahdidlarni kamaytirish kengashi elektron jinoyatlarni uchta alohida turga ajratadi: raqamli tizimlarga qaratilgan sof onlayn jinoyatlar, internet orqali kuchaytirilgan an‘anaviy jinoyatlar va internet orqali osonlashtirilgan an‘anaviy jinoyatlar. Kiberjinoyatlar moliyaviy yo‘qotishlarga olib kelishi va moliyaviy institutlar faoliyatini buzishi, iste‘molchilar ishonchini yo‘qotishi va tizimli xavflarni keltirib chiqarishi mumkin. Ushbu jinoyatlar, shuningdek, xarajatlarni oshirish va huquqiy va tartibga solish muammolarini keltirib chiqarish orqali raqamli biznesning o‘sishiga to‘sqinlik qiladi.

1.3 Moliyaviy jinoyatlarga qarshi kurash tamoyillari umuman xatti-harakatlarning ayrim xavflarini, shu jumladan pul yuvish, terrorizmni moliyalashtirish, bozorni suiiste‘mol qilish, korrupsiya, firibgarlik va sanksiyalardan bo‘yin tovlash bilan kurashish choralarini qoplash uchun mo‘ljallangan. Moliyaviy jinoyatlarga qarshi kurashish moliya tizimining yaxlitligi va barqarorligini ta’minlashning muhim jihati hisoblanadi. XVF va Jahon bankining G20 transchegaraviy to‘lovlar maqsadlariga erishish uchun transchegaraviy to‘lovlar bo‘yicha texnik yordam (TA) ko‘rsatish bo‘yicha ko‘p yillik strategiyasi. Kriptovalyutalarning anonimligi va markazlashtirilmaganligi ularni jinoiy daromadlarni legallashtirish, terrorizmni moliyalashtirish va boshqa noqonuniy harakatlar uchun jinoyatchilarga murojaat qilishga majbur qildi. Aksariyat yurisdiktsiyalarda pul yuvishga qarshi kurash (AML) va terrorizmni

moliyalashtirishga qarshi kurash (CFT) to‘g‘risidagi qonunlar va qoidalar moliya institutlaridan keng qamrovli bajarilishini talab qiladi.

1.4 Moliyaviy elektron jinoyatlar uchun institutsional tartibga solish standartlari elektron moliyaviy jinoyatlarning turli shakllarini oldini olish, aniqlash va ularga javob berishga yordam berish uchun ishlab chiqilgan. Payment Card Industry Data Security Standard (PCI DSS) kredit kartalari bilan operatsiyalarni amalga oshiradigan tashkilotlarga qo‘yiladigan talablarni, jumladan, karta egasi ma’lumotlarini ruxsatsiz kirish, foydalanish yoki oshkor qilishdan himoya qilish choralarini belgilaydi. ISO/IEC 27001 standarti tashkilotlarga axborot xavfsizligini boshqarish tizimini yaratish va ularning hajmi va ehtiyojlariga moslashtirilgan risklarni boshqarish jarayonini qo‘llash va ushbu omillar rivojlanishi bilan zarur bo‘lganda uni kengaytirish imkonini beradi. Moliyaviy sanoatni tartibga solish organi (FINRA) moliyaviy firmalar uchun mijozlar ma’lumotlarini himoya qilish va kiberjinoyatlarning oldini olish, shu jumladan kiberxavfsizlik xavfini baholash, hodisalarga javob berish rejalari va ma’lumotlarni shifrlash bilan bog‘liq choralarni ta’minlash uchun qoidalar va ko‘rsatmalar beradi.

1.5 Kiberxavflarni boshqarish raqamli aktivlarni himoya qilish uchun potentsial kiber tahdidni aniqlash, tahlil qilish va hal qilish jarayonini anglatadi. Turli xalqaro tashkilotlar va hukumatlar qonunlar va siyosat tashabbuslarini ishlab chiqdilar. SEPA (yagona yevro to‘lov maydoni) va tezkor (banklararo moliyaviy telekommunikatsiyalarning Global hamjamiyati) ular kiber tahdidlardan himoya qilish va moliyaviy xabarlar va o‘tkazmalarning yaxlitligini ta’minlash uchun xavfsizlik protokollari, ma’lumotlarni shifrlash va autentifikatsiya qilish choralarini amalga oshirish orqali xalqaro moliyaviy operatsiyalarni xavfsiz va samarali o‘tkazishga hissa qo‘shadilar. Hamdo‘stlik kiberjinoyatchilik tashabbusi (CCI) kiberxavfsizlik imkoniyatlarini mustahkamlash va Hamdo‘stlikka a’zo davlatlar o‘rtasida kiberjinoyatchilikka qarshi kurashda hamkorlikni rivojlantirish, jumladan, namunaviy qonunlar, salohiyatni oshirish dasturlari va axborot almashish mexanizmlarini ishlab chiqishga qaratilgan.

1.6 Jinoyatni tergov qilish jinoiy faoliyat haqidagi haqiqatni ochishga qaratilgan tizimli va uslubiy jarayondir. U jinoyatni tan olishdan boshlanadi, so‘ngra dalillarni sinchkovlik bilan to‘plash va hujjatlashtirish bilan davom etadi. Tergov usullari korporativ tekshiruvlarni o‘tkazish uchun muhim amaliyot bo‘lib, asosli xulosalarga kelish uchun dalillarni to‘plash va tahlil qilish uchun juda muhimdir. Umumjahon yurisdiktsiyani o‘z ichiga olgan ichki qonunlar milliy sudlarga jinoyat qayerda sodir etilganligidan, jinoyatchilar yoki jabrlanuvchilarning millatidan qat‘i nazar, urush jinoyatlari, insoniyatga qarshi jinoyatlar, genotsid va qiynoqlar kabi xalqaro ahamiyatga molik jinoyatlarni hal qilish imkonini beradi. Xalqaro jinoiy sud (XJS) milliy adliya tizimlarini “bir-birini to‘ldirish” tamoyili asosida takomillashtirishda muhim rol o‘ynaydi. Ushbu tamoyil, xususan, "ijobiy bir-birini to‘ldirish" orqali, ICC prokuraturasini dastlabki tekshiruvlar paytida haqiqiy milliy sud jarayonlarini rag‘batlantirish uchun o‘z vositalaridan foydalanishni o‘z ichiga oladi.

1.7 Tegishli qonun jarayoni barcha sud ishlarini adolatli va xolis bo‘lishga majbur qiladigan asosiy huquqiy prinsipdir. Bu qonun bo‘yicha odamlarga teng

munosabatda bo‘lishni, adolatli sud qilish huquqini va tinglash imkoniyatini kafolatlaydigan konstitutsiyaviy kafolatdir. Tegishli jarayon konsepsiyasi Magna Carta, inson huquqlari Umumjahon Deklaratsiyasi, fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro Pakt (ICCPR), inson huquqlari bo‘yicha Yevropa Konvensiyasining 6-moddasi va inson va xalqlar huquqlari bo‘yicha Afrika Xartiyasi kabi turli xil huquqiy hujjatlarda mustahkamlangan. Pokiston Konstitutsiyasi 10A-moddasi inson huquqlarini himoya qilishni mustahkamlab, adolatli sudlov va tegishli jarayon huquqini kafolatlaydi. Xuddi shunday, O‘zbekiston Respublikasi Konstitutsiyasida ham insonning daxlsiz huquq va erkinliklari qonun bilan himoyalanganligi qat‘iy belgilab qo‘yilgan. VII bobda bir qancha asosiy huquqlar, jumladan, yashash, sha’n va qadr-qimmatga bo‘lgan huquqlar, o‘lim jazosi va har qanday g‘ayriinsoniy munosabatni aniq ta’qiqlab qo‘yilgan.

1.8 Milliy me‘yoriy hujjatlarni xalqaro sa’y-harakatlar bilan uyg‘unlashtirish konsepsiyasi xalqaro hamkorlik tamoyillariga asoslanadi. Hamkorlik va uyg‘unlikni rivojlantirish uchun bir nechta xalqaro tashkilotlar va tuzilmalar yaratilgan, masalan, UNODC ning Kiberjinoyatchilik bo‘yicha Global dasturi texnik yordam va salohiyatni oshirishni ta’minlaydi, Yevropa Kengashining 60 dan ortiq mamlakatlar tomonidan ratifikatsiya qilingan Kiberjinoyatlar bo‘yicha Budapesht konventsiyasi asos bo‘lib xizmat qiladi. kiberjinoyatchilikka qarshi milliy qonunlarni uyg‘unlashtirgan FATF jinoiy faoliyatdan olingan daromadlarni legallashtirish, terrorizmni moliyalashtirish va boshqa tahdidlarga qarshi kurashish bo‘yicha standartlarni belgilovchi va huquqiy, tartibga solish va operativ choralarni samarali amalga oshirishga yordam beruvchi hukumatlararo tashkilotdir. Europolning Yevropa kiberjinoyatchilik markazi (EC3) Yevropa Ittifoqiga a’zo davlatlarni kiberjinoyatlarga qarshi kurashish bo‘yicha operativ va tahliliy salohiyatni rivojlantirishda qo‘llab-quvvatlaydi. INTERPOLning Kiberfusion markazi INTERPOLga a’zo mamlakatlarga kiberjinoyat tahdidlarini bartaraf etishda operativ yordam va ekspertiza bilan ta’minlaydi.

1.9 Moliyaviy elektron jinoyatlarga qarshi kurashda ko‘p tomonlama sheriklik tushunchasi jamoaviy harakat va hamkorlikda boshqaruv nazariyasidan kelib chiqqan. Bu nazariya shuni ko‘rsatadiki, murakkab ijtimoiy muammolar ko‘pincha turli manfaatlar va resurslarga ega bo‘lgan bir nechta sub‘ektlarning ishtiroki va muvofiqlashtirilishini talab qiladi. Bular Milliy kiber-kriminalistika va trening alyansi (NCFTA), moliyaviy xizmatlar ma’lumotlarini almashish va tahlil qilish markazi (FS-ISAC), kiberjinoyatlarni qo‘llab-quvvatlash tarmog‘i (CSN), milliy kiber tergov qo‘shma ishchi guruhi (NCIJTF) kabi bir nechta tashabbuslardir. moliyaviy elektron jinoyatlarga qarshi kurash sohalari. Sektorlar bo‘ylab hamkorlikni mustahkamlash, tahdidlar haqida ma’lumot, murosa ko‘rsatkichlari va ilg‘or tajribalarni almashish uchun xavfsiz va samarali mexanizmlarni yaratish. Huquqni muhofaza qilish organlari, nazorat qiluvchi organlar va xususiy sektor sub‘ektlari o‘rtasidagi hamkorlikni kuchaytirishni rag‘batlantirish. Fuqarolik jamiyati tashkilotlarini, jumladan, notijorat, ilmiy muassasalar va iste‘molchilar huquqlarini himoya qilish guruhlarini jalb qilish.

