RIVOJLANAYOTGAN MAMLAKATLARDA KIBERJINOYATLAR VA ULARNING HUQUQIY JIHATLARI TAHLILI

Habibjonov Izzatbek Dilshodjon o‘g‘li
Alfraganus university Ijtimoiy fanlar fakulteti
Milliy g‘oya va huquq yo‘nalishi 3 – bosqich talabasi
xabibjonovizzatbek22@gmail.com
Po‘latov Sherdor Ne‘matjonovich
Ilmiyrahbar: f.f.d, dotsent

Annotatsiya. *Ushbu tadqiqotda rivojlanayotgan mamlakatlarda kiberjinoyatlarning tarqalish holati, shakllari va ularni oldini olishga qaratilgan huquqiy mexanizmlar tahlil qilinadi. Internet texnologiyalarining jadal rivojlanishi bilan birga, kiberjinoyatlar soni ham ortib bormoqda va bu holat axborot xavfsizligiga, shaxsiy ma’lumotlarni himoya qilishga, moliyaviy tizimlar barqarorligiga jiddiy tahdid solmoqda. Tadqiqot doirasida mazkur jinoyatlarning eng ko‘p uchraydigan turlari, ularning sodir etilish sabablari, mavjud qonunchilik bazasi va xalqaro tajribalar asosida huquqiy bo‘shliqlar o‘rganiladi. Shuningdek, tadqiqot natijalari asosida rivojlanayotgan mamlakatlarda kiberjinoyatlarga qarshi kurashish samaradorligini oshirish, qonunchilikni takomillashtirish va xalqaro hamkorlikni mustahkamlash bo‘yicha taklif va tavsiyalar ishlab chiqiladi.*

Kalit so’zlar: *Kiberjinoyatlar, axborot xavfsizligi, raqamli huquqbuzarliklar, kiberhujumlar, huquqiy tartibga solish, xalqaro tajriba, internet jinoyatchiligi, raqamli qonunchilik, kiberxavfsizlik siyosati, rivojlanayotgan mamlakatlar.*

Kirish

Raqamli texnologiyalar jadal rivojlanib borayotgan hozirgi davrda kiberjinoyatlar global miqyosda dolzarb muammolardan biriga aylanmoqda. Ayniqsa, rivojlanayotgan mamlakatlarda raqamli infratuzilmaning zaifligi, kiberxavfsizlik bo‘yicha yetarli tajriba va huquqiy asoslarning yetishmasligi bu muammoni yanada keskinlashtirmoqda. Xalqaro miqyosdagi statistik ma’lumotlarga ko‘ra, 2023 yilda butun dunyo bo‘yicha kiberjinoyatlar tufayli yetkazilgan zarar 8,5 trillion AQSh dollarini tashkil etgan bo‘lsa, rivojlanayotgan mamlakatlar bu ko‘rsatkichning 28 foizini tashkil qilgan. Bu esa bu davlatlarda axborot xavfsizligini ta’minlash bo‘yicha tizimli choralar ko‘rish zaruratini ko‘rsatmoqda.

O'zbekistonda ham raqamli iqtisodiyotga o'tish jarayonida kiberxavfsizlik masalalari tobora dolzarb bo‘lib bormoqda. 2023 yilda Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi tomonidan qayd etilgan ma’lumotlarga ko‘ra,

mamlakatda 2300 dan ortiq kiberhujum holatlari aniqlangan. Ulardan ko‘pi davlat idoralari, bank tizimi va ta’lim muassasalariga qaratilgan bo‘lib, bu sohalarda axborot tizimlarining zaif himoyada ekanligini ko‘rsatadi. Shu bois, raqamli texnologiyalar bilan bog‘liq jinoyatlarga qarshi kurashishda zamonaviy yondashuv va mustahkam huquqiy mexanizmlarni ishlab chiqish zarurati ortib bormoqda.