1.10 Sug‘urta va kompensatsiya mexanizmlari xavflarni kamaytirish va moliyaviy himoya va tuzatishni ta’minlashga qaratilgan. Kiberxavfsizlik sug‘urtasi - bu biznes va jismoniy shaxslarni kiberjinoyatlarning moliyaviy oqibatlaridan himoya qilish uchun mo‘ljallangan sug‘urta polisi turi. Bu tergov, yuridik to‘lovlar, mijozlarni xabardor qilish, kredit monitoringi va ma’lumotlarni tiklash bilan bog‘liq xarajatlarni qoplashga yordam beradigan yangi kontseptsiya. Jahon kibersug‘urta bozori hajmi 2023-yilda 16,66 milliard AQSH dollarini tashkil etdi. Bozor 2024-yilda 20,88 milliard dollardan o‘sishi prognoz qilinmoqda. AQShning ayrim shtatlarida xarajatlarni qoplash uchun zo‘ravonlik jinoyatlari qurbonlariga moliyaviy yordam ko‘rsatuvchi jabrlanuvchilarga tovon to‘lash dasturlari mavjud. Sug‘urta va kompensatsiya mexanizmlari xatarlarni boshqarish strategiyasining muhim tarkibiy qismi bo‘lib, tashkilotlar va shaxslarga kiberjinoyatlar bilan bog‘liq moliyaviy risklarni o‘tkazish yoki yumshatishda yordam beradi.

II. Qonun hujjatlarini takomillashtirish bo‘yicha taklif va tavsiyalar

2.1 Qonun chiqaruvchi organlar transchegaraviy elektron jinoyatlar uchun jinoiy va ma’muriy kodekslarda aniq ta’riflar va jazolarni belgilashlari kerak. Bu samarali sud jarayonlarini osonlashtiradi va moliyaviy kiber tahdidlarga qarshi samarali to‘sqinlik qiladi. Kriptovalyuta tarqalishi sharoitida pul yuvish xavfini cheklash uchun raqamli tokenlarni tartibga solish bo‘yicha tuzatishlar ham kiritilishi kerak.

2.2 To‘lov tizimlarini tartibga soluvchi me’yoriy hujjatlar, xususan, “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi qonunning 21-moddasi, kibertahdidlar bo‘yicha davlat-xususiy axborot almashishni rag‘batlantiruvchi qo‘shimcha qoidalar bilan mustahkamlanishi kerak. Bu bir nechta chegaralarni qamrab olgan moliyaviy tarmoqlarga qilingan hujumlarga qarshi choralar ko‘rish imkonini beradi. Markaziy bank bunday hamkorlikni ta’minlovchi sanoat forumlarini tashkil qilishi mumkin.

2.3 “Kiberxavfsizlik to‘g‘risida”gi qonun kabi kiberxavfsizlik qonunchiligi huquqni muhofaza qilish organlari uchun kengaytirilgan raqamli sud ekspertizasi va tahdidlarni razvedka dasturlarini o‘z ichiga olishi kerak. Ilg‘or ma’lumotlarni yig‘ish vositalari va ofitserlar uchun mobil qurilmalar sud-tibbiyot ekspertizasi, tarmoqni tekshirish metodologiyasi va ma’lumotlar buzilishini bartaraf etish bo‘yicha maxsus treninglar murakkab transmilliy kiberguruhlarga qarshi javob berish imkoniyatlarini sezilarli darajada oshiradi.

2.4 “Tezkor-qidiruv faoliyati to‘g‘risida”gi qonunning qayta ko‘rib chiqilishi INTERPOL protokollari asosida kiberjinoyatlar bo‘yicha xalqaro tergov ishlarini yanada yumshoq muvofiqlashtirish imkonini berishi kerak. Bu raqamli dalillarni to‘plash/o‘tkazish bo‘yicha transchegaraviy hamkorlik tartiblarini va jinoiy surishtiruvlarga to‘sqinlik qiluvchi mahalliy ma’lumotlar maxfiyligi qoidalarini bekor qilish qoidalarini talab qiladi.

2.5 “Shaxsiy ma’lumotlar to‘g‘risida”gi qonunning qo‘llanilishi xalqaro konventsiyaning kiberjinoyat qonunchiligi to‘g‘risidagi Budapesht konventsiyasi kabi xorijiy yordam so‘rovlarini osonlashtiradigan tegishli qoidalarini o‘z ichiga olgan holda baholanishi kerak. Global me‘yorlar bilan qo‘shimcha ma’lumotlarni uyg‘unlashtirish mahalliy himoyani saqlab qolgan holda dalillarni uzluksiz almashish imkonini beradi.

2.6 Hukm berish bo‘yicha ko‘rsatmalar, hodisalarning pul bo‘lmagan oqibatlarini hisobga olgan holda, faqat moliyaviy yo‘qotishlarga tayanmasdan, elektron jinoyatlarning miqyosi va murakkabligiga qarab jazolarni ajratib ko‘rsatishi kerak. Saqlash shartlari transmilliy muvofiqlashtirish, texnik murakkablik, infratuzilmaning buzilishi va o‘zaro bog‘liq tahdidlardan kelib chiqadigan iqtisodiy yuqumli xavflarni hisobga olishi kerak.

2.7 Qonun chiqaruvchilar mahalliy foydalanuvchi ma’lumotlari yoki texnologiya aktivlarini saqlaydigan xalqaro firmalarga standartlashtirilgan kiberbardoshlilik bo‘yicha majburiyatlarga rioya qilishni talab qiluvchi qoidalarni ishlab chiqishlari kerak. Ehtiyotsizlik firibgarlik, pul yuvish yoki terrorizmga olib keladigan beparvolik uchun korporativ beparvolikka o‘xshash jazolarni o‘z ichiga olishi kerak.

2.8 Qimmatli qog‘ozlar depozitariylari, to‘lov tizimlari yoki kredit reyting agentliklari kabi tizimli ahamiyatga ega bo‘lgan institutlarning taqlid qilingan inqiroz sharoitida kiber-tayyorligini tekshirish uchun qonunlar muntazam stress-testlarni talab qilishi kerak. Kamchiliklar qonunchilik va nazorat aralashuvi kabi ehtiyotkorona nazoratni talab qilishi kerak. Hukumatlar ma’lumot almashish bo‘yicha ko‘p tomonlama bitimlar tuzishi mumkin, bu esa mamlakatlarga moliyaviy manbalardan foydalanish imkoniyatini beradi.

2.9 Xalqaro to‘lovlarni solishtirish va ma’lumotlarni uzatish bo‘yicha muvofiqlik yuklarini engillashtirishga qaratilgan qoidalar iste’molchilar va to‘lov protsessorlari uchun foydali bo‘ladi. Tranzaksiya formatlarini, valyuta konvertatsiyasini oshkor qilish normalarini, to‘lovlarni, nizolarni hal qilish muddatlarini va ma’lumotlarni o‘chirish protokollarini xalqaro miqyosda standartlashtirish davlat-xususiy hamkorlikni talab qiladi.

2.10 Moliyaviy institutlarga yig‘imlar orqali moliyalashtiriladigan kompensatsiya fondlarini halokatli ma’lumotlarning buzilishidan ko‘rgan yo‘qotishlarni qoplashni talab qiluvchi qonunlar xususiy sug‘urtani yaxshilash sifatida o‘rganishga loyiqdir. Regulyatorlar tomonidan nazorat qilinadigan bunday jamlangan resurslar shikastlangan iste‘molchilar uchun travma bo‘yicha maslahat, kredit monitoringi yoki shaxsni o‘g‘irlashni bartaraf etishni moliyalashtirishi mumkin.

2.11 Kimyoviy qurollarni taqiqlash kabi bank tizimlariga qarshi davlat tomonidan qo‘llab-quvvatlanadigan hujumlarga qarshi kurash bo‘yicha global kelishuvlar diplomatik forumlarda amalga oshirilishi kerak. Ular butun dunyo bo‘ylab moliyaviy barqarorlikka qaratilgan proksi-kiber militsiyalarni qo‘llab-quvvatlovchi rejimlarga qarshi jamoaviy sanktsiyalarni qo‘llash imkonini beradi. Moliyaviy infratuzilmani urush uchun taqiqlangan deb e‘lon qilgan ramziy konsensus ham taraqqiyot bo‘ladi.

2.12 Huquqiy an‘analar va yurisdiksiyamurakkabliklaridagi tub farqlardan tortib, maxfiylik, ma’lumotlar va kuzatuv atrofidagi ziddiyatli me‘yorlargacha bo‘lgan xalqaro huquqbuzarliklar bo‘yicha qonunlarni uyg‘unlashtirishdagi muammolar muhim ahamiyatga ega. Rivojlanayotgan iqtisodlar qonunchilik islohotlarini amalga oshirishda texnik va huquqiy ekspertiza yo‘qligi sababli qo‘shimcha resurs to‘siqlariga duch kelmoqda. Biroq, bu to‘siqlarni bartaraf etishga qaratilgan tashabbuslar mavjud. 2015-yilda tashkil etilgan va BMT Bosh Assambleyasi tomonidan ma’qullangan Birlashgan Millatlar Tashkilotining Hukumat ekspertlar

guruhi (UNGGE) normalari kibermakonda davlatning masʻuliyatli xatti-harakati uchun asos yaratadi. Bundan tashqari, Buyuk Britaniyaning CyberFirst maktab dasturlarida koʻrsatilganidek, kiberxavfsizlik va onlayn xavfsizlikni asosiy ta’lim oʻquv dasturlariga kiritish xabardorlikni oshirish va boshlangʻich salohiyatni oshirishga yordam beradi.

2.13 Yana bir muhim sa’y-harakatlar axborot xavfsizligini boshqarish tizimlari (ISMS) uchun ISO/IEC 27001 kabi global miqyosda tan olingan standartlarni qabul qilishdir. Ushbu standart hajmi yoki sektoridan qatʻi nazar, tashkilotning AXBT tizimini yaratish, joriy etish, qoʻllab-quvvatlash va doimiy ravishda takomillashtirishga tizimli yondashuvni ta’minlaydi. Ixtiyoriy boʻlsa-da, uning keng qoʻllanilishi amaliyotlarni uygʻunlashtirishga yordam beradi va kiberxavfsizlik va kiberjinoyatlarga qarshi kurashda transchegaraviy hamkorlikni osonlashtiradi. Oxir oqibat, xalqaro meʻyorlar, ta’lim tashabbuslari va eʻtirof etilgan standartlarga rioya qilishni birlashtirgan koʻp qirrali yondashuv tobora oʻzaro bogʻliq boʻlgan dunyoda kiberjinoyat qonunchiligi va ijro etilishining murakkab manzarasini boshqarish uchun juda muhimdir.

III. Amaliyotni takomillashtirish boʻyicha ilmiy sharhlar va tavsiyalar

3.1 Xalqaro jinoiy sudning yurisdiktsiyasi kiberjinoyatlarni qamrab olish uchun kengaytirilishi kerak, bu huquqbuzarliklar global xavfsizlik va shaxsiy daxlsizlikka olib kelishi mumkin boʻlgan ogʻir va keng qamrovli oqibatlarni eʻtirof etadi. Ushbu qoʻshilish, geografik joylashuvidan qatʻi nazar, kiberjinoyatlar aybdorlariga nisbatan izchil qonuniy choralar koʻrishni ta’minlab, yanada mustahkam va muvofiqlashtirilgan xalqaro javob choralarini koʻrish imkonini beradi. Ushbu jinoyatlarning transmilliy mohiyatini koʻrib chiqish orqali ICC butun dunyo boʻylab raqamli tizimlarning barqarorligi va yaxlitligiga tahdid soladigan kiber-bogʻliq jinoyatlarning oldini olishi va jinoiy javobgarlikka tortishi mumkin.