“O’zbekiston–2030” strategiyasida raqamli iqtisodiyotni rivojlantirish, axborot texnologiyalarini keng joriy etish va raqamli xavfsizlikni ta’minlash ustuvor yo‘nalishlar sifatida belgilangan. Ushbu strategiya doirasida davlat boshqaruvi, moliya, sog‘liqni saqlash va boshqa sohalarni raqamlashtirish choralari ko‘rilayotgani sababli, axborot tizimlarini himoyalash, kiberjinoyatlarga qarshi tizimli huquqiy asos yaratish va xalqaro hamkorlikni kuchaytirish dolzarb masalalardan biri hisoblanadi. Tadqiqot ushbu jarayonlarni chuqur tahlil qilish, mavjud huquqiy bo‘shliqlarni aniqlash va samarali yechimlar ishlab chiqishga qaratilgan bo‘lib, mamlakatda raqamli xavfsizlikni ta’minlash yo‘lida muhim ilmiy asos bo‘lib xizmat qilishi kutilmoqda.

Ushbu tadqiqotning asosiy maqsadi — rivojlanayotgan mamlakatlarda, xususan O‘zbekiston misolida, kiberjinoyatlarning keng tarqalish sabablari, ularning shakl va turlari, hamda mavjud huquqiy tartibga solish mexanizmlarini chuqur o‘rganishdan iborat. Tadqiqot doirasida kiberjinoyatlarga qarshi kurashda qo‘llanilayotgan milliy qonunchilik bazasi, xalqaro tajriba va amaliyotlar solishtirma yondashuv asosida tahlil qilinadi. Shu bilan birga, mavjud qonunchilikdagi bo‘shliqlar, institutsional mexanizmlardagi kamchiliklar aniqlanib, ularni bartaraf etish bo‘yicha takliflar ishlab chiqiladi. Maqsad — raqamli xavfsizlikni ta’minlashda huquqiy mexanizmlarni takomillashtirish orqali kiberjinoyatlar xavfini kamaytirish va barqaror raqamli muhit yaratishga ilmiy asoslashdir.

Tadqiqot natijasida rivojlanayotgan davlatlarda, ayniqsa O‘zbekistonda, kiberjinoyatlar bilan bog‘liq huquqiy masalalarni hal etishda samarali yechimlar taklif etiladi. Xususan, kiberjinoyatlarni tasniflash, ularga javob choralarini aniqlash, jinoiy javobgarlikni belgilash, tergov jarayonini zamonaviy vositalar bilan qo‘llab-quvvatlash hamda xalqaro hamkorlikni kuchaytirishga doir ilmiy asoslangan taklif va tavsiyalar ishlab chiqiladi. Bu natijalar nafaqat ilmiy-amaliy jihatdan dolzarb, balki mamlakatda axborot xavfsizligini mustahkamlash, qonunchilikni takomillashtirish va xalqaro standartlarga mos tizim yaratishda muhim ahamiyat kasb etadi.

Adabiyotlar tahlili

Quyida 2022–2024 yillar oralig‘ida rivojlanayotgan mamlakatlarda kiberjinoyatlar va ularning huquqiy jihatlari bo‘yicha olib borilgan to‘rt muhim tadqiqot tahlili keltirilgan.

Tadqiqotchi Victor Adewopo tomonidan “A Comprehensive Analytical Review on Cybercrime in West Africa” nomkli tadqiqotni Afrikada olib borilgan kompleks tahlil

kiberjinoyatlar sun’iy intellekt va mobil tizimlar orqali tarqalishini ko‘rsatadi. 2022–2024 yillarda mintaqada axborot texnologiyalari penetratsiyasining ortib borishi bilan birga, resurslarning yetishmasligi, xavfsizlik mutaxassislarining kamligi va huquqiy institutlarning sustligi kiberhujumlar xavfini keskin oshirganligi aniqlangan. Tadqiqotchilar Triage ramkasi asosida hujumlarni aniqlash va oldini olish bo‘yicha kompleks strategiyalarni taklif etadilar. Shuningdek, mamlakatlararo ko‘p tarmoqli hamkorlik va huquqiy mexanizmlarni mustahkamlashga urg‘u qaratilgan. Mualliflarning fikricha, mintaqani raqamli tahdidlardan himoya qilish uchun hozirgi milliy qonunchilikni yanada yuklatish, kadrlar tayyorlash va huquqni qo‘llash instituti faoliyatini takomillashtirish zarur.