3.2 Toʻlov kartalari sanoati ma’lumotlar xavfsizligi standarti (PCI-DSS) kiberjinoyatlarni tekshirish samaradorligini oshirish uchun keng qamrovli huquqiy choralar bilan toʻldirilishi kerak. Kuchli huquqiy protokollarni integratsiyalashgan holda, PCI-DSS barcha sohalar boʻylab nozik ma’lumotlarni himoya qila oladi va barcha tomonlar qatʻiy xavfsizlik standartlariga rioya qilishlarini ta’minlaydi. Ushbu integratsiya huquqni muhofaza qilish organlariga puxta tergov oʻtkazish, dalillar toʻplash va toʻlov tizimlari va moliyaviy ma’lumotlarning yaxlitligini buzgan kiberjinoyatchilarni jinoiy javobgarlikka tortish uchun zarur huquqiy asoslar bilan ta’minlaydi.

3.3 Birlashgan Millatlar Tashkilotining kiberjinoyatchilikka oid konventsiyasi barcha mamlakatlarda huquqiy bazalarni uygʻunlashtirishga koʻmaklashish uchun kiberjinoyat nima ekanligini aniq va keng qamrovli ta’riflashi kerak. Ushbu muhim qadam barcha mamlakatlarda ushbu huquqbuzarliklarning koʻlami va tabiati haqida yagona tushunchaga ega boʻlishini ta’minlaydi, ularni tasniflash va hal qilishda noaniqlik va nomuvofiqliklarni bartaraf etadi. Keng qamrovli ta’rif samarali xalqaro hamkorlik va kiberjinoyatlar keltirib chiqaradigan global tahdidga qarshi kurashda hamkorlik uchun asos yaratadi.

3.4 Kiberjinoyatlarning global tabiatini hisobga olgan holda, Birlashgan Millatlar Tashkilotining taklif etilayotgan konventsiyasi ushbu huquqbuzarliklarni tergov

qilish boʻyicha yagona koʻrsatmalarni oʻz ichiga olishi kerak. Ushbu koʻrsatmalar uzluksiz xalqaro hamkorlikni osonlashtiradi, tekshiruvlar samarali, adolatli va raqamli dalillar va transchegaraviy yurisdiksiya muammolari bilan bogʻliq noyob muammolarni hisobga olgan holda oʻtkazilishini ta’minlaydi. Yagona koʻrsatmalar, shuningdek, ilgʻor tajriba almashishga yordam beradi va butun dunyo boʻylab kiberjinoyatlarni tekshirishning umumiy sifatini oshiradi.

3.5 Tekshiruv jarayonida izchillik va puxtalikni ta’minlash uchun Birlashgan Millatlar Tashkilotining taklif etilayotgan konventsiyasi barcha a’zo davlatlar amal qilishi kerak boʻlgan kiberjinoyatlar uchun standart tergov protokolini yaratishi kerak. Ushbu standartlashtirilgan yondashuv oʻrnatilgan ilgʻor tajribalarga rioya qilgan holda va raqamli sud ekspertizasining eng soʻnggi texnologik yutuqlaridan foydalangan holda tergovning yuqori darajadagi qatʻiylik bilan oʻtkazilishini ta’minlaydi. Yagona metodologiyani qoʻllab-quvvatlash orqali standart protokol kiberjinoyatlarni boshqarishning umumiy sifatini yaxshilaydi, bu esa yanada samarali oldini olish, aniqlash va jinoiy javobgarlikka tortish imkonini beradi.

3.6 Barcha a’zo davlatlar kiberjinoyatlarni tergov qilish chogʻida Birlashgan Millatlar Tashkilotining taklif qilingan konventsiyasida koʻrsatilgan koʻrsatmalarga rioya qilishlari muhim. Doimiy rioya qilish xalqaro huquqni muhofaza qilish organlarining hamkorligini kuchaytirib, razvedka, dalillar va resurslarni chegaralar orqali almashish imkonini beradi. Ushbu muvofiqlashtirilgan yondashuv kiberjinoyatlarni hal qilish boʻyicha sa’y-harakatlar samaradorligini oshiradi, ushbu huquqbuzarliklarning transmilliy xususiyatini koʻrib chiqadi va yurisdiktsiyadagi boʻshliqlar yoki qonunchilik bazasidagi nomuvofiqliklardan foydalanishga intilayotgan aybdorlarning oldini oladi.

3.7 Kiberjinoyatlarga qarshi kurashda oʻz imkoniyatlarini kuchaytirish uchun a’zo davlatlar oʻz mamlakatlarida ushbu jinoyatlar ustidan keng qamrovli yurisdiktsiyaga ega boʻlgan ixtisoslashgan tergov idoralarini yaratishlari kerak. Ushbu maxsus agentliklar kiber jinoyatlarning nüansları va murakkabliklariga eʻtibor qaratadilar, kiberjinoyatlarning oldini olish va ta’qib qilishda yanada maqsadli va samarali yondashuvni ta’minlash uchun ekspertiza oʻtkazadilar va moslashtirilgan strategiyalarni qabul qiladilar. Resurs va sa’y-harakatlarni jamlash orqali ushbu ixtisoslashgan agentliklar rivojlanayotgan kiber tahdidlardan oldinda qolish qobiliyatini oshiradi.

3.8 Kiberjinoyatlar keltirib chiqaradigan noyob muammolarni hal qilish uchun barcha a’zo mamlakatlar ushbu ishlarni koʻrib chiqishga bagʻishlangan maxsus sudlarni tashkil etishlari kerak. Onlayn rejimda ishlaydigan yoki ilgʻor raqamli texnologiyalardan foydalanadigan ushbu ixtisoslashtirilgan sudlar kiberjinoyatlarning murakkab texnik jihatlarini hal qilish uchun jihozlangan boʻlar edi. Raqamli landshaftni va kiber bilan bogʻliq huquqbuzarliklarning nuanslarini chuqur anglagan holda, ushbu sudlar kiberjinoyatlar boʻyicha ishlarni adolatli va samarali koʻrib chiqishni ta’minlaydigan soddalashtirilgan va texnologik jihatdan moslashtirilgan sud jarayonini taklif qiladi.

3.9 Birlashgan Millatlar Tashkiloti rivojlanayotgan mamlakatlarga kiberjinoyatlarga qarshi samarali kurashish qobiliyatini oshirish uchun resurslar, oʻqitish va salohiyatni oshirish tashabbuslarini taqdim etish orqali yordam berishi

kerak. Ushbu mamlakatlarda tajriba va infratuzilmani oshirish kibertahdidlarga qarshi mustahkam global mudofaani yaratish va kiberxavfsizlik resurslaridan adolatli foydalanishni ta’minlash uchun juda muhimdir. Birlashgan Millatlar Tashkiloti kiberbardoshli tizimlarni rivojlantirish uchun texnik yordam, bilimlarni uzatish va qo‘llab-quvvatlashni taklif qilish orqali ushbu mamlakatlarga kiberjinoyatlarning ortib borayotgan muammosiga qarshi kurashish bo‘yicha global sayi-harakatlarda faol ishtirok etish imkoniyatini berishi mumkin.

SCIENTIFIC COUNCIL ON AWARDING SCIENTIFIC DEGREES PhD.07/03.06. 2023.Yu.22.04 AT THE TASHKENT STATE UNIVERSITY OF LAW

TASHKENT STATE UNIVERSITY OF LAW

NAEEM ALLAHRAKHA

PREVENTING CROSS-BORDER E-CRIMES FOR FINANCIAL STABILITY IN THE DIGITAL ECONOMY

12.00.10 – International law

ABSTRACT
of doctoral (Doctor of Philosophy) dissertation on legal sciences

Tashkent – 2024

The theme of the dissertation of the Doctor of Philosophy (PhD) is registered by the Supreme Attestation Commission under the Cabinet of Ministers of the Republic of Uzbekistan with number № B2024.2.PhD/Yu1491

The doctoral dissertation is prepared at the Tashkent State University of Law.

The abstract of the dissertation is posted in three languages (Uzbek, English and Russian (summary)) on the website of Scientific council (www.tsul.uz) and Information educational portal «Ziyonet» (www.ziyonet.uz).

Scientific supervisor:	**Rustambekov Islambek Rustambekovich** Doctor of Science in Law, Professor
Official opponents:	**Umarkhanova Dildora Sharipkhanovna,** Doctor of Sciences (DSc) in Law, Professor
	Tillaboyev Mirzatilla Alisherovich, Doctor of Philosophy (PhD) in Law, Professor
The leading organization:	**The Law Enforcement Academy of the Republic of Uzbekistan**

The defense of the dissertation will be held on 5 th of december 2024 at 10:00 at the session of the Scientific Council under the Scientific Council PhD. 07/03.06. 2023.Yu.22.04 at the Tashkent State University of Law. (Address: 100047, Sayilgokh street, 35 Tashkent city. Phone: (99871) 233-66-36; fax: (998971) 233-37-48; e-mail: info@tsul.uz).

The doctoral dissertation is available at the Information-Resource Center of Tashkent State University of Law (registered under No. 1298), (Address: 100047, Tashkent city, A. Timur Street, 13. Phone: (99871) 233-66-36).

Abstract of the dissertation submitted on 4th November 2024.

(Registry protocol №. 11 from 4th November 2024.

S.S. Gulyamov

Chairman of Scientific Council for awarding scientific degrees, Doctor of Science in Law, Professor

D.N. Maxkamov

Secretary of Scientific Council for awarding scientific degree, Doctor of Science in Law, Associate Professor

Sh.X. Fayziyev

Vice-Chairman of Scientific Council for awarding scientific degree, Doctor of Science in Law, Professor

INTRODUCTION (abstract of PhD thesis)

The actuality and relevance of the dissertation theme. The Fourth Industrial Revolution marks an era where the digital and physical manufacturing systems work together flexibly. This revolution builds upon the Third Industrial Revolution, also known as the Digital Revolution, which introduced us to computers, various electronics, and the internet.[5] It blends traditional and digital businesses through the adoption of digital technologies and processes across different industries. This revolution extends the capabilities of earlier inventions with four key disruptive technologies: connectivity, data, computational power, and cloud computing sensors, applicable throughout the value chain. Digital platforms based in the "cloud" are critical components of this digital shift. The rise of the Platform Economy has led to an increase in work moved to digital platforms, providing significant and fair income opportunities.[6]

In 2023, the worldwide market for digital transformation was estimated at $2.27 trillion. It is projected to expand from $2.71 trillion in 2024 to $12.35 trillion by 2032, growing at an annual rate of 20.9%. By 2023, there were approximately 2.64 billion online shoppers globally, making up more than 33% of the world‘s population (Statista). The rise in digitalization has also increased activities in the financial sector, which includes banks, non-bank lenders, insurance companies, securities markets, and investment funds. This sector also includes entities like clearing counterparties, payment providers, central banks, and financial regulators and supervisors. The financial systems are increasingly becoming digitalized, supporting the growth of the global digital economy. The market for global cross-border payments was valued at $181.9 trillion in 2022 and is expected to reach $356.5 trillion by 2032, with a growth rate of 7.3% annually from 2023 to 2032 (Yahoo Finance).