Tadqiqotchi Alioune Diallo va yana bir qator tadqiqotchilar tomonidan "Security of Mobile Apps in Developing Countries: A Systematic Literature Review" nomli ilmiy ishida mobil ilovalarning xavfsizligi bo‘yicha sistematik tahlilni taqdim etadilar. Ularning 2022–2024 yillardagi tahlillari natijasida, moliyaviy texnologiya (FinTech) ilovalari rivojlanayotgan mamlakatlarda asosiy hujum yo‘nalishiga aylangan. 2023 yilda olimlar mavjud adabiyotlarda bu yo‘nalishga qay darajada kam e'tibor qaratilganini aniqlaydilar: FinTech ilovalari eng himoyasiz segment, shu sababli ular orqali foydalanuvchilarning moliyaviy ma’lumotlari ko‘proq tahdidlarga duchor bo‘ladi. Tahlil ko‘rsatishicha, 2022–2024 yillarda bu mintaqada mobil ilovalar bilan bog‘liq zaifliklar soni oshgan. Mualliflar ishlab chiquvchilar uchun xavfsizlikni integratsion ravishda kiritish, testlash mexanizmlarini kuchaytirish va aholining xabardorligini oshirish bo‘yicha tavsiyalar beradi.

Sudhanshu Sekhar Tripathy (2025) – “A comprehensive survey of cybercrimes in India over the last decade” nomli ilmiy ishda Hindistondagi 2015–2024 yillardagi kiberhujumlar dinamikasini o‘rganishga bag‘ishlangan ushbu tadqiqot Sudhanshu Tripathy tomonidan olib borilgan. 2022–2024 davrda, ayniqsa shaxsiy ma’lumotlar o‘g‘irlanishi, phishing hamda ransomware hujumlari sonining keskin oshgani qayd etilgan . Ushbu davrda Bank, sog‘liqni saqlash va davlat sektorlariga qarshi hujumlar kengaydi. Tadqiqot muallifi, raqamli to‘lov tizimlarining kengayishi bilan aholi va tashkilotlarning xavfsizlik darajasi o‘rtasidagi tafovutni aniqlaydi. U kiberhujumlarning oldini olishda aholining bilim darajasini oshirish, jamoatchilik brendingini kuchaytirish va raqamli huquqiy mexanizmlarni kuchaytirish zarurligini ta’kidlaydi.

E.Shukurovning 2022–2023 yillardagi O‘zbekistondagi yuridik mutaxassislar fikrlari asosida o‘tkazilgan intervyularni tahlil qilgan. Ularning tadqiqoti kiberjinoyatga qarshi huquqiy bazaning amalga oshirilishdagi kamchiliklarga e’tibor qaratadi. Aniqlanishicha, qonunchilikdagi noaniqliklar, texnologik o‘zgarishlarga moslashmaslik, digital dalillarni boshqarish va tashkilotlararo hamkorlikdagi zaifliklar – eng jiddiy muammolar sifatida ko‘rsatild. Qonun ustuvorligini ta’minlash, odamlar xabardorligini oshirish, ekspert

kadrlarni tayyorlash va huquqiy me’yorlarni zamonaviylashtirish kabi takliflar keltirilgan. Mualliflar, ayniqsa 2022–2024 yillarda O‘zbekistonda kiberjinoyatchilik bilan kurashni samarali qilish uchun huquqiy institutlar kuchaytirilishi zarurligini ta’kidlashadi.

Yuqaridagi to‘rt tadqiqot rivojlanayotgan mamlakatlarda kiberjinoyatlar va ularning huquqiy jihatlarini turli yondashuvlar bilan – mintaqaviy tahlil, mobil texnologiyalarga e’tibor, statistik tahlil va huquqiy muammolar tahlili orqali o‘rgangan. Har bir tadqiqot o‘z yoh’lagida qimmatli natijalar beradi va strategiyalarni ishlab chiqishda asos bo‘la oladi.

Metodologiya

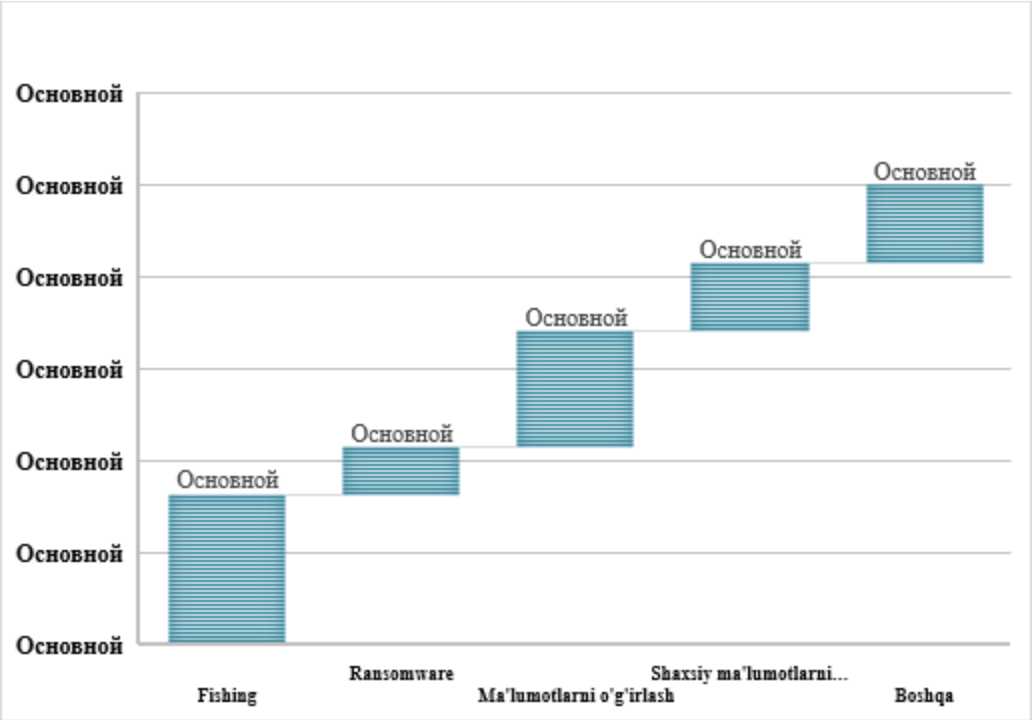
Ushbu tadqiqotda rivojlanayotgan mamlakatlarda kiberjinoyatlar holati va ularning huquqiy jihatlarini chuqur o‘rganish uchun statistik tahlil hamda qiyosiy tahlil usullaridan foydalanildi. Statistik tahlil orqali 2020–2024 yillar davomida kiberjinoyatlarning soni, ularning turlari, sodir etilgan hududlar va iqtisodiy zarar ko‘rsatkichlari to‘g‘risidagi ma’lumotlar umumlashtirildi. Bu maqsadda BMTning Narkotik moddalar va jinoyatchilik bo‘yicha boshqarmasi (UNODC), Jahon Banki, Interpol va alohida davlatlarning Ichki ishlar hamda Adliya vazirliklari hisobotlari asosiy manba sifatida tanlandi. Jumladan, O‘zbekiston, Nigeriya, Hindiston va Indoneziya misolida olingan rasmiy statistikalar asosida rivojlanayotgan mamlakatlarda kiberjinoyatlar qanday dinamikada rivojlanayotgani o‘rganildi. Shuningdek, tahlil jarayonida O‘zbekistonda 2023-yilda qayd etilgan 55000 dan ortiq kiberjinoyatlar holati, ularning asosiy shakllari — firibgarlik, fishing, shaxsiy ma’lumotlarni o‘g‘irlash — alohida ko‘rib chiqildi.