Financial systems are becoming heavily digitalized, enabling global digital economics. The rise of digital technology has also increased cybercrimes, which pose a threat to economic stability. Cybercrimes in the financial sector involve illegal activities aimed at monetary gains. This includes identity theft, ransomware attacks, and various forms of internet and email fraud.[7] Criminals engage in activities like stealing payment card details (carding), accessing financial accounts to make unauthorized transactions, and extortion. For example, in May 2023, the LockBit ransomware group attacked BSI, one of the largest banks in Indonesia. The bank declined to pay the ransom demand of 20 million USD, leading the attackers to release over 1.5 terabytes of confidential data online. This leaked information

[5] Raja Santhi, A., & Muthuswamy, P. (2023). Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. *International Journal of Interactive Design and Manufacturing*, *17*(3), 947–979. https://doi.org/10.1007/s12008-023-01217-8

[6] Javaid, M., Haleem, A., Singh, R. P., & Sinha, A. K. (2024). Digital economy to improve the culture of industry 4.0: A study on features, implementation and challenges. *Green Technologies and Sustainability*, *2*(2), 100083. https://doi.org/10.1016/j.grets.2024.100083

[7] Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). Rising cyber threats pose serious concerns for financial stability. *IMF Blog*. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

included the personal and financial details of approximately 15 million customers and employees.[8]

The number of ransomware attacks on financial services has surged from 34% in 2021 to 64% in 2023, with more than 20,000 cyberattacks reported over the past two decade (IMF). To combat this, robust regulatory resilience is essential to prevent such cyber incidents from causing systemic crises that could destabilize the economy by eroding public confidence or disrupting critical services. Notable regulations addressing financial data security include the Payment Card Industry Data Security Standard (PCI DSS), the EU‘s General Data Protection Regulation (GDPR), and the Payment Services Directive 2 (PSD2), which enhances competition and security in banking. Additionally, institutions using SWIFT services must comply with the SWIFT Customer Security Program (SWIFT CSP), and ISO/IEC 27001 provides a framework for managing security risks in financial information handling.

In Uzbekistan, a series of regulations have been established to ensure financial stability. These include the Law on Cybersecurity (No. ZRU-764) enacted on April 15, 2022, and the Criminal Code of Uzbekistan (No. 2012-XII) dated September 22, 1994, with its latest amendments on February 21, 2024. Similarly, the Administrative Responsibility Code of Uzbekistan (No. 2015-XII), also originating from September 22, 1994, was revised on February 29, 2024. The Law on Personal Data (No. ZRU-547) from July 2, 2019, and the Law on Bank Secrecy (No. 530-II) from August 30, 2003, were amended last on November 28, 2023, and April 11, 2022, respectively. Other critical statutes include the Law on Banks and Banking Activities (No. 216-I) from April 25, 1996, revised on February 21, 2024, the Law on Payments and Payment Systems (No. ZRU-578) from November 1, 2019, amended on February 7, 2024, and the Law on Countering the Legalization of Income from Criminal Activity (No. 660-II) from August 26, 2004, updated last on November 28, 2023. The Law on Insurance Activity (No. ZRU-730) was introduced on November 23, 2021. Additional governance includes the Presidential Decree on the Strategy for Reforming the Banking System of Uzbekistan for 2020-2025 (No. UP-5992) dated May 12, 2020, with amendments as of July 12, 2023. Furthermore, the Central Bank of Uzbekistan issued Resolution No. 3268 on June 30, 2020, to regulate information security in payment systems, and Resolution No. 3/13 on February 15, 2020, concerning electronic money regulations within the country.

The research presented in this dissertation align to the essence of the President Decree No. PP-381 (November 30, 2023) “On measures to strengthen consumer protection of digital products (services) and combat offenses committed through digital technologies” highlight that the digital sector of the economy has expanded rapidly, driven by e-commerce platforms, digital services, and financial technologies that ensure the quality and security of transactions. Concurrently, a rise in bank card theft and fraud highlights the lack of digital financial literacy among the population, inadequate training of law enforcement, and the absence of modern systems to

[8] Hasham, S., Joshi, S., & Mikkelsen, D. (2019, October). *Risk Practice: Financial crime and fraud in the age of cybersecurity*. Mc Kinsey & Company.

prevent legal violations in commercial banks, payment organizations, and among payment system operators.

The dependence of the research on the priority areas of development of science and technologies in the Republic. The Research‘s Relevance to the Republic‘s Prioritized Fields of Scientific and Technological Advancement, this research hinges on the strategic sectors identified by the Presidential Decree of the Republic of Uzbekistan (of January 15, 2024 No. UP-10), about measures for raising on qualitatively new level of research activities in the field of ensuring public safety and fight against crime.

The extent of study of the problem. Financial crime involves the use of technology to commit illegal activities. The literature review part examines the existing scholarly research and explore their finding as under. An assessment of the effectiveness of these frameworks in different jurisdictions, as well as their adaptability to the rapidly evolving nature of cyber threats, would be critical (Saeed et al., 2023). The challenges and successes of international collaborations in enhancing cyber resilience, such as the work by Fran (2022), which provides insights into the legal challenges of cross-border cybercrime investigations (Fran Casino et al., 2022). There should be a focus on the interoperability of legal systems and the potential for a unified regulatory approach that could simplify the prosecution and prevention of financial e-crimes (Spapens, Peters & Daele, 2015).

Research on the development and deployment of cybersecurity technologies, including block-chain and artificial intelligence, should be analyzed for their efficacy in preventing e-crimes (Ferrag, Maglaras, & Benbouzid, 2023).

Important references here might include works by (Bellasio et al., 2020), who discuss the role of technology in both committing and combating cybercrime, and (Lu, He, & Yan, 2022), who look at the implications of technology on financial stability. The policy initiatives of various countries and international bodies are detering financial e-crimes (McDowell & Novis, 2001).

For instance, the Financial Action Task Force (FATF) recommendations on combating money laundering and terrorist financing might be reviewed to understand their impact on curbing financial e-crimes (Schott, 2006). This would involve studying reports from international financial institutions such as the International Monetary Fund (IMF) and the World Bank, which analyze the economic implications of cyber threats on global financial systems (Gulyás & Kiss, 2023).

A review of the relevant literature of scientists of the Republic of Uzbekistan is considers of Said Gulyamov, I. Rustumbekov, Bobokulov I. I., Eshmatova Feruza Farkhodovna, Safarov Nurbek Abdivalievich, Tillabaev Mirzatillo Alisherovich, Umarkhanova D. Sh., Gafurova S. A., Tursunov Husan Mirzaevich, Shukurov Holbek Nazarovich, D. Sh. Umarkhanova, Kadirkulov A.O., V. A. Artykova, Mirzairova S. Z., A. A. Kasimova, Sh. Sh. Mirzaev, H. A. Kazakkhanov, Azimov M. M., Kakharov S. R., 2004).

Despite the extensive coverage of technological advancements and international legal frameworks in combating digital financial crime, the literature reveals several notable gaps. Key among these is the insufficient exploration of how

legal systems adapt to rapidly evolving technologies, particularly concerning the adequacy of current laws to address new forms of cybercrime. Furthermore, while the importance of international cooperation is recognized, there is a lack of detailed analysis on the effectiveness of such collaborations across different jurisdictions and their impact on financial stability. Additionally, the literature suggests a potential for unified regulatory approaches but lacks depth in discussing their feasibility and implementation, especially in a global context with diverse legal systems. These gaps highlight a critical need for comprehensive research into the dynamic interaction between technological innovations, legal adaptations, and international regulatory efforts to effectively combat e-crimes in the digital economy.

Relation of the dissertation research with the research plans of the higher educational institution where the dissertation is performed. The dissertation research on regulatory strategies for combating financial e-crimes aligns seamlessly with the research plans of Tashkent State University of Law, which is dedicated to advancing legal frameworks and ensuring financial stability in the digital age.

The aim of the research is to identify regulatory strategies for combating financial crimes and fostering stability for digital economics.

Research tasks

Analyze the digital connectivity, digital economy and the growth of transnational cyber threats

Examine the impacts of e-crimes in financial system stability and development of digital economy

Define the regulatory principles and approaches

Disclose the global institutional regulatory standards

Determine the tension in managing cyber risks in digital economy

Highlight the monitoring, investigation and prosecuting e-crimes across borders

Explain the global standards of due process and prosecutions

Harmonizing national regulations and responses

Classify the role of partnership across public, private, and civil sectors

Insuring and compensating cybercrime impacts

Develop proposal and recommendations for improving legal frameworks and enforcement practices.

The object of research is the identification and analysis of international regulatory frameworks and their efficacy in mitigating e-financial crimes to bolster the resilience of digital economies.

The subject of research is the delineation and analysis of the existing measures, identify lacunae, and evaluate the effectiveness of current strategies within the context of a rapidly evolving digital financial landscape.

Research methods of this research use qualitative research with a doctrinal approach to thoroughly review legal documents and ground theory for analyzing literature. The study‘s methodological framework incorporates a purposive sampling strategy, targeting regulatory texts and scholarly articles relevant to financial e-crimes in the digital economy. Data collection is Doctrinal Approach Analysis is

conducted through Grounded Theory interpretation to identify regulatory gaps and effective strategies.

The scientific novelty of the research incorporates the following;

Amendments have been made regarding administrative liability in the Republic of Uzbekistan‘s Code on Administrative Responsibility for illegally modifying the international mobile equipment identity code or the subscriber device identification module, violating legislation in the field of circulation of crypto assets, and conducting mining activities illegally. In particular, articles 155 (3) and 155 (a) of the Code consider these under the scope of Law No. ZRU-899 dated January 19, 2024.

The scientifically substantiated proposal of this research on ‘creating the necessary conditions for unhindered access to the global information network Internet, ensuring cybersecurity in the national Internet space, and improving citizens‘ literacy in using the Internet‘ was used in the development of paragraph 96 of the ‘Uzbekistan – 2030‘ Strategy, approved by the Decree of the President of the Republic of Uzbekistan ‘On the Strategy "Uzbekistan – 2030"‘ dated September 11, 2023, No. UP-158.

The authorized state body, within its competencies, participates in international events in the field of cybersecurity of critical information infrastructure and exchanges information on cybersecurity threats and incidents in accordance with international treaties" was used in the development of clause 8 of the Regulation on the Procedure for Ensuring Cybersecurity of Critical Information Infrastructure Objects of the Republic of Uzbekistan, approved by the Decree of the President of the Republic of Uzbekistan "On additional measures to improve the system of ensuring cybersecurity of critical information infrastructure objects of the Republic of Uzbekistan" dated May 31, 2023, №PP-167.