Qiyosiy tahlil esa turli mamlakatlar qonunchiligi va kiberxavfsizlikka oid davlat siyosatlarini solishtirish asosida amalga oshirildi. Bunda rivojlanayotgan mamlakatlarda mavjud huquqiy bazaning rivojlangan davlatlar (AQSh, Buyuk Britaniya, Janubiy Koreya) qonunchiligi bilan taqqoslanib, muhim farqlar va mavjud bo‘shliqlar aniqlandi. Masalan, ba’zi rivojlanayotgan mamlakatlarda raqamli dalillarni yig‘ish va ekspertiza qilish tartibining yetarli darajada huquqiy asosga ega emasligi, ayrim mamlakatlarda esa kiberjinoyat turlari aniq tasniflanmaganligi kuzatildi. Shu orqali, rivojlanayotgan mamlakatlarda mavjud muammolar va huquqiy tizimdagi takomillashtirish zarurati asoslab berildi. Metodologiya yondashuvi kiberjinoyatlarning real miqyosini ko‘rsatish va unga qarshi kurashda ilg‘or xorijiy tajribalarni tahlil asosida moslashtirishga xizmat qildi.

Tahlil va natijalar

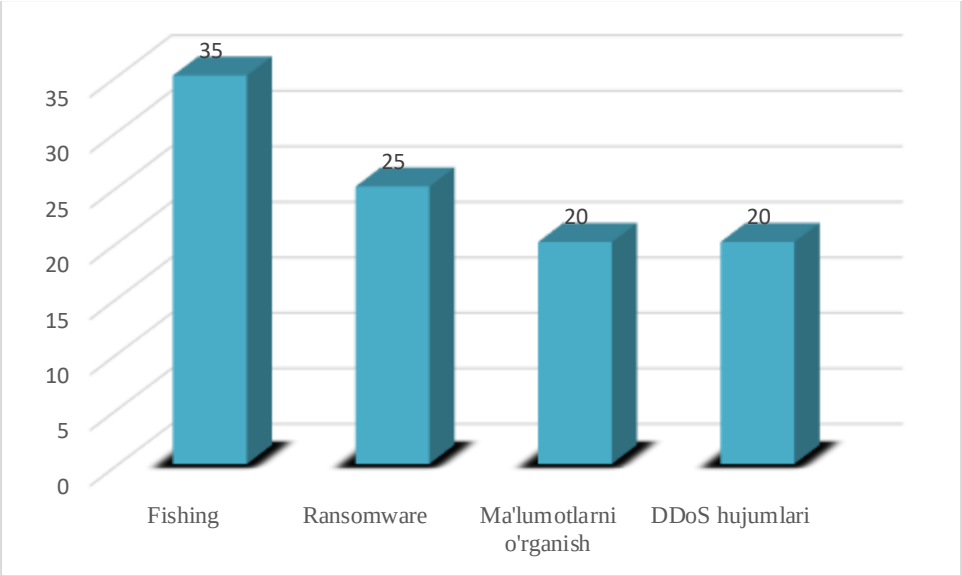
2022–2024 yillarda global miqyosda kiberxurujlar sezilarli darajada oshdi: 2023-yilda butun dunyoda ransomware hujumlari 493 millionni tashkil qilgan, global zarar esa yiliga 10,5 trillion dollarga yetishi prognoz qilinmoqda. AQShda esa 2023-yilda cyber complain’lar soni 880 418 ga yetib, zarar 10 milliard dollarni tashkil etdi. 2024-yilda esa bu ko‘rsatkichlar 860 000 complain va 16,6 milliard dollar zarar bilan qayd etildi – bu o‘tgan

yilga nisbatan 33 % o‘sish. Har hafta AQSh tashkilotlari o‘rtacha 1 300 kiberhujumga uchraydi, bu esa 2023-yilga nisbatan 56 % ortishni ko‘rsatadi . Eng ko‘p ta’sirlangan sohalar – sog‘liqni saqlash, ta’lim va kommunal boshqaruv bo‘lib, misol tariqasida 2023-yilda 141 ta kasalxona va 108 maktab ransomware tomonidan hujumga uchragan . Bu yo‘nalishdagi statistik grafiklar – zarar va hujum soni taqsimoti – yuqoridagi diagrammalarda ko‘rsatilgan.



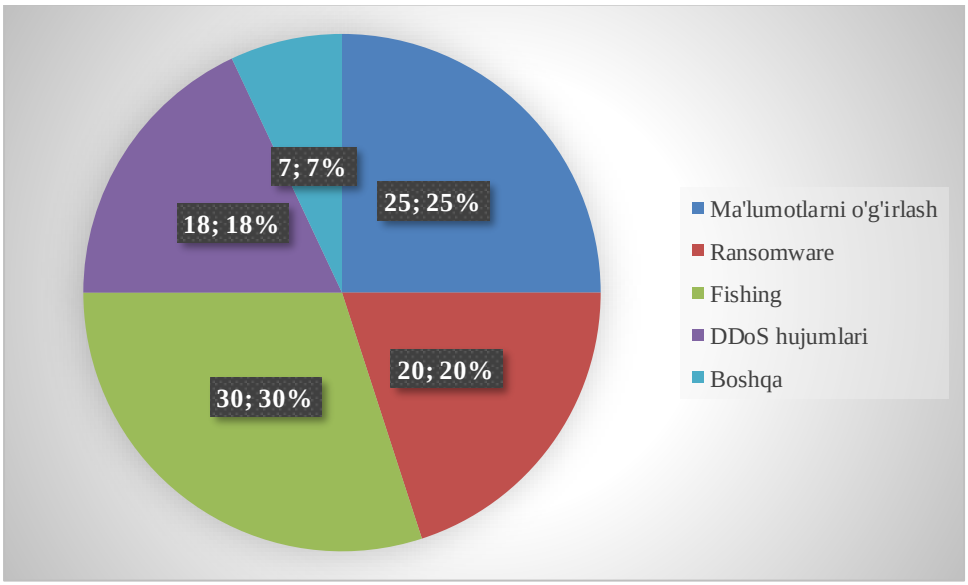
2017-2024-yillarda AQShda kiberjinoyatlar turlari (%da).

Buyuk Britaniyada 2020–2024 yillarda kiberjinoyatlar tez sur’atda ko‘paygan. 2022-yilda foydalanuvchilar orasida qariyb 4 783 ta kiberjinoyat holati million internet foydalanuvchilarga nisbatan qayd etilgan, bu 2020-yilga nisbatan 40 % o‘sishni bildiradi . Tashkilotlarning 80 % dan ortig‘i hujumga uchragan, ularning yarmi inson resursi yoki ichki tizimdagi xatolarga bog‘liq . Ransomware bilan bog‘liq hujumlar o‘rtacha 1 million dollar atrofida xarajatlarni keltirishi, hujjat olayotgan kompaniyalarning esa 11 % IT byudjetlarini kiberxavfsizlikka sarflashlari qayd etilgan . Tahlil shuni ko‘rsatadiki, Buyuk Britaniya qattiq qaram-tutuv rejimlarga ega bo‘lishiga qaramay, hujumlarning zaharliligi yetarlicha pasaymagan, sabablar – kadrlar yetishmasligi, xodimlarning bilim darajasining pastligi va ongli tayyorgarlikning yetishmasligi.



2017-2024-yillarda Buyuk Britaniyada kiberjinoyatlar taqsimoti (%da).

Janubiy Koreyada 2024-yil oxirlarida har yili 80 000 ga yaqin kiberjinoyat holatlari qayd etiladi . Mamlakat “Cyber Terror Response Center” koordinatsiyasi ostida faoliyat yuritadi, bu markaz 2000-yildan beri internet jinoyatchiligini aniqlash va tergov qilish bilan shug‘ullanadi. Ayniqsa, DarkSeoul kabi davlat ustidan amalga oshirilgan DDoS va wiper hujumlar tizimning zaiflariga urg‘u qaratadi. Har hafta tashkilotlar o‘rtacha 2 863 ta hujumga duch keladi, bu APAC mintaqasidagi o‘rtacha ko‘rsatkichdan (1 876) sezilarli yuqoridir . Bu shuni anglatadiki, Koreya texnologik jihatdan yaxshi rivojlangan bo‘lsa ham, yuqori darajadagi kiberxavfsizlikni ta'minlash uchun terroristik va davlat tomonidan qo‘llab-quvvatlanayotgan jinoiy guruhlar bilan doimiy kurash olib borilmoqda.