The proposals of this research on the necessity to "define the concept of ‘electronic (digital) evidence‘, procedures for detecting, collecting, verifying, examining, evaluating, recording, storing electronic evidence, as well as the rights and obligations of the participants in these processes; establish a procedure for conducting searches and inspections in cyberspace without the presence of witnesses, using mandatory video recording for crimes committed using information technologies; and also set specific requirements (types of information) for data storage when storing digital fingerprints in information resources" were used in developing the implementation mechanism for item 8 of the "Roadmap" for improving the system to combat legal violations committed through digital technologies and protecting the rights of consumers of digital products (services), approved by the Decree of the President of the Republic of Uzbekistan "On measures to strengthen the protection of the rights of consumers of digital products (services) and combat legal violations committed through digital technologies" dated November 30, 2023, No. PP-381.

Practical results of the research provide a roadmap for regulatory strategies to combat e-financial crimes and enhance the resilience of digital economies.

The current definition states "cumulative offenses," which is vague. It could be more specific by listing common types of cybercrimes, "for the purpose of

occupancy by information, its changes, destruction or breaking of information systems and resources." While these are common motives, cybercrimes can also be committed for financial gain, espionage, or other malicious purposes. Many cybercrimes have a transnational dimension, with perpetrators operating from different countries than their victims. The definition could acknowledge this aspect by stating that cybercrimes may involve offenses committed across national borders or against computer systems located in different jurisdictions. The definition could differentiate between cybercrimes that target specific individuals, organizations, or systems (e.g., advanced persistent threats, targeted phishing campaigns) and those that are more indiscriminate or opportunistic (e.g., widespread malware distribution, automated attacks). Many cybercrimes involve the use of botnets (networks of compromised devices) or hijacked computer systems to carry out attacks. The definition could include a reference to the exploitation of compromised systems or networks as part of cybercriminal activities Article 3 of the law on cybersecurity).

Establish mechanisms for cooperating with relevant authorities in other countries to introduce requirements for real-time monitoring, information-sharing and reporting of transactions by implementation of robots and secure digital identity solution, such as biometrics to enhance customer due diligence and prevent identity theft (Article 21 of the law on Payments and Payment Systems).

To Include financial data and banking information as a category of “Financial Data” that requires heightened protection (Article 25 of the law on personal data). It explicitly prohibits the processing of banking information by unauthorized third party. Introduce severe penalties and fines for unauthorized access, misuse, or unlawful dissemination of financial data and banking information (Article 33 of the law on personal data). There should be regular audits and compliance checks for financial institutions.

Incorporate provisions aligned with the FATF‘s ‘Travel Rule‘ that requires the collection and transfer of customer information during crypto-asset transactions to share relevant originator and beneficiary information from virtual asset transactions in the (President Decree dated July 3, 2018 No. RP-3832 “On measures to develop the digital economy and the sphere of crypto-assets turnover in Republic of Uzbekistan”).

Introduce a provision that requires insurance companies, across both life and general insurance sectors, to implement robust cybersecurity measures and data protection controls for their digital operations and electronic transactions. Introduce specific requirements for cross-border insurance activities to be conducted through secure electronic channels and platforms (Article 5 and 6 of the Law on Insurance Activities)

To use Open-Source Intelligence (OSINT) for the collection, analysis, and dissemination of information that is publicly available and legally accessible for the monitory and investigating the illicit financial activity especially that are organizing and conducting by non-banking channels (Article 21 of the law on Criminal Procedure Code).

To adopt ISO 20022 in the bank means embracing a new global standard that helps financial institutions and the businesses they transact with exchange

information securely and efficiently. It provides a rich, structured, and global data standard for financial information in the payments, foreign exchange (FX), trade finance, and securities markets.

To adopt the NIST Cybersecurity framework (NIST 800-53R5) that offers a comprehensive catalog of security and privacy controls. These controls are designed for information systems and organizations to safeguard their operations, assets, individuals, other organizations, and the nation from various threats and risks. These risks include hostile attacks, human errors, natural disasters, and structural vulnerabilities.

Reliability of research results is significantly enhanced by using data from international regulations and scholarly articles by reputed authors, ensuring findings are based on well-established principles and vetted information for consistent and replicable outcomes in studying dynamic digital financial threats.

Scientific and practical significance of research results. The research provides a substantial contribution to both theoretical and practical aspects of cybercrime management in the digital economy.

Theoretically, it expands the academic discourse by identifying gaps within international regulatory frameworks and emphasizing the need for a cohesive multi-jurisdictional governance approach.

Practically, it offers actionable insights for policymakers and practitioners on implementing effective policy and technological measures to combat Cybercrimes.

Implementation of research results, centered on the regulation of financial cybercrimes to bolster digital economy stability, has profound real-world applications. The results obtained based on the shown below;

Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to the Criminal, Criminal Procedure Codes of the Republic of Uzbekistan and the Code of the Republic of Uzbekistan on Administrative Liability” Adopted by the Legislative Chamber on September 19, 2023 and Approved by the Senate on November 24, 2023

a. The study has led to significant amendments to the Code of the Republic of Uzbekistan on administrative liability. Notably, Article 155. Addresses the illegal modification of the international unique identification code of a mobile device or identification module of a subscriber device.

b. The study has prompted changes and additions to the Criminal Code of the Republic of Uzbekistan, particularly focusing on cybersecurity offenses. Criminal liability is now established for actions such as extortion through the destruction, alteration, or blocking of a victim‘s information resources.

Decree of the President of the Republic of Uzbekistan, dated September 11, 2023, No. UP-158 ABOUT THE STRATEGY “UZBEKISTAN – 2030”

a. The study has contributed to the improvement of standards and control bases in the banking sector. The strategy emphasizes the introduction of internationally recognized minimum standards and requirements in banks.

b. The research findings are reflected in the strategic plan, aiming to consistent transformation and institutional reforms, creating a favorable investment and business climate.

Resolution of the President of the Republic of Uzbekistan of May 31, 2023 No. PP-167 “About additional measures for enhancement of system of ensuring cyber security of objects of critical information infrastructure of the Republic of Uzbekistan”

a. These regulations encompass a comprehensive approach, including legal, organizational, financial, and technical measures to prevent cyber-attacks, identify threats, and protect against incidents.

Approbation of research results have been shared in guest lectures at universities and national and international conferences.

Publication of research results have been published in the 2 national conference and 5 International conference. Furthermore, the research has been published in 2 monographs, 1 national journal and 19 international journals (including 4 Scopus).

Structure and volume of the dissertation consist of an introduction, three chapters, conclusion and bibliography. The volume of the research is consisted of 153 pages.

THE MAIN CONTENT OF THE DISSERTATION

In the **introductory** part of the dissertation (doctoral dissertation annotation) the relevance and necessity of the research topic, the relevance of the research to the main priorities of the development of science and technology, the degree of study of the problem, the relevance of the dissertation to the research institution, goals and objectives. object and subject, methods, scientific novelty and practical results of research, reliability, scientific and practical significance of research results, their introduction, approbation of research results, publication of results, scope and structure of the dissertation.

The first chapter of the dissertation, entitled “**Conceptualizing and optimally regulating the risks of cross-border e-crime in the digital economy**” delves into the nature and scope of cross-border e-crimes, their potential impacts, and the legal and regulatory frameworks required to combat them effectively. Drawing from the transnational policy development theory, which recognizes the influence of international agendas and non-state actors on national policies, this chapter explores the interconnectedness of economic, socio-cultural, and political transnationalism in the digital age.

The rapid growth of the digital economy, fueled by technological advancements and global connectivity, has transformed the way businesses and individuals conduct transactions across borders. However, this evolution has also given rise to a new breed of transnational cyber threats, posing significant risks to financial systems, consumer protection, and economic stability. Cross-border e-crimes, such as identity theft, phishing, ransomware attacks, and hacking, exploit vulnerabilities in digital infrastructures, transcending national boundaries and jurisdictions.

Digital economy: The broad spectrum of economic and commercial activities rooted in the utilization of digital technologies and electronic communications, including e-commerce, digital marketing, and financial technologies.

Cross-border e-crimes: Illegal activities that exploit the internet and networked computers to commit or facilitate crimes across national borders, such as identity theft, industrial espionage, and credit card fraud.

Transnational policy development: The cross-border flow of ideas, information, people, and resources, transcending traditional national boundaries and shaping policies related to human and social development.

Borderless world theory: The diminishing importance of national boundaries in an integrated global economy, facilitating the unrestricted flow of resources, capital, labor, and technology across international borders.

Risk-based and adaptable regulatory approaches: Tailoring regulations to local realities while promoting global standards, considering the diverse capacities and unique financial landscapes of different nations.

First chapter draws from various sources, including reports from organizations such as the Association of Chief Police Officers (ACPO) UK, the OECD, and the World Bank, as well as academic literature on the digital economy, cybercrime, and international cooperation frameworks. It examines the legal and regulatory challenges posed by cross-border e-crimes, the role of emerging technologies in both enabling and combating these threats, and the need for global standards and harmonization of laws.

The second chapter of the dissertation, entitled "**International legal regulations of cross-border e-crimes**" discusses the intricate realm of international legal regulations and the challenges posed by cross-border e-crimes. It examines the vital aspects of jurisdiction, investigation, prosecution, and the preservation of due process in the digital age. The chapter draws upon various legal frameworks, international treaties, and scholarly works to address the complexities arising from the borderless nature of cyberspace.

Jurisdiction: The legal authority of a state or court to govern and adjudicate cases within its territory or subject matter.

Complementarity: A principle that establishes the International Criminal Court‘s (ICC) role as complementary to national judicial systems in prosecuting international crimes (Rome Statute).

Due process: A fundamental legal principle that ensures fairness, impartiality, and the protection of individual rights in legal proceedings.

Budapest convention on cybercrime: A pioneering international treaty aimed at harmonizing national laws, fostering cooperation, and establishing legal frameworks for combating cybercrime.

Extradition: The transfer of an accused or convicted individual from one jurisdiction to another for legal proceedings or punishment.

The chapter draws upon various legal theories and principles, including the concept of state sovereignty (Jean Bodin, Thomas Hobbes), the doctrine of complementarity (Rome Statute), and the principles of due process (Magna Carta, Edward III‘s statute). It also builds upon scholarly works on cybercrime jurisdiction (Brenner, 2004; Clough, 2010) and the challenges posed by the borderless nature of the internet (Goldsmith & Wu, 2006). The chapter references international treaties and conventions, such as the Budapest Convention on Cybercrime (Council of

Europe, 2001), the United Nations Convention against Transnational Organized Crime (UNTOC), and regional agreements like the League of Arab States Convention on Combating Information Technology Offences (2010).

The regulation of online payments, data privacy, and cybercrime jurisdiction is a complex and multifaceted issue that requires a balanced approach to address the competing interests of security, innovation, and individual rights. The chapter emphasizes the need for international collaboration, the establishment of a unified legal framework, and the prioritization of robust data security measures, transparency, and user control over personal information.