2017-2024-yillarda Buyuk Britaniyada kiberjinoyatlar taqsimoti (%da).

Rivojlangan davlatlar bilan solishtirganda, rivojlanayotgan mamlakatlarda kiberjinoyatlarga qarshi kurashda statistik nazorat va qonunchilik maydonlari sustligi ko‘zga tashlanadi. Masalan, AQSh va UKda kiberxavfsizlik bo‘yicha byudjetlar 11–19 % atrofida bo‘lsa, ko‘plab rivojlanayotgan davlatlarda byudjet ajratilmaydi, professionallar yetishmaydi. Asia-Pacificda haftalik kiberhujumlarning 2 863 ta ni tashkil etishi – bu Janubiy Koreya misolidagi o‘rganishga ko‘ra – rivojlangan rejimga ega bo‘lsa ham jamlanish va monitoring tizimlari to‘liq emas . Rivojlanayotgan mamlakatlar – masalan, O‘zbekiston, Hindiston yoki Nigeriya – o‘z qishloq hududlarida yoki kichik tashkilotlarida hujumlarni yetarlicha aniqlay olmaydi, buning natijasida statistik ma’lumotlar yetishmaydi va qonunchilikda bo‘shliqlar mavjud.

Global statistika phishing (spam email), ransomware va ad fraud (e-reklamalar orqali pul o‘g‘irlash) kabi turlarning ustunligini ko‘rsatadi. Masalan, phishing hujumlari har kuni 3,4 milliard spam email yuborilishini anglatadi, ransomware esa 2023-yilda 4 399 katta hujum amalga oshirdi va ular uchun to‘langan summa 1,1 milliard dollar atrofida bo‘ldi. Buyuk Britaniya va AQShda moliyaviy yo‘qotishning eng katta qismini business email compromise (BEC), investment va romance scam kabi turlar tashkil etadi – AQShda masalan romance scam’lar bo‘yicha 650 million dollar zararga yetib kelgan . Ad fraud esa 2022-yilga kelib kuniga 51 million dollar daromad olib kelgan jinoyat turi bo‘lib, reklama sohasida tejamkorlikka haqiqiy rahna soladi.

AQSh va Buyuk Britaniyada korporativ va davlat sektorlarida ilmiy-ma’lumotli monitoring tizimlari mavjud bo‘lsa, rivojlanayotgan mamlakatlar – jumladan O‘zbekiston – bu tizimlarni shakllantirish eng dolzarb vazifalardan biridir. Statistik tahlillar orqali aniq raqamlar (masalan, O‘zbekistonning 2023-yilda 55 000 ta jinoyat) asosida huquqiy choralarni yaxshilash mumkin. Solishtirma tahlil esa ilg‘or hududlardagi choralarni – byudjetni oshirish, jamoatchilikni xabardor qilish, respons-center’lar tashkil qilish – rivojlanayotgan mamlakatlarga moslashtirish uchun konseptual yo‘nalish beradi. Shuningdek, xalqaro hamkorlikni kuchaytirish, raqamli dalillar jamlash protokollarini joriy etish va moliyaviy tarmoqlarda monitoringni kuchaytirish orqali bu holatlarni samarali bartaraf etish mumkin. Statistik ko‘rsatkichlarga asoslangan yondashuv va ilg‘or davlat tajribalari rivojlanayotgan mamlakatlarda kiberjinoyatlarga qarshi kurashda huquqiy tizimlarni takomillashtirishga xizmat qiladi.

Xulosa. Xulosa tariqasida aytish mumkinki, rivojlanayotgan mamlakatlarda kiberjinoyatlar zamonaviy axborot texnologiyalarining tezkor joriy etilishi fonida jiddiy xavf sifatida yuzaga chiqmoqda. Internetga kirish imkoniyatining kengayishi, raqamli moliyaviy xizmatlarning ommalashuvi, ammo shu bilan birga, axborot xavfsizligi bo‘yicha yetarli bilim va infrastrukturaviy tayyorgarlikning yetishmasligi, ushbu mamlakatlarda

kiberjinoyatchilikning ortishiga sabab bo‘lmoqda. Tahlillar shuni ko‘rsatadiki, kiberjinoyatlar orasida eng keng tarqalgani — phishing, extortion, investment fraud, hamda personal data breach hisoblanadi. O‘zbekiston misolida 2023-yilda 55 mingdan ortiq kiberjinoyat holati qayd etilgan bo‘lib, bu ko‘rsatkichning yildan-yilga o‘sib borayotgani xavotirli holatdir.