The chapter also highlights the challenges faced by countries in combating cybercrimes, such as resource constraints, jurisdictional complexities, training deficits, and outdated legal frameworks. It underscores the importance of legislative reforms, including strengthening international law enforcement cooperation, investing in specialized training, and harmonizing legal frameworks to keep pace with technological advancements. Furthermore, the chapter reaffirms the significance of upholding due process, a fundamental legal principle that guarantees fairness and impartiality in legal proceedings. It recognizes the challenges posed by the increasing use of technology in law enforcement and judicial processes, necessitating clear legal frameworks and protocols to ensure the respect of privacy rights and proper procedures.

In the third chapter of the dissertation, entitled "**Governance framework for systemic resilience**" in the realm of cybersecurity. It examines the various policies, strategies, and frameworks established by governments, international organizations, and the private sector to enhance cybersecurity and address the challenges posed by cyber threats. The chapter explores three main aspects: harmonizing national regulations and responses, fostering partnerships across public, private, and civil sectors, and the role of insurance and compensation in mitigating the effects of cybercrimes.

Cybersecurity: The application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyberattacks (Uzbek law of Cybersecurity).

Confidentiality, integrity, availability, authenticity, and non-repudiation: The five fundamental principles of cybersecurity (mentioned in the text).

National cyber-security strategy: A comprehensive approach to enhance a nation‘s cyber-security, emphasizing governance, risk management, preparedness, resilience, critical infrastructure protection, capability building, legal frameworks, and international cooperation (National Cyber-security Strategy Good Practice).

Governance frameworks: Policies, strategies, and frameworks established to enhance cybersecurity and address cyber threats.

The chapter draws upon several key theoretical frameworks and literature in examining governance frameworks for systemic cyber resilience. It references the National Cyber-security Strategy Good Practice which outlines a comprehensive national approach, as well as the International Telecommunication Union‘s Guide to Developing a National Cyber-security Strategy. The Civil Society Guide: UNCAC and the Private Sector by UNCAC emphasizes the role of civil society in

engaging the private sector on anti-corruption efforts. The Guide to Good Governance in Cyber-security highlights applying security sector governance principles to cyberspace. The UK government‘s Civil Society Strategy provides a model for collaborating with civil society organizations. Microsoft‘s whitepaper advocates for principled national cyber strategies.

The chapter concludes that securing the digital world requires a coordinated approach from governments, international organizations, and industry across various sectors. It emphasizes the importance of cyber-security principles, governance frameworks, risk management, preparedness, resilience, and legal frameworks. The chapter also highlights the role of international organizations in fostering global cooperation, providing technical assistance, and developing policies to enhance cyber-security resilience.

The chapter underscores the importance of partnerships across public, private, and civil sectors in combating e-crimes, as well as the role of cyber insurance in mitigating the financial impacts of cybercrimes. The chapter acknowledges the challenges posed by disparate national standards, legal traditions, jurisdictional complexities, and resource barriers in developing economies. It also recognizes the need to address the widening legislative gaps due to rapid technological shifts in fields like social media, cryptocurrency, and the Internet of Things (IoT).

CONCLUSION

The digital revolution has transformed economies and societies globally, ushering in an era of unprecedented connectivity, efficiency, and innovation. This rapid digitization has also opened the doors to complex transnational cyber threats that exploit the vulnerabilities of our interconnected world. Digital technologies proliferate across critical infrastructure, cyber risks have evolved from isolated events into systematic threats with dire implications for national security, economic stability, and public safety.

I. Scientific and theoretical conclusion

1.1. The digital economy is an economic system that is primarily driven by digital connectivity refers to the ability to access and exchange information through digital technologies, such as the internet, mobile networks, and other communication channels. Network Society Theory proposed by Manuel Castells posits that modern societies are structured around networks facilitated by digital communication technologies. the global internet user penetration rate reached 63.5% by the end of 2022, with more than 5 billion people using the internet worldwide with estimates ranging from 4.5% to 15.5% of global GDP, according to various reports. Transnational cyber threats are malicious cyber activities that transcend national borders and can originate from anywhere in the world. The 2022 SonicWall Cyber Threat Report revealed a 105% increase in ransomware attacks globally in 2021, The Center for Strategic and International Studies (CSIS) estimated that the global cost of cybercrime reached $945 billion in 2020.

1.2. In the Uzbek law of cybersecurity; cybercrime - cumulative offenses, performed in cyberspace with use of the software and technical means, for the

purpose of occupancy by information, its changes, destruction or breaking of information systems and resources. Electronic crime (e-crime) means Identity theft, industrial espionage, credit card fraud, phishing, ransom exploitation. the Home Office of UK and the Serious and Organized Crime Agency (SOCA) led Cyber Threat Reduction Board categorize e-crime into three distinct types: pure online crimes targeting digital systems, traditional crimes amplified by the internet, and internet-facilitated conventional crimes. Cybercrimes can cause financial losses and disrupt the operations of financial institutions, eroding consumer trust and posing systemic risks. These crimes also hinder the growth of digital businesses by increasing costs and creating legal and regulatory challenges.

1.3. The Financial Crime Compliance Principles are intended to cover certain conduct risks in general including measures to counter money laundering, terrorist financing, market abuse, corruption, fraud and the evasion of sanctions. Combating financial crimes is a critical aspect of maintain the integrity and stability of the financial system. The IMF‘s and World Bank‘s multi-year strategy to provide cross-border payments technical assistance (TA) to meet the G20 cross-border payments targets. Cryptocurrencies‘ anonymity and decentralized nature have made them appealing to criminals for money laundering, terrorism financing, and other illegal acts. Most jurisdictions have enacted Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) laws and regulations that require financial institutions to implement comprehensive.

1.4. Institutional regulatory standards for financial e-crimes are designed to help prevent, detect, and respond to various forms of electronic financial crimes. Payment Card Industry Data Security Standard (PCI DSS) establishes requirements for organizations that handle credit card transactions, including measures to protect cardholder data from unauthorized access, use, or disclosure. The ISO/IEC 27001 standard enables organizations to establish an information security management system and apply a risk management process that is adapted to their size and needs, and scale it as necessary as these factors evolve. Financial Industry Regulatory Authority (FINRA) provides rules and guidance for financial firms to ensure the protection of customer data and the prevention of cybercrime, including measures related to cybersecurity risk assessments, incident response plans, and data encryption.

1.5. Cyber risk management refer to the process of identifying, analyzing and addressing potential cyber threat to protect the digital assets. There are various international organizations and governments have developed regulations and policy initiatives. SEPA (Single Euro Payments Area) and SWIFT (Society for Worldwide Interbank Financial Telecommunication) facilitate secure and efficient cross-border financial transactions by implementing security protocols, data encryption, and authentication measures to protect against cyber threats and ensure the integrity of financial messaging and transfers. The Commonwealth Cybercrime Initiative (CCI) aims to strengthen cybersecurity capabilities and promote cooperation among Commonwealth member countries in combating cybercrime, including through the development of model laws, capacity-building programs, and information-sharing mechanisms.

1.6. The investigation of crime is a systematic and methodical process aimed at uncovering the truth about criminal activities. It begins with the recognition of a crime, followed by the meticulous collection and documentation of evidence. Investigative techniques are essential practices for conducting corporate investigations, crucial for evidence collection and analysis to reach informed conclusions. Domestic laws that incorporate universal jurisdiction allow national courts to adjudicate crimes of international concern such as war crimes, crimes against humanity, genocide, and torture, irrespective of where the crime was committed or the nationalities of the perpetrators or victims. The International Criminal Court (ICC) plays a significant role in enhancing national justice systems under the principle of "complementarity." This principle, particularly through "positive complementarity," involves the ICC Prosecutor‘s Office using its leverage during preliminary examinations to encourage genuine national proceedings.

1.7. Due process is a fundamental legal principle that mandates all legal proceedings to be fair and impartial. It is a constitutional guarantee that ensures individuals are treated equally under the law, with the right to a fair trial and an opportunity to be heard. The concept of due process has been established by various legal instruments such as the Magna Carta, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), Article 6 of the European Convention on Human Rights, and the African Charter on Human and Peoples‘ Rights. The Constitution of Pakistan enshrines the protection of individual rights through Article 10A, guaranteeing the right to a fair trial and due process. Similarly, the Constitution of the Republic of Uzbekistan firmly upholds individual rights and freedoms as inviolable and protected by law. Chapter VII delineates several fundamental rights, including the right to life, honor, and dignity, explicitly prohibiting the death penalty and any form of inhumane treatment.

1.8. The concept of harmonizing national regulations with international efforts are based on the principles of international cooperation. There are Several international organizations and frameworks have been established to promote cooperation and harmonization likes The UNODC‘s Global Program on Cybercrime provides technical assistance and capacity-building support, Council of Europe‘s Budapest Convention on Cybercrime, ratified by over 60 countries, serves as a framework for harmonizing national cybercrime laws, The FATF is an intergovernmental organization that sets standards and promotes effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, and other related threats. Europol‘s European Cybercrime Centre (EC3) supports EU member states in building operational and analytical capacities to combat cybercrime. INTERPOL‘s Cyber Fusion Centre provides operational support and expertise to INTERPOL member countries in addressing cybercrime threats.

1.9. The concept of multi-stakeholder partnerships in combating financial e-crimes is rooted in the theory of collective action and collaborative governance. This theory suggests that complex societal challenges often require the involvement and coordination of multiple actors with diverse interests and resources. These are several initiatives like National Cyber-Forensics and Training Alliance (NCFTA),

Financial Services Information Sharing and Analysis Center (FS-ISAC), Cybercrime Support Network (CSN), National Cyber Investigative Joint Task Force (NCIJTF) established to facilitate partnerships across sectors in combating financial e-crimes. To strengthen partnerships across sectors, establish secure and efficient mechanisms for sharing threat intelligence, indicators of compromise, and best practices. Encourage increased collaboration between law enforcement, regulatory agencies, and private sector entities. Engage civil society organizations, including non-profits, academic institutions, and consumer protection groups.

1.10. Insurance and compensation mechanisms aim to mitigate risks and provide financial protection and remediation. Cybersecurity insurance is a type of insurance policy designed to protect businesses and individuals from the financial consequences of cybercrimes. This is a new concept which help to cover expenses related to investigation, legal fees, customer notification, credit monitoring, and data restoration. The global cyber insurance market size was valued at USD 16.66 billion in 2023. The market is projected to grow from USD 20.88 billion in 2024. In some states of US have victim compensation programs that provide financial assistance to victims of violent crimes to cover expenses.

II. Proposal and recommendations on the improvement of legislation

2.1 Legislatures should establish clear definitions and penalties for cross-border e-crimes in criminal and administrative codes. This would facilitate efficient legal proceedings and provide effective deterrents against financial cyber threats. Amendments to regulate digital tokens should also be introduced to limit money-laundering risks amid cryptocurrency proliferation.

2.2 Regulations governing payments systems, especially article 21 of the Law "On Payments and Payment Systems", must be strengthened with additional provisions promoting public-private information sharing on cyber threats. This would enable preemptive responses against attacks on financial networks spanning multiple borders. The Central Bank could establish industry forums facilitating such collaboration.