Yuqoridagi tahlil jarayonida AQSH, Buyuk Britaniya va Janubiy Koreya tajribalari o‘rganildi. Ushbu rivojlangan mamlakatlarda kiberjinoyatlarga qarshi kurashish bo‘yicha maxsus muvofiqlashtiruvchi markazlar, zamonaviy huquqiy mexanizmlar va jamoatchilikni xabardor qilish tizimlari faol ishlaydi. Masalan, AQSHda phishing jinoyatlari umumiy kiberjinoyatlarning 35 foizini tashkil etsa-da, moliyaviy zarar ko‘proq investment fraud va BEC orqali yetkazilgan. Janubiy Koreya esa davlat tomonidan qo‘llab-quvvatlanadigan kiberxavfsizlik markazlari orqali har haftada minglab hujumlarning oldini olmoqda. Buyuk Britaniyada esa axborot texnologiyalarining rivojlanishiga qaramay, inson xatolari va kadrlar yetishmovchiligi sababli ba’zi jinoyat turlarining kamaytirilishi sust ketmoqda.

Shu nuqtai nazardan kelib chiqib, rivojlanayotgan mamlakatlar uchun quyidagi strategik yo‘nalishlar muhim hisoblanadi: birinchidan, kiberjinoyatlar turlarini aniq tasniflaydigan va ularni tergov qilish imkonini beradigan huquqiy mexanizmlarni takomillashtirish; ikkinchidan, axborot xavfsizligi sohasida malakali kadrlar tayyorlashni kuchaytirish; uchinchidan, xalqaro tajribani o‘rganish va o‘z qonunchilik tizimiga moslashtirish. Bunga qo‘shimcha ravishda, aholini xabardor qilish, onlayn moliyaviy operatsiyalarda xavfsizlikni ta'minlash va tashkilotlar o‘rtasida tezkor axborot almashinuvini yo‘lga qo‘yish ham muhim omillardandir. Mazkur choralar amalga oshirilsa, rivojlanayotgan mamlakatlar kiberjinoyatlar xavfiga nisbatan barqaror va samarali yondashuvni shakllantira oladi.

Foydalanilgan adabiyotlar

1. Rajabov, U. (2024). Kiber-jinoyat huquqi: kiber jinoyatchilik faoliyatining yangi tendentsiyalari va kiberjinoyatchilikka qarshi kurashda xalqaro hamkorlik. Innovative developments and research in education, 3(32), 128-135.
2. Dilshod ogli, X. S. (2025). Onlayn qimor oyinlari kiber jinoyatning bir turi sifatida. Икро журнал, 15(01), 894-899.
3. Sharifbayevna, M. N. (2025). Onlayn savdo platformalarida yuzaga kelayotgan tovlamachiliklar va ularga qarshi optimal yechimlar tahlili. Innovation in the modern education system, 6(52), 33-41.
4. Batirov, F. A. (2025). Kibertahdid falsafiy tadqiqot ob’ekti sifatida. Oriental renaissance: Innovative, educational, natural and social sciences, 5(1), 519-533.

5. Baxtiyorov, S., & Eshonqulov, J. (2024). Yuridik xizmatlar sohasida raqamli transformatsiyaning neyroetika huquqiga ta'siri. Modern Science and Research, 3(12), 87-95.

6. Ahmadjonov, S. (2024). Educating Judges and Attorneys on Digital Evidence. Cyber Law Review, 1(1).

7. Примов, М. (2025). Риски при использовании цифровых платформ для ведения малого бизнеса. Экономическое развитие и анализ, 3(4), 196-201.