2.3 Cybersecurity legislation, like the Law "On Cyber Security", should incorporate expanded digital forensics and threat intelligence programs for law enforcement. Advanced data mining tools and specialized training for officers in mobile device forensics, network investigation methodologies, and data breach remediation would significantly enhance response capacities against sophisticated transnational cyber groups.

2.4 Revisions to the Law "On Operational Search Activity" should enable smoother coordination in international cybercrime investigations in line with INTERPOL protocols. This would necessitate cross-border collaboration procedures for digital evidence collection/transfer and provisions to override local data privacy regulations impeding criminal inquiries.

2.5 The applicability of the Law "On Personal Data" should be evaluated to incorporate relevant provisions from international frameworks like the Budapest Convention on cybercrime legislation facilitating foreign assistance requests. Additional data harmonization with global norms would enable smooth evidence sharing while retaining local protections.

2.6 Sentencing guidelines should be established distinguishing penalties based on the scale and complexity of e-crimes rather than relying solely on financial losses, given the non-monetary consequences of incidents. Custodial terms should account for transnational coordination, technical sophistication, infrastructure disruption, and economic contagion risks from interconnected threats.

2.7 Legislators need to draft regulations mandating international firms maintaining domestic user data or technology assets to comply with standardized cyber-resilience obligations. Non-compliance should permit penalties akin to corporate malpractice for negligence enabling fraud, money laundering or terrorism.

2.8 Laws should require regular stress-testing to validate the cyber-preparedness of systemically important institutions like securities depositories, payment systems or credit rating agencies under simulated crisis conditions. Deficiencies should warrant legislative and supervisory intervention akin to prudential oversight. Governments could establish multilateral information sharing agreements that enable requesting countries access to financial.

2.9 Regulations to ease compliance burdens around international payment reconciliations and data transfers would benefit consumers and payment processors. Standardizing transaction formats, currency conversion disclosure norms, fees, dispute settlement timeframes, and data erasure protocols internationally needs public-private collaboration.

2.10 Laws mandating compensation funds financed via levies on financial institutions to offset losses from catastrophic data breaches merit exploration as enhancements to private insurance. Such pooled resources supervised by regulators could fund trauma counseling, credit monitoring or identity theft remediation for affected consumers.

2.11 Global accords around combating state-sponsored attacks against banking systems similar to chemical weapons bans should be pursued at diplomatic forums. They would enable collective sanctions against regimes fostering proxy cyber militias targeting financial stability worldwide. Even symbolic consensus declaring financial infrastructure off-limits for warfare would be progress.

2.12 The challenges in harmonizing cybercrime laws across nations are significant, ranging from fundamental differences in legal traditions and jurisdictional complexities to conflicting norms around privacy, data, and surveillance. Developing economies face additional resource barriers in implementing legislative reforms due to a lack of technical and legal expertise. However, there are initiatives aimed at addressing these hurdles. The United Nations Group of Governmental Experts (UNGGE) Norms, established in 2015 and endorsed by the UN General Assembly, provide a framework for responsible state behavior in cyberspace. Additionally, incorporating cybersecurity and online safety into mainstream educational curricula, as seen in the UK‘s CyberFirst school programs, can help raise awareness and build capacity from the ground up.

2.13 Another key effort is the adoption of globally recognized standards like ISO/IEC 27001 for information security management systems (ISMS). This standard provides a systematic approach to establishing, implementing, maintaining, and continually improving an organization‘s ISMS, regardless of size or sector.

While voluntary, its widespread adoption can help harmonize practices and facilitate cross-border cooperation in cybersecurity and combating cybercrime. Ultimately, a multi-pronged approach combining international norms, educational initiatives, and adherence to recognized standards is crucial for navigating the complex landscape of cybercrime legislation and enforcement in an increasingly interconnected world.

III. Scientific comments and recommendation on improving the practice

3.1 The International Criminal Court‘s jurisdiction should be extended to cover cybercrimes, recognizing the severe and far-reaching consequences these offenses have on global security and individual privacy. This inclusion would enable more robust and coordinated international responses, ensuring consistent legal action against perpetrators of cybercrimes, irrespective of their geographic location. By addressing the transnational nature of these crimes, the ICC can deter and prosecuting cyber-related offenses that threaten the stability and integrity of digital systems worldwide.

3.2 The Payment Card Industry Data Security Standard (PCI-DSS) must be augmented with comprehensive legal measures to enhance the effectiveness of cybercrime investigations. By integrating robust legal protocols, PCI-DSS can safeguard sensitive information across industries, ensuring that all parties adhere to stringent security standards. This integration would empower law enforcement agencies with the necessary legal framework to conduct thorough investigations, gather evidence, and prosecute cybercriminals who compromise the integrity of payment systems and financial data.

3.3 To promote harmonization of legal frameworks across nations, the United Nations‘ proposed convention on cybercrime should provide a clear and comprehensive definition of what constitutes a cybercrime. This crucial step would ensure that all countries have a unified understanding of the scope and nature of these offenses, eliminating ambiguities and inconsistencies in how they are classified and addressed. A comprehensive definition would lay the foundation for effective international cooperation and collaboration in combating the global threat posed by cybercrimes.

3.4 Given the inherently global nature of cybercrimes, the proposed United Nations convention should include uniform guidelines for conducting investigations into these offenses. These guidelines would facilitate seamless international cooperation, ensuring that investigations are conducted efficiently, fairly, and with due consideration for the unique challenges posed by digital evidence and cross-border jurisdictional issues. Uniform guidelines would also promote the exchange of best practices and enhance the overall quality of cybercrime investigations worldwide.

3.5 To promote consistency and thoroughness in the investigation process, the proposed United Nations convention needs to establish a standard investigation protocol for cybercrimes that all member countries should follow. This standardized approach would ensure that investigations are conducted with a high level of rigor, adhering to established best practices and leveraging the latest technological advancements in digital forensics. By fostering a uniform methodology, the standard

protocol would enhance the overall quality of cybercrime management, enabling more effective prevention, detection, and prosecution efforts.

3.6 It is important for all member countries to adhere to the guidelines provided by the proposed United Nations convention during their cybercrime investigations. Consistent adherence would strengthen international law enforcement collaboration, enabling the sharing of intelligence, evidence, and resources across borders. This coordinated approach would increase the effectiveness of cybercrime resolution efforts, addressing the transnational nature of these offenses and deterring perpetrators who seek to exploit jurisdictional gaps or inconsistencies in legal frameworks.

3.7 To bolster their capabilities in combating cybercrimes, member states should create specialized investigation agencies with comprehensive jurisdiction over these offenses within their respective countries. These dedicated agencies would focus on the nuances and complexities of cyber-related offenses, building expertise and adopting tailored strategies to provide a more targeted and effective approach to cybercrime prevention and prosecution. By concentrating resources and efforts, these specialized agencies would enhance their ability to stay ahead of evolving cyber threats.

3.8 To address the unique challenges posed by cybercrimes, all member countries should establish special courts dedicated to handling these cases. These specialized courts, ideally operating online or leveraging advanced digital technologies, would be equipped to address the intricate technical aspects of cybercrimes. With a deep understanding of the digital landscape and the nuances of cyber-related offenses, these courts would offer a streamlined and technologically adept judicial process, ensuring fair and efficient adjudication of cybercrime cases.

3.9 The United Nations should assist developing countries by providing resources, training, and capacity-building initiatives to bolster their ability to combat cybercrimes effectively. Enhancing expertise and infrastructure in these nations is crucial for building a robust global defense against cyber threats and ensuring equitable access to cybersecurity resources.

НАУЧНЫЙ СОВЕТ PhD.07/03.06. 2023.Yu.22.04 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ ГОСУДАРСТВЕННОМ ЮРИДИЧЕСКОМ УНИВЕРСИТЕТЕ

ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ

НАИМ АЛЛАХРАХА

ПРЕДУПРЕЖДЕНИЕ ТРАНСГРАНИЧНЫХ ЭЛЕКТРОННЫХ ПРЕСТУПЛЕНИЙ ДЛЯ ФИНАНСОВОЙ СТАБИЛЬНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

12.00.10 – Международное право

АВТОРЕФЕРАТ
докторской (доктора философии) диссертации по юридическим наукам

Ташкент – 2024

Тема диссертации доктора философских наук (PhD) зарегистрирована Высшей аттестационной комиссией при Кабинете Министров Республики Узбекистан под номером № B2024.2.PhD/Yu1491 .

Докторская диссертация подготовлена в Ташкентском государственном юридическом университете.

Автореферат диссертации размещен на трех языках (узбекском, английском и русском (аннотация)) на сайте Ученого совета (www.tsul.uz) и Информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Рустамбеков Исламбек Рустамбекович** доктор юридических наук, профессор
Официальные оппоненты:	**Умарханова Дилдора Шарипхановна,** доктор юридических наук, профессор
	Тиллабоев Мирзатилла Алишерович доктор философии (PhD) в области юридических наук, профессор
Ведущая организация:	**Академия правоохранительных органов Республики Узбекистан**

Защита диссертации состоится 5 декабря 2024 года в 10:00 на заседании Ученого совета при Ученом совете PhD.07/03.06. 2023.Ю.22.04 в Ташкентском Государственном Юридическом Университете. (Адрес: 100047, улица Сайилгоха, 35 г.Ташкент. Телефон: (99871) 233-66-36; факс: (998971) 233-37-48; электронная почта: info@tsul.uz).

Докторская диссертация размещена в Информационно-ресурсном центре Ташкентского государственного юридического университета (зарегистрирован под № 1298), (Адрес: 100047, г.Ташкент, улица А.Тимура, 13. Телефон: (99871) 233-66-36).

Автореферат диссертации представлен 4 ноября 2024.

(Протокол реестра №. 11 от 4 ноября 2024.

Гулямов С.С.
Председатель ученого совета по присуждению ученых степеней, доктор юридических наук, профессор

Д. Н. Махкамов
Секретарь ученого совета, доктор юридических наук, доцент

Ш. Х. Файзиев
Председатель научного семинара при Ученом совете, доктор юридических наук, профессор

ВВЕДЕНИЕ (Автореферат диссертации доктора философии (PhD))

Целью исследования является определение стратегий регулирования для борьбы с финансовыми преступлениями и обеспечения стабильности цифровой экономики.

Объектом исследования является выявление и анализ международной нормативно-правовой базы и ее эффективности в смягчении последствий электронных финансовых преступлений для повышения устойчивости цифровой экономики.

Научная новизна исследования заключается в следующем.

В Кодекс административной ответственности Республики Узбекистан включены предложения по применению административной ответственности за незаконное изменение международного идентификационного кода мобильных устройств или идентификационного модуля абонентского устройства, нарушение правовых документов в сфере криптоактивов. оборот и незаконное осуществление горнодобывающей деятельности;

«Необходимость создания необходимых условий для беспрепятственного доступа к глобальной информационной сети Интернет, обеспечения кибербезопасности в национальном Интернет-пространстве, а также установления в законодательстве норм по повышению грамотности граждан в использовании Интернета. обоснованный;

Введение нормы об участии компетентного государственного органа в международных мероприятиях в сфере обеспечения кибербезопасности важной информационной инфраструктуры в пределах его полномочий и обмена информацией об угрозах и инцидентах кибербезопасности в соответствии с международными соглашениями;

Предложения о необходимости определения понятия «электронные (цифровые) доказательства», порядка выявления, сбора, проверки, проверки, оценки, фиксации, хранения электронных доказательств, а также прав и обязанностей участников с использованием обязательной видеозаписи преступлений, совершенных с использованием информационных технологий в этих процессах без присутствия понятых, научно обоснованы предложения по определению порядка проведения обысков и проверок в киберпространстве, а также по определению конкретных требований (видов информации) к хранению цифровых отпечатков пальцев в информации.

Внедрение результатов исследований. Результаты исследования были использованы:

Внесены изменения ов Кодекс об административной ответственности Республики Узбекистан за незаконное изменение международного идентификационного кода мобильного оборудования или модуля идентификации абонентского устройства, нарушение законодательства в сфере обращения криптоактивов, а также незаконное ведение майнинговой деятельности. В частности, статьи 155(3) и 155(a) Кодекса относят их к сфере действия Закона № ЗРУ-899 от 19 января 2024 года.

Научно обоснованное предложение настоящего исследования о «создании необходимых условий для беспрепятственного доступа к глобальной информационной сети Интернет, обеспечения кибербезопасности в национальном интернет-пространстве, повышения грамотности граждан в использовании сети Интернет» было использовано при разработке пункта 96 настоящего исследования. Стратегии «Узбекистан – 2030», утвержденной Указом Президента Республики Узбекистан «О Стратегии «Узбекистан – 2030»» от 11 сентября 2023 года № УП-158.

Уполномоченный государственный орган в пределах своей компетенции участвует в международных мероприятиях в области кибербезопасности критической информационной инфраструктуры и осуществляет обмен информацией об угрозах и инцидентах кибербезопасности в соответствии с международными договорами» использовано при разработке пункта 8 Положения о Порядке по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан, утвержденный Указом Президента Республики Узбекистан «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» от 31 мая 2023 г., №ПП-167.

Высказаны предложения настоящего исследования о необходимости «определить понятие «электронные (цифровые) доказательства», процедуры обнаружения, сбора, проверки, исследования, оценки, регистрации, хранения электронных доказательств, а также права и обязанности участников. в этих процессах установить порядок проведения обысков и проверок в киберпространстве без присутствия понятых, с использованием обязательной видеозаписи преступлений, совершенных с использованием информационных технологий, а также установить конкретные требования (виды информации) к хранению данных при хранении цифровых отпечатков пальцев в информации; Ресурсы» использованы при разработке механизма реализации пункта 8 «Дорожной карты» по совершенствованию системы противодействия правонарушениям, совершаемым с использованием цифровых технологий, и защите прав потребителей цифровых продуктов (услуг), утвержденной Указом Президента Республики Казахстан. Республики Узбекистан «О мерах по усилению защиты прав потребителей цифровой продукции (услуг) и борьбе с правонарушениями, совершаемыми с использованием цифровых технологий» от 30 ноября 2023 года № ПП-381.

Практические результаты исследования представляют собой дорожную карту для международных стратегий регулирования по борьбе с электронными финансовыми преступлениями и повышению устойчивости цифровой экономики.

Оправданно создание механизмов сотрудничества с соответствующими органами других стран для внедрения требований по мониторингу транзакций в реальном времени, обмену информацией и отчетности путем внедрения роботов и безопасного решения для цифровой идентификации в целях

усиления должной осмотрительности клиентов и предотвращения кражи личных данных;

Финансовые данные и банковские данные должны быть включены в категорию «Финансовые данные», требующую усиленной защиты, чтобы гарантировать, что обработка банковских данных неуполномоченными третьими лицами, а также несанкционированный доступ к финансовым данным и банковским данным, введение. серьезных наказаний за неправильное использование или незаконное распространение оправдано;

Научно обосновано включение правила об обязательном сборе и передаче информации о клиентах при операциях с криптоактивами в целях обмена актуальной информацией об отправителе и получателе операций с виртуальными активами;

Оправдано введение правил, требующих от страховых компаний в секторах страхования жизни и иного, чем страхование жизни, поддерживать надежные меры кибербезопасности и средства контроля защиты данных для своих цифровых операций и электронных транзакций.

Структура и объем диссертации состоят из введения, трех глав, заключения и библиографии. Объем исследования составил 153 страницы.

Nashr etilgan asarlar ro‘yxati
List of published works
Список опубликованных работ

I.Articles

1. AllahRakha, N. (2024). Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today’s Worlds. *Lex Scientia Law Review*, *8*(1), 405-432. https://doi.org/10.15294/lslr.v8i1.2081
2. AllahRakha, N. (2024). Global Perspectives on Cybercrime Legislation. *Journal of Infrastructure, Policy and Development*, *8*(10), 6007. https://doi.org/ 10.24294/jipd.v8i10.6007
3. AllahRakha, N. (2024), Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. International Journal of Law and Policy, 2(6), 1–9. https://doi.org/10.59022/ijlp.193
4. AllahRakha, N. (2024), Sustainable ICT Infrastructure and Green Technologies in the Caribbean, *Industrial Engineering and Management Journal*, Vol.3, No.1, June 2024, pp.4-12 (ISSN 3006-810X)
5. AllahRakha, N. (2024). Demystifying the Network and Cloud Forensics‘ Legal, Ethical, and Practical Considerations. Pakistan Journal of Criminology, 16(2), 119-132. https://doi.org/10.62271/pjc.16.2.119.132
6. AllahRakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 16(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892
7. AllahRakha, N. (2024). Rethinking Digital Borders to Address Jurisdiction and Governance in the Global Digital Economy. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.124
8. AllahRakha, N. Modernizing Criminal and Evidence Laws to Facilitate Tourism in Pakistan. Available at *SSRN*: https://ssrn.com/abstract=4707544 or http://dx.doi.org/10.2139/ssrn.4707544
9. AllahRakha, N. (2023). Legal Challenges for International Fintech Startups. *International Journal of Law and Policy*, *1*(8). https://doi.org/10.59022/ijlp.148
10. AllahRakha, N. (2023). Fair Play in Sport: The Urgent Need for a World Anti-Match Fixing Agency. *Svensk Idrotts Juridisk Forening*, Nr 28, 21-36
11. Allahrakha, N. (2023). Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. *Legal Issues in the Digital Age*, *4*(2), 78-121. Retrieved from https://lida.hse.ru/article/view/17666
12. AllahRakha, N. (2023). Exploring the Role of Block-chain Technology in Strengthening International Legal Guarantees for Investment Activity. International Journal of Law and Policy, 1(3). https://doi.org/10.59022/ijlp.37 Retrieved from https://irshadjournals.com/index.php/ijlp/article/view/37
13. AllahRakha, N. (2023). The role of the international olympic committee (IOC) in sports: The integration of it in sports and the future of online gaming. *Journal of Legal, Ethical and Regulatory Issues,* 26(S4), 1-9 retrieved from

https://www.abacademies.org/articles/the-role-of-the-international-olympic-committee-ioc-in-sports-the-integration-of-it-in-sports-and-the-future-of-online-gaming-15962.html

14. AllahRakha, Naeem, Analysis of the Primary Components Contributing to the Growth of the Digital Economy. *SSRN Electronic Journal*, 2022, http://doi.org/10.2139/ssrn.4286088.

15. AllahRakha, Naeem, HOW THE EU CREATES LAWS. *Eurasian Journal of Law, Finance and Applied Sciences,* Vol 2, Issue No. 6 (2022), pp. 4-9, https://doi.org/10.5281/zenodo.6615907

16. AllahRakha, Naeem, SIGNIFICANCE OF REGULATION FOR ENHANCING ONLINE ACTIVITY. *Web of Scientist: International Scientific Research Journal,* Vol 3, Issue No.5 (2022), pp. 1854-1859, https://doi.org/10.17605/OSF.IO/CA5KZ

17. AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan "on payments and payment system". TSUL Legal Report International Electronic Scientific Journal, 5(1), 38-55. Retrieved from https://legalreport.tsul.uz/index.php/journal/article/view/176

18. AllahRakha, N. (2023). REGULATORY SANDBOXES: A GAME-CHANGER FOR NURTURING DIGITAL START-UPS AND FOSTERING INNOVATION. *Евразийский журнал права, финансов и прикладных наук*, *3*(8), 120–128. извлечено от https://in-academy.uz/index.php/EJLFAS/article/view/19825

19. AllahRakha, Naeem. "GOVERNANCE OF DIGITAL ECONOMY" Yurisprudensiya, Vol, Issue No. (2022), pp. 159-162, ISSN 2181-1938

II. Other Publications

20. AllahRakha, N. (2023). *Legal aspect of artificial intelligence in the digital economy: An overview of the EU, US, UK, Japan, China and Uzbek policy framework*. LAMBERT Academic Publishing. (Monograph)

21. AllahRakha, N. (2022). *An overview of digital economy regulation in the European Union*. Irshad Publishers. (Monograph)

22. AllahRakha, N. (2024, February 21). *Business compliance in international commercial transactions across Asia Pacific*. Towards a Cross-Border Cyber-security Legal Framework: Examining Data Protection Compliance Risks in Digital Trade across the Asia Pacific. The University of Sydney, Australia. (Conference)

23. AllahRakha, N. (2023, December 5-7). The role of digital forensics for justice in the age of emerging technology. In *ASFSFM 2023*. Naif Arab University for Security Science. (Conference)

24. AllahRakha, N. (2023, November 23-25). *Sustainable ICT infrastructure and green technologies in the Caribbean*. Paper presented at the CAS23 Conference on the Sustainability and Development Initiatives of the Caribbean, University of West Indies, Augustine, Trinidad & Tobago. (Conference)

25. AllahRakha, N. (2023, June 29-30). *Revolution in learning through digitization: How technology is changing the landscape of education*. Learning at City Conference, University of London. (Conference)

26. AllahRakha, N. (2023, May 23-26). *Artificial intelligence and sustainability*. Sustainability Science Days 2023 Conference, University of Helsinki, Finland. (Conference)

27. AllahRakha, N. (2024). *FOSTERING CYBER RESILIENCE: A MULTIDIMENSIONAL APPROACH TO SECURING THE DIGITAL ECONOMY*. Topical Issues of Legal Science and Law Enforcement Practice, Academy of Law Enforcement. Uzbekistan

28. AllahRakha, N. (2024). COMBATING CROSS-BORDER E-CRIMES: STRATEGIES FOR BOLSTERING FINANCIAL STABILITY IN THE DIGITAL ECONOMY. ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI Available Online at: https://www.uznauka.uz 7/2024

Avtoreferat TDYU Yuridik fanlar Axborotnomasi jurnali tahririyatida tahrirdan o‘tkazilib, o‘zbek, ingliz var us tillaridagi matnlar o‘zaro muvofiqlashtirildi